



IT-Grundschutz

Informationsdienst

IT und Recht

Cloud Computing: Klare Sicht in der Wolke

Seite 10



Quelle: iStockphoto

NEWS

Jeder Zweite surft im Job auch privat *Seite 2*

Netzwerk für die Cloud *Seite 2*

Indevis nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert *Seite 2*

Workshops

Cloud Computing und die IT-Security Richtig handeln bei Datenpannen *Seite 7*
Seite 5

Praxis und Anwendungen

Layer-2-Verschlüsselungslösungen statt IPSec-Netzwerk *Seite 14*

Studien und Analysen

Interview: Die Rolle von Normen in der IT-Sicherheit *Seite 3*

IT und Recht

Cloud Computing: Klare Sicht in der Wolke *Seite 10*

Rubriken

Editorial *Seite 2*

Veranstaltungen *Seite 16*

Impressum *Seite 9*



Liebe Leserin, lieber Leser,

Wenn zur Zeit von Wolken die Rede ist, geht es vermutlich nicht um die Wetterlage, sondern den Megatrend Cloud Computing. Ein erklecklicher Prozentsatz der täglichen News-Meldungen trägt das Wörtchen „Cloud“ im Betreff und bei Produktneuvorstellungen sind die Hersteller sichtlich bemüht, die Cloud-Fähigkeit der neuen Schöpfung herauszustellen. Doch bevor sich Firmen mit der Aussicht auf Kosteneinsparungen auf das neue Konzept stürzen, sollten sie genau die rechtlichen, technischen und organisatorischen Voraussetzungen prüfen. Ein Artikel von Fachanwalt Jan Schneider und ein Text von zwei Consultants des Sicherheitsdienstleisters Secaron helfen dabei. Fazit: Cloud Computing ist vor allem dann machbar, wenn es nicht um unternehmenskritische Daten geht oder wenn die Sicherheit der Daten über jeden Zweifel erhaben ist. Doch wenn „über jeden Zweifel erhaben“ möglich wäre, woher kommen dann die diversen CDs mit Steuerländerkonten? Die Banken dachten bestimmt auch, dass sie alles für die Sicherheit getan haben. Cloud Computing ist als Konzept und in der Anwendung verlockend, doch man muss sich darüber im Klaren sein, dass man die Kontrolle über Unternehmensdaten aus der Hand gibt. Nicht in allen Fällen ist dieses Risiko kalkulierbar.

Herzlichst Ihr Elmar Török

Indevis nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert

Die indevis IT Consulting and Solutions GmbH erhielt als erster Managed Security Service Provider vom Bundesamt für Sicherheit in der Informationstechnik das Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz. Zu den zertifizierten Diensten gehören unter anderem der Hotline Support (Helpdesk), Managed AntiSpam Service, Managed Authentication, Managed Firewall/VPN Services, Managed Secure Remote Access und die Serverhousing-Infrastruktur (Rechenzentrum). Im BSI-Verfahren wurden alle für diese MSSP-Dienstleistungen erforderlichen IT-Systeme und Prozesse sowie das Rechenzentrum einschließlich der Netzwerk- und Kommunikationsverbindungen zu den Kunden untersucht. Das Deutsche IT-Sicherheitszertifikat ist bis zum 15. Januar 2013 gültig.

„Die Zertifizierung gibt unseren Kunden ein sicheres Gefühl, weil sie wissen, dass wir uns bei IT-Sicherheitskonzeption und -maßnahmen vollständig an die BSI-Empfehlungen zur Vorgehensweise nach IT-Grundschutz halten“, freut sich indevis-Geschäftsführer Wolfgang Kurz. „Diese sind heute vor allem in der öffentlichen Verwaltung sowie in der Privatwirtschaft zum De-Facto-Standard geworden.“

Netzwerk für die Cloud

Seit kurzem vertritt EuroCloud Deutschland_eco die deutsche Cloud Computing-Wirtschaft auf internationalem Parkett: EuroCloud Deutschland_eco ist deutscher Partner bei EuroCloud, Europas erstem Zusammenschluss für Cloud Services. Seine Ziele und Arbeitsschwerpunkte will der Verband am 2. März in einer Pressekonferenz auf der CeBIT vorstellen. Auf dem dynamischen Markt der Cloud Services ist vieles in Bewegung, und viele Fragen sind offen. Compliance, Standards und Datensicherheit sind neben dem häufig

unklaren Rechtsrahmen nur einige Themen, mit denen sich Anwender und Anbieter beschäftigen müssen. EuroCloud Deutschland_eco will als eigenständige Branchenvereinigung den Dialog von Anwendern und Anbietern fördern, sich für rechtssichere Rahmenbedingungen einsetzen und die Transparenz auf dem Cloud Services-Markt verbessern. Eco und EuroCloud Deutschland_eco finden Sie auf der Webciety am Stand H 02.

Jeder Zweite surft im Job auch privat

Wie der Hightech-Verband BITKOM ermittelt hat, verwendet jeder zweite berufliche Internet-Nutzer (49 Prozent) das Web während der Arbeit für private Zwecke. BITKOM rät Unternehmen, klare Regeln für die private Internet-Nutzung im Job zu formulieren. „Gerade bei sportlichen Großereignissen wollen viele Mitarbeiter die Wettkämpfe auch während der Arbeitszeit mitverfolgen“, sagte BITKOM-Präsident Prof. Dr. August-Wilhelm Scheer. „Arbeitgeber sollten offen mit der privaten Internetnutzung am Arbeitsplatz umgehen. Sie sollten Regeln formulieren, eine geordnete und richtig dosierte Internetnutzung zulassen und gleichzeitig ein exzessives, die Arbeitsleistung beeinträchtigendes Surfen im Web verhindern.“ Die Grenzen zwischen Job und Privatleben sind in der digitalen Ära längst gefallen. Das gilt umgekehrt genauso: Zwei Drittel (65 Prozent) der berufstätigen Anwender nutzen das Netz in der Freizeit auch beruflich. Viele sind nach Büroschluss für Kunden, Kollegen oder Chefs per Internet und Handy erreichbar. Sowohl Firmen als auch Arbeitgeber profitieren also von einer gewissen Flexibilität im Umgang mit dem Web. Ob die private Internetnutzung im Job erlaubt ist, regelt in Deutschland kein spezielles Gesetz.

Die Rolle von Normen in der IT-Sicherheit

Interview Melanie Balkenhol, Defense AG

Elmar Török, bits+bites

Melanie Balkenhol ist Junior Consultant beim Münchner IT-Sicherheitsdienstleister Defense AG. Ihr Spezialgebiet ist die Planung, Implementierung und Pflege von Managementsystemen im Bereich ITIL und ISMS sowie die Zertifizierung nach ISO 20000 und 27001. Wir sprachen mit Frau Balkenhol über die Bedeutung von Normen in der IT-Sicherheit.

IT-Grundschutz: Frau Balkenhol, welche Rolle spielen Vorgaben und Normen wie ISO oder IT-Grundschutz im Unternehmen?

Balkenhol: Ich bin der Meinung, dass Normen, darunter auch ISO und BSI IT-Grundschutz Best-Practice Ansätze sind. Man kann sie in voller Bandbreite umsetzen, muss das aber nicht unbedingt tun.

IT-Grundschutz: Da könnte das BSI anderer Meinung sein.

Balkenhol: Ja und Nein. Ein Stück weit spielen natürlich auch rechtliche Anforderungen eine Rolle. Wer sich laut Gesetz zertifizieren lassen muss, der kommt nicht darum herum. Aber ich lege Firmen wenn möglich immer nahe, solche Vorgaben vor allem als Best-Practice zu nutzen. Prinzipiell kann und sollte jedes Unternehmen so etwas machen. Nur weil ISO eine Norm ist, heißt das nicht, dass es 1:1 für meine Firma umgesetzt werden muss. Und viel wichtiger: Es heißt auch nicht, dass eine 1:1 Umsetzung reicht! Jedes Unternehmen muss selbst definieren wie seine Anforderungen und Ziele aussehen und wie sie gewährleistet werden sollen.

IT-Grundschutz: Kann man pauschal sagen, für wen ISO oder IT-Grundschutz besser geeignet ist?

Balkenhol: Ich könnte das nicht auf Branchen oder einzelne Firmen aufteilen, das kommt ganz auf die individuellen Anforderungen des Unternehmens an. Natürlich gibt es externe Gründe. Wenn Sie Lieferant eines großen Kfz-Herstellers sein wollen, müssen Sie wahrscheinlich ISO zertifiziert sein, selbst wenn es nicht ideal zur realen Anforderung passt.

IT-Grundschutz: Können und sollen Firmen eigene Normen für die IT-Sicherheit definieren?

Balkenhol: Wenn Bedarf besteht, warum nicht? Alles selbst neu zu definieren macht aber auch keinen Sinn, das Rad muss man nicht neu erfinden. Und in kleinen Firmen ist der Aufwand viel zu hoch. Solche Ansätze sehen wir vor allem in Großunternehmen, die besonderen Compliance-Anforderungen entsprechen müssen. Im Pharmabereich zum Beispiel kommen noch erhöhte Compliance Anforderungen, zusätzlich ISO und BSI IT-Grundschutz dazu.

IT-Grundschutz: Wenn man den Aufwand betreiben möchte: Geht es ganz ohne Normen?

Balkenhol: Klare Antwort: Nein!

IT-Grundschutz: Wie schätzen Sie die Lage ein? Welche Normen müssen sein?

Balkenhol: Pflicht ist alles, was die gesetzlichen Vorgaben abdeckt. Das ist der größte und wichtigste Punkt. Was in einer spezifischen Branche notwendig ist und beachtet werden muss ist ein großes Thema, man benötigt sehr umfangreiche und branchenspezifische Kenntnisse, um hier alles richtig zu machen. Etwas genereller betrachtet komme ich gern auf ISO zurück. Der Best-Practice Ansatz ist eine sehr gute Sache um sich abzusichern. Das gilt sowohl für das Management, den IT-Leiter und den IT-Sicherheitsbeauftragten.

Sollte man eine Zertifizierung anpeilen, ist der IT-Grundschutz meiner Ansicht nach sehr starr. Die ISO Norm bietet deutlich mehr Möglichkeiten, sie an die Bedürfnisse des Unternehmens anzupassen.

IT-Grundschutz: Wo behindern Normen mehr als dass sie helfen?

Balkenhol: Der Zustand ist schnell erreicht, wenn man die Sache von hinten anpackt, also Normen implementiert, ohne sie vorher auf die Eignung für Unternehmen zu prüfen. Ich muss unbedingt vorher durchleuchten, was ich für Risiken und Bedürfnisse habe. Dann kann ich an den eigenen Alltag und meine ganz individuellen Anforderungen angelehnt, meine eigenen Vorgaben entwickeln und dazu fertige Normen als Hilfestellung



Melanie Balkenhol, Junior Consultant beim Münchner IT-Sicherheitsdienstleister Defense AG.

nehmen. Der umgekehrte Weg, Unternehmen und Strukturen an die Sicherheitsprozesse anzupassen, ist zum Scheitern verurteilt.

IT-Grundschutz: Wie finde ich die am besten passende Norm für mein Unternehmen?

Balkenhol: Das ist eine Frage, die mir sehr häufig gestellt wird. Es ist in der Tat schwierig, wenn man sich nicht sehr intensiv mit dem Thema befasst hat. Wir nutzen bei der Defense AG ein Basis-Risk Assessment und beleuchten die Risiken bei unseren Kunden von A bis Z. Dann sehen wir, wo Handlungsbedarf besteht und wo gesetzliche Anforderungen betroffen sind.

IT-Grundschutz: Was ist die größte Gefahr beim Einsatz von Normen in Unternehmen?

Balkenhol: Irgendwas als de-facto Standard einführen und dann das Unternehmen an die erforderlichen Prozesse anpassen zu wollen. Das kann man bis zur Zertifizierung und dem Testat hinbekommen, aber danach fällt das Konzept auseinander. Man kann die Vorgaben der IT-Sicherheit im täglichen Arbeitsalltag nicht mit Leben füllen. Die größte Herausforderung ist es, das Sicherheitskonzept lebendig zu gestalten, wenn man von Anfang an mit dem falschen Rahmen arbeitet, funktioniert das nicht. Jeder Mitarbeiter muss sich mit dem Sicher-

heitskonzept identifizieren können und das Gefühl haben, einen Vorteil daraus ziehen zu können.

IT-Grundschutz: Was sind häufige Fehler bei der Implementierung von Normen?

Balkenhol: Oft sehen wir, dass Firmen die Mitarbeiter nicht einbeziehen, dass sie in Teilbereichen anfangen, statt das große Ganze im Auge zu behalten und das Risiken kleingeredet und vertuscht werden.

IT-Grundschutz: Ist es nicht besser zumindest in einem Teilbereich anzufangen, als gar nichts zu tun?

Balkenhol: Doch, natürlich. Aber nur wenn vorher eine Basisfeststellung da ist. Man muss wissen, welche Prozesse, welche Technik, und welche Mitarbeiter von der Sicherheitsmaßnahme betroffen sind, sonst erreicht man nichts.

IT-Grundschutz: Das mag stimmen, aber für einen Mittelständler mit knappem Budget kann die Basisfeststellung schlichtweg zu teuer sein.

Balkenhol: Ich würde nicht sagen, dass man das nicht im Budget unterbringen kann.

Wir ziehen unser IT-Risk Assessment in der Regel in drei Tagen vor Ort durch. Das gilt für Firmen bis 200 Angestellte. Man muss einem externen Dienstleister eben sagen, dass er nur das Notwendigste tun soll, dann bleibt auch der Aufwand überschaubar. Außerdem gibt es fast immer schon Information über die Sicherheitsanforderungen und den Stand der Dinge. Alte Audits, Dokumentationen, Prüfungen - das verkürzt die Basisanalyse.

IT-Grundschutz: Entspricht Ihr Assessment der Schutzbedarfsfeststellung des BSI?

Balkenhol: Nein, wir beziehen alle Normen mit ein, die in der IT-Security relevant sind wie ITIL, SOX, ISO und IT-Grundschutz. Sollte jemand

bereits wissen, dass er eine Schutzbedarfsfeststellung machen will, kann er die Ergebnisse natürlich weiterverwenden.

IT-Grundschutz: Wo fehlt es bei der Umsetzung von Normen am meisten?

Balkenhol: All zu oft werden die Bedürfnisse der Mitarbeiter nicht berücksichtigt. Ein typisches Beispiel ist die Zugangskontrolle. Da wird auf Gedeih und Verderb hermetisch abgeriegelt, nur um dann festzustellen, dass es in der Praxis nicht handhabbar ist. Ich habe eine Firma erlebt, die ihr Rechenzentrum mit allem ausgestattet hatte, was zu dieser Zeit technisch machbar war. Doch wenn ein Gerät angeliefert wurde, dass größer als eine Schuhschachtel war, standen die Türen trotzdem mit einem Türstopper offen. Man muss die Mitarbeiter einbeziehen und vorher fragen: Wer und was muss in diesen Raum, wie oft wird geliefert und wie groß sind diese Lieferungen. Sonst kann man sich die Sicherheitsschleuse auch gleich sparen.

IT-Grundschutz: Haben Sie noch ein Beispiel für uns?

Balkenhol: Natürlich, da gibt es genügend. Nehmen wir zum Beispiel die Absicherung eines Rechenzentrums mit Zugangskarte und einer Zahlenkombination. Wenn in dem Fall niemand den Mitarbeitern sagt, dass die Zahlen geheim und individuell sein sollen, erleben wir schon mal, dass die Mitarbeiter einfach die Kartenummer als Code nutzen. Wenn dann das System diese Praxis auch zulässt, hat man eine neue Sicherheitslücke. In solchen Fällen muss man einfach kommunizieren und per Richtlinie verdeutlichen, was der Sinn der Zahlenkombination ist. An den Anwendern vorbei lässt sich keine Sicherheitsmaßnahme auf Dauer erfolgreich umsetzen.

IT-Grundschutz: Frau Balkenhol, wir danken Ihnen für das Gespräch!

Konkurrenz belebt das Geschäft

Layer-2-Verschlüsselungslösungen statt IPSec-Netzwerk

Leonhard Zilz, Sales Director Central & Eastern Europe, InfoGuard AG

In gleichem Maß, in dem der Kostendruck auf Unternehmen steigt, gewinnen preisgünstige Technologien an Beliebtheit. Ein Trend ist, dass IT-Verantwortliche von Legacy-Netzen auf Ethernet wechseln und in der Folge ihre IT-Sicherheitsarchitektur anpassen. Noch dominieren IPSec-Gateways bei der Übertragung sensibler Daten, aber auch Layer-2-Verschlüsselungslösungen haben ihre Vorteile.

Kosteneffizienz ist natürlich nicht nur in wirtschaftlich schwierigen Zeiten ein zentrales Kriterium bei allen unternehmerischen Entscheidungsprozessen. Doch die aktuelle Wirtschafts- und Finanzkrise sorgt für eine außergewöhnlich hohe Drucksituation, in der alle Bereiche im Unternehmen auf dem Prüfstand stehen. Deshalb konsolidieren Firmen ihre Daten und Rechenzentren, setzen auf Serverebene verstärkt Virtualisierungslösungen ein und lagern Informationsdienste kostengünstig aus. Cloud Computing ist nicht zuletzt deswegen im Moment ein Megatrend in Europa, Asien und den USA. Für viele bislang genutzte Legacy-Netzwerke bedeutet diese Entwicklung das Aus - sie bringen nicht die notwendige Flexibilität für die geforderten Aufgaben mit.

Die IT-Verantwortlichen stehen vor der Herausforderung, zentrale Applikationen im Rahmen eines verteilten Standortnetzes zur Verfügung zu stellen. Und sie müssen die erforderliche Bandbreite für einen steigenden Bedarf an IT-, Sprach- und Video-Daten vorhalten. Dazu kommt, dass Firmen über Ländergrenzen hinweg fusionieren und ihre IT-Infrastruktur zusammenschließen. Andere Anforderungen wie der ortsunabhängige Zugriff auf Geschäftsdaten und eben IT-

Managementkonzepte wie Cloud Computing fördern diese Entwicklung zusätzlich. Neben einer höheren Flexibilität ist dabei von entscheidender Bedeutung, dass sich die eingesetzten Technologien bedarfsgerecht skalieren lassen. Das wiederum führt dazu, dass die Nachfrage nach integrierten Diensten steigt und Struktur sowie Architektur der Netzwerktechnologien von Grund auf verändert werden.

Flexibilität und Skalierbarkeit

In zunehmendem Maß setzen die Provider die Anforderungen mittlerweile über Ethernet-Services um, die sich als Alternative zu Layer-3- (IPSec) und Legacy-Technologien wie Leased Line, ATM, Frame Relay etabliert haben. Niedrigere Investitions- und Service-Kosten gegenüber Legacy-Netzwerken sprechen für Ethernet-Leitungen. Um Unternehmen weder bei der Wahl des Service-Angebots noch bei der Architektur des Netzwerks einzuschränken, werden Ethernet Services als Punkt-zu-Punkt-Verbindung, als Punkt-zu-Multipunkt-Topologie oder als Any-to-Any-Konfiguration eingesetzt. Außerdem handelt es sich hier um eine bewährte Technologie, die Verfügbarkeitsquoten von nahezu 100

Prozent erreicht. Dank garantierten Umschaltzeiten von 50ms eignen sich Ethernet Services zudem für hochverfügbare und ausfallsichere Netzwerke, was sich auch mittels Service Level Agreements (SLAs) absichern lässt. Neben dem Faktor Zuverlässigkeit punktet Ethernet durch Einfachheit, denn im Regelfall ist das notwendige Technikwissen bereits im Unternehmen vorhanden.

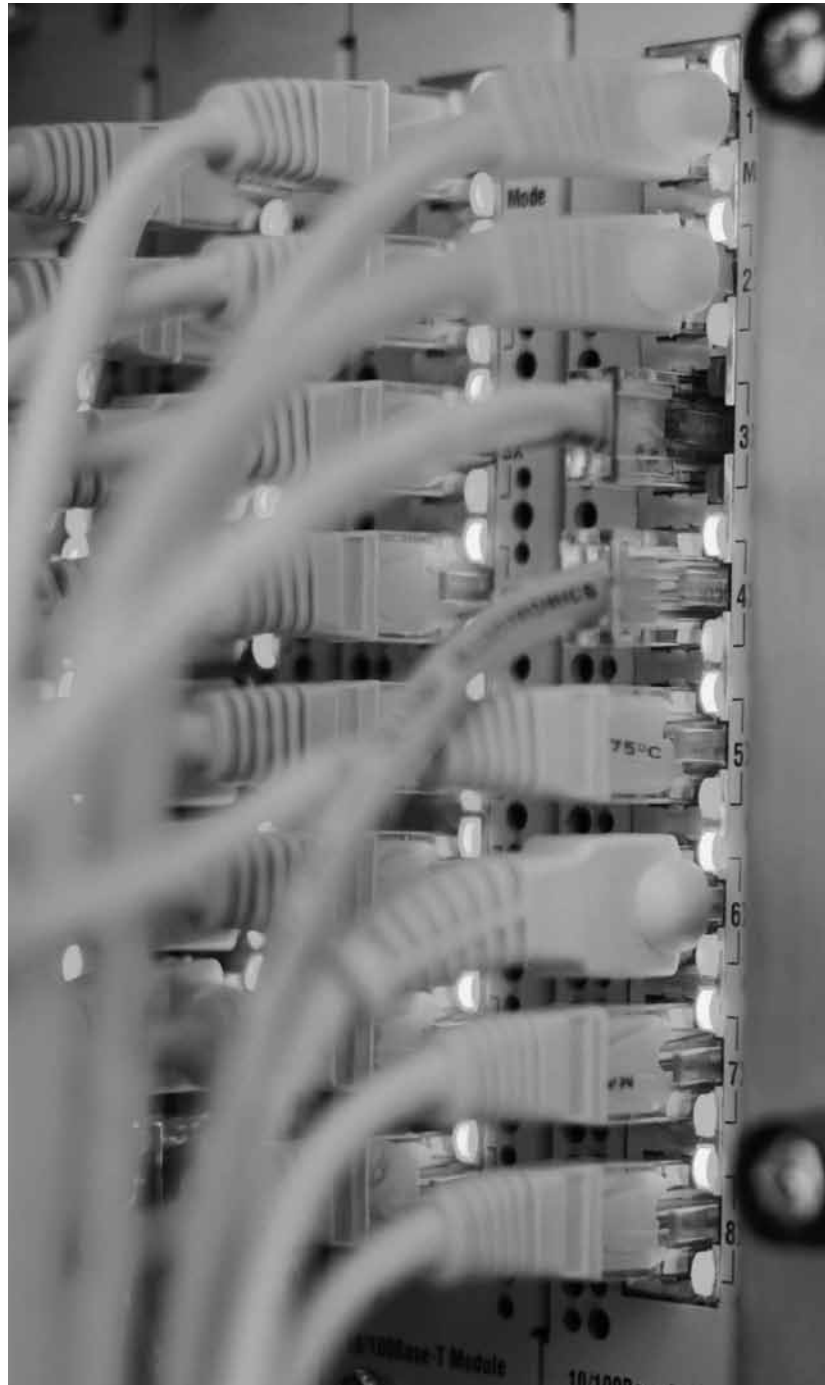
Ein weiterer Ethernet-Vorteil ist, dass sich der Datendurchsatz von einem Megabit pro Sekunde auf bis zu mehrere Gigabit pro Sekunde steigern lässt. Das zahlt sich bei der Anbindung verschiedener Standorte, Server-Farmen und Backup- und Disaster-Recovery-Infrastrukturen aus. Die Provider greifen dabei fast ausschließlich auf Glasfaserleitungen zurück, um große Datenmengen verzögerungsfrei über weite Entfernungen transportieren zu können. Vor allem global operierende Konzerne und Institute aus dem Finanz-, Telekommunikations- und öffentlichen Sektor bauen auf die Lichtwellenleiter als zuverlässige Übertragungswege. Geschwindigkeit, Kapazität und Wirtschaftlichkeit sprechen für den Einsatz von Glasfasernetzen, die außerdem nicht anfällig für elektrische Störungen von außen sind.

Optische Täuschungen in Glasfasernetzen

Mit dem Wechsel auf modernere Leitungsnetze ist es aber nicht getan. In der IDC-Studie „Optische Glasfasernetze: Ist Sicherheit nur eine optische Täuschung?“ warnt der Analyst Romain Fouchereau vor den Gefahren durch Wirtschaftsspionage. Seine Kernaussage: Unternehmensnetze werden mit Firewalls und Intrusion-Protection-Systemen wirksam geschützt, aber bei der Übertragung von Unternehmensdaten zwischen den Standorten gibt es Nachholbedarf. IDC identifiziert neben dem öffentlichen Sektor insbesondere die Banken-, Versicherungs- und Pharmaziebranche als akut gefährdet. Glasfasernetze galten in der allgemeinen Wahrnehmung lange als sicher, aber die Studie führt gleich mehrere Beispiele für Lauschangriffe auf optische Glasfasernetze an. So sei es gelungen, der US-amerikanischen Supermarktkette Hannford circa 4,2 Millionen Kreditkartendaten zu rauben.

Beim Thema Datenschutz gibt es also Nachholbedarf und die gefährdeten Branchen haben bereits Gegenmaßnahmen ergriffen. Neue Gesetzesvorgaben und brancheninterne Vorgaben sollen die Sicherheit und Verfügbarkeit von Daten verbindlich gewährleisten. Der Payment Card Industry Data Security Standard (PCI DSS) ist ein gutes Beispiel für die eingeforderten Verschlüsselungsrichtlinien, die Handelsunternehmen zur Absicherung der Daten integrieren müssen. Alle Firmen und Dienstleister, die Kreditkartenzahlungen akzeptieren, sind an das Regelwerk gebunden, das die Speicherung und Übermittlung der Transaktionen minutiös vorschreibt. PCI DSS sieht insgesamt zwölf Einzelmaßnahmen vor, wie die verschlüsselte Übertragung sensibler Daten von Kreditkarteninhabern in öffentlichen Rechnernetzen. Bei Nichtbefolgung können Strafgebühren verhängt, Einschränkungen ausgesprochen oder letztlich der Kreditkarteneinsatz komplett untersagt werden.

Unabhängig von der Vermeidung finanzieller Kosten ist eine hohe Sorgfaltspflicht beim Schutz digitaler Daten ohnehin im Eigeninteresse. Kern aller IT-Strategien sollte immer die verschlüsselte Übertragung von Daten sein, um Missbrauchsszenarien von vornherein vorzubeugen. Der wirtschaftliche Schaden beschränkt sich nicht nur auf den Datendiebstahl selbst, sondern kann bei Bekanntwerden noch größere Verwerfungen zur Folge haben. Die breite Berichterstattung über den Diebstahl persönlicher Kundendaten bei T-Mobile, Telekom sowie Süddeutscher und Norddeutscher Klassenlotterie ist ein anschauliches Beispiel dafür, wie sich Datendiebstahl als Imageschaden in der öffentlichen Wahrnehmung negativ niederschlägt. Spätestens unter dem massiven Druck der Medien sind private Unternehmen und öffentliche Behörden dazu gezwungen, sensible Informationen zuverlässig gegen Diebstahl zu sichern.



Bandbreite in Netzkabeln: Mit Layer-2 Verschlüsselung besser ausnutzen

Probleme beim IPSec-Protokoll

Für den abhörsicheren Austausch digitaler Informationen ist IPSec, kurz für Internet Protocol Security, die gängigste Übertragungstechnologie. Zum Aufbau eines verschlüsselten Virtual Private Networks (VPN) kamen Administratoren bisher an dem bekannten, aber auch sehr komplexen Sicherheitsprotokoll nicht vorbei. Das IPSec-Verbindungsprotokoll eignet sich sowohl zur Kopplung von ganzen Standorten (Site-to-Site VPN) als auch für den Zugriff von Außendienstmitarbeitern auf Information im internen Unternehmensnetz (Remote

Access). Aufgrund der Komplexität des Sicherheitsprotokolls sowie einer Vielzahl an Funktionen und Einsatzmöglichkeiten erfordern IPSec-Szenarien allerdings einen hohen Administrationsaufwand.

Hauptmanko von IPSec-Übertragungen ist, dass die verfügbare Bandbreite durch den generierten Overhead mehr oder weniger stark eingeschränkt wird. Da die chiffrierten Datenpakete auf der Vermittlungsschicht (OSI Layer-3) laufen, sinkt der Durchsatz deutlich ab, wenn die Hardware nicht über spezielle Funktionen zur Beschleunigung von Verschlüsselungsaufgaben verfügt. Zudem vergrößert das IPSec-Protokoll die Datenpakete, je nach Ursprungsgröße des Pakets

kann die Zunahme bis zur doppelten Größe führen. Ein ursprünglich 64 Byte großes IP-Paket erhält einen zusätzlichen 57 Byte großen Datenzusatz. Natürlich sinkt dadurch der nutzbare Anteil der Bandbreite für die eigentlich zu übertragenden Daten. Durch die Fragmentierung und den höheren Rechenaufwand steigt auch die Latenzzeit. Der Negativeffekt wirkt sich besonders nachteilig aus, weil nach Studien 65 Prozent des weltweiten IP-Verkehrs aus kleinen 64- und 128-Byte großen Datenpaketen bestehen.

Als Alternative sehen einige Hersteller die Verwendung von Verschlüsselungslösungen, die auf einer niedrigeren OSI-Schicht ansetzen. Die InfoGuard AG aus der Schweiz

verschlüsselt die Daten in ihren Produkten auf der Sicherungsschicht (Layer-2) des OSI-Modells. Bei der Layer-2-Verschlüsselung benötigen die chiffrierten Einzelpakete keine neuen IP-Header, so dass unnötiger Datenballast und die daraus resultierenden Performanceprobleme vermieden werden. Dadurch steigt zum einen der Datendurchsatz auf Gigabit-Geschwindigkeit und zum anderen wird die verfügbare Bandbreite nahezu vollständig mit den Nutzdaten gefüllt. Zudem senkt die Verschlüsselung auf der Sicherungsschicht den Komplexitätsgrad und vermeidet arbeitsintensive Netzwerkanpassungen. Mit der Layer-2 Verschlüsselung bekommen IPSec-Netzwerke ernst zu nehmende Konkurrenz.

Veranstaltungen

Messen Kongresse

CeBIT

Deutsche Messe AG
02. - 06.03.2010, Hannover
www.cebit.de

it security 2010

IT Verlag
26. - 28.04.2010,
München-Unterhaching
www.it-verlag.de

WebhostingDay 2010

intergenia
17. - 19.03.2010, Brühl
www.webhostingday.com

Seminare

Schulung: IT-Forensik – Praxiserprobte Vorgehensweisen

isits
15. - 17.03.2010
www.is-its.org

Praxisseminar – Die Top Ten Datenschutz Themen im

Unternehmen
Filges IT Beratung
16. - 17.03.2010, Oberhausen
www.filges.de

Certified Professional for Secure Software Engineering

Secorvo Security Consulting
16. - 18.03.2010, Karlsruhe
www.secorvo.de/college

Zertificon Tutorial 2010

Zertificon Solutions
17.03.2010, Nürnberg
www.zertificon.com/tutorials.php

BDSG 2009 – Datenschutzrecht aktuell

Datenschutzwissen.de
22.03.2010, Berlin
www.datenschutzwissen.de

Linux und Sicherheit

Lanworks AG
22. - 24.03.2010, Neuss
www.lanworks.de

Datenschutz in der Finanz- u. Versicherungswirtschaft

PROKODA
22.03.2010, Stuttgart
www.prokoda.de

Recht und IT-Sicherheit

CAST e.V.
25.03.2010, Darmstadt
www.castforum.de

ISMS gemäss ISO27001/2 implementieren und verbessern (Kompaktkurs)

ITACS Training
31.03.2010, Zürich
www.itacs.ch

Zertifizierung - Der Informa- tions-Sicherheitsbeauftragte / IS-Beauftragte ITSIBE

CBT Training & Consulting
12. - 16.03.2010, München
www.cbt-training.de

Advanced Web Application Security Testing

SIGS Datacom
14. - 15.04.2010, München
www.sigs-datacom.de

Wireless-LAN Sicherheit

KOMZET der Handwerkskammer
Rheinhausen
19. - 20.04.2010, Mainz-
Hechtsheim
www.komzet-hwk.de

Weitere Termine zum
Thema IT-Security und
IT-Grundschutz unter
www.sicherheitstermine.de

Hier abonnieren:
www.grundschutz.info



IT-Grundschutz
Informationsdienst

Der Informationsdienst „IT-Grundschutz“ ist eine ideale aktuelle Ergänzung zu den IT-Grundschutz-Katalogen. Der monatlich erscheinende Informationsdienst liefert Neues zu Rechtsprechung, Technik, Anwendungen und Trend-Themen - leicht verständlich und praxisnah.

Probeseiten und News unter:
www.grundschutz.info

Jahresabonnement Informationsdienst IT-Grundschutz:

Inland 98,00 € / Ausland 116,10 €
(inkl. MwSt. und Versandkosten)

Koppelabopreis für <less>
und WIK-Abonnenten:
Inland 76,00 € / Ausland 84,53 €

SecuMedia

Der Verlag für
Sicherheits-Informationen

SecuMedia Verlag
Postfach 12 34, 55205 Ingelheim
vertrieb@secumedia.de
Tel. +49 6725 9304-0