

# McAfee® Security Journal

Sicherheitsvision von McAfee® Avert® Labs Sommer 2009



## RISIKO-MANAGEMENT UND COMPLIANCE

Vorschriften und Compliance Anforderungen sorgen für große Veränderungen bei der Unternehmenssicherheit

## KEIN MANAGEMENT

ohne Messung – Zur Einschätzung der Sicherheit müssen Sie die Kernprobleme verstehen

# Inhalt



- 3 **Die Herausforderungen von Risiko-Management und Compliance** Mögliche Schwierigkeiten bei der Implementierung von Sicherheitsbestimmungen. **Jeff Green**
- 4 **Risiko-Management und Compliance: Erste Schritte zur Sicherheit** Wir versuchen, dieses ungeliebte Thema so spannend wie möglich zu gestalten und zu erklären, warum es so wichtig ist. **Stuart McClure**
- 7 **Was dürfen Audits kosten?** Konflikte über Umfang und Kosten von IT-Audits verursachen seit Jahren Reibungen zwischen Auditoren und IT-Abteilungen. **Evelyn DeSouza**
- 10 **PCI DSS: Besser als gar nichts** Die Kreditkartenindustrie entwickelte einen Sicherheitsstandard, der den Interessen der Unternehmen und Kunden dient. **Anthony Bettini**
- 13 **Umgestaltung von Audits und Compliance** Vorgaben und Bestimmungen gibt es überall die effektive Einhaltung ist ein schwierige Aufgabe. **Kent Landfield**
- 19 **Malicious Messaging – ein globaler Überblick** Die Bedrohungslandschaft und die Natur von Malware- und Messaging-Bedrohungen haben sich erheblich verändert. **David Marcus**

## McAfee Security Journal

Sommer 2009

### Herausgeber

Dan Sommer

### Autoren

Anthony Bettini  
Evelyn DeSouza  
Jeff Green  
Kent Landfield  
David Marcus  
Stuart McClure

### Marketing

Beth Martinez  
Jennifer Natwick

### Redaktion

Mary Karlton

### Design und Layout

Pair Design, LLC

### Grafik

Doug Ross

### Druck

RR Donnelley

### Übersetzungen

McAfee Localisation

### Public Relations

Joris Evers  
The Red Consultancy Ltd.

### Senior Vice President, McAfee Avert Labs

Jeff Green

### Director, Security Research and Communications

David Marcus

# Die Herausforderungen von Risiko-Management und Compliance

Jeff Green



Risiko-Management und Compliance sind die Bereiche der Computersicherheit, die am wenigsten verstanden und am häufigsten falsch angegangen werden. Selbst erfahrenen Experten auf diesem Gebiet fällt es zuweilen schwer, Computersicherheit wirklich zu quantifizieren.

Welche Auswirkungen haben Sicherheitslücken? Welche Kosten lassen sich dadurch einsparen, dass Systeme nicht gehackt und von Malware infiziert werden? Sind meine Maßnahmen auf Netzwerkebene wirksam, und kann ich das auch beweisen? Kalkuliere ich ein mögliches Risiko regelmäßig? Und welche Rollen spielen Auditoren?

## Hervorragende Forscher

In dieser fünften Ausgabe des *McAfee Security Journals* konzentrieren wir uns auf die Gegebenheiten, Umsetzungen, Absurditäten sowie die Geschichte von Risiko-Management und Compliance. Dazu haben wir hervorragende Autoren engagiert. Einer der vielen Unterschiede von McAfee Avert Labs gegenüber anderen Forschungseinrichtungen ist die Bandbreite der Forscher aus unterschiedlichsten Sicherheitsdisziplinen. Forscher und Koryphäen wie Anthony Bettini, Kent Landfield, Stuart McClure sowie Evelyn DeSouza gehen die Vorurteile und Grundsätze von Sicherheits-Management und Compliance sowie Vorschriften und Audits an.

Unternehmen haben es heute mit sehr schwierigen Compliance-Herausforderungen zu tun. Überall – nicht nur in den USA – gelten entsprechende Bestimmungen. Die Artikel in dieser Ausgabe untersuchen die Grundlagen von Risiken und Compliance. Wir vertiefen uns aus globaler Sicht in die Probleme, die sich aus Vorschriften und Bestimmungen ergeben. Wir betrachten die Kreditkartenstandards und beurteilen die Vor- und Nachteile.

Außerdem befassen wir uns mit dem permanenten Konflikt zwischen Auditoren und IT-Mitarbeitern sowie dem daraus resultierenden Phänomen der Audit-Müdigkeit, die derzeit viele Unternehmen befällt. Compliance mit Bestimmungen und/oder Richtlinien ist in keinsten Weise gleichbedeutend mit Sicherheit, und in dieser Ausgabe nehmen wir dieses Missverständnis genau unter die Lupe.

Abschließend geben wir einen Einblick in die Entwicklung globaler Messaging-Bedrohungen – die Statistiken dazu werden einige Leser wahrscheinlich überraschen.



**Jeff Green** ist Senior Vice President bei McAfee Avert Labs im Bereich der Produktentwicklung. Er verantwortet weltweit den gesamten Forschungsbereich von McAfee in Amerika, Europa und Asien und leitet die Forscherteams, die sich auf Viren, Hacker und gezielte Angriffe, Spyware, Spam, Phishing, Schwachstellen und Patches sowie Host- und Network Intrusion Technologien spezialisiert haben. Green leitet außerdem die langfristige Sicherheitsforschung um sicherzustellen, dass McAfee den entstehenden Bedrohungen immer einen Schritt voraus bleibt.

# Risiko-Management und Compliance: Erste Schritte zur Sicherheit

Stuart McClure



Holen Sie sich einen starken Kaffee, und schnallen Sie sich an. Sie sollten wach bleiben, denn wir brauchen Ihre gesamte Aufmerksamkeit, um einen Aspekt der Unternehmenssicherheit zu besprechen, den viele nicht besonders aufregend finden.

Das einschläfernde Thema heißt: Risiko und Compliance. Wie kommt es, dass manche Leute bereits bei der bloßen Erwähnung der Worte „Risiko und Compliance“ Erschöpfung überkommt? Der Grund ist einfach: Nur sehr wenige Menschen verstehen und beziehen Risiko- und Compliance-Faktoren in ihr tägliches Leben mit ein. Und das, obwohl sie ständig von Risiko- und Compliance-Faktoren umgeben sind. Daher wollen wir dieses scheinbar alltägliche Konzept entmystifizieren. Wir versuchen, dieses Thema so spannend wie möglich zu gestalten, gelingt uns das nicht, dann wollen wir wenigstens erklären, warum es so wichtig ist.

Jeder von uns trifft täglich Risikoentscheidungen, und nur die wenigsten sind uns bewusst. Wir treffen eine Entscheidung, die zu einem positiven Ergebnis führt. Wir treffen eine weitere Entscheidung, und diese führt zu einem negativen Ergebnis. Dasselbe gilt für den Bereich der Sicherheit. Beim Umgang mit Risiken im täglichen Leben, wägen wir die bekannten Risiken mit den Kosten dieser Entscheidungen ab und treffen die bestmögliche Wahl. Risiko basiert auf der grundlegenden Annahme, dass jeder Vorgang eine Konsequenz nach sich zieht, sei diese gut oder schlecht. Wir kennen das Ergebnis unserer Entscheidungen häufig nicht. Es ist aber sicher, dass alle Entscheidungen entweder eine positive oder eine negative Folge haben. Und genau darum geht es beim Risiko-Management.

## Risiko

Ich fahre seit vielen Jahren Auto und habe die Risiken des Autofahrens akzeptiert (Unfall, Verletzungen oder sogar Tod), da die Alternative (Laufen, Fahrradfahren oder öffentlicher Nahverkehr) nicht immer zur Verfügung steht oder zu unbequem ist. Ich akzeptiere diese Risiken täglich meistens völlig unbewusst – manchmal jedoch auch bewusst, wenn ich zum Beispiel an einem Unfall vorbeifahre. Häufig vergesse ich jedoch, dass schlechte Straßenbedingungen (schmutzige Fahrbahn, Regen, Schotter) meine Reaktionsfähigkeit beim Autofahren

beeinträchtigen können und ich das Risiko eingehe, mein Auto zu beschädigen, oder noch schlimmer, einem anderen zu schaden. In Anbetracht der Tatsache, dass die Tätigkeit sowieso riskant ist, stellt sich die Frage, was wohl geschehen würde, wenn ich kein Armaturenbrett hätte, das meine Geschwindigkeit aufzeigt. Was wäre, wenn ich keine Spiegel hätte, die mir zeigen was sich hinter oder neben mir befindet? Wie würde ich wissen, ob ich sicher fahre und so das Unfallrisiko mindere? Ich könnte es nicht. Die Anzeigen und visuellen Hilfen liefern die Informationen, die ich als Fahrer benötige, um sicher fahren zu können. Wenn ich sie ignoriere, dann zu meinem eigenen Schaden. Dasselbe gilt für Sicherheitsrisiken: Je mehr Sie wissen, desto größer ist Ihre Chance, Probleme oder tatsächliche Schäden vorherzusagen – und diese zu vermeiden. Und je mehr Sie Risiken ignorieren, desto wahrscheinlicher werden Sie Probleme bekommen.

Um ein Armaturenbrett für Sicherheit anzulegen müssen Sie wissen, wie Sicherheit messbar wird. Das Armaturenbrett in Ihrem Auto ist mit diversen Eingabeparametern verbunden, z. B. mit der Drehung der Räder (Geschwindigkeit), der Reifenhaftung (Haftungssteuerung), der Temperatur des Motorblocks, den Wasserständen und vielem mehr. Ohne diese Quellen in Ihrem Auto wäre ein Armaturenbrett wertlos. Dasselbe gilt für den Bereich der Sicherheit. Jedes erfolgreiche Risiko- und Compliance-Programm muss die internen Quellen feststellen und sie täglich messen. Hierzu müssen wir Sicherheitsprogramme entwickeln, in denen die Grundlagen des Sicherheitsrisikos berücksichtigt und qualitative und quantitative Maße auf die Formel angewendet werden. Wir müssen diese Maße dann über einen längeren Zeitraum weiter verfolgen, um Fortschritte oder Rückschritte sehen zu können.

## Sicherheitsmaßen

Kein Management ohne Messung. Das ist das Mantra aller erfolgreichen Unternehmen. Auch wenn dieses Modell im Sicherheitsbereich größtenteils gemieden wurde, ist es gerade im Wandel begriffen. Gesetze und Compliance-Anforderungen verursachen diesen Wechsel. Die meisten Sicherheitstechnologien behandeln die Symptome und nicht die Ursachen. Um Sicherheit aber messbar zu machen, muss man die Kernprobleme und Ursachen kennen. Was verursacht sicherheitsrelevante Vorfälle? Es gibt zwei Hauptgründe oder Chancen: Designfehler und die falsche Anwendung von Funktionen. Es gibt außerdem zwei Angriffsvektoren oder Motivationen: böswillige Hacker und Fehleinschätzungen durch die Benutzer. Wenn Sie Hauptgründe und Vektoren kombinieren, erhalten Sie eine Mixtur für eine nahezu unbegrenzte Anzahl von sicherheitsrelevanten Vorfällen. Und wenn Sie diese Angriffsmethoden nicht überwachen und verwalten, werden Sie immer und immer wieder damit konfrontiert werden.

## Kernprobleme

Ein Konzeptionsfehler, das erste Kernproblem, ist ein Euphemismus, der auch folgendermaßen formuliert werden kann: „Entwickler, die Sicherheit nicht verstehen, schaffen Möglichkeiten, die negative Vorfälle zulassen“. Das beinhaltet Schwachstellen in der Hard- und Software, die durch Netzwerk-, System-, Anwendungs- und Datenbankentwickler und -lieferanten verursacht werden wie Microsoft, Oracle und SAP, aber auch jedes Unternehmen, das eigene Anwendungen entwickelt, wie große Banken, Webentwicklungsfirmen, Onlinehandel und andere.

Konzeptionsfehler sind weitreichend und – aufgrund der Tatsache, dass Menschen diese Technologien entwickeln, codieren und implementieren – immer vorhanden. Wenn solche Fehler in der Automobilindustrie auftreten, führt dies häufig zu einer Rückrufaktion. Wenn festgestellt wird, dass ein grundlegender Fehler in der Verkabelung oder im Benzintank einen Unfall oder den Tod zur Folge haben kann, muss dieser Fehler behoben werden. Genauso wie ein grundlegender Fehler im Auto zu Problemen oder Schlimmerem führen kann, besteht eine ähnliche Last bei Computerhardware und -software. Die Entwickler dieser Technologien berücksichtigen die Sicherheitsaspekte in ihren Entwürfen und Plänen nicht immer. Dies führt zu Fehlern und potentiellen Angriffsflächen. Heutzutage besteht die Möglichkeit einer Rückrufaktion im Computerbereich nicht, aber ich bin so kühn und behaupte, dass es sie im nächsten Jahrzehnt geben wird. Hardware und Software werden durch ein unabhängiges Organ zurückgerufen werden, das in der Lage sein wird, die Rückgabe unsicherer Produkte anzuordnen.

Konzeptionsfehler in Computersystemen können nicht so leicht gemessen werden, da sie meist unbekannt sind. Genauso wenig, wie Kfz-Ingenieure vorhersagen können, ob ein bestimmter Entwurf fehlerhaft sein wird oder nicht. Aber wir können bekannte Fehler in Computersystemen messen. Denn diese treten in Form von Schwachstellen auf. Es gibt Tausende bekannter Schwachstellen. Alles, angefangen vom Router, schnurlosen Geräten oder einem Smartphone bis hin zum PC, Apple Macintosh, einer Web-, ERP-Anwendung oder Datenbank, kann eine bekannte Schwachstelle enthalten. Und es ist Ihre Aufgabe, jeden dieser Fehler zu kennen und in Ihrer eigenen IT-Umgebung aufzuspüren. Messen Sie die Anzahl und die Art der vorhandenen Schwachstellen, können Sie deren Auswirkungen mindern. Überwachen Sie die Schwachstellen nicht, werden Sie Konzeptionsfehler in Ihrer Systemumgebung nie maßgeblich reduzieren können.

Die falsche Anwendung von Funktionen, das zweite Hauptproblem, umfasst unter anderem tägliche Funktionen eines Computernetzwerks, Systems oder einer Applikation und die Arten der falschen Anwendung. Sehen Sie sich die normalen Funktionen eines Computers aus der Perspektive eines Angreifers an, und Sie werden das Problem sofort erkennen. Jetzt nutzen wir noch einmal die Analogie zum Auto. In einem Auto dient das Gaspedal zum Antrieb des Fahrzeugs. Wenn Sie jedoch das Gaspedal statt der Bremse verwenden, kann dies zu Verletzungen oder Todesfällen führen. In der Computerwelt entspricht das in etwa einem DoS-Angriff (Denial-of-Service). Die zentrale TCP/IP-Funktion, die die Internetverbindung ermöglicht, kann auch gegen sich selbst gerichtet werden und in Nullkommanichts Ressourcen vernichten. Diese Funktionen sind nicht ursprünglich böswillig, aber wenn sie auf „böswillige“ Weise verwendet werden, verursachen sie Probleme.

Die Messung falscher Anwendungen von Funktionen ist nicht ganz einfach, aber ein Großteil kann messbar gemacht werden, indem Sie die Konfigurationseinstellungen Ihrer IT-Umgebung untersuchen und sie mit den bekannten bewährten Praktiken vergleichen: mit IT-Kontrollen oder Compliance-Vorlagen. Die Computer- und Sicherheitsbranche ist inzwischen so weit gereift, dass ihnen bewusst ist, dass bestimmte Standardfunktionen entfernt werden müssen, um Assets sicherer zu machen. Diese bewährten Praktiken müssen in Ihrer Umgebung implementiert werden. Wenn Sie diese bekannten „guten“ Richtlinien für die Assetkonfiguration nicht befolgen, werden Sie nicht nur Probleme mit Sicherheitsvorfällen, sondern auch mit beträchtlichen Compliance-Verstößen haben. Tatsächlich hat die Sicherheitsbranche eine Anzahl von Richtlinien für empfohlene Praktiken ausgegeben (z. B. PCI, HIPAA, SOX, GLBA, ISO 27002 und CoBiT), die Unternehmen eine Anleitung bei der Einrichtung ordnungsgemäßer Sicherheitskonfigurationen geben. Die Verwendung dieser Benchmarks in Ihrer Umgebung ist ein zentraler Bestandteil bei der Messung falsch verwendeter Funktionen.

Wir kennen das Ergebnis unserer Entscheidungen häufig nicht. Es ist aber sicher, dass alle Entscheidungen entweder eine positive oder eine negative Folge haben. Und genau darum geht es beim Risiko-Management.

## Angriffsvektoren

Der erste Angriffsvektor ist der böswillige Hacker. Die Quantität und Qualität von Hackern in der gesamten Welt zu bemessen ist schwierig, aber wir können ihre Fähigkeit uns anzugreifen einschätzen, indem wir die Durchlässigkeit Ihres Netzwerks messen. Je offener und verfügbarer Ihrer Ressourcen für Angreifer sind, desto größer ist die Wahrscheinlichkeit, dass ein Angriff Erfolg hat. Daher sollten Sie die Anzahl der offenen Ports von außen und von innen messen und diese in Echtzeit (oder so „echt“ wie möglich) überwachen.

Der zweite Angriffsvektor ist die Fehleinschätzung durch den Benutzer. Es wird häufig behauptet, dass unsere Systeme tatsächlich sicher sein könnten, wenn es keine Benutzer gäbe. Aber gerade diese Nutzer sind der Grund dafür, dass wir nicht arbeitslos sind. Kurz gesagt: Wenn ein ungeschulter Nutzer und eine Angriffsmöglichkeit zusammentreffen, haben Sie ein Problem. Der typische Fall ist ein Nutzer, der auf einen Link in einer E-Mail klickt oder einen E-Mail-Anhang ausführt. Trifft ein Nutzer solch schlechte Entscheidungen, setzt er sich selbst einem Angriff aus. Solange die Benutzer nicht ausreichend geschult sind, müssen wir uns auf die Probleme mit Konzeptionsfehlern und falsch verwendeten Funktionen konzentrieren. Darauf sind die meisten Sicherheitsprodukte und -leistungen ausgerichtet. Dabei wird leicht übersehen, welche Bedrohung jedes einzelne dieser Probleme darstellt. Deshalb ist die Einschätzung des Benutzerbewusstseins und der Sicherheitsfähigkeit ein zentraler Punkt. Durch das regelmäßige Ausfüllen von Fragebögen in kurzen Abständen und der Vergabe von Punkten, können Mitarbeiter im Sicherheitsbereich leichter schätzen, wie groß die Wahrscheinlichkeit ist, dass ihre Benutzer Risiken ausgesetzt sind.

Um im Cyber-Krieg zu bestehen, müssen wir alle zentralen Probleme kennen und sie sowohl einzeln als auch gemeinsam angehen. Das erreichen wir mithilfe von Risiko- und Compliance-Lösungen. In der Auto-Analogie verfügen wir über ein Armaturenbrett, Spiegel, Messgeräte, ein System für die elektronische Stabilität und viele andere Faktoren, die unsere Chancen auf ein sicheres Fahren erhöhen.

Durch die Einschätzung von Risiken erreichen Sie Transparenz über den Stand Ihrer Compliance. Wie neueste Beispiele jedoch zeigen, ist Compliance nicht mit Sicherheit gleichzusetzen.

## Compliance

Compliance bedeutet einfach die Einhaltung von Regeln. Es handelt sich um die Einschätzung, ob wir die Regeln befolgen, die uns davor bewahren, falsche Entscheidungen zu treffen. Für die Einhaltung der Regeln auf der Straße, sorgen die Polizei und die Straßenverkehrsordnung. Wenn Sie zu schnell fahren, bekommen Sie einen Strafzettel. Wenn Sie zu dicht auffahren, erhalten Sie einen Strafzettel wegen Nötigung. In der Welt der Computer können Wirtschaftsprüfer (wie Ernst & Young oder PricewaterhouseCoopers) feststellen, dass Ihr Unternehmen wesentliche oder signifikante Schwachstellen aufweist. Möglicherweise erhalten Sie eine Geldstrafe durch die überwachenden Unternehmen (z. B. Visa oder MasterCard).

Zusätzlich zu Geldstrafen können weitere beträchtliche Kosten auf Ihr Unternehmen zukommen. Möglicherweise müssen Sie für den Aufwand zahlen, dass die betroffenen Parteien (Kunden) über eine Sicherheitslücke informiert werden. Sie können sich Compliance wie den Erfolg oder das Versagen beim Befolgen der Straßenverkehrsordnung vorstellen. Bei Versagen tritt ein negatives Ergebnis ein. Bei Erfolg ist die Wahrscheinlichkeit eines negativen Ergebnisses viel geringer.

Durch die Einschätzung von Risiken bekommen Sie Transparenz über den Status Ihrer Compliance. Wie neueste Beispiele jedoch zeigen, ist Compliance nicht mit Sicherheit gleichzusetzen. Sie können in einem anderen Teil dieser Ausgabe darüber lesen, dass ein Unternehmen konform mit dem Payment Card Industry Data Security Standard (PCI DSS, Standard zur Datensicherheit bei Kreditkartentransaktionen) sein und trotzdem angegriffen werden und Kundendaten verlieren kann. Letztes Jahr war die Lebensmittelkette Hannaford Brothers in einen spektakulären Fall verwickelt (weitere Informationen finden Sie auf Seite 11). Dieses Jahr wurde festgestellt, dass das Unternehmen Heartland Systems PCI-konform war und dennoch Hackerangriffen zum Opfer fiel, bei denen etwa 100 Millionen Kundenkonten erbeutet wurden.<sup>1</sup>

Compliance bedeutet noch keine Sicherheit. Compliance ist nur die Mindestanforderung. Erst ein Management-Programm für Sicherheitsrisiken führt zu echter Sicherheit. Wir beginnen dieses Programm mit Risiko-Management und Compliance. Dadurch können wir die Ursache und nicht nur die Symptome des Problems angehen. Unser Mantra liegt in der Einschätzung der Schlüsselindikatoren, darin, das Risiko von Sicherheitslücken und Nicht-Compliance zu senken und letztendlich auch nicht-unternehmerische Risiken in unseren Alltag einzubeziehen.



**Stuart McClure** ist Vice President im Bereich „Operations and Strategy“ der Abteilung „Risk and Compliance“ bei McAfee. Er war zuvor Senior Vice President bei McAfee Avert Labs und hatte mehrere höhere Positionen im Bereich Sicherheit bei Kaiser Permanente, Foundstone, Ernst & Young sowie in der Kommunalverwaltung und Landesregierung inne. McClure ist Coauthor von *Das Anti-Hacker-Buch* (Osborne/McGraw-Hill), das in mehr als 30 Sprachen übersetzt wurde.

### ENDNOTEN

- <sup>1</sup> Open Security Foundation, DataLossDB. <http://datalossdb.org/incidents/1518-malicious-software-hack-compromises-unknown-number-of-credit-cards-at-fifth-largest-credit-card-processor>

# Was dürfen Audits kosten?

Evelyn DeSouza



Leidet Ihr Unternehmen an „Audit-Müdigkeit“? Die Einhaltung aktueller Sicherheitsstandards ist für viele Unternehmen schwer zu schultern.

Wir trafen vor kurzem den IT-Leiter eines großen multinationalen Unternehmens und hörten, dass das Wort *Audit* so begeistert vernommen wurde wie die Ankündigung einer Zahnwurzelbehandlung. Später während unserer Besprechung, winkte der IT-Leiter seinen internen Prüfern müde zu, als diese am Fenster des Besprechungsraums vorbeigingen. Dann führte er detailliert aus, wie sehr IT-Audits seine Abteilung belasten. Er berichtete, dass das Unternehmen schon Millionen Dollar für Compliance ausgegeben hatte, und das meiste davon aus seinem IT-Budget stammte. Aufgrund der Audits musste man auch Pläne für andere IT-Projekte umwerfen. Das von ihm beschriebene Szenario ist leider so häufig, dass McAfee einen Begriff dafür prägte: „Audit-Müdigkeit“. Sie entsteht, wenn dauernd und umfangreich Arbeit und IT-Ressourcen der Compliance gewidmet werden.

Wenn wir dieses Phänomen im Kontext der derzeitigen wirtschaftlichen Situation betrachten – mit leidenden Wirtschaftsbereichen, Ländern unter Druck und sinkenden Währungskursen sowie extrem knappen Budgets –, kommen wir nicht umhin, uns zu fragen: „Warum fallen Unternehmen der Audit-Müdigkeit zum Opfer?“

Audit-Müdigkeit überrascht kaum in Anbetracht der steigenden Anzahl der einzuhaltenden Vorschriften und des ständigen Rampenlichts, in dem einige von ihnen stehen, darunter der Sarbanes-Oxley Act von 2002 (US-Gesetz für Aktiengesellschaften

mit Sitz in den USA) mit seinen internationalen Varianten und der Payment Card Industry Data Security Standard (PCI DSS, Standard zur Datensicherheit bei Kreditkartentransaktionen). Network Frontiers (ein Unternehmen, das ein gemeinsames Rahmenwerk für die unterschiedlichen Standards und Vorschriften schafft) schätzt, dass sich weltweit über 400 Vorschriften auf die IT auswirken. Die meisten großen, international tätigen Unternehmen unterliegen ohne Weiteres 40 oder mehr Vorschriften, je nachdem, wie vielfältig ihre Geschäftsbereiche sind. Unternehmen können es nicht riskieren, ein Audit nicht zu bestehen, da dies ihren Ruf schädigen und sie an der Abwicklung ihrer Geschäfte hindern kann.

Konflikte über Umfang und Kosten von IT-Audits verursachen Spannungen zwischen (internen wie externen) Auditoren und IT-Abteilungen, seit nach dem Enron-Skandal der Sarbanes-Oxley Act erlassen wurde, der strengere Audits vorschreibt. Dies und die steigende Vorschriftenflut, die aus der Notwendigkeit von Datenschutz und Datenintegrität erwächst, führte dazu, dass Audits anders gehandhabt werden. Diese Änderung hat weltweit Kreise gezogen. Unternehmen in Australien und Indien stehen daher vor ähnlichen Herausforderungen.

**Audit-Müdigkeit ist in Anbetracht der steigenden Anzahl der einzuhaltenden Vorschriften und des ständigen Rampenlichts, in dem der Sarbanes-Oxley Act und PCI DSS stehen, kaum überraschend.**





IT-Abteilungen müssen ständig beweisen, dass ihre System- und Netzwerkeinstellungen richtig konfiguriert sind. Das bedeutet oft manuelle Arbeit, da die meisten Unternehmen nicht über Automatisierungstools verfügen.

Härte und gesunder Menschenverstand gehen jedoch nicht immer Hand in Hand. IT-Abteilungen beklagen regelmäßig, dass Auditoren keine klaren Vorgaben machen und einfach eine Checkliste abhaken, statt sich auf das Wesentliche zu konzentrieren. IT-Abteilungen müssen ständig beweisen, dass ihre System- und Netzwerkeinstellungen richtig konfiguriert sind. Das bedeutet oft manuelle Arbeit, da die meisten Unternehmen nicht über die erforderlichen Automatisierungstools und -prozesse zur Durchführung von Systemkonfigurations-Audits verfügen. In einer vor kurzem von McAfee in Auftrag gegebenen Umfrage gaben mehr als 51 Prozent der großen Unternehmen an, dass sie für die Durchführung von Audits Tabellen verwenden. Ein Unternehmen sagte aus, dass bei der Vorbereitung auf das PCI-Audit pro Woche etwa 1.000 Arbeitsstunden aufgewendet werden, nur um Konfigurationseinstellungen zu überprüfen. Man stellte danach fest, dass viele dieser Schritte in der Folgewoche für die Vorbereitung auf ein weiteres vierteljährliches Audit wiederholt werden mussten. Ein anderes Unternehmen verbrachte in einem einzigen Jahr mehr als 18.000 Stunden mit Vorbereitungen auf externe Audits. In Anbetracht der gewaltigen Anzahl der einzuhaltenden Vorschriften ist dies kaum überraschend.

Manuelle Audits sind nicht haltbar, da das IT-Personal für jedes anstehende Audit strenge Systemüberprüfungen durchführen muss. Außerdem stellt sich die Frage nach der Datenintegrität. Die Genauigkeit eines manuellen Audits kann nicht 100-prozentig gewährleistet werden, da der Prüfer voreingenommen sein oder einfach Fehler machen könnte.

IT-Abteilungen sind sich durchaus bewusst, dass Audits erforderlich sind, um Betrug abzuwenden und die Datenintegrität zu wahren. Dennoch wächst der Eindruck, dass die Prüfer Teil einer Verschwörung sind, deren Ziel es ist, IT-Mitarbeiter von der Arbeit abzuhalten. IT-Abteilungen fühlen sich ihren Auditoren häufig völlig ausgeliefert, weil sie nicht nur die notwendigen Daten bereitstellen, sondern auch auf die Ergebnisse der Audits reagieren müssen. Ein Anbieter von Gesundheitsdienstleistungen gab an, dass er in den letzten 4 Jahren 22 Audits unterzogen wurde, bei denen über 400 Probleme zum Vorschein kamen. Das Ergebnis waren teure und zeitaufwändige Behebungsmaßnahmen.

Compliance kann nicht automatisch mit Sicherheit gleichgesetzt werden. IT-Experten sind zunehmend um das Gleichgewicht zwischen dem Zeitaufwand für Compliance und dem für die Wahrung der Sicherheit besorgt. Während die meisten Vorschriften aus dem Wunsch der Datensicherung in Unternehmen entstehen, garantieren sie keine Sicherheit – schon gar nicht, wenn sie durch Abhaken von Checklisten umgesetzt werden sollen.

Dieses Problem ist jedoch auch eine Chance. Wir identifizierten drei wesentliche Schritte zur Überwindung von Audit-Müdigkeit:

#### **Richten Sie einen Ausschuss ein, der**

**Unternehmensvorschriften definiert:** Etablierte Unternehmen verfügen im Allgemeinen über einen Ausschuss für Unternehmensvorschriften, der die Abteilungen für IT, Risiko-Management sowie Audits und Compliance miteinander koordiniert. Dieser Ausschuss mildert nicht nur mögliche Kommunikationsbrüche zwischen den Abteilungen, sondern erhöht auch die Effizienz von Verfahren. Er bringt Führungskräften die Realität des täglichen Betriebs nahe und hilft dem Unternehmen, seine Ausgaben für Compliance auf die Bereiche zu konzentrieren, in denen sie am wichtigsten sind – beispielsweise indem er Problemlösungen anhand ihres Wertes für die Risikovermeidung, für das Geschäft und für Ressourcen priorisiert.

**Automatisieren Sie IT-Audit-Prozesse:** IT-Abteilungen müssen mithilfe automatisierter Verfahren belegen können, dass sie externe und interne Vorschriften einhalten. Statt wiederholte manuelle Audits durchzuführen, sollten IT-Abteilungen in Tools investieren, mit denen sie Berichte erstellen können, die die Vorschriften-Compliance der Systemkonfiguration zeigen und die beweisen, dass Steuermechanismen für die ständig IT erfolgreich angewendet werden. So vermeiden IT-Mitarbeiter, von einem Audit zum anderen zu „schwimmen“ und können die IT-Ausgaben auf strategisch wichtigere Bereiche konzentrieren.

Etablierte Unternehmen verwenden im Allgemeinen gut strukturierte Rahmenwerke. Sie entwerfen ihre Prozesse anhand von Prozessreifemodellen und verknüpfen IT-Steuermechanismen für unterschiedliche Vorschriften anhand eines grundlegenden Standards.

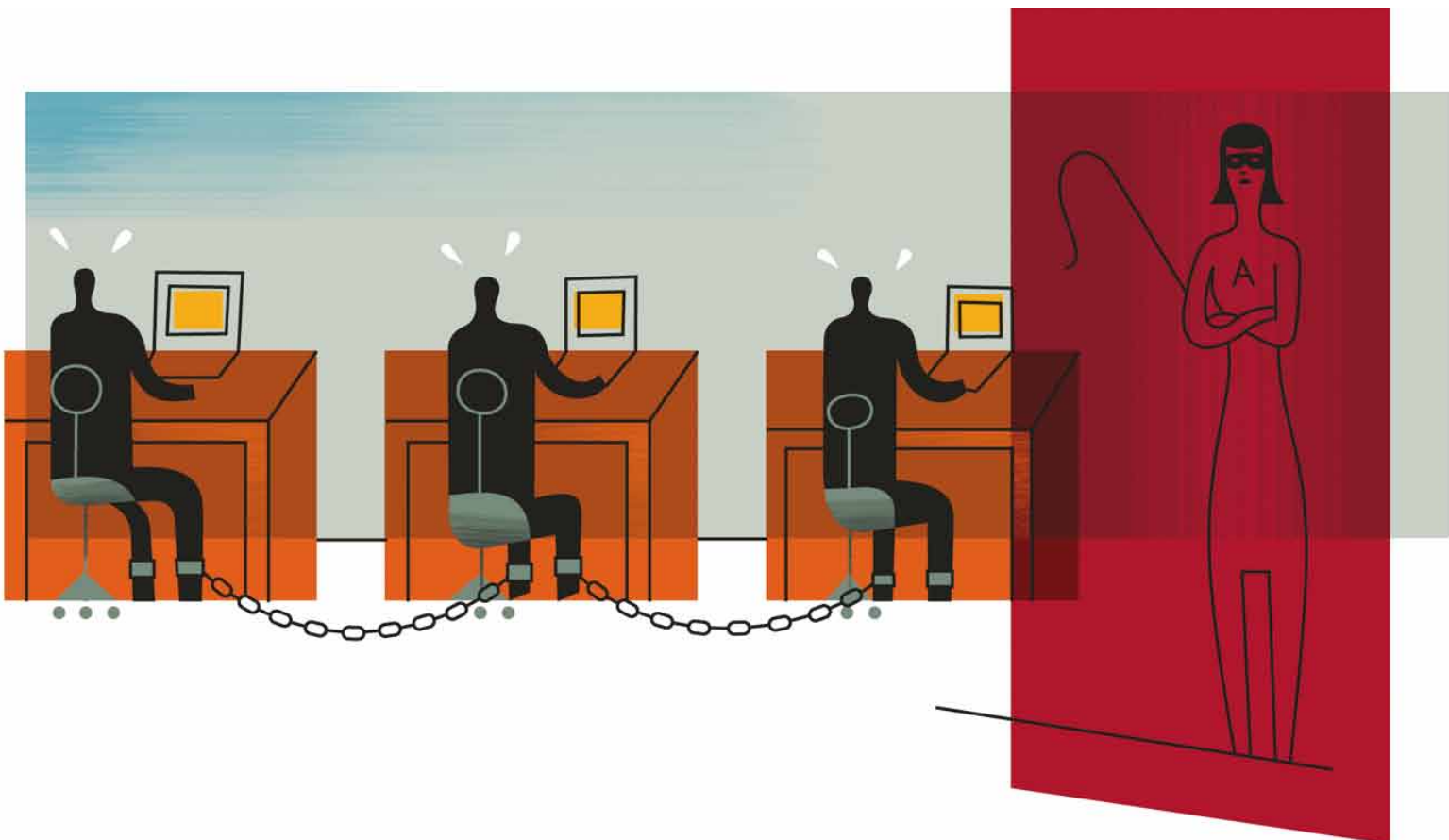
### Seitzen Sie ein gut strukturiertes Rahmenwerk auf:

Etablierte Unternehmen verwenden im Allgemeinen gut strukturierte Rahmenwerke. Sie entwerfen ihre Prozesse anhand von Prozessreifemodellen und verknüpfen IT-Steuermechanismen für unterschiedliche Vorschriften anhand eines grundlegenden Standards wie ISO 27002 oder dem Unified Compliance Framework. Das vereinfacht die Reduzierung erforderlicher separater Audits und führt zu wesentlichen Einsparungen bei der Erhaltung der Compliance. Außerdem müssen IT-Mitarbeiter dadurch nicht für mehrere Standards geschult werden. Es steht ein gemeinsames Rahmenwerk zur Verfügung, das die Kommunikation mit den Auditoren erleichtert und als Basis für angemessene Sicherheitsrichtlinien dienen kann.

Wenn IT-Abteilungen belegen können, dass sie ihre Umgebungen unter Kontrolle haben, indem sie sie mit anderen geschäftlichen Aufgaben koordinieren, umfassende Berichte zur Einhaltung von IT-Vorschriften automatisiert erstellen und über ein integriertes Steuerungsrahmenwerk verfügen, haben sie alle notwendigen Schritte durchgeführt, um externen Auditoren klare Grenzen zu setzen und zugleich die IT-Integrität ihrer Unternehmen zu wahren.



**Evelyn DeSouza** ist Senior Manager für Risiko-Management- und Compliance-Lösungen bei McAfee, Inc. Sie entwickelt einheitliche Lösungen für Initiativen zur Einhaltung von Vorgaben wie PCI DSS. De Souza spricht sich nachdrücklich für die Einrichtung automatisierter, wiederholbarer Prozesse aus, mit denen Unternehmen Vorschriften effizienter einhalten und zugleich ihre Sicherheit erhöhen können. In ihrer Freizeit holt sich Evelyn DeSouza ihren Adrenalinschub beim Trainieren für Halbmarathons in ihrer Gegend.



# PCI DSS: Besser als gar nichts

Anthony Bettini



Die Kreditkartenindustrie entwickelte einen Sicherheitsstandard, der die Anforderungen der Unternehmen und Kunden erfüllt und deren Interessen dient.

## Vorgeschichte

Stellen Sie sich vor, Sie führen ein kleines Unternehmen, in dem Sie Kreditkarten als Zahlungsmittel akzeptieren. Der Zahlungsvorgang funktioniert ganz einfach, und Sie müssen keine großen Mengen an Bargeld bereithalten. Allerdings verlangen die Kartenunternehmen die Einhaltung ihrer Sicherheitsrichtlinien. Im Hinblick auf den Schutz Ihrer Interessen scheint das sinnvoll zu sein. Was passiert aber, wenn jedes Kartenunternehmen eigene Regeln aufstellt, die Sie einhalten müssen?

Genau dieser Herausforderung sahen sich Besitzer kleiner und mittlerer Unternehmen (KMU) in der Vergangenheit gegenüber. KMUs – und dabei insbesondere solche, die e-commerce betreiben Webanwendungen mit ihren verschiedenen Kunden – mussten eine Vielzahl von unterschiedlichen Kreditkarten akzeptieren. Die Unternehmer sahen sich mit einer Reihe von Problemen konfrontiert, wenn sie die verschiedenen Programme und Richtlinien der Kreditkartenunternehmen einhalten wollten: z. B. das Programm Site Data Protection (SDP) von MasterCard zum Schutz der Daten auf Webseiten, das Programm Cardholder Information Security Program (CISP) von Visa zum Schutz der Daten von Karteninhabern, die Datenschutzrichtlinie Data Security Operating Policy (DSOP) von American Express, das JCB-Datensicherheitsprogramm und die Richtlinie Discover Information Security and Compliance (DISC) von Discover zur Datensicherheit und Einhaltung von Regeln. Folglich wurde der Payment Card Industry Data Security Standard (PCI DSS), ein Regelwerk zur Datensicherheit bei Kreditkartentransaktionen, ins Leben gerufen. Ziel dieses Regelwerks ist ein einheitlicher und sich ständig entwickelnder Sicherheitsstandard für Unternehmen, die für die Abwicklung von Kreditkartentransaktionen zuständig sind.

Der PCI DSS wurde aus den einzelnen Datensicherheitsstandards der größten Kreditkartenunternehmen MasterCard, Visa, American Express, JCB und Discover entwickelt. Da jedes dieser Unternehmen zuvor über einen eigenen Standard verfügte, wurde deren praktische Umsetzung bei KMU-Händlern erheblich erschwert. Diese Händler machen jedoch den Großteil des Kundenstamms der Kreditkartenanbieter und häufig auch den Großteil der abgewickelten Transaktionen aus.

Die führenden Kreditkartenanbieter blicken auf eine lange Geschichte bei der Bekämpfung von Betrug zurück. Obwohl Betrügereien mit großer Wahrscheinlichkeit nie ganz verhindert werden können, wird die Messlatte bei der Sicherheit immer weiter angehoben, da immer kostengünstigerer Verfahren zur Reduzierung der Betrugsraten entwickelt werden. Der PCI DSS funktioniert ähnlich. Es handelt sich nicht um ein abgeschlossenes Regelwerk, sondern um ein sich ständig weiterentwickelnder Standard, mit dem betrügerische Transaktionen immer mehr erschwert werden sollen. Indem sichergestellt wird, dass alle Händler zumindest eine gewisse Grundsicherheit gewährleisten, kann die Kreditkartenindustrie wahrscheinlich Betrügereien reduzieren, die Ausgaben verringern und aufgrund des wachsenden Kundenvertrauens weitere Kreditkartentransaktionen begünstigen – während sie und die Händler sich höherer Einnahmen erfreuen.

PCI DSS scheint also ein Gewinn für die Kreditkartenindustrie zu sein. Er bringt auch Vorteile für eCommerce-Webseiten und für Kunden. Für eine kleine eCommerce-Webseite ist es oft nicht leicht, dem Kunden ihre Botschaft oder ihr Produkt zu vermitteln. Neben der häufig von eCommerce-Webseiten eingesetzten Suchmaschinenoptimierung (SEO, search engine optimization) sind so genannte Vertrauenssiegel (engl.: trustmark) ein weiterer Weg, das Vertrauen der Kunden zu gewinnen und damit die Einnahmen zu steigern. Diese Siegel signalisieren dem Kunden, dass eine Webseite bestimmte Sicherheitstests bestanden hat. Weil ein Vertrauenssiegel letztlich zu höheren Einnahmen führt, ist es eine kostengünstige Möglichkeit zur Gewinnoptimierung für die Unternehmen. Für die Kunden liegt der Vorteil auf der Hand. Ein Vertrauenszeichen auf der Webseite ihres Lieblingsinternetshops bedeutet, dass diese Seite mindestens die grundlegenden Sicherheitsanforderungen erfüllt. Zusätzlich bieten einige Anbieter von Vertrauenssiegeln weitere Compliance-Tests an, mit denen Unternehmen die Einhaltung der PCI DSS-Richtlinien bestätigen.

## Kritikpunkte

Die Vorteile für alle Beteiligten sind offensichtlich, ein Sicherheits-Nirwana wird wahrscheinlich trotzdem ein schöner Traum bleiben. Es sind bereits einige Fälle bekannt, in denen die Daten und Systeme von großen, bekannten und PCI DSS-konformen Dienstleistern kompromittiert wurden. Es waren unter anderem US-amerikanische Einrichtungen wie die Supermarktkette Hannaford Brothers, das Skigebiet Okemo Mountain Resort sowie der Kreditkarten-Abrechnungsdienstleister Heartland Payment Systems betroffen. Das Medieninteresse war in jedem dieser Fälle groß, da alle drei Opfer PCI DSS-zertifiziert waren und dennoch Kreditkartennummern von Kunden gestohlen wurden.

Obwohl Fälle wie diese zunächst wie unvorhergesehene, seltene Ausnahmen erscheinen (Kompromittierung trotz PCI DSS-Konformität), können sie nur selten als solche bewertet werden. Sehen wir uns das erste Beispiel genauer an. Hannaford Brothers ist eine Supermarktkette im Nordosten der USA, die Opfer eines Malware-Angriffs war, bei dem etwa 4,2 Millionen Kreditkartennummern gestohlen wurden. In einem von Bank Info Security veröffentlichten Artikel über die Datenkompromittierung bei Hannaford fanden wir ein interessantes Zitat, das wir genauer analysieren möchten. Es wurde sowohl als Herausforderung als auch als Verteidigung des PCI DSS genutzt.

„Eine PCI-Bewertung ist eine Bewertung zu einem bestimmten Zeitpunkt“, so David Taylor (Präsident der PCI Security Vendor Alliance). „Die Gegebenheiten in einem Netzwerk und an anderen Stellen in den Systemen und Verfahren können sich ändern und dazu führen, dass das Unternehmen nicht mehr PCI DSS-konform ist.“<sup>1</sup>

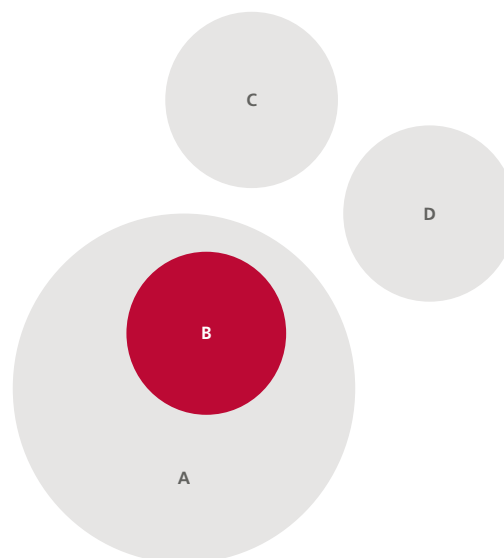
Das ist zwar zweifelsohne richtig. Es stimmt aber auch, dass viele PCI DSS-Zertifizierungsstellen, darunter auch McAfee® SECURE™, häufiger Scans durchführen (McAfee scannt beispielsweise täglich). Die PCI DSS-konformen Systeme von Hannaford Brothers wurden nicht aufgrund von Bewertungen, die nur einen bestimmten Zeitpunkt widerspiegeln, kompromittiert. Die Erklärung ist viel einfacher: Nicht alle Bedrohungen können realitätsnah getestet werden. Bedenken Sie, dass die Schwachstellendatenbank (National Vulnerability Database, NVD) der US-amerikanischen Behörde für Standards und Technologie (National Institute of Standards and Technology, NIST) 35.441 Datensätze zu Schwachstellen enthält, die jeweils mit einer Datenbank über häufige Schwachstellen und Sicherheitslücken (Common Vulnerabilities and Exposures, CVE) verknüpft sind.<sup>2</sup> Da täglich neue Schwachstellen und Bedrohungen entdeckt werden, entsteht eine Lücke bei der Absicherung der Sicherheitsanbieter, die wiederum zu einer Lücke beim Umfang der Sicherheitsbewertung und der Schutztechnologien führt, die die PCI DSS-Compliance zertifizieren.

Die PCI DSS-konformen Systeme von Hannaford Brothers wurden nicht aufgrund von Bewertungen, die nur einen bestimmten Zeitpunkt widerspiegeln, kompromittiert. Die Erklärung ist viel einfacher: Nicht alle Bedrohungen können realitätsnah getestet werden.

Es ist daher möglich, dass Softwareprogramme, die eine Einhaltung des PCI DSS bestätigen, nicht alle PCI DSS-Schwachstellen entdecken, die zu einer Nicht-Compliance der Systeme führen (selbst wenn viele dieser Schwachstellen vorhanden und öffentlich bekannt sind). Der Grund dafür liegt darin, dass die Entdeckung den Schutz von Schwachstellen überholt. Einfacher gesagt: Bedrohungen werden schneller entdeckt als Schutz davor gewährt werden kann. Dieser Trend wird sich wahrscheinlich auch in Zukunft nicht ändern und kann in Bedrohungsszenarien sowohl bei Schwachstellen als auch bei Malware beobachtet werden. Von diesem Problem ist aber nicht nur die Sicherheitssoftware an sich betroffen, auch manuelle, von Personen gesteuerte Tests (die sich oft auf mindestens ein automatisiertes Verfahren stützen) hätten mit diesem Problem unvollständiger Tests zu kämpfen.

Im folgenden Venn-Diagramm ist das Problem grafisch dargestellt, ohne dabei genaue Größenverhältnisse abzubilden.

Das Element „Von PCI DSS-Zertifizierungsanbietern getestete Schwachstellen“ (B) stellt die Schwachstellen von Webanwendungen dar, die für eine benutzerdefinierte Webapplikation spezifisch sind. Die beiden Kreise (C) und (D) repräsentieren Schwachstellen, die auf Netzwerk-anwendungen bzw. Betriebssysteme abzielen könnten oder Webapplikationsspezifisch sind (z. B. Schwachstellen von websiteübergreifender Skripterstellung oder SQL-Injektion in benutzerdefinierten Anwendungen). Im Allgemeinen sind Schwachstellen, die für eine benutzerdefinierte Webapplikation spezifisch sind, nicht in der NVD des NIST enthalten und haben höchstwahrscheinlich eine kurze Nutzungsdauer, sofern sie öffentlich bekannt sind.



- A 35.441 öffentlich bekannte Schwachstellen in der NVD (einschließlich einiger Schwachstellen in Webanwendungen)
- B Von PCI-DSS-Zertifizierungsanbietern getestete Schwachstellen
- C Vorhandene, aber unter Verschluss gehaltene Schwachstellen
- D Vorhandene, aber weder öffentlich bekannte noch unter Verschluss gehaltene Schwachstellen

Es besteht also eine Diskrepanz zwischen den vorhandenen (sowohl bekannten als auch unbekannt) und den getesteten Schwachstellen. Da sich dieser Zustand in naher Zukunft nicht ändern wird, müssen wir auch weiterhin mit Kompromittierungen der allgemeinen Sicherheit bei Kreditkartendienstleistern rechnen, selbst bei Anbietern mit zertifizierter PCI DSS-Compliance.

Eine weitere Herausforderung ist konkrete Zertifizierung der Einhaltung der PCI DSS-Richtlinien. Obwohl der Test von Netzwerkschwachstellen in den PCI DSS-Bewertungsvorgaben sehr genau festgelegt ist, wurde der Schwachstellentest von benutzerdefinierten Webanwendungen nicht ausreichend beschrieben. Wenn beispielsweise eine große Internetanwendung mit Einkaufswagenfunktion (z. B. eine Auktionsseite oder ein elektronischer Buchhandel) eine PCI DSS-Zertifizierung erhalten möchte, sollen Entwickler die websiteübergreifenden oder SQL-Injektionstests dann einfach auf der Hauptseite ausführen oder die gesamte Site durchsuchen und jede Seite testen? Und ab wann soll der Tester – egal ob automatisiert oder manuell – die Site nicht weiter durchkämmen und die Compliance bestätigen können? Dieser Aspekt wird derzeit nicht im PCI DSS berücksichtigt. Das führt zu unterschiedlichen Testkriterien bei den Händlern, die eine Einhaltung dieses Standards bestätigen.

## Fazit

Wir sollten uns nicht über Sicherheitskompromittierungen bei PCI DSS-konformen Unternehmen wundern. Manch einer denkt nun wahrscheinlich, dass das Ansehen der kompromittierten Unternehmen darunter gelitten hat. Sowohl der PCI DSS selbst als auch Anbieter von Vertrauensiegeln, die eine PCI DSS-Zertifizierung anbieten, tun alles derzeit Mögliche und arbeiten sehr wahrscheinlich so, wie vom PCI Security Standards Council vorgesehen. Konkret heißt das: Das System verbessert den Datensicherheitsstatus bei Kreditkartendienstleistern, um Betrügereien zu verringern und das Vertrauen der Kunden zu erhöhen. Oder anders gesagt: Der PCI DSS ist besser als gar nichts.



**Anthony Bettini** gehört zur führenden Management-Ebene von McAfee Avert Labs. Er hat sich auf die Sicherheit und Schwachstellenerkennung von Windows spezialisiert. Bettini arbeitete bereits für Foundstone, Guardent, BindView sowie als freier Anbieter. Er hielt einen Vortrag im Bereich der Anti-Tracing-Techniken auf der National Information Systems Security-Konferenz des NIST sowie für zahlreiche Global-2000-Unternehmen. In der Zeit bei Foundstone veröffentlichte Bettini Schwachstellen, die er bei Windows, ISS Scanner, PGP, Symantec ESM und anderen weit verbreiteten Anwendungen fand. Er ist der technische Herausgeber von *Das Anti-Hacker-Buch*, 5. Auflage.

Manch einer denkt nun wahrscheinlich, dass das Ansehen der kompromittierten Unternehmen darunter gelitten hat. Sowohl der PCI DSS selbst als auch Anbieter von Vertrauensiegeln, die eine PCI DSS-Zertifizierung anbieten, tun ihr Bestes.



## ENDNOTEN

- 1 McGlasson, Linda: „Hannaford Data Breach May be ‘Tip of the Iceberg,‘“ (Datenkompromittierung bei Hannaford möglicherweise nur Spitze des Eisbergs), Bank Info Security, 4. April 2008, [http://www.bankinfosecurity.com/articles.php?art\\_id=810](http://www.bankinfosecurity.com/articles.php?art_id=810)
- 2 Schwachstellendatenbank der US-amerikanischen Behörde für Standards und Technologie (NIST), 23. Februar 2009, <http://nvd.nist.gov>

## GLOSSAR

**PCI** Kreditkartenindustrie  
**PCI DSS** Payment Card Industry Data Security Standard  
**SEO** Search Engine Optimization (Suchmaschinenoptimierung)

## LITERATURHINWEISE

- Reber, Greg: „PCI compliance falls short of assuring website security“ (PCI-Compliance kann Webseiten-sicherheit nicht garantieren), SearchSoftwareQuality.com, 27. Oktober 2008. [http://searchsoftwarequality.techtarget.com/news/column/0,294698,sid92\\_gci1335662,00.html](http://searchsoftwarequality.techtarget.com/news/column/0,294698,sid92_gci1335662,00.html)
- Vijayan, Jaikumar: „Heartland data breach sparks security concerns in payment industry“ (Datenkompromittierung bei Heartland sorgt für Beunruhigung in der Kreditkartenindustrie), Computerworld, 22. Januar 2009. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126608>
- Vijayan, Jaikumar: „Q&A: Head of PCI council sees security standard as solid, despite breaches“ (Fragen und Antworten: Vorsitzender der PCI sagt, dass der Standard trotz Kompromittierungen ausgereift ist), Computerworld, 16. April 2008. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Financial&articleId=9078059>
- Whittaker, Zack: „Ethical Hacking: the next generation security specialists“ (Ethisches Hacking: Sicherheitsexperten der nächsten Generation), ZDNet Blogs, 22. Januar 2009. <http://blogs.zdnet.com/igeneration/?p=826>

# Umgestaltung von Audits und Compliance

Kent Landfield



Die Aufgabe, Compliance-Anforderungen zu erfüllen, bereitet den meisten IT-Mitarbeitern richtige Kopfschmerzen. Diese Schmerzen bekämpft man mit einer Mixtur aus Akronymen.

Unternehmen müssen schon seit einer halben Ewigkeit Bestimmungen einhalten – von internen Sicherheitsrichtlinien über staatliche Gesetze bis hin zu branchenweit bewährten Praktiken. Die Einhaltung von Vorschriften sichert nicht nur den Arbeitsplatz des Netzwerkadministrators, sondern verhindert heute auch zivil- und strafrechtliche Gerichtsverfahren für den Unternehmensvorstand.

Zu den staatlichen Bestimmungen und Richtlinien, die Unternehmen heute befolgen müssen, gehören Unternehmensführung, Beurteilung interner Kontrollvorgänge, verbesserte Offenlegung finanzieller Daten sowie der Schutz von Gesundheitsdaten. Die letztgenannte Aufgabe ist besonders diffizil: die Einhaltung entsprechender Maßnahmen zur Gewährleistung der Sicherheit gesundheitsbezogener Patientendaten in Netzwerk- und realer Umgebung. Vertikale Sektoren wie die Finanzbranche, müssen andere Regeln befolgen, und die Liste wird immer länger. Öffentliche Organisationen kommen um die Einhaltung der Bestimmungen des US-Kongresses und der staatlichen Gesetzgebung nicht herum. Doch nicht nur Regierungen legen Anforderungen fest. Branchengruppen wie das Payment Card Industry Security Standards Council fassen die Anforderungen an Unternehmen zusammen, die Kreditkartentransaktionen verarbeiten.<sup>1</sup> Die jährliche Compliance-Zertifizierung der Payment Card Industry (PCI, Kreditkartenbranche) soll Unternehmen dabei helfen, dass Karteninhaberdaten geschützt sind und die für die Transaktionsverarbeitung verwendete Infrastruktur dem Payment Card Industry Data Security Standard (PCI DSS, Datenschutzstandard für Kreditkartenunternehmen) entspricht. Erhält ein Unternehmen das PCI-Zertifikat nicht, verliert es das Recht, Kreditkartendaten verarbeiten zu dürfen. In Kürze wird die Einhaltung von NERC-Compliance (North American Electric Reliability Corporation) erforderlich sein. Die angedrohten Strafen belaufen sich auf 1 Mio. US-Dollar pro Tag, sollte ein Unternehmen nach dem 30. Juni 2009 die Richtlinien nicht erfüllen.

Glauben Sie, dass diese Tatsache nur in den USA Kopfschmerzen verursacht? Ganz und gar nicht. Unternehmen aus aller Welt unterliegen den gleichen Compliance-Anforderungen in ihren Ländern. Vorgaben und Bestimmungen sind all gegenwärtig, und die effektive Einhaltung ist ein schwierige Aufgabe. Wie sollen Unternehmen sicherstellen, dass sie der stetig wachsenden Anzahl von Compliance-Anforderungen entsprechen, wenn für deren Einhaltung nur eingeschränkte Ressourcen zur Verfügung stehen?

Viele Unternehmen versuchen es mit Einfallsreichtum. Ihre Netzwerkmitarbeiter versuchen, dem Problem mit selbst erstellten Skripts und Lösungen zu begegnen. In den meisten Fällen bedeutet das die Verwendung unterschiedlicher kommerzieller Produkte, einschließlich Netzwerkscannern, Systemkonfigurationsprüfern sowie Erkennungs- und Ressourcenberichtstools – mit jeweils proprietären Inhalten und Ergebnisformaten. Das Unternehmen verwendet die eigens entwickelten Skripts, um die Daten aus den proprietären Produktdatenbanken abzurufen und in etwas Verwendbares umzuwandeln. Anschließend müssen die Mitarbeiter sicherstellen, dass die erforderlichen Berichte mithilfe der erfassten Daten geschrieben werden. Dies kann bei kleinen Unternehmen erfolgreich funktionieren, doch bei größeren Unternehmen ähnelt diese Vorgehensweise eher einem Drahtseilakt.

Die Probleme hier sind gut bekannt – viele Unternehmen waren gezwungen, so vorzugehen. Wenn ein Teil dieser Compliance-Infrastruktur nicht mehr funktioniert und dessen Autor nicht verfügbar ist, versuchen die übrigen Mitarbeiter häufig hektisch herauszufinden, was mit diesem Teil erreicht werden sollte und wie das Problem behoben werden kann.

Das NIST entwickelte das Security Content Automation Protocol (SCAP), dank dessen Anbieter und Community Audits innerhalb eines Unternehmens standardisiert und automatisiert werden können.



Verlässt der Autor das Unternehmen, trifft das auch häufig auf die Compliance-Architektur des Unternehmens zu, die damit teilweise oder vollständig mit ihm zusammen verschwindet. Bei der Änderung eines Bereichs des Datenbank- oder Berichtserstellungsformats durch einen Sicherheitsanbieter, müssen die Angestellten die selbst erstellten Tools und Skripts entsprechend anpassen, damit diese weiterhin funktionieren. Muss eine neue Bestimmung eingehalten werden, müssen die Angestellten die Bestimmung analysieren und sorgfältig alle entsprechenden Teile der Infrastruktur anpassen. Falls der Anbieter einer Anwendung die neue Bestimmung nicht unterstützt, gerät dieser Prozess ins Stocken, die Angestellten müssen eine Alternative finden, bei der die speziellen Anforderungen des Unternehmens berücksichtigt werden. Dieses Compliance-Berichtssystem ist sehr anfällig und teuer.

## Zukünftige Standards

Das Ziel der Security Automation Conference im Jahr 2006, die von der US-amerikanischen Behörde für Standards und Technologie (National Institute of Standards and Technology, NIST) abgehalten wurde, bestand in der Automatisierung der Sicherheits- und Richtlinien-Compliance. Die Konferenz konzentrierte sich auf die Integration vorhandener Sicherheitsstandards in reelle Betriebsabläufe. Als Ergebnis wurde das SCAP-Protokoll (Security Content Automation Protocol) entwickelt, mit dem Sicherheitsanbietern und der Community eine Methode zur Verfügung stehen soll, um die Standardisierung und Automatisierung aller Sicherheitsabläufe in Unternehmen zu ermöglichen.

SCAP ist kein einzelnes Protokoll, sondern eine Sammlung von Komponentenstandards und wird von NIST wie folgt beschrieben:

„SCAP ist eine Suite ausgewählter offener Standards, die Softwarefehler, sicherheitsrelevante Konfigurationsprobleme und Produktnamen benennen; Systeme kontrollieren, um das Vorhandensein von Schwachstellen zu erkennen; Mechanismen zum Einstufen (Bewerten) der gewonnenen Daten zur Verfügung stellen, damit der Einfluss der entdeckten Sicherheitsprobleme eingeschätzt werden kann. SCAP definiert, wie diese Standards kombiniert werden.“<sup>2</sup>

SCAP nutzte die Vorteile vorhandener Standards in der Sicherheits-Community und fasste sie zusammen, um Sicherheits-Compliance-Audits zu automatisieren. Bei diesen Bemühungen wurden zunächst die folgenden Standards integriert:

- **CVE** – Common Vulnerabilities and Exposures<sup>3</sup>
- **OVAL** – Open Vulnerability and Assessment Language<sup>4</sup>
- **XCCDF** – eXtensible Configuration Checklist Description Format<sup>5</sup>
- **CVSS** – Common Vulnerability Scoring System<sup>6</sup>
- **CPE** – Common Platform Enumeration<sup>7</sup>
- **CCE** – Common Configuration Enumeration<sup>8</sup>

XCCDF ist hier der zentrale Eckpunkt für den Haupteinsatzzweck für SCAP: Eine Methode zur Automatisierung der Compliance-Prüfung.

Die XCCDF-Spezifikation 1.1.4 besagt Folgendes:

„Dieses Dokument spezifiziert das Datenmodell und die Darstellung von XML (eXtensible Markup Language) für das eXtensible Configuration Checklist Description Format (XCCDF) der Version 1.1.4. Ein XCCDF-Dokument ist eine strukturierte Sammlung von Sicherheitskonfigurationsregeln für bestimmte Sätze von Zielsystemen. Mit der XCCDF-Spezifikation sollen Informationsaustausch, Dokumentengenerierung sowie die Anpassung an organisatorische und situationsbedingte Voraussetzungen unterstützt und automatisierte Compliance-Tests und die Einstufung von Compliance ermöglicht werden. Die Spezifikation definiert außerdem ein Datenmodell und -format zum Speichern der Ergebnisse von Sicherheitsempfehlungen oder von Compliance-Tests anhand von Prüflisten. Das Ziel von XCCDF besteht darin, eine einheitliche Grundlage für die Formulierung von Sicherheitsprüflisten und anderen Konfigurationsleitlinien zur Verfügung zu stellen und auf diese Weise die Verbreitung der Anwendung guter Sicherheitsmethoden zu fördern.“<sup>9</sup>

Dank XCCDF können gesetzliche Vorschriften oder Konfigurationsleitlinien in eine Standardstruktur gefasst werden, die SCAP-kompatible Produkte anschließend importieren und verarbeiten können. Die Vorteile von XCCDF sind vielfältig. Der Text der eigentlichen Richtlinie kann eingeschlossen, angezeigt und aus einem XCCDF-Prüflistendokument heraus gedruckt werden. Im Dokument sind außerdem die technischen Kontrollüberprüfungen enthalten, die – in OVAL geschrieben – die tatsächlichen Prüfungen des Systems im Netzwerk durchführen.

Kunden sind nicht mehr davon abhängig, dass ein Produktanbieter eine neue Richtlinie oder die neue Version einer vorhandenen Richtlinie unterstützt. Mit SCAP-kompatible Produkte können das XCCDF-Leitliniendokument verarbeiten und direkt darauf reagieren. Kunden müssen nicht mehr darauf warten, dass ein Produktanbieter das Dokument in die eigene proprietäre Prüf- und Richtliniensprache konvertiert. Dadurch, dass die Standardprüfungen im XCCDF-Dokument enthalten sind, ist die Branche nicht mehr für Interpretationsfehler anfällig, die häufig dann entstehen, wenn ein Produktanbieter versucht, anhand eines Dokuments die eigentlichen Absichten der Leitlinienautoren zu verstehen. Die von einem SCAP-kompatiblen Tool eines Anbieters generierten Ergebnisse sind mit denen identisch, die beim Auswerten der Prüfliste mit einem anderen Tool generiert werden.

Dank SCAP sind Kunden nicht mehr davon abhängig, dass ein Produktanbieter eine neue Richtlinie oder die neue Version einer vorhandenen Richtlinie unterstützt.

Die Autoren von Leitlinien für Vorschriften müssen jetzt nur noch ein einziges XCCDF-Dokument erstellen, das die Richtlinien-dokumentation enthält und zusammen mit den technischen Kontrollen für die Compliance-Prüfung ausgedruckt werden kann. Dieses Dokument enthält also alle erforderlichen Informationen. Als Beweis für die Echtheit der Richtlinie kann es zudem elektronisch signiert werden. Durch diese Konsolidierung entfällt nicht nur die Interpretation des Produktanbieters – mit XCCDF-kompatible Produkte können das Dokument sofort nach der Veröffentlichung der XCCDF-Richtlinienprüfliste lesen und verwenden.



## Warum ist das für Sie wichtig?

Die Schwierigkeit für ein Unternehmen besteht darin, dass es teure externe Audits bezahlt, die zu Arbeitszeitunterbrechungen bei den Mitarbeitern führen. Diese müssen sich auf die Audits vorbereiten, um sicherzustellen, dass die Netzwerksicherheit an einem bestimmten Tag den Anforderungen einer bestimmten Richtlinie entspricht. Und letztlich erhalten Sie für den ganzen Batzen Geld lediglich eine Momentaufnahme des Tages, an dem das Audit durchgeführt wurde. Wenn Sie immer noch der Meinung sind, dass das in Ordnung ist, denken Sie noch einmal darüber nach.

Wenn Sie jedoch den Zustand Ihres Netzwerk aufgeschlüsselt nach Wochen oder Tagen sehen, eine standardmäßige Automatisierung einführen und Ihren Mitarbeitern zudem großen Aufwand ersparen möchten, sollten Sie sich mit SCAP befassen. Das Protokoll und die zugehörigen Automatisierungen revolutionieren die Effizienz und Genauigkeit und reduzieren dabei erheblich die Kosten für die Überprüfung der Compliance. Die von einer mit SCAP kompatiblen Überprüfung generierten Ergebnisse bieten der Unternehmensführung außerdem einen besseren Einblick in Abläufe, sodass sie bekannte und unbekannte Möglichkeiten zur Verbesserung der Effizienz und zur Verringerung des Verwaltungsaufwands nutzen kann.

In anderen Branchen wurden ähnliche Veränderungen beobachtet. Ein gutes Beispiel hierfür sind die Barcodes, insbesondere der Universal Product Code (UPC). Viele von uns erinnern sich noch daran, wie Supermarktmitarbeiter einzelne Lebensmittelverpackungen mit einem Preisetikett versehen mussten. Sobald die Preise sich änderten, erhielten diese Verpackungen neue Preisetiketten – ein sehr zeitaufwändiger Prozess.

Anschließend mussten die Kassierer den Preis für jede Verpackung und jedes Produkt einzeln per Hand eingeben. Und am Ende der Woche musste der Verkaufsstellenleiter herausfinden, welche Waren neu bestellt werden muss, um die Regale aufzufüllen. Dazu gingen die Mitarbeiter durch die Reihen des Supermarkts und überprüften manuell, welche Produkte noch ausreichend verfügbar sind. Dies wurde häufig nach Ladenschluss getan, um die Kunden nicht beim Einkauf zu stören. Zum Glück ist das heute nicht mehr nötig.

Dank Barcodes sind Produkte bereits vom Anbieter mit Informationen zum Ursprungsland und zum Hersteller sowie mit der speziellen Artikelnummer und einer Prüfsumme gekennzeichnet, mit der der UPC-Code sich selbst überprüfen kann. Verpackungen müssen dadurch von den Verkäufern nicht mehr manuell gekennzeichnet werden.

Der Verkaufsstellenleiter kann dies einmal wöchentlich oder täglich in seinem Büro erledigen – das zum Verwalten des Bestands eingesetzte Computersystem kennt den Verkaufspreis. An der Kasse werden Ihre Einkäufe einzeln gescannt. Dabei registriert das System den Preis und hält gleichzeitig die Änderung im Bestand fest.

Durch diese Automatisierung stehen den Verkaufsstellenleitern mehrere Möglichkeiten der Nachbestellung zur Verfügung. Sie können Produkte separat verwalten und müssen nicht mehr auf regelmäßige Audits aller verfügbaren Produkte warten. Sie können kurzfristige Bestellungen vornehmen oder das gesamte Lager auffüllen lassen. Wenn angezeigt wird, dass der Bestand eines bestimmten Produkts oder einer Produktfamilie zur Neige geht, kann der Verkaufsstellenleiter das System so konfigurieren, dass eine automatische Bestellung an den Anbieter gesendet wird, damit die Bestände dieses Produkts wieder aufgefüllt werden. Durch diese Management-Möglichkeiten wurden die Kosten für die Aktualität der Preise im Supermarkt erheblich reduziert. Zudem haben Verkaufsstellenleiter einen besseren Überblick über die Vorgänge in ihrem Supermarkt: Sie sehen, was und wann die Kunden einkaufen, und sie können Kaufrends besser nutzen.

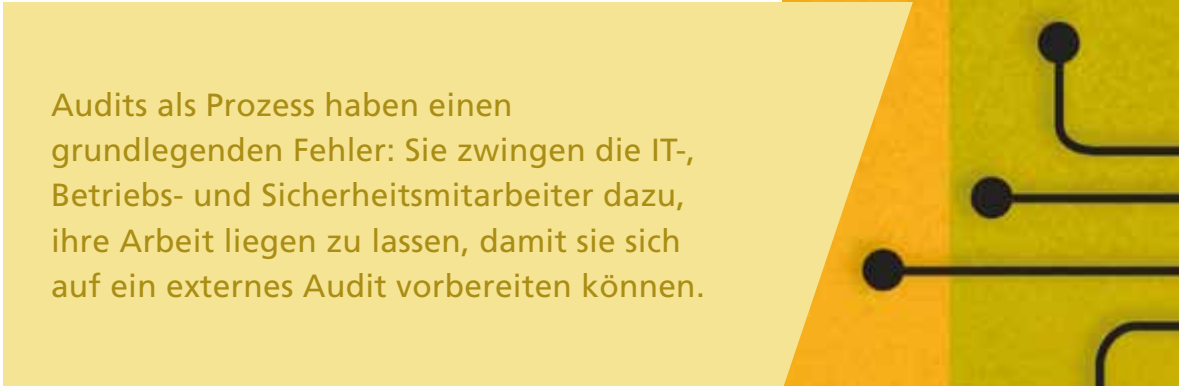
Die Verwendung von Barcodes veränderte nicht nur die Prozesse im Lebensmittelhandel – sie bilden heute die Grundlage des Einzelhandels und werden häufig auch in der Industrie eingesetzt. Viele Postdienste verwenden sie zum automatischen Sortieren von Post anhand von Postleitzahlen. Wird eine gute Technologie entwickelt, wird sie in vielen Fällen auch in anderen Bereichen eingesetzt.

## SCAP in Aktion

Heute liegt die wichtigste Aufgabe von SCAP darin, die Grundlage für die Richtlinien- und Compliance-Prüfung zur Verfügung zu stellen. SCAP ist jedoch auch in anderen Bereichen hilfreich, zum Beispiel:

- Schwachstellenerkennung
- Ressourcen-Management
- Risikoüberwachung und Reaktionen auf Risiken
- Hersteller und Kunden von Sicherheitsprodukten
- Veröffentlichung von und Benachrichtigungen über Bedrohungen

Die von einer mit SCAP kompatiblen Überprüfung generierten Ergebnisse bieten der Unternehmensführung einen besseren Einblick in Abläufe, sodass sie Möglichkeiten zur Verbesserung der Effizienz nutzen kann.



Audits als Prozess haben einen grundlegenden Fehler: Sie zwingen die IT-, Betriebs- und Sicherheitsmitarbeiter dazu, ihre Arbeit liegen zu lassen, damit sie sich auf ein externes Audit vorbereiten können.

## Neue Entwicklungen

SCAP wurde so entworfen, dass weitere Funktionen oder Komponentenstandards hinzugefügt werden können. So wird beispielsweise für CCEs eine Ergänzung zu CVSS entwickelt, die auf Softwarefehlern beruht. Es wurde vorgeschlagen, das Common Configuration Scoring System (CCSS) als Maßstab für die Einstufung von Fehlkonfigurationen und dadurch entstehende Risiken festzulegen.

Eine der Schwachstellen des aktuellen SCAP-Ansatzes besteht darin, dass er sich auf die Automatisierung von Compliance-Prüfungen konzentriert, die sich auf vernetzte Systeme beziehen. Obwohl dies von Jahr zu Jahr immer wichtiger wird, ist das nur ein Teil des ganzen Problems beim Bewerten von Organisationen in Bezug auf gesetzliche Richtlinienanforderungen. Bei einem Organisations-Audit gibt es viele Fragen, die von den Angestellten beantwortet werden müssen. Ohne diese Antworten ist das Audit nicht einmal ansatzweise vollständig. So kann eine Anforderung zum Beispiel sein, dass Backups an einem anderen Standort aufbewahrt werden müssen. Dies muss von einem entsprechenden Angestellten überprüft werden und lässt sich nicht über das Netzwerk testen.

Um diese Schwachstelle zu eliminieren, entwickeln die NIST und Branchenteilnehmer einen neuen Standard – die Open Checklist Interactive Language (OCIL). Diese Sprache definiert die Rahmenbedingungen für die Fragen an Angestellte und spezifiziert die Prozesse für die Interpretation der Antworten. Sobald OCIL in SCAP integriert ist, können vollständige Audits durchgeführt werden, d. h. die Audits können dann sowohl vernetzte Systeme als auch organisationsbezogene Geschäftspraktiken überprüfen. Die Entwickler von OCIL gehen davon aus, dass dieser Standard auch in anderen Bereichen Anwendung finden wird.

## SCAP verändert die Audits

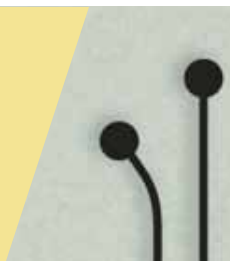
Audits als Prozess haben einen grundlegenden Fehler: Sie zwingen die IT-, Betriebs- und Sicherheitsmitarbeiter dazu, ihre Arbeit liegen zu lassen, damit sie sich auf ein externes Audit vorbereiten können. Sehr häufig wird der Auditor von den Angestellten als Feind betrachtet, da sie das Gefühl haben, dass ihre Leistung zu einem

bestimmten Zeitpunkt benotet wird. Es liegt in der Natur von Audits, dass der Prüfer etwas zu finden versucht, das die enormen Kosten des Audits rechtfertigt. Und letztendlich liefert das Audit lediglich einen Schnappschuss der Arbeitsumgebung zu einem bestimmten Zeitpunkt. In der Zwischenzeit vernachlässigen die Angestellten ihre Arbeit, da sie versuchen, dem Prüfer die Compliance des Unternehmens mit den Audit-Anforderungen zu beweisen.

SCAP verändert die Dynamik der Audits und damit die Art und Weise, wie sie durchgeführt werden:

- Auditoren müssen keine eigenen Tools mitbringen, um Netzwerkressourcen direkt prüfen zu können.
- Vom Auditor bestätigte und signierte Prüflisten werden im Netzwerk ausgeführt.
- IT-Mitarbeiter übergeben dem Auditor die signierte Prüfliste und die signierte Konfigurationsanpassungsdatei und gewähren Zugriff auf die signierten Ergebnisdateien des Unternehmens, die die Zusammenfassung der OCIL-Reaktionen enthalten.
- Der Auditor kann die Prüfliste, die Ergebnisse und die Signaturen überprüfen und bestimmen, ob weitere Bereiche vor Ort überprüft oder einem Audit unterzogen werden sollen. Die Auditoren geben Empfehlungen für die Verbesserung von Unternehmenspraktiken oder Systemkonfigurationen. Sobald diese akzeptiert werden, integrieren die Angestellten sie in die SCAP-Prüfliste.
- Die Verbesserungen werden umgesetzt, und weitere Elemente werden überprüft.
- Das Betriebspersonal und die Management-Ebene haben ständig einen Überblick über den Zustand des Netzwerks.
- Der Vorgang der Compliance-Prüfung lenkt die Angestellten nicht von der Arbeit ab, der Auditor wird als Partner gesehen, der dem Unternehmen bei der Verbesserung der Sicherheitslage hilft.
- Die Management-Ebene kann die Sicherheitslage der Netzwerke sowie die allgemeinen betrieblichen Abläufe schneller, umfassender und mit erheblich geringeren Kosten überprüfen und erfassen.

SCAP liefert heute einen Standard für Computer zum Austausch von Informationen zu Schwachstellen, Konfigurationen und Status quo und ermöglicht dadurch die Kompatibilität zwischen Produkten und Dienstleistungen mehrerer Anbieter.



## SCAP heute

SCAP liefert heute einen Standard für Computer zum Austausch von Informationen zu Schwachstellen, Konfigurationen und Status quo und ermöglicht dadurch die Kompatibilität zwischen Produkten und Dienstleistungen mehrerer Anbieter. SCAP ist ein standardbasierter Ansatz zur Implementierung der technischen Überprüfungen, die nur einmal geschrieben werden müssen und anschließend von unterschiedlichen Richtlinien genutzt werden können. SCAP stellt eine konsistente Methode zur Bewertung von Richtlinien-Compliance dar und bietet dadurch die Bedingungen für die Bereitstellung einer Infrastruktur, die exakte und schnelle Berichterstellung des Zustands der Netzwerkkumgebung unterstützt.

Die konstante Standardisierung ermöglicht Autoren von Leitlinien die Erstellung eines einzelnen Dokuments, das direkt als Grundlage für Aktionen dienen kann. Unternehmen können aktuelle Leitlinien so anpassen, dass sie bestimmten lokalen Bedürfnissen entsprechen. Sie können eigene Handbücher für Sicherheitsrichtlinien erstellen und dafür Archive vorhandener technischer Prüfungen verwenden, die von Anbietern und Community-Repositories bereitgestellt werden. Da die Inhalte standardisiert sind, könnten sie sogar eigene Überprüfungen entwerfen.

Sobald ein Unternehmen entschieden hat, welche Richtlinien verwendet werden sollen, kann die installierte SCAP-kompatible Software die Richtlinien-Prüflisten planen und auf entsprechende Systeme innerhalb des Unternehmens anwenden. Die Ergebnisse der automatisierten Compliance-Tests werden anschließend aggregiert und in Berichten zusammengefasst – ohne dass die Angestellten dazu anwesend sein müssen.

Mit anderen Worten: Die durch SCAP ermöglichte automatisierte Compliance-Prüfung erlaubt Unternehmen eine transparente, interoperable und reproduzierbare Methode zur Einschätzung von Fehlern in der Sicherheitssoftware und fehlerhaften Konfigurationen innerhalb des Unternehmens.

Die Automatisierung ist der Hauptgrund für den Erfolg von SCAP. Früher gab es keinen Rahmen für automatisierte und integrierte Sicherheitsinhalte, Vorschriftenleitlinien und Ergebnisberichte zwischen den Produkten mehrerer Anbieter. Mit SCAP ist das heute Realität.



**Kent Landfield** ist Leiter des Forschungsteams für Risiko- und Compliance-Sicherheit bei McAfee Avert Labs. Er ist seit den POSIX-Arbeitsgruppen in den späten 1980er Jahren an der Entwicklung von Sicherheitsstandards beteiligt. Landfield wirkte an der Entwicklung von Standards für die Internet Engineering Task Force und die Trusted System Interoperability Group mit. Er gehörte zu den ursprünglichen Mitgliedern der Kommission, die CVE ausgearbeitet hat, ist Mitglied der OVAL-Kommission und beteiligt sich aktiv an den CPE- und CCE-Arbeitsgruppen.

### ENDNOTEN

- 1 PCI Security Standards Council: <https://www.pcisecuritystandards.org/>
- 2 NIST: „Security Content Automation Protocol“. <http://nvd.nist.gov/scap/docs/SCAP.doc>
- 3 The Mitre Corporation: „Common Vulnerabilities and Exposures“. <http://cve.mitre.org/>
- 4 The Mitre Corporation: „Open Vulnerability and Assessment Language“. <http://oval.mitre.org/>
- 5 NIST: „XCCDF – eXtensible Configuration Checklist Description Format“. <http://nvd.nist.gov/xccdf.cfm>
- 6 FIRST: „Common Vulnerability Scoring System“. <http://first.org/cvss/>
- 7 The Mitre Corporation: „Common Platform Enumeration“. <http://cpe.mitre.org/>
- 8 The Mitre Corporation: „Common Configuration Enumeration“. <http://cce.mitre.org/>
- 9 NIST: „XCCDF Specification 1.1.4“. <http://nvd.nist.gov/xccdf.cfm>

---

# Malicious Messaging – ein globaler Überblick

David Marcus



In den vergangenen Jahren haben sich die Bedrohungslandschaft und die Natur von Malware- und Messaging-Bedrohungen erheblich verändert.

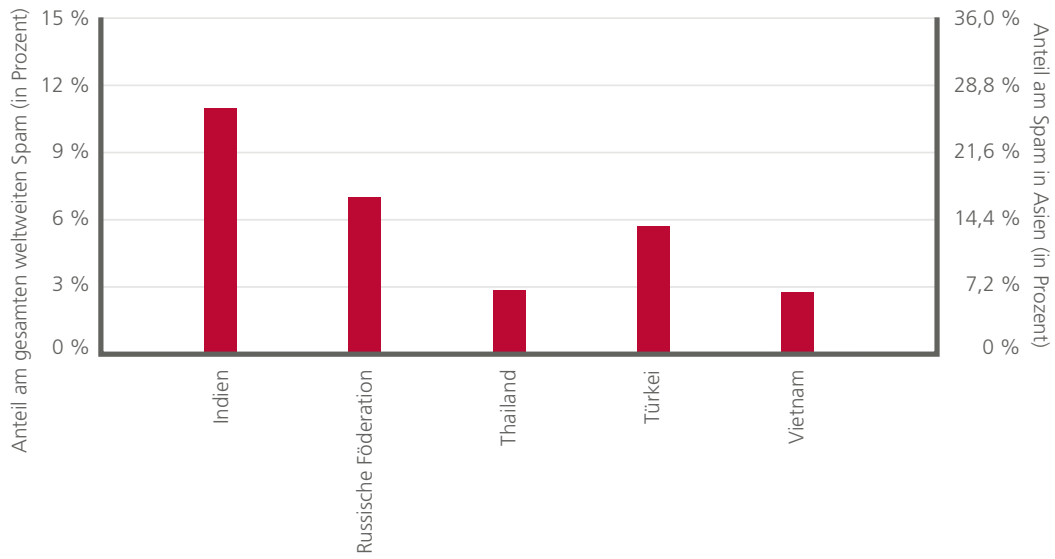
Vor gerade einmal zwei oder drei Jahren – im Internet eine Ewigkeit – gab es kaum Daten, die auf regionale Bedrohungen hinwiesen. Angriffe richteten sich hauptsächlich gegen englischsprachige Benutzer und solche, die englische Versionen von Betriebssystemen und Applikationen einsetzten. Die Zielrichtung der Angriffe war insgesamt eher unspezifisch.

Diese Zeiten sind vorbei. Wie in dieser Ausgabe des *McAfee Security Journal* gezeigt wird, sind Compliance und das Befolgen von Vorschriften weltweit ein Thema und haben Auswirkungen auf Unternehmen auf der ganzen Welt. Ereignisbezogene und kulturspezifische Bedrohungen in der jeweiligen Muttersprache sind seit einigen Jahren fester Bestandteil der Internetwelt. Weltweit gibt es immer mehr Menschen mit attraktivem Einkommen und wertvollen Daten. Gerade diese Personen, die mehrheitlich das Internet bevölkern, stellen die lohnendsten Ziele dar. Sowohl die Quellen als auch die Ziele von Malware und Messaging-Bedrohungen ändern sich häufiger als je zuvor. Auf den folgenden Seiten werfen wir einen Blick auf einige der größten Quellen und weltweite Zahlen. Bedenken Sie dabei, dass es sich hier nur um die derzeit größten Absender böswilliger Inhalte handelt! Auf eines können Sie sich verlassen: Solange sich Bedrohungen weiterentwickeln, wird sich diese Auflistung immer wieder verändern.

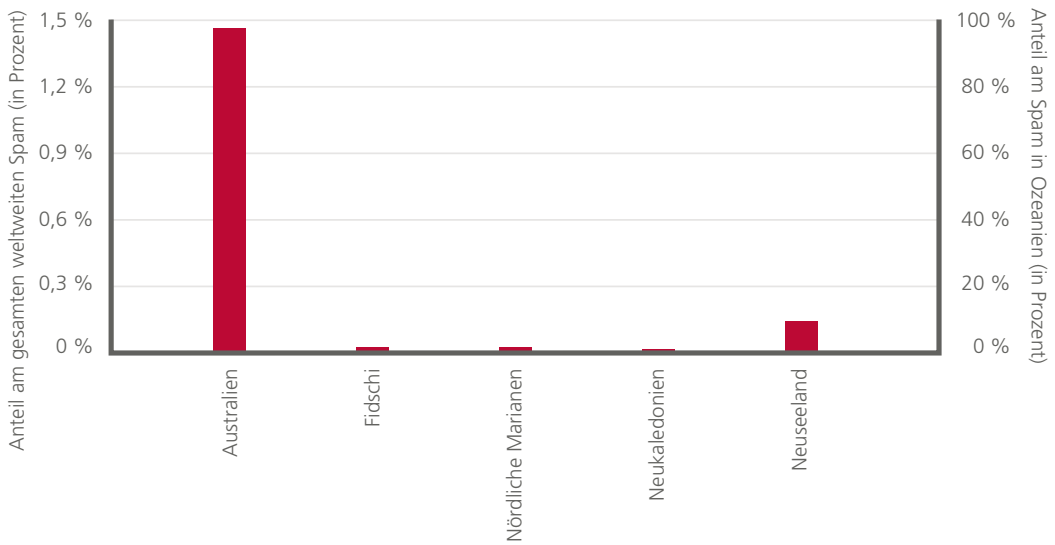


**David Marcus** ist Direktor im Bereich der Sicherheitsforschung und Kommunikation bei McAfee Avert Labs. Er sorgt dafür, dass die umfangreichen Sicherheitsforschungen von Avert Labs die Kunden von McAfee und die große Sicherheitsgemeinde erreichen und ist für alle Avert Labs-Veröffentlichungen, einschließlich dem *McAfee Security Journal*, verantwortlich.

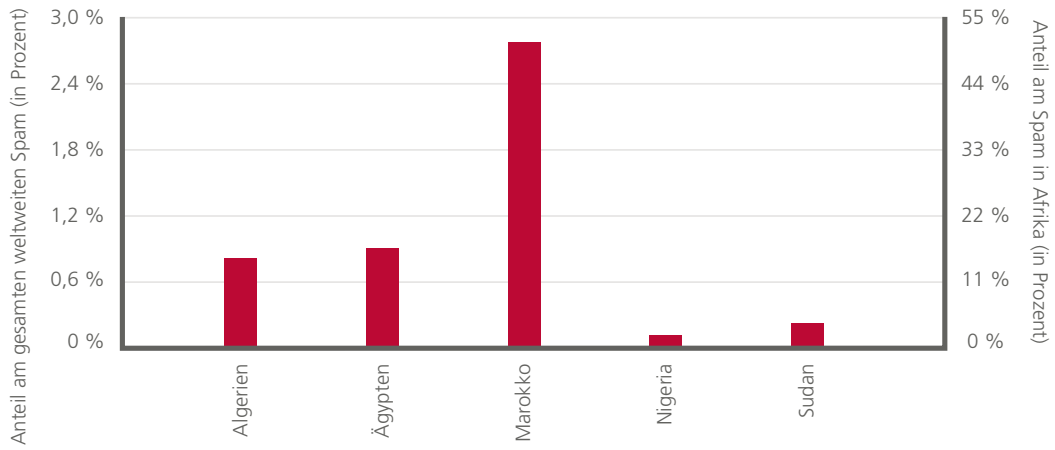
## Asien



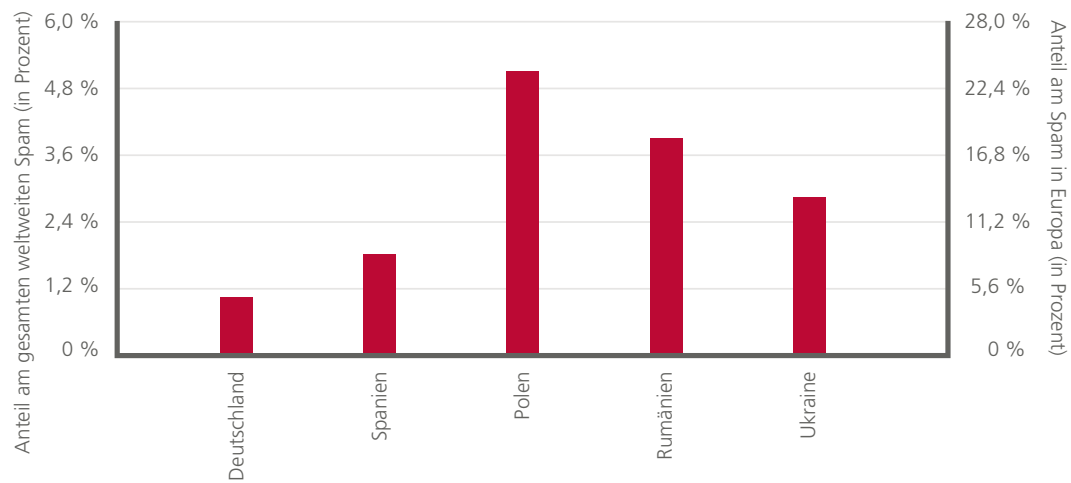
## Ozeanien



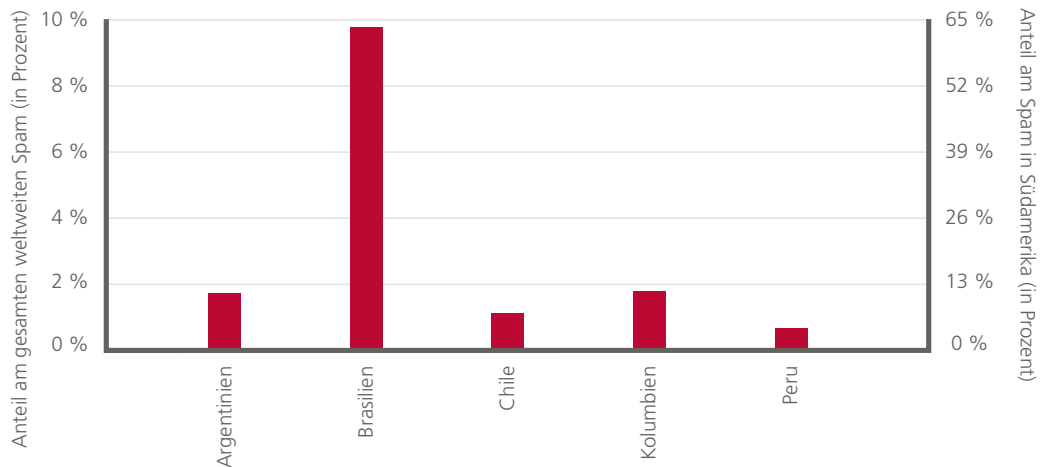
## Afrika



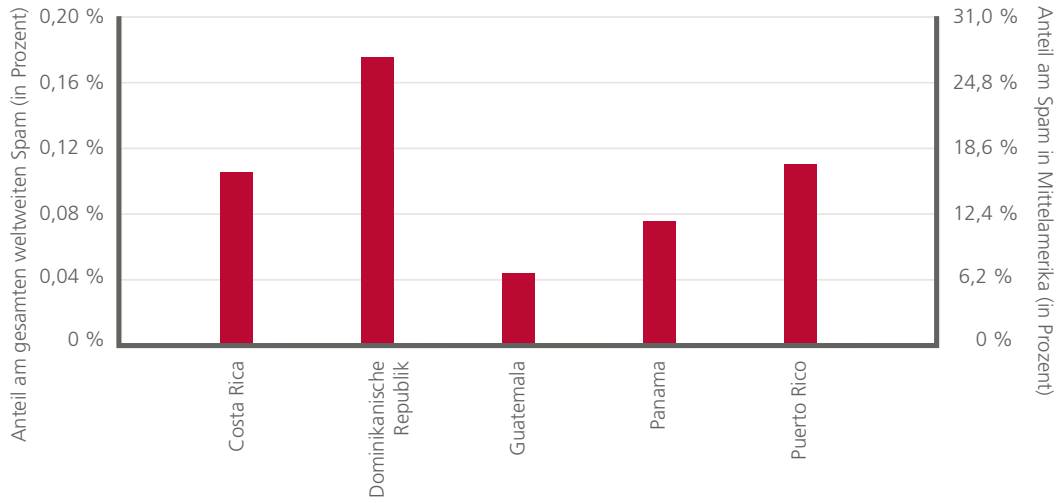
## Europa



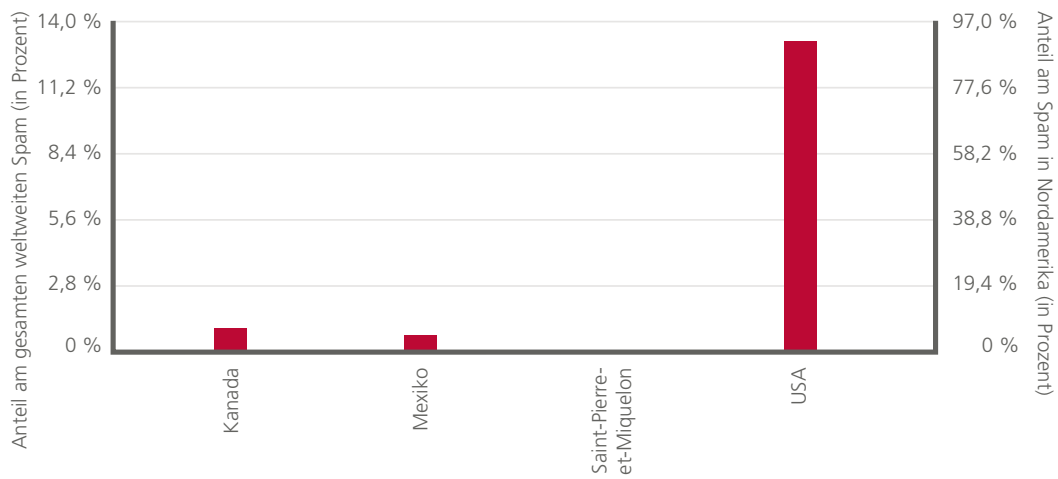
## Südamerika



## Mittelamerika



## Nordamerika





# McAfee®

McAfee GmbH  
Ohmstr. 1  
85716 Unterschleißheim  
Deutschland

+49 (0)89 37 07-0

[www.mcafee.com/de](http://www.mcafee.com/de)

McAfee und/oder andere in diesem Dokument enthaltene Marken sind eingetragene Marken oder Marken von McAfee, Inc., und/oder der Tochterunternehmen in den USA und anderen Ländern. Die Farbe McAfee-Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee-Produkte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind alleiniges Eigentum ihrer jeweiligen Besitzer.  
© 2009 McAfee, Inc. Alle Rechte vorbehalten.

5910\_sec-jrnl\_sum09