

IT-Grundschutz

Für CIOs, IT-Manager und -Sicherheitsverantwortliche



Liebe Leserinnen & Leser,

Microsoft jubelt, Windows Vista ist fertig. In den Unternehmen ist die Freude verhaltener. Auf vielen PC läuft noch Windows 2000, den Schritt zu einem ganz neuen Betriebssystem werden die wenigsten in absehbarer Zeit in Angriff nehmen. Das mag auch an den, zwar entschärften aber immer noch umfangreichen, Lizenzbestimmungen für Windows Vista liegen, die wir in einem Artikel vorstellen. Darüber hinaus beschäftigt sich ein Artikel mit dem Thema Produktpiraterie – nicht nur bei Uhren und Handtaschen gibt es Fakes, auch Router und Computer werden gefälscht. Und zwei Autoren beschreiben in einem Nachtrag zum Thema Compliance wie vielfältig Unternehmen an Regeln und Regularien gebunden sind.

Herzlichst Ihre

Nicola D. Schmidt

INHALT

IT UND RECHT

Steuerlich relevante E-Mails	2
Lizenzbedingungen bei Vista	3
Studien und Analysen	4
Das ewige Post-It	4

PRAXIS UND ANWENDUNGEN

Gefälschte Computerprodukte	5
Roadmap-sichere SAP-Systeme	6

WORKSHOP

Sicher telefonieren III	8
Compliance im Unternehmen	10

Dezember 2006

1. Jahrgang - Heft 10

Steuerlich relevante E-Mails

Dr. Ivo Geis, Rechtsanwalt für Recht der Informationstechnologie

Geschäftsprozesse werden zunehmend durch E-Mail-Kommunikation abgewickelt. E-Mail-Dokumente sind nach den Grundsätzen des Handelsrechts und Steuerrechts zu archivieren. Rechtliche Aspekte der Archivierung sind die Ordnungsmäßigkeit, die Beweissicherheit und das Filtern unerbetener E-Mail.

Ordnungsmäßige Archivierung und E-Mail-Kommunikation

Die Finanzbehörde ist berechtigt, im Rahmen einer Außenprüfung Einsicht in die gespeicherten Daten zu nehmen und das Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen, § 147 Abs. 6 AO. Um der Finanzbehörde dies zu ermöglichen, muss der Steuerpflichtige die steuerlich relevante E-Mail-Kommunikation elektronisch archivieren und sicherstellen, dass die Dokumente während der Aufbewahrungsfrist maschinell ausgewertet werden können.

Diese gesetzlichen Anforderungen hat das Bundesfinanzministerium (BMF) mit seinem Schreiben vom 16. Juli 2001 „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU; BStBl. 2001 I, S. 415 =

www.bundesfinanzministerium.de) und ergänzenden „Fragen und Antworten zum Datenzugriffsrecht der Finanzverwaltung“ vom 6. März 2003

(www.bundesfinanzministerium.de) konkretisiert. Hiermit werden die seit dem Schreiben des BMF vom 7.11.1995 bestehenden „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“ (GoBS; BStBl. 1995 I S. 738. = www.bundesfinanzministerium.de) ergänzt.

Pflicht zur Archivierung

Originär digitale Unterlagen sind nach Abschnitt III. 1 Satz 2 GDPdU

die im Datenverarbeitungssystem erzeugten Daten und die in das Datenverarbeitungssystem in elektronischer Form eingehenden Daten. Im elektronischen Geschäftsverkehr ist dies E-Mail-Kommunikation einschließlich Anhang. E-Mail-Kommunikation mit steuerlich relevantem Inhalt muss damit während der gesamten gesetzlichen Aufbewahrungsfrist elektronisch archiviert werden („Fragen und Antworten“ III. 8). Eine alleinige Aufzeichnung auf Mikrofilm oder Papier reicht nicht mehr aus. § 147 Abs. 2 AO ist bewusst so gefasst worden, dass keine bestimmten Speichermedien vorgeschrieben sind. Zulässig und damit ordnungsmäßig im Sinne der handelsrechtlichen Aufbewahrungsvorschriften des § 257 Abs. 3 HGB und der steuerlichen Aufbewahrungsvorschrift des § 146 Abs. 5 AO sind alle Speichermedien: die CD-ROM, die nicht wiederbeschreibbare Platte, die wiederbeschreibbare Platte und das Speicherband (Schreiben des BMF vom 7. 11. 1995, I. „Anwendungsbereich“).

Entscheidend für die Ordnungsmäßigkeit sind die hardwaremäßigen, softwaremäßigen und organisatorischen Sicherheitsfunktionen, die für das jeweilige Speichermedium besonders ausgeprägt sein können (Anlage zum BMF-Schreiben vom 7.11.1995 Ziffer 5 „Datensicherheit“).

Maschinelle Auswertbarkeit und Indexierung

Während der Archivierung müssen die Dokumente für die Finanzbehörden maschinell auswertbar sein. In Ziffer I 1. der GDPdU interpretiert das Bundesfinanzministerium das Recht, im Rahmen der Außenprüfung Einsicht in die gespeicherten Daten zu nehmen, als „Nur-Lesezugriff“, der das Lesen, Filtern und Sortieren der Daten umfasst. Im „Nur-Lesezugriff“ kann die Finanzbehörde unmittelbar mit der Hard- und Software des Steuerpflichtigen auf die Daten zugreifen oder mittelbar, indem nach ihren Vorgaben die Daten von dem Steuerpflichtigen maschinell ausgewertet werden. Die maschinelle Auswertbarkeit ist entsprechend der GoBS (Abschnitt VIII. „Wiedergabe der auf Datenträgern geführten Unterlagen“) durch einen unveränderbaren Index sicherzustellen, unter dem das archivierte Dokument bearbeitet und verwaltet werden kann.

Ordnungsmäßige elektronische Archivierung wirkt sich auf die Beweisqualität elektronisch archivierter Dokumente aus, denn die Grundsätze der ordnungsmäßigen Archivierung dienen der Beweissicherheit (Münchener Kommentar HGB/Ballwieser, § 257 Rdnr. 16). Der Beweis mit einem elektronischen Dokument wird geführt, indem dem Gericht das Dokument auf einem Datenträger vorgelegt oder elektronisch übermittelt wird, § 371 Abs. 1, S. 2 ZPO. Als Objekt des Augenscheins unterliegt das elektronische Dokument

der freien Beweiswürdigung des Gerichts (5 Allgemeine Meinung: Geis, Rechtssicherheit des elektronischen Geschäftsverkehrs, Heidelberg 2004, S. 41; Zöller/Greger, Kommentar zur ZPO, 21. Aufl. 1999, § 371 Rdnr. 1.4).

Die freie Beweiswürdigung wird bestimmt durch Hinweise auf die Integrität und Authentizität des Dokuments. Hierfür ist die entsprechend den Grundsätzen der Ordnungsmäßigkeit erreichte Unveränderbarkeit des elektronisch archivierten Dokuments entscheidend. Deshalb gilt die Ordnungsmäßigkeit als Indiz für die Beweissicherheit elektronisch archivierter Dokumente.

Filtern von Werbe-E-Mail

Das deutsche Recht verhindert durch das Opt-In-Prinzip die SPAM-Mail-Flut. Das amerikanische Recht begünstigt sie durch das Opt-Out-Prinzip.

Nach der deutschen Rechtsprechung gilt das Opt-In-Prinzip: Werbung kann dem Empfänger nur nach seiner vorherigen Zustimmung

zugewandt werden, und im Rechtsstreit muss der Absender das Einverständnis des Empfängers beweisen (BGH, Urteil vom 11.3.2004 in CR Computer und Recht 2004, S. 445). Seit dem 8.7.2004 ist diese Rechtslage mit § 7 Abs. 2 Nr. 3 UWG (Gesetz gegen unlauteren Wettbewerb) gesetzlich geregelt. Handels- und steuerrechtlich bestehen gegen das Ausfiltern unerbetener E-Mail keine Bedenken, da diese nicht steuerlich relevant ist.

Die SPAM-Flut wird durch das am 1. Januar 2004 in Kraft getretene amerikanische Gesetz zur E-Mail-Werbung, den CANSPAM Act, begünstigt. Die Gesetzesbezeichnung steht für „Controlling the Assault of Non-Solicited Pornography and Marketing“. Das Gesetz enthält in Sec. 5(a)(4) als wesentlichen Bestandteil ein Opt-out-Prinzip: Danach ist die Zusendung von E-Mail-Werbung nur unzulässig, wenn der Empfänger seinen Widerspruch erklärt hat. Damit er dies tun kann, müssen Werbe-E-Mails Anweisungen enthalten, wie die Opt-out-Erklärung abgegeben werden kann.

Durch die Möglichkeit der erstmaligen unerbetenen Zusendung wird die SPAM-Produktion begünstigt (Ausführlich: Fritzemeyer, K&R Kommunikation und Recht 2005, S. 49 und Wendlandt, MMR Multimedia und Recht 2004, S. 365).

Fazit

Steuerlich relevante E-Mail-Kommunikation muss nach den Grundsätzen der Ordnungsmäßigkeit elektronisch archiviert werden. Die ordnungsmäßige Archivierung hat einen beweisrechtlichen Mehrwert: Sie bedeutet im Rahmen der freien Beweiswürdigung Beweissicherheit. Das Filtern unerbetener Werbe-E-Mail ist berechtigt. Werden an Mitarbeiter adressierte Nachrichten mit privatem Inhalt ausgefiltert, so sollte dies in eine Betriebsvereinbarung aufgenommen werden, um eine Strafbarkeit wegen Verletzung des Fernmeldegeheimnisses zu vermeiden. ◀

IT UND RECHT

Lizenzbedingungen bei Vista

Nicola D. Schmidt

Kurz vor der Markteinführung von Windows Vista hat Microsoft die Lizenzbedingungen bekannt gegeben, schon im Vorfeld gab es von den Anwendern heftige Proteste. Unternehmen müssen jetzt auch mit Volumenlizenzen jede Installation aktivieren. Microsoft will damit die Verbreitung von illegalen Kopien eindämmen.

Bisher mussten Kunden mit Volumenlizenzen Windows-XP-Installationen nicht aktivieren, das ändert sich jetzt bei Vista. Der neue Aktivierungsprozess, Volume Activation 2.0 (VA 2.0), verlangt innerhalb von 30 Tagen eine Aktivierung. Auf diese Weise will Microsoft verhindern, dass Unternehmenslizenzen „entwendet und anderweitig installiert“ werden. Es gibt jetzt zwei Typen

von Volumenlizenzen: Der Multiple Activation Key (MAK) aktiviert PCs über eine direkte Verbindung mit Microsoft-Servern über das Internet oder telefonisch. Mit dem Key Management Service (KMS) können Unternehmen selbst Computer in ihrem Netzwerk aktivieren. Die PCs müssen sich allerdings zur regelmäßigen Prüfung mindestens einmal alle sechs Monate in-

tern mit dem Key Management Service in Verbindung setzen und reaktivieren. Die Lizenzbestimmungen von Windows Vista legen für jede Edition die genauen Nutzungsrechte für die Verwendung innerhalb virtueller Hardwaresysteme fest. Sie berechtigen dazu, die auf dem lizenzierten Gerät installierte Software innerhalb dieses Systems zu verwenden. Es ist aber nicht er-

laubt, eine Lizenz auf einem Gerät zu installieren und eine Kopie davon in einer virtuellen Maschine zu verwenden. Für alle weiteren Installationen – ob virtuell oder auf einem PC – muss eine neue Lizenz gekauft werden.

Eine Ausnahme sind Windows-Lizenzen, die im Rahmen von Software Assurance erworben wurden. Sie gewähren das Recht auf die Windows Vista Enterprise Edition und damit das zusätzliche Nutzungsrecht, bis zu vier Kopien innerhalb virtueller Umgebungen zu verwenden. Alle Windows-Vista-Versionen können ein virtuelles Gast-Betriebssystem enthalten. Die Editionen Business, Enterprise und Ultimate können als solche Gast-Betriebssysteme dienen. Upgrades auf umfangreichere Windows-Vista-Editionen inklusive Lizenznachweis erfolgen durch Windows Anytime Upgrade, das sich derzeit noch in der Entwicklung befindet. Details zu Funktionen oder Fertigstellungstermin standen zu Redaktionsschluss noch nicht fest.

Wollen Privatkunden das Programm auf einem neuen PC installieren oder rüsten sie einen Computer mit neuen Hardware-Bestandteilen auf, brauchen sie eine neue Lizenz. Sie können jedoch auch die vorhandene Lizenz reaktivieren, wenn sie die Software auf dem alten Gerät gelöscht haben und die Lizenz nicht auf mehreren Geräten gleichzeitig genutzt wird. Microsoft wollte ursprünglich untersagen, dass eine Vista-Lizenz mehrmals auf verschiedene Computer transferiert werden kann. Nach massiven Protesten der Benutzer hat das Unternehmen diese Ankündigung nun entschärft: Die Reaktivierung der Lizenz funktioniert so oft wie gewünscht, sie darf nur nicht parallel auf mehreren Computern betrieben werden. Nach einer Änderung an der Hardware-Ausstattung seines Rechners hat der Nutzer drei Tage Zeit, um die Lizenz zu reaktivieren. Dies funktioniert online oder telefonisch. Bei starken Hardware-Änderungen verlangt Microsoft allerdings, der Kunde möge „telefonischen Kontakt mit dem Support-Team“

aufnehmen. Windows Genuine Advantage (WGA) prüft regelmäßig die Lizenz von Windows Vista. Die Software will wissen, ob auf dem PC eine Original-Software-Lizenz von Windows Vista eingesetzt wird. Ist das Ergebnis negativ, verliert der Nutzer Zugriff auf bestimmte Funktionen, darunter gehören Windows Aero, einige Spyware-Filter des Windows Defender und Windows ReadyBoost für die Nutzung von USB-Sticks zum schnelleren Arbeiten. Außerdem öffnen sich regelmäßig Meldungen, die die illegale Kopie monieren.

Die Garantiezeit von Windows Vista hat Microsoft von 90 Tagen auf ein Jahr verlängert und stimmt jetzt mit den meisten anderen Microsoft-Produkten überein. Und jeder Privatanutzer darf jetzt – wenn auch nur eine – Backup-Kopie von Windows Vista anlegen. Entwickler mit MSDN-Abonnement können dagegen so viele Kopien des Programms nutzen, wie sie für ihre Arbeit benötigen. ◀

STUDIEN UND ANALYSEN

Das ewige Post-It

Nicola D. Schmidt

Login als Memory-Spiel: Mit mehr als 15 Passwörtern müssen manche Mitarbeiter hantieren, um auf alle Applikationen ihrer Firma zugreifen zu können. Und nur einer unter 20 Mitarbeitern hat damit keine Probleme. Die Ergebnisse der zweiten Jahresstudie zum Thema Passwörter von RSA zeigen, dass zu viele Passwörter Anwender überfordern und zu risikoträchtigem Verhalten verführen.

Für die meisten Unternehmen sind Passwörter eng mit Compliance, also der Einhaltung von Regularien und Gesetzen, verknüpft. In den USA ist dieses Bewusstsein besonders stark ausgeprägt: 66 Prozent der Befragten gaben an, dass Passwörter „sehr wichtig“ seien, hingegen nur 48 Prozent in Europa. Die Studie befragte 1300 IT-Profis weltweit, die in ihrem Arbeitsalltag mit Passwörtern zu tun haben oder

für die Passwort-Verwaltung ihrer Firma zuständig sind. Daher verwundert es auch nicht, dass nur 4 Prozent weltweit angaben, Passwörter wären „unwichtig“ – sie würden ja ihren eigenen Job untergraben.

Sie sind auch der Meinung, dass Passwörter einen großen Effekt auf die generelle IT-Sicherheit eines Unternehmens haben können –

positiv wie negativ. Auch hier sind die US-amerikanischen IT-Experten am meisten besorgt: 45 Prozent gaben an, Passwörter und IT-Sicherheit hängen sehr eng zusammen, während davon nur ein Drittel der Europäer ausgeht.

16 Passwörter sind zuviel

Bei der Frage, ob eine Passwort schon einmal zu einer Sicherheitslücke geführt hat, gehen die Mei-

nungen auseinander. In den USA war den meisten Befragten nichts dergleichen bekannt. mehr als 80 Prozent können sich an keinen Vorfall erinnern. In Europa und Asien hingegen hat jeder Dritte bereits von solchen Vorkommnissen gehört – entweder sind die Systeme weniger sicher oder die Leute in Europa und Asien besser informiert.

Unstrittig ist auf jeden Fall weltweit, dass die meisten Mitarbeiter mit all ihren Passwörtern überfordert sind. Die meisten müssen mit mehr Kennwörtern jonglieren, als sie sich merken können: Fast jeder fünfte muss 16 oder mehr Passwörter im Kopf haben, 95 Prozent der Befragten bereitet das Probleme. Immerhin ebenfalls jeder fünfte hat es nur mit 1 bis 3 Passwörtern zu tun. 4 bis 5 Passwörter scheinen die Menge zu sein, mit der die meisten noch gut umgehen können. Über vierzig Prozent gaben an, das sei noch leicht zu merken.

Großteil der Nutzer ist durch Passwortflut frustriert

Entsprechend groß ist die Frustration der Anwender. Global gesehen

bezeichnen sich 12 Prozent als „extrem frustriert“ über das Passwort-Management ihres Arbeitgebers: 15 Prozent in den USA, 12 Prozent im asiatisch-pazifischen Raum und neun Prozent in Europa. Hier sind auch die meisten zufriedenen Nutzer zu Hause. 23 Prozent der Befragten aus Europa gaben an, sie seien „überhaupt nicht frustriert“. Weltweit ist der Großteil der Anwender – nämlich 82 Prozent – beim Umgang mit Passwörtern mehr oder weniger unzufrieden.

Trotz aller Aufklärung haftet noch immer der Post-It mit dem Systempasswort an so manchem Monitor: 40 Prozent der Befragten hatten solche Haftnotizen schon bei ihren Mitarbeitern gesehen. 66 Prozent wissen, dass Mitarbeiter Passwörter auf Papier notieren, 59 Prozent haben schon Tabellen auf dem Computer mit Login-Passwort-Kombinationen entdeckt und die Hälfte weiß, dass ihre Mitarbeiter Passwörter im Handheld speichern. Damit bekommt auch der häufige Verlust solcher Geräte eine weitere pikante Note – wer es schafft, an die Daten auf dem PDA zu gelan-

gen, hat meist auch Zugang zu den Firmensystemen.

Wie sichere Passwörter aussehen, das hat sich weltweit mittlerweile herumgesprochen: 70 Prozent der Befragten gaben an, dass in ihrem Unternehmen Passwörter acht bis 14 Zeichen haben und aus Buchstaben, Nummern und Sonderzeichen bestehen müssen. Allerdings hinkt Europa hinterher, hier geben 21 Prozent an, dass es keine Richtlinie gibt, wie Passwörter auszusehen haben.

Die Endnutzer träumen von Master-Passwörtern, die ihr Leben vereinfachen, dem so genannten Single-Sign-On: die meisten glauben, so etwas wäre „hilfreich“. Mehr als die Hälfte war enthusiastischer und nannte es „extrem hilfreich“, während nur sechs Prozent glauben, dass ihnen das überhaupt nichts bringen würde. Allerdings sind sich alle bewusst, dass solche Masterpasswörter dann wieder mit einem speziellen Konzept abgesichert werden müssten. ◀

PRAXIS UND ANWENDUNGEN

Gefälschte Computerprodukte

Matthias Wiemers, Pressesprecher, Borgmeier Public Relations

Auf den Basaren vieler Urlaubsländer stapeln sich unzählige Designer-Handtaschen oder Armbuhren bestimmter Luxusmarken zu einladend günstigen Preisen. Unrechtmäßig kopierte Produkte erobern nahezu alle Bereiche des täglichen Lebens, seien es Bekleidung, MP3-Player, Sportartikel, Zigaretten, Rasierklingen oder Computerteile.

Allein im Jahr 2005 zog der deutsche Zoll bei 7.216 Beschlagnahmefällen an der Grenze rund 500.000 nachgemachte Druckerpatronen für Hewlett-Packard-Geräte aus dem Verkehr. Über 440.000 gefälschte Datenträger des Unternehmens Philips Electronics fanden die Experten ebenfalls. Um Kunden von der angeblichen Echtheit ihrer

Fabrikate zu überzeugen, gehen raffinierte Preller jeden Weg. Firmenlogos, Verpackungen und Funktion sind auf den ersten Blick authentisch, erst bei genauerem Hinsehen ergeben sich häufig erste Abweichungen. Weitere Unterschiede sind zudem bei der Langlebigkeit spürbar. Max Kühne, Managing Director der Tecowin GmbH,

kennt diese Probleme aus erster Hand. Als Händler für Computernetzwerktechnik stieß er bereits auf zahlreiche imitierte Geräte, die als defekt reklamiert wurden. Laut Kühne gestaltet sich die Unterscheidung von Original und Fälschung als zunehmend problematisch. Sogar die Hersteller sind häufig zu umfangreichen Tests gezwungen, um zwei-

felsfrei eine unerlaubte Kopie als solche einzustufen. Als Grund nennt Kühne unter anderem die Zulieferbetriebe, die echte Einzelteile oder ganze Baugruppen herstellen und Überproduktionen zu lukrativen Konditionen an die Fälschungsindustrie verkaufen. Doch diese hohe Qualität ist nicht die Regel. Oftmals genügt eine wachsamer Musterung der soeben erstendenden Produkte.

Worauf zu achten ist

Die deutsche Zollverwaltung mit Sitz in München nennt hierzu einige Merkmale, auf die auch Endkunden beim Kauf achten sollten. Zunächst gibt der Preis einen ersten Hinweis: Liegt dieser bei Neuware deutlich unterhalb der Herstellerempfehlung, ist Vorsicht geboten. Solche Angebote bei Online-Auktionsbörsen deuten nicht selten auf Piraterie, Diebesgut oder Grauiimporte. In jedem Fall entstehen dem Käufer Nachteile, etwa bei Garantieansprüchen. Besteht die Möglichkeit, Liefer- oder Zollpapiere einzusehen, erschließen sich auch hier wichtige Erkennungszeichen. Weichen essenzielle Angaben wie Zollverfahren, Namen oder Anschriften vom

bekanntem Muster ab, sollte dies Anlass zur näheren Prüfung sein. Auch die Verpackung der Ware ist ein Sicherheitsmerkmal. Spezielle Umkartons, besondere Formen, Farbgebungen, Druckqualität, Sicherheitsmerkmale, Hologrammaufkleber oder Aufdrucke wie die Artikelbezeichnung spielen bei der Echtheitsverifizierung eine große Rolle. Zusätzlich liefert die Ausstattung Anhaltspunkte: Das Fehlen obligatorischer Dreingaben oder eine minderwertige Qualität von Beipackzetteln, Garantiezertifikaten, Sicherheitsetiketten, Kabeln, CD-ROMs oder Gebrauchsanleitungen kann das auf einen Betrug hindeuten. Schon bei geringen Verdachtsmomenten hilft die Kontaktaufnahme mit dem Händler oder Hersteller bei der Klärung des Sachverhaltes.

Juristische Konsequenzen

Neben der zu erwartenden Minderqualität stehen darüber hinaus juristische Konsequenzen für Händler und Hersteller im Raum. Nachahmung von Design und Technologien oder die unerlaubte Nutzung bekannter Produktnamen gilt als Zu-

widerhandlung gegen Patent-, Gebrauchsmuster-, Geschmacksmuster- oder Namensrechte. Häufig kopierte Erzeugnisse wie Musikstücke, Bücher, Hörbücher oder Filme stehen unter dem Schutz des geistigen Urheberrechts. Bei Verstößen nennt der auf Marken- und Urheberrecht spezialisierte Hamburger Rechtsanwalt Nikolai Klute strafrechtliche Maßnahmen wie hohe Geld- oder Freiheitsstrafen von bis zu fünf Jahren. Zivilrechtliche Schritte können nicht minder finanziell belastende Beschlagnahmungen, Unterlassungs- und Schadensersatzansprüche sein. Gesetze wie das Urheberrecht (§§106, 107 und 108 UrhG) sowie das Markengesetz (§ 143 MarkenG) geben entsprechende Anhaltspunkte. Für Endkunden stehen in der Regel kaum rechtliche Konsequenzen zu befürchten. Wer jedoch nachgemachte Ware wieder veräußern möchte, tritt in den Kreis des Handels, und es gelten wieder die genannten Strafen. Daher bergen illegal erstellte Artikel stets unkalkulierbare Risiken. ◀

PRAXIS UND ANWENDUNGEN

Roadmap-sichere SAP-Systeme

Jörg Altmeier, Managing Director, wikima4 AG

Die Anforderungen an die Sicherheit von SAP-Systemen steigen mit der Komplexität der eingesetzten Funktionalitäten. Eine Studie zum Status quo ergibt eine Liste der wichtigsten Verbesserungen und zeigt überraschende Ergebnisse bei Selbsteinschätzung und Benchmarking. Eine Roadmap gibt Hilfestellung bei der Umsetzung der wichtigsten Schritte und stellt Kosten-Nutzen-Betrachtungen in den Vordergrund.

Bei den meisten Unternehmen war in der Vergangenheit SAP-Sicherheit gleich bedeutend mit Verfügbarkeit des Gesamtsystems. Entsprechend konzentrierte sich die Aufmerksamkeit auf den Schutz des Produktivsystems und Berechtigungskonzepte, das Netzwerk sowie Entwicklungs- und Testqualität

stand im Vordergrund. Dadurch, dass mehr und mehr sensible, kritische und wertvolle Daten in den SAP-Systemen bearbeitet und gespeichert werden, kommt seit einigen Jahren verstärkt die Notwendigkeit auf, diese Daten vor Missbrauch wie Datenschutz, Spionage oder Diskreditierung zu schützen

und die Auditierbarkeit der Systeme zu gewährleisten. Aufgrund des zunehmenden Gewichts der verschiedenen Regulatorien, der Sarbanes Oxley Act, seien als prägnantes Beispiel genannt, reagieren Unternehmen mit der Etablierung von IT-Governance-Maßnahmen im Sicherheitsbereich. Sie etablieren

nachhaltig einen Sicherheitslevel, der in der Unternehmenskultur verankert ist. Dadurch wollen sie zukünftig in der Lage sein, eine gelassene und pro-aktive Haltung gegenüber immer neuen Regulatorien, Gesetzesnormen oder Bedrohungsszenarien einzunehmen.

Die SAP AG setzt neben einer verstärkten Software-Qualitätssicherung vor allem auf Maßnahmen, die einen direkten Nutzen für die Kunden bringen sollen. Die bereits seit längerem existierenden Security-Leitfäden (unter <http://help.sap.com/>) wurden vollständig überarbeitet und um wichtige Aspekte erweitert. Die Präsenz von sicherheitsrelevanten Themen auf dem Service Marketplace wurde erhöht und soll mit der Etablierung des monatlich erscheinenden Security Newsletters verstärkt werden.

Status quo und Verbesserungsbereiche

Herauszufinden, wie es tatsächlich um die Sicherheit von SAP-Systemen bestimmt ist, war das Ziel einer vom Autor initiierten und durchgeführten Studie. Etwa 140 Interviewpartner aus 40 Anwenderunternehmen verschiedener Branchen nutzten die Gelegenheit zu einer Selbsteinschätzung des Security-Niveaus ihrer SAP-Installationen. Die Gesprächspartner sind für die Sicherheit von über 50.000 Benutzern zuständig, die SAP produktiv zur Abwicklung ihrer Kerngeschäftsprozesse einsetzen. Analysiert man die Aussagen, so stehen nicht etwa technische Anforderungen im Vordergrund. Verbesserungswünsche kamen fast ohne Ausnahme aus den organisatorischen Bereichen. An erster Stelle wurde der Informationsaustausch zu sicherheitsrelevanten Themen zwischen Hersteller und Sicherheitsverantwortlichen genannt, dicht gefolgt vom ungenügenden Einsatz von Monitoring-Tools und dadurch zu spätes Erkennen von Security

Incidents. Als Drittes beklagten die Firmen zu zahlreiche Authentifizierungs-Mechanismen, Passwörter können deswegen nicht im Kopf behalten und müssen notiert werden, was dem Sicherheitsgedanken zuwider läuft. Eine Studie von RSA-Security in dieser Ausgabe nennt Passwörter ebenfalls als maßgeblichen Faktor für die Gesamtsicherheit im Unternehmen.

Defizite sahen die Gesprächspartner auch beim zu sorglosen Umgang mit sensitiven Daten beim Export wie auch beim Drucken, dazu kommt eine zu geringe Fokussierung auf Geschäftsprozesse und eine fehlende finanzielle Schadensabschätzung. Probleme im Praxisbetrieb sehen die Befragten oft bei produktiven SAP-Systemen, die nur rudimentär gegen böswillige oder ungewollte Veränderungen geschützt sind. Wie in vielen anderen Bereichen auch, bemängelten die Sicherheits-Profis auch bei SAP-Security die Qualität der Dokumentation. Dass die Client-Server-Kommunikation unverschlüsselt erfolgt, trägt auch nicht zur Sicherheit bei, ebenso das Fehlen oder zu seltene Durchführen von Sicherheitsüberprüfungen. Beim letzten Faktor auf der Liste wird eine bereichs- und unternehmensübergreifende Klage geführt: zu wenig Ressourcen, Kompetenzen und Know-how bei den SAP-Sicherheitsbeauftragten.

Roadmap zur Umsetzung

Betrachtet man die für Sicherheit relevanten Komponenten losgelöst vom konkreten Umfeld, läuft man leicht Gefahr, deren Einfluss als wenig kritisch einzustufen. Häufig ergeben sich im Falle des vorsätzlichen oder fahrlässigen Störfalls durch das Zusammenspiel der einzelnen Bereiche fatale Auswirkungen. Auf diese Situation sind die wenigsten untersuchten Unternehmen ausreichend vorbereitet. Eine 10-Punkte-Roadmap stellt unter

dem Gesichtspunkt Kosten-Nutzen-Optimierung die wesentlichen Maßnahmen zusammen. So sind Maßnahmen mit hoher Wirkung nicht unbedingt auch mit hohen Kosten verbunden. Das fängt schon bei der Dokumentation an. So dürfte eine Prozess-Landkarte mit der Beschreibung der beteiligten Organisations- und Systemeinheiten wertvolle Unterstützung leisten. Auch eine Erweiterung der Sicherheitsorganisation um SAP-spezifische Aufgabenstellungen hilft. Sie stellt sicher, dass die meist stark divergierenden Sprachen und Kulturen bei SAP und Sicherheit einen gemeinsamen Ankerpunkt haben. SAP-Administratoren sollten darüber hinaus darauf achten, dass die Unternehmensvorgaben detailliert auf SAP-Besonderheiten eingehen. So ist sichergestellt, dass eher allgemein gehaltene Vorgaben in eine Sprache übersetzt werden, die von den für die Umsetzung verantwortlichen Personen auch wirklich verstanden wird. Insbesondere in Fällen, in denen spezifische IT-Aufgaben in abgegrenzten Unternehmenseinheiten oder gar durch einen Outsourcing-Partner bearbeitet werden, ist es zwingend erforderlich, dass jeder am Prozess Beteiligte weiß, was zu tun ist. Das setzt eine klare Aufgabenteilung bei der Kontinuitätsplanung voraus.

Notwendig sind aber auch technische Maßnahmen. So sollten alle empfohlenen Mittel zur Sicherung der Netzwerkkommunikation umgesetzt werden. Prägnantes Beispiel ist die Verschlüsselung der Kommunikation zwischen Server und Client, die bei SAP per Default ungeschützt erfolgt. Datenbanken müssen ebenso, egal ob Bestandteil des SAP-Systems oder externe Systeme durch sparsam vergebene Administrationsrechte vor unbefugten Zugriffen bewahrt werden. Dabei hilft auch die Verteilung der Rechte und Rollen auf unterschiedliche Personen. Die Umsetzung der

von Regulatoren geforderten Gewaltentrennung sollte auf das Organisationsbild abgestimmt sein, damit alle Rollen durch genau definierte Mitarbeiter oder Gruppen ausgeübt werden. Das gilt insbesondere bei der Realisierung des 4-Augen-Prinzips für die technischen Funktionalitäten. Entwickler sollten auf produktiven Systemen keine Entwicklungsrechte erhalten, Supporter nur die Rechte, die sie zur Analyse von Fehlern benötigen. Noch strenger sind die Rechte beim Produktionssystem zu handhaben. Weitreichende Zugriffsrechte dürfen nur maximal zwei inaktive Notfalluser haben, deren Konten man in den Fällen einsetzt, in denen ein Eingriff in produktive Systeme unumgänglich ist.

Zu guter Letzt darf ein unternehmensspezifisches Monitoring-Konzept nicht vernachlässigt werden. Schließlich erlauben die in die SAP-Standardsoftware integrierten Prüfwerkzeuge, die Erkennung möglicher Sicherheitsvorfälle oder -lücken.

Kosten-Nutzen-Betrachtungen

Mit der Umsetzung von Verbesserungsmaßnahmen werden nicht nur Sicherheitslücken geschlossen. Die Etablierung eines adäquaten Security Levels der eingesetzten SAP-Systeme schafft messbaren geschäftlichen Nutzen. Als Beispiel für einen positiven Effekt gilt die verringerte Wahrscheinlichkeit des Eintretens eines Schadensereignisses durch adäquate Rechte-Vergabe. Dabei spielt es keine Rolle, ob es sich um externe Angreifer oder um Fahrlässigkeiten von Mitarbeitern handelt. Durch das konsequent am Standard ausgerichtete SAP-System wird die Verwaltung vereinfacht und kostengünstiger. Zudem verringert sich die Abhängigkeit von externem Know-how. Zahlreiche Unternehmen haben durch die Beschäftigung mit sicheren Prozessen und Systemen Kosteneinsparungen erreicht, sei es durch die verbesserte Prozessabwicklung, eine effizientere Wartung oder der quasi nebenbei erreichten Erfüllung von Anforderungen seitens internationaler Regulatoren wie beispielsweise Datenschutzgesetze oder dem Sarbanes Oxley Act.

Roadmap

1. Dokumentation, welche Prozesse abgedeckt werden und welche Mitarbeitenden damit arbeiten.
2. Erweiterung der Sicherheitsorganisation um SAP spezifische Aufgabenstellungen.
3. Detaillierung der Unternehmensvorgaben auf SAP-Besonderheiten.
4. Klare Aufgabenteilung bei der Kontinuitätsplanung.
5. Umsetzung der empfohlenen Maßnahmen zur Netzwerkkommunikation.
6. Schutz von Datenbank und Betriebssystem gegen unerlaubten Zugriff.
7. Eindeutige Zuordnung von Tätigkeiten auf Betriebs-Mitarbeitende.
8. Realisierung des 4-Augen-Prinzips auch für die technischen Funktionalitäten.
9. Reduktion der Rechte zur Veränderung des Produktsystems auf maximal zwei inaktive Notfalluser.
10. Aufbau eines unternehmensspezifischen Monitoring-Konzepts

WORKSHOP

Sicher telefonieren III

Nicola D. Schmidt, bitsundbites.de

Der letzte Teil unserer Serie zum neuen Baustein über VoIP „B 4.7 VoIP“ gibt einen Überblick, worauf bei Umsetzung, Betrieb und Aussonderung von VoIP-Anlagen zu achten ist. Wer nicht plötzlich ohne Kontakt zur Außenwelt dastehen möchte, sollte sich insbesondere um die Notfallvorsorge kümmern.

Wie sorgfältig der Einsatz von VoIP auch geplant wurde, erst im Betrieb zeigt sich, ob die Maßnahmen ausreichend waren. Wichtig ist vor allem, dass diejenigen, die letztlich für den laufenden Betrieb verantwortlich sind, ausreichend geschult wurden, um Protokolle und Funktionen

zu verstehen sowie die Sicherheitsmerkmale optimal zu nutzen. Auch rechtliche Aspekte und Angriffsszenarien sollten in einer solchen Schulung behandelt werden.

Um VoIP zu nutzen, ist es in einigen Unternehmen sinnvoll, die Daten-

und Sprachnetze zu trennen, wenn sie unterschiedlichen Schutzbedarf haben. Damit lässt sich auch die Skalierbarkeit erhöhen oder die Dienstqualität verbessern, wie Autor Holger Schildt in Maßnahme M 2.376 erklärt. Dies kann durch logische oder physikalische Segmentie-

rung erfolgen, allerdings ist diese Segmentierung nicht immer unproblematisch. In erster Linie entsteht mehr Aufwand, da die VoIP-Komponenten auf Benutzerverzeichnisse zugreifen oder DNS-Namensauflösung brauchen und diese Daten in den meisten Fällen im Datennetz vorliegen. Bei einer strikten Trennung müssten sie also doppelt vorgehalten werden. Auch Software-Aktualisierungen können wegen der Segmentierung nicht einfach über das Datennetz auf die VoIP-Geräte gespielt werden. Für diesen Fall und für die Remote-Konfiguration wäre ein separates IT-System zur Konfiguration notwendig. Schildt empfiehlt, die Probleme durch entsprechende Gateways zwischen Daten- und Sprachnetz zu lösen: *„Für viele Dienste könnte ein Proxy-Server im Sprachnetz betrieben werden, von dem die Anfragen aus dem Sprachnetz in das Datennetz weitergeleitet werden.“*

Günstig erreichbar sein oder nicht?

Wer nicht nur über VoIP aus seinem internen Netz hinaustelefonieren, sondern auch kostengünstig für seine Anrufer erreichbar sein möchte, geht ein Sicherheitsrisiko ein (M 4.289). Wenn ein Angreifer eine Verbindung zu einer internen IP-Adresse in das Unternehmensnetz aufbauen kann, eröffnen sich viele Einbruchsmöglichkeiten. Außerdem hat die Spam-Plage längst auch die Internet-Telefonie erreicht – wer von außen erreichbar ist, könnte bald mit SPIT (Spam over IP-Telefonie) zu kämpfen haben. Wer seine Gesprächspartner jedoch zwingt, über das leitungsvermittelte Telefonnetz anzurufen, bürdet ihnen auch die erhöhten Kosten dafür auf. Dennoch mahnt Schildt: *„Da diesem Nachteil jedoch viele Vorteile, besonders bei sicherheitskritischen Anwendungsfällen, gegenüberstehen, sollte die Erreichbarkeit über VoIP von außen kritisch betrachtet werden.“*

Wer trotz allem von außen für VoIP-Anrufe erreichbar sein möchte, der sollte seinen Datenverkehr über einen zentralen Gateway leiten, Schildt nennt ihn „Konzentrator“, der wie ein Proxy-Server Verbindungsanfragen annimmt und nach einer Prüfung weiterleitet. Der Konzentrator dient als Tor zum Internet: Sowohl alle Sprach- als auch alle Signalisierungsinformationen sollten über diesen Server laufen, kein einziges VoIP-Paket darf an ihm vorbeigehen. Um möglichst alle VoIP-Anrufe annehmen zu können, sollte der Server so viele Signalisierungsprotokolle wie möglich unterstützen, damit nicht ein Anrufer wegen mangelnder Kompatibilität abgewiesen wird. Gleichzeitig muss der Zugang von außen beschränkt bleiben, der Konzentrator sollte genau festlegen, welche Funktionen außer der Sprachanrufe externen Nutzern zur Verfügung stehen. Wer den Server mit manipulierten, also nicht protokollkonformen Paketen bombardiert, sollte sofort abgewiesen werden.

Um von innen nach außen zu telefonieren, muss sich jeder Mitarbeiter am Konzentrator authentisieren, nur so lässt sich einem Missbrauch der Telefonanlage entgegenwirken. Auch wenn es mehr Arbeit bedeutet, der Konzentrator ist die Tür ins Internet und daher steht hier Sicherheit an allererster Stelle. Damit diese Tür nicht zum Nadelöhr wird, müssen die Ressourcen des Systems ausreichend ausgelegt sein. Wer ständig erreichbar sein muss, sollte über ein redundantes System nachdenken, hier unterscheidet sich VoIP nicht von anderen Netzkomponenten.

Schildt nennt als Alternative für proprietäre Systeme die Open-Source-Telefonanlage Asterisk. Die Software kann auch als Appliance betrieben werden und erfüllt viele der genannten Anforderungen.

„Können Sie mich hören?“

Die meisten Anwender von VoIP sind erst einmal skeptisch, was die neue Technik in der Praxis wirklich leisten kann. Ihre Bedenken beziehen sich häufig auf die „Dienstgüte“ – also die Sorge, dass Telefonate plötzlich unter schlechter Qualität oder Knacken, Rauschen oder Unterbrechungen leiden. Maßnahme M 5.136 zeigt, wie sorgfältiges Netzmanagement dem entgegenwirkt, wenn es sich nicht nur auf Sicherheitsaspekte konzentriert, sondern auch um die Verfügbarkeit des Dienstes kümmert. Um Überlastung und schlechte Sprachqualität oder sogar Ausfälle zu verhindern, kann man nach verschiedenen Ansätzen vorgehen, der Baustein nennt: Differentiated Services, Overprovisioning, MPLS, Traffic Shaping und Resource Reservation Protocol und beschreibt die Vor- und Nachteile der einzelnen Techniken. Natürlich gelten auch hinsichtlich der Sicherheit des Gateways, der den Übergang zwischen öffentlichem und privatem Netz verantwortet, besondere Voraussetzungen. Die Maßnahme M 4.290 beschreibt detailliert, wie ein Sicherheitsgateway für VoIP ausgesucht und betrieben werden muss. Denn es ist ja nicht nur für die Sicherheit, sondern auch für die Qualität des Dienstes verantwortlich. Eine Kriterienliste hilft dabei, das richtige Gateway auszusuchen.

Für den Betrieb von VoIP ist die sichere Administration unerlässlich (M 4.287 und M 4.288), aber nicht nur die zuständigen IT-Mitarbeiter, auch die Nutzer müssen über die grundlegenden Gefahren der neuen Technik informiert sein. Auch wenn eine „Benutzer-Schulung über die Benutzung eines Telefons oft nicht wirtschaftlich und sinnvoll“ ist, wie Schildt anmerkt, so sollten sie doch alle Warnanzeigen und „*abnormes Verhalten*“ der TK-Anlage erkennen und melden. Hierzu sind regelmä-

ßige Auffrischungen, Merkblätter oder kurze Informationen die richtigen Maßnahmen.

Für den Notfall vorsorgen

Hat die VoIP-Anlage ausgedient, gilt dasselbe wie für eine Festplatte: Alle relevanten Informationen müssen gelöscht werden. VoIP-Hardware kann Anruflisten, Benutzernamen und Passwörter, aber auch Ansagen auf Anrufbeantwortern oder Zertifikate und Schlüssel enthalten, in manchen Fällen sogar die Aufzeichnungen von ganzen Telefongesprächen. Daher ist hier besonders darauf zu achten, dass nicht nur bei Weitergabe, sondern auch bei Verschrottung alle Daten so gelöscht werden, dass sie nicht wiederherstellbar sind. Dazu gehört auch, die Beschriftung von Schnellwahl-tasten oder Adresslisten am Telefon zu entfernen.

Für die meisten Unternehmen ist der Ausfall des Mailservers eine

teure und ärgerliche Angelegenheit – der Ausfall der Telefonanlage jedoch undenkbar. Bei VoIP sollte noch stärker als beim analogen Telefonnetz darauf geachtet werden, dass ein Notfallvorsorgekonzept diesen Fall abfedert. Selbst wenn es nicht am VoIP-System liegt, kann es viele „single points of failure“ im Netz geben, die die Firma plötzlich von der Außenwelt abschotten. Schildt mahnt in M 6.100 daher, dass „bei einem Ausfall von VoIP eine Telekommunikation weiter möglich sein“ muss. Zumindest der Anruf bei Polizei oder Feuerwehr sowie dem zuständigen Support-Dienstleister muss gewährleistet sein, damit der Fehler behoben werden kann. Ein Systemausfall kann zusätzlich zu Datenverlusten führen. Sollen die Mitarbeiter nicht alle ihre Telefonbücher neu eingeben müssen, empfiehlt der Autor, in diesem Konzept auch Endgeräte zu berücksichtigen. Möglich wäre beispielsweise, die internen Telefon-

nummern von einem Verzeichnisdienst, wie LDAP, bereitzustellen, damit wären sie dann auf diesem Server gesichert. Andere Lösungen verwalten die Telefonnummern auf dem VoIP-Server, „je nach unterstütztem Verfahren könnten die Backupdateien über (S)FTP, (S)HTTP oder einem anderen Dienst bezogen werden. Basiert der VoIP-Server auf einem IT-System, können Sie natürlich jeden beliebigen Backupdienst installieren“, so Schildt. Bei Hardphones ist diese Sicherung produktabhängig. Bei Softphones kann eine Datensicherung von den Backup-Routinen des Clients selbst erledigt werden. Und auch der kleinere Wartungsfall sollte vorgeplant sein: Arbeitet ein Mitarbeiter mit einem Softphone auf seinem Computer, so sollte es eine Ausweichmöglichkeit geben, wenn der Rechner abstürzt oder repariert werden muss.

WORKSHOP

Compliance im Unternehmen

Edgar Scholl, IT-Dozent, und Dagmar Schulz, Marketing und Comm. Manager, Borderware

Compliance ist zur Zeit in aller Munde. Strenge Richtlinien, neue Regeln, die Einhaltung derselben – man könnte meinen, Compliance wäre der eigentliche Unternehmenszweck. Doch mit der Definition tun sich Firmen und Gremien schwer.

Bei der Frage, was Compliance ist, kommen Lexika und Online-Quellen zu recht unterschiedlichen Ergebnissen. Langenscheidt hüllt sich in Schweigen, bei Google findet sich in der Top-Ten-Liste der Titel des „CCO“ – des Chief Compliance Officer“, wie es ihn tatsächlich bereits in Unternehmen unterschiedlicher Größenordnungen gibt. Und Wiki weiß immerhin, dass es sich beim Thema Compliance um etwas handelt, das mit Gesetzen, Richtlinien und Maßnahmen zu tun hat, die nicht nur Unternehmen betreffen, sondern auch jeden einzelnen

Mitarbeiter und die externen Partner, mit denen ein Unternehmen arbeitet.

Juristische Aspekte

Wer sich als Unternehmer mit dem Thema auseinandersetzt, wird zunächst damit konfrontiert, dass man selbst als Firma und als Geschäftsführer die verantwortliche Instanz zum Thema Compliance ist. Das Einhalten von gesetzlichen Vorschriften und Regularien mittels IT betrifft dabei sowohl den Zugriff und dessen Kontrolle auf Daten als auch die physische Hard- und Software-

Ausstattung als Grundlage. Hier konkurrieren Datenschutz, Verordnungen von Aufsichtsbehörden, DIN- oder ISO-Standards und nicht zuletzt die Dokumentationspflichten für mögliche Audits um die Aufmerksamkeit des Geschäftsführers, IT-Leiters oder/und Sicherheitsbeauftragten. Wieder stellt sich die Frage, was aus der Sicht des jeweiligen Ansprechpartners Compliance ist, vor allem dann, wenn im Falle eines Falles tatsächlich der Verschuldensmaßstab angelegt werden muss. Dabei sind zusätzliche Auflagen der jeweiligen Branchen oder

die Auswirkungen auf Tochterneiderrlassungen von US-amerikanischen Unternehmen und deren Partner und Dienstleister noch gar nicht berücksichtigt.

Weder ist ein Geschäftsführer geschützt, weil er sich beispielsweise als Vertreter eines nicht börsennotierten Unternehmens nicht in der Pflicht sieht oder fälschlich annimmt, dass eine Managerhaftpflichtversicherung ihn im Falle „compliant oder nicht“ schützt. Das ist nicht der Fall. Schlimmer noch: aus der persönlichen Haftung können zusätzlich noch strafrechtliche Konsequenzen resultieren.

Neben den grundsätzlichen juristischen Kontrollmöglichkeiten gelten für jede Leistungs- und Verhaltenskontrolle eines Mitarbeiters eine Vielzahl von juristischen und betriebsverfassungsrechtlichen Einzelheiten wie die Mitbestimmungsrechte des Betriebsrates. Natürlich sind auch die Persönlichkeitsrechte der Mitarbeiter zu beachten: er muss über die Art der Datengewinnung informiert sein, die Datennutzung darf nur zu diesen Zweck betrieben werden, der Grundsatz der Verhältnismäßigkeit muss gewahrt bleiben und nicht zuletzt gelten die Richtlinien für eine Archivierung von Daten. Hinzu kommt das Fernmeldegeheimnis, das in den Bereich des Telekommunikationsgesetzes fällt, denn hier geht es ja nicht nur um einen zu kontrollierenden Mitarbeiter, sondern auch um den jeweiligen Kommunikationspartner, also einen Dritten, dessen Daten ebenfalls geschützt werden müssen. Die IT ist so auszurichten, dass sie den entsprechenden Richtlinien genügt und dass dies auch nachweislich dokumentiert ist. Compliance betrifft also nicht nur die „klassischen“ IT-Schutz- und Kontrollmaßnahmen, sondern immer auch eine Vielzahl anderer Gesetze, Vorschriften und Regularien, die auf die eine oder andere Weise mit den „klassischen“

Compliance-Regelungen verbunden sind.

Compliance kann viele Formen haben

Über die amerikanische Muttergesellschaft eines großen, deutschlandweit agierenden Unternehmens unterliegen Unternehmen und beauftragte Dienstleister wie das ausgelagerte Rechnungswesen oder die Buchhaltung dem Sarbanes Oxley Act (SOX). Dabei gibt es grundsätzlich zwei Möglichkeiten. Erstens: das Unternehmen setzt nur Dienstleister ein, die sich nach den entsprechenden Richtlinien haben zertifizieren lassen. Zweitens: setzt man einen nicht zertifizierten Dienstleister ein, muss dieser wiederum Kontrollen durch einen Auditor des beauftragten Unternehmens zulassen. Für Service-Provider umfassen die entsprechenden SOX-Vorgaben zum Beispiel Risiko-Management und Anforderungen an das interne Controlling. Zusätzlich unterliegt der Provider dem Corporate Governance Codex (dazu gehören Ablaufdokumentationen, EDV-Sicherheit, Zugriffsschutz, Serverbetrieb und Datensicherheit). Die Kontrollaufgaben selbst werden dabei in aller Regel aus der Unternehmens-IT herausgenommen, um die Prozesse entsprechend den geschäftskritischen Abläufen zu definieren, zu dokumentieren und eine Art Risiko-Mapping zu entwerfen.

Beispiel 2: Ein kleines, börsennotiertes Unternehmen mit zirka 200 Mitarbeitern unterliegt den Erfordernissen des KontraG, Basel II und anderen. Hier gibt es beispielsweise ein Zertifikat der TÜV Industrie Service GmbH, bei dem die Sicherheitsanforderungen denen der genannten Regularien entsprechen und in einer ISO-Norm abgebildet werden. Der Abdeckungsbereich des Zertifikats ist mannigfaltig: es geht um die Sicherheitspolitik und die Organisation der Sicherheit im

Unternehmen, reicht über den Bereich personelle und physische Sicherheit der Firma bis hin zum Management der Kommunikation des Betriebes und der Systementwicklung und -wartung. Der einmal zertifizierte Status quo muss natürlich beständig überwacht, die Einhaltung der Verpflichtungen kontrolliert werden. Dabei ist ein wesentliches Element das Risiko-Management. Durchläuft ein Unternehmen diesen umfangreichen Zertifizierungsprozess, besteht das Ziel darin, die Informationssicherheit mit den definierten Verfahren und Prozessen dokumentieren zu können. Erst in zweiter Linie geht es darum, bei Kunden und potentiellen Kunden Vertrauen aufzubauen und aus der Warte eines unabhängigen Dritten dokumentieren zu lassen. Interne Audits, in denen die Sicherheitsmaßnahmen überprüft werden, sind erste Schritte und können mit Hilfe von Fragebögen, Penetrationstests und anderen Maßnahmen zur Systemüberprüfung durchgeführt werden.

Compliance aus Sicht der Lösungsanbieter

Betrachtet man Compliance aus der Perspektive der Hersteller, die sich des Themas annehmen, findet man eine Vielzahl von Ansätzen. Jeder Anbieter nähert sich von einem anderen Standpunkt aus der Thematik und hat unterschiedliche Lösungsvorschläge für Teilbereiche oder auch umfassende Komplettlösungen parat. Ein Thema taucht bei den meisten Herstellern als zentraler Dreh- und Angelpunkt auf. Das ist die Realität der Wirtschaftskriminalität, die sich auch hierzulande vielfältig dokumentieren lässt. Erschreckend: Die Bereitschaft von Mitarbeitern, Daten weiterzugeben, erstaunlich hoch, der dafür bezahlte Betrag laut Aussagen von so genannten „Schmierern“ erstaunlich niedrig. (Quelle: Sonia Shinde <http://www.tebiko.de/shinde/artikel.p>

hp?nummer=27). Schon für zirka 2.500 Euro waren Mitarbeiter bereit, unternehmenswichtige Daten des Arbeitgebers zu verkaufen. Compliance bedeutet auch, sich davor und vor allem vor den Folgen eines solchen Ausverkaufs zu schützen. Dazu gehört ebenso der Verlust von Laptops, auf denen sich Daten befinden, die unverschlüsselt auf der Festplatte gespeichert wurden.

Jedes Unternehmen verwaltet eine Vielzahl sensibler Daten auf den Rechnern der Mitarbeiter. Die Daten müssen gesichert werden, ganz gleich, welcher Methoden man sich im Einzelnen bedient. Hersteller adressieren die Problematik mit Verschlüsselungslösungen für Festplatten und für jede Art von mobilen Endgeräten wie PDAs oder Smartphones. Wesentlich ist: alle Sicherheitslösungen müssen zusammenpassen, E-Mail-Sicherheit und Sicherheitslösungen für die Netzinfrastruktur müssen mit der Endgerätesicherheit verknüpft sein. Auch Instant Messaging und Voice-over-IP gehören in das Konzept einbezogen.

Compliance betrifft also unternehmenskritische Daten, personenbezogene Daten sowie unternehmerische Verantwortung und Haftung. Es geht weniger darum, Opfer, Täter und Schuldige auszumachen, als Firma, Nutzer und Administrator in die Lage zu versetzen, sich mit allen Geschäftsabläufen rund um das eBusiness im Rahmen der Verordnungen zu bewegen.

Und dann der Mensch ...

„Der wichtigste Faktor in diesem Szenario ist der Mensch selbst – egal in welcher Funktion im Unternehmen. Wenn man sich die Resonanz in unseren Workshops und Seminaren ansieht, zeigt die Realität, dass mehr als 80 Prozent der deutschen Unternehmen dringenden Handlungsbedarf haben“, so Edgar Scholl, Trainer und Dozent

für IT-Sicherheit. Neben den technischen Grundlagen geht es hier um die Prozesse der Bewusstseinsbildung (Awareness) jedes Einzelnen sowie um eine ganzheitliche Sicht auf das Unternehmen, statt auf einzelne Bereiche. Von zentraler Bedeutung ist also der User und sein Verhältnis zu den Daten, mit denen er in einem Unternehmen oder auch einer behördlichen Einrichtung täglich umgeht. Die technische Umsetzung ist machbar, sie erlaubt es richtlinien- und standardkonform Business zu betreiben und entsprechende Policies für ein Unternehmen zu erstellen. Sie müssen dann allerdings umgesetzt und in allen Bereichen gelebt werden. Das reale Anwenderverhalten ist nicht von Haus aus mit dem konform, was in einem Audit festgelegt und nachzulesen ist. Richtlinienkonformität, E-Mail-Sicherheit und Verschlüsselung sowie individuelle Rechtssicherung sind nur einige Stichworte.

Compliance ist ein Thema auf Management- und IT-Ebene, das den strategischen Ansatz betrifft. Für die tägliche Umsetzung sollte man nach individuellen und maßgeschneiderten Lösungen für ein Unternehmen oder eine Organisation suchen. Eine Möglichkeit ist, entsprechende Schulungen und Sicherheitstrainings in einzelnen Abteilungen durchzuführen und jeweils einen Mitarbeiter oder eine Mitarbeiterin zu bestimmen, der/die in Zukunft für die entsprechenden Belange zuständig ist. Hier greift Compliance ganz konkret in die Organisation ein und schafft eine Art „Human Policy“, die erst sicherstellt, dass die technischen Lösungen optimal ein- und umgesetzt werden. Grundsätzlich besteht hier per Definition ein hoher Beratungsbedarf – Unternehmen allein können Compliance kaum umsetzen. ◀

IMPRESSUM

Verlag

Bundesanzeiger Verlagsges.mBH.
Amsterdamer Straße 192, 50735 Köln
www.bundesanzeiger-verlag.de

Redaktion

Bits und Bites
Elmar Török, Fachjournalist
Nicola D. Schmidt, freie Journalistin
Luccastrasse 22, 86956 Schongau
E-Mail: info@bitsundbites.de

Redaktion im Verlag

Anne Bayrli
Tel.: +49-221-9 76 68-181; Fax: -271
E-Mail: zeitschriften@bundesanzeiger.de

Abo-Service

Ulrike Vermeer
Tel.: +49-221-9 76 68-229; Fax: -288
E-Mail: vertrieb@bundesanzeiger.de

Anzeigenverwaltung

Regina Gärtner
Tel.: +49-221-97668-128; Fax: -271
E-Mail: regina.gaertner@bundesanzeiger.de

Manuskripte

Manuskripte sind bei der Schriftleitung per E-Mail einzureichen. Unverlangt eingesandte Beiträge werden bei Nichtannahme nicht zurückgesandt. Beiträge werden nur zur Alleinveröffentlichung angenommen. Mit schriftlicher Annahme der Beiträge erwirbt der Herausgeber vom Verfasser alle Rechte, insbesondere das Recht zur Veröffentlichung und weiteren Vervielfältigung zu gewerblichen Zwecken im Wege des fotomechanischen oder eines anderen Verfahrens.

Bezugspreise/Bestellungen/Kündigung

Der Jahresabopreis beträgt im Inland € 147,66 inkl. USt. (Versandkosten Inland 1,50 €/Ausland 3,- € je Ausgabe). Vorzugspreis für die Bezieher der IT-Grundschutz-Kataloge: € 104,86 inkl. USt. (Versandkosten Inland 1,50 €/Ausland 3,- € je Ausgabe). Ein Einzelheft kostet € 10,70 inkl. USt. (Versandkosten Inland 1,50 €/Ausland 3,- € je Ausgabe). Bestellungen über jede Buchhandlung oder direkt beim Verlag. Kündigungen sind nach Ablauf von 12 Monaten möglich. Sie müssen bis zum 15. des Vormonats beim Verlag eingegangen sein.

Urheber- und Verlagsrechte

Alle in diesem Informationsdienst veröffentlichten Beiträge sind urheberrechtlich geschützt. Jegliche Verwendung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und Einspeicherung in elektronische Systeme.

Haftung/Gewährleistung

Die in diesem Informationsdienst veröffentlichten Beiträge wurden nach bestem Wissen und Gewissen zusammengestellt. Eine Gewähr für die Richtigkeit und Vollständigkeit kann seitens des Verlages und der Redaktion nicht übernommen werden. Verlag und Redaktion haften ebenfalls nicht für etwaige mittelbare und unmittelbare Folgeschäden und Ansprüche Dritter.

Herstellung/Grafik

Gerhard Treinen, Reinald Gerhards

Erscheinungsweise: monatlich