OKTOBER 2014

ISSN 1864-0907 • 7,- €

IT-SICHERHEIT

Made in Germany

Datensicherheit

Endpoint Security

ATP

Backdoor

Data Leakage

Compliance

Verschlüsselung

Patch Management

Powered by:

SecurITy made in Germany

TeleTrusT Quality Seal www.teletrust.de/itsmig

Vogel Business Media

Eine Publikation von IT-BUSINESS

Security Insider

Ihr Schutzschild gegen Lauschangriffe

Smartphones werden abgehört. Millionenfach, Tag für Tag, auf der ganzen Welt. Secusmart hat etwas dagegen: einen elektronischen Schutzschild, der die Kommunikation der deutschen Bundesbehörden, Ministerien, Verteidigungseinrichtungen und vieler Unternehmen und Regierungen weltweit abhörsicher macht.

Jetzt kommt Secusmart für alle: die mobile Verschlüsselungs-App, die handelsübliche Smartphones so abhörsicher macht wie das Kanzlerhandy. Holen Sie sich die Kontrolle über Ihre Geheimnisse zurück!

- Die App von den Erfindern des Kanzlerhandys
- Weltweit abhörsicher telefonieren
- Für Android/iOS/Blackberry

www.secusmart.com

secusmart

High Security. Made in Germany

Sicherheit der IT hat endlich einen hohen Stellenwert

Dr. Holger Mühlbauer
Geschäftsführer von TeleTrusT – Bundesverband IT-Sicherheit e.V.

Die Sicherheit war viele Jahre lang ein Stiefkind der IT. Weder private Nutzer noch Wirtschaft oder Verwaltung schenkten ihr die gebührende Aufmerksamkeit. Sicherheit ist nicht sexy, kostet Geld und ein direkter Nutzen ist nicht zu erkennen – so das jahrelange Credo.

Mit dem Siegeszug mobiler Endgeräte und der entsprechenden Applikationen setzte auf breiter Front endlich das überfällige Umdenken ein. Heute steht die Sicherheit ganz oben auf den To-do-Listen von IT-Abteilungen und privaten Anwendern. Firewalls und Virenschutz sind mittlerweile Standards. Die Snowden-Debatte, der lasche Umgang vieler sozialer Plattformen mit ihren Nutzerdaten und nicht zuletzt die zunehmende Cyberkriminalität mit ihren mafiösen Strukturen und konkreten Bedrohungsszenarien waren wesentliche Faktoren für diese Entwicklung.

Wirtschaft und Verwaltung sowie private Anwender sind mehr denn je auf sichere und vertrauenswürdige Informationsinfrastrukturen angewiesen. Dies erfordert Sicherheitsmaßnahmen und IT-Sicherheitsprodukte, die adäquaten Schutz auf hohem Niveau bieten und der Bedeutung der zu schützenden Daten oder Güter angemessen sind. Deutsche IT-Sicherheitsunternehmen sind weltweit führend bei der Herstellung von Produkten, die höchsten Ansprüchen im Hinblick auf Vertrauenswürdigkeit und Informationssicherheit genügen.

In unserem Bestreben um noch mehr Sicherheit in der IT werden wir als Bundesverband IT-Sicherheit auch in Zukunft nicht nachlassen. Gemeinsam mit Politik, Wirtschaft und den einschlägigen Herstellern wollen wir beispielsweise erreichen, dass vertrauenswürdige, robuste IT-Systeme, die die Probleme „Softwaresicherheit“ beziehungsweise „Malwarebefall“ adressieren, ganz speziell gefördert werden. Im Gegenzug wollen wir aber auch erreichen, dass die rechtliche Verantwortung für IT-Lösungen erhöht wird, um Hersteller und Dienstleister zu mehr IT-Sicherheit zu motivieren. Hersteller müssen Verantwortung übernehmen, um Vertrauen zu schaffen. Ein pragmatischer und ausgewogener Rechtsrahmen sollte dem Schutzbedürfnis der Anwender ebenso gerecht werden wie der unternehmerischen Risikokalkulation.

Der Erfolg der TeleTrusT-Initiative „IT Security made in Germany“ zeigt, dass deutsche Sicherheitsunternehmen bei allem Wettbewerb bereit sind, unter dieser Dachmarke zusammen zu arbeiten und gemeinsam einen wichtigen Beitrag für mehr Vertrauenswürdigkeit und Informationssicherheit zu leisten. Davon profitieren letztendlich wir alle.

Diese Sonderpublikation informiert Sie über Lösungen und Entwicklungen, die deutsche Unternehmen im Bereich der IT-Sicherheit entwickelt haben. Gemeinsam mit den Mitgliedern von TeleTrusT wünsche ich Ihnen eine informative Lektüre und hoffe, dass Sie zahlreiche Anregungen erhalten, um die IT-Sicherheit im Unternehmen und in Ihrem privaten Umfeld weiter voran zu treiben. □

GRUNDLAGEN

VERSCHLÜSSELUNG

REDAKTION

TeleTrusT-Initiative „IT Security made in Germany“

„ITSMIG“ („IT Security made in Germany“) wurde 2005 auf Initiative des Bundesministeriums des Innern (BMI), des Bundesministeriums für Wirtschaft und Technologie (BMWi) sowie Vertretern der deutschen IT-Sicherheitswirtschaft etabliert und 2008 in einen eingetragenen Verein überführt. Sowohl BMI als auch BMWi hatten eine Schirmherrschaft übernommen.
Nach intensiven Erörterungen sind TeleTrusT und ITSMIG 2011 übereingekommen, dass sich auf ihren Handlungsfeldern Synergien erschließen lassen. Zukünftig werden die ITSMIG-Aktivitäten unter dem Dach des TeleTrusT als eigenständige Arbeitsgruppe „ITSMIG“ fortgeführt.

Die TeleTrusT-Arbeitsgruppe „ITSMIG“ verfolgt das Ziel der gemeinsamen Außendarstellung der an der Arbeitsgruppe mitwirkenden Unternehmen und Institutionen gegenüber Politik, Wirtschaft, Wissenschaft und Öffentlichkeit auf deutscher, europäischer bzw. globaler Ebene. BMWi und BMI sind im Beirat der Arbeitsgruppe vertreten.

Ist Sicherheit aus Deutschland eine bessere Sicherheit?

Dr. Andreas Bergler
CvD
IT-BUSINESS

Peter Schmitz
Chefredakteur
Security-Insider.de

PRO

Die Schreckensmeldungen über Spionageprogramme, Sicherheitslücken oder gezielten Datendiebstahl reißen nicht ab. Die fast beliebige Entnahme von Daten aus vermeintlich geschützten Quellen wird dabei auch noch von gewissen Staaten sanktioniert. Soeben hat ein US-Gericht Microsoft in einem Urteil wieder gezwungen, E-Mails eines Kunden herauszugeben, dessen Daten auf einem Server in Irland gespeichert sind.

Natürlich ist die Forderung nach einem Datenschutz unter deutscher Flagge nur ein politisches Argument. Technisch gesehen mag man erwidern, dass sowieso jede Mail mehrmals um den Erdball kreist, bevor sie zum Empfänger gelangt, also von jedem beliebigen Bösewicht ausgelesen werden kann. Das Argument verfängt aber nicht. Denn erstens stromert nicht jede Information unkontrolliert im Internet, zweitens lässt sie sich verschlüsseln und drittens kann sie explizit geschützt werden – mit Technologien, die eben keine Backdoors zu ausländischen Diensten bereithalten. Dazu müssen sie allerdings aus dem Inland kommen.

Dr. Andreas Bergler
CvD IT-BUSINESS

CONTRA

Die Herkunftsbezeichnung „Made in Germany“ gilt seit Jahrzehnten als Gütesiegel für hohe Produktqualität. Wer sich mit IT-Sicherheit befasst, der kann nicht gegen mehr oder bessere Sicherheit sein. Deshalb ist „IT-Security Made in Germany“ auf den ersten Blick scheinbar sinnvoll. Aber auch im Jahr 1 nach Snowden sollte man IT-Sicherheit mit Fakten bewerten und nicht mit Gefühlen.

Es gibt viele Gründe, warum man sich für die Sicherheitslösungen eines bestimmten Herstellers entscheidet. Entweder die Lösung ist für den Einsatzzweck die beste auf dem Markt (Best of Breed), oder der Hersteller bietet ein besonders gut zusammenarbeitendes Komplettsystem (Alles aus einer Hand), oder das Produkt hat schlicht und einfach das beste Preis-Leistungs-Verhältnis.

Aber sich wegen des Herkunftslandes und angeblich nicht vorhandener Backdoors für eine Sicherheitslösung zu entscheiden, verbessert die Sicherheitslage des eigenen Unternehmens nicht unmittelbar. Auch wenn es, wirtschaftlich gesehen, lobenswert patriotisch ist.

Peter Schmitz
Chefredakteur Security-Insider.de

AGENDA

10:00 – 10:30	Teilnehmerregistrierung, Begrüßungskaffee
10:30 – 10:45	Begrüßung und Moderation: Dr. Jörg Schröper, Chefredakteur LANline
	Keynotes
10:45 – 11:15	**Herausforderung Datensicherheit** **Dr. Markus Söder**, Staatsminister der Finanzen, für Landesentwicklung und Heimat, MdL, CIO des Freistaates Bayern
11:15 – 11:45	**„Digitale Souveränität" – Chancen für Deutschland und Europa** *Christian Schallenberg, Mitglied der Geschäftsleitung & CTO, Lancom Systems*
11:45 – 12:15	**„The Age of Flexibility" – Wie neue Technologien Leben und Arbeit verändern** *Claus Hessberger, Leiter Enterprise Mobility Services, Deutsche Telekom AG Products & Innovation*
12:15 – 12:45	Zeit für Gespräche mit Referenten und Ausstellern
12:45 – 13:15	**Die Herausforderungen der strategischen Ausrichtung, Anbindung und Vernetzung mobiler Endgeräte in Unternehmen** *Patrick Oliver Graf, Vice President Global Sales & Marketing, NCP engineering GmbH*
13:15 – 14:00	**Mittagspause**
14:00 – 14:45	**„Spannungsfelder moderner Technologien"** *Boris Bärmichl, Vorstand KoSib eG – Kompetenzzentrum für Sicherheit in Bayern eG*
14:45 – 15:00	Zeit für Gespräche und Erfrischungen
15:00 – 15:45	**Vortragsreihe 1**
	→ **Kryptographie in Hinblick auf Anwendung bei VPN mit SSL/TLS und IPsec** *Dr. Florian Scheuer, IT-Security Consultant SSP EUROPE GmbH*
	→ **VPN aus der Cloud – Sicher und Multimandantenfähig** *Martin Wohlert, Geschäftsführer MAWOH GmbH*
	→ **Neue Geschäftsmodelle auf Basis sicherer mobiler Identitäten** *Helmut Friedel, CEO Certgate GmbH*
15:45 – 16:15	Diskussion und Gespräche in Center Lounge mit Ausstellern und Referenten
16:15 – 17:00	**Vortragsreihe 2**
	→ **Managed Security Services (MSS) – Made in Germany – IT Security Outsourcing im Spannungsfeld von Kosten, Service & Qualität** *Andreas Mertz, CEO/Founder IT-Cube Systems GmbH*
	→ **Sicherheit für mobile Rechner bei Diebstahl und Angriffen über Internetverbindungen – Verschüsselung mit Zulassung VS NfD** *Dr. Schirmer, Senior Software Architekt – Leiter Bereich Endpoint Security Sirrix AG*
	→ **Große Remote Access Umgebungen sicher einrichten und unkompliziert verwalten** *Jörg Hirschmann, CTO NCP engineering GmbH*
17:05 – 17:50	**Vortragsreihe 3**
	→ **Wie machen wir unsere Netze sicher** *Dr. Martin Krebs, Leiter Produktmanagement Lancom Systems*
	→ **„Change or Die" – Sicherheit neu Denken** *Michael Hinrichs, Leiter Produktmanagement Enterprise Mobility Services Deutsche Telekom AG Products & Innovation*
	→ **Remote Access VPN mit VS-NfD Zulassung** *Swen Baumann, Produktmanager NCP engineering GmbH*
ab 18:00	Get together bei „Drei im Weggla" und fränkischem Bier

T..

LANCOM Systems

MAWOH secure your company

SSP EUROPE

NCP Remote Access Kongress

Save the Date

13. November 2014

Nürnberg Convention Center West (NCC West)

The Importance of Secure Network Communication and Mobility – Made in Germany

Der erste Kongress, der führende deutsche IT Unternehmen im Bereich Remote Access zusammenbringt und Sie themenübergreifend über Datenkommunikation und Sicherheit informiert.

Einzigartig – Themenübergreifend – Unabhängig!

Alle weiteren Informationen finden Sie unter:
www.ncp-e.com/de/remote-access-kongress

certgate · iT-CUBE SYSTEMS · Sirrix AG security technologies · NCP SECURE COMMUNICATIONS

Vertrauen ist eine binäre Größe

Geschäfte werden zwischen Menschen gemacht, die sich vertrauen. Neben der technischen Ebene haben die Schlapphut-Skandale daher auch eine zwischenmenschliche Dimension. Dem Vertrauensverlust und Generalverdacht begegnen US-Unternehmen nun mit einem gemeinsamen Protest.

IT-BUSINESS / Dr. Stefan Riedl

Seit den Enthüllungen von Edward Snowden wird offen darüber diskutiert, wie westliche Geheimdienste in erheblichem Ausmaß Wirtschaftsspionage betreiben.

Bild: alphaspirit – Fotolia.com

Bild: NSA

Der NSA-Skandal führt teilweise zu einem Generalverdacht gegenüber US-Anbietern.

Die Deutsche Bank warb in den 90er Jahren mit dem Slogan: „Vertrauen ist der Anfang von allem." Nachdem das Geldinstitut in erhebliche juristische Schwierigkeiten in Hinblick auf Ramschhypotheken, Währungstricks und Zinsmanipulationen geraten ist, möchte man mit einem Zitat von Otto von Bismarck antworten: „Das Vertrauen ist eine zarte Pflanze; ist es zerstört, so kommt es sobald nicht wieder." Oder, um es konkret auf den Werbespruch zu beziehen: „Kein Vertrauen ist der Anfang vom Ende."

Image-Schäden

Das gilt nicht nur für die Finanz-, sondern auch für realwirtschaftliche Branchen wie die IT-Industrie. Vertrauen ist ein kritischer Erfolgsfaktor. Sinkt das Vertrauen in die Produkte eines Unternehmens, sinken auch die Umsätze und Gewinne. Vor diesem Hintergrund haben die Enthüllungen von Edward Snowden eine immense wirtschaftliche Bedeutung.

Denn es wird offen darüber diskutiert, wie westliche Geheimdienste in erheblichem Ausmaß Wirtschaftsspionage betreiben. In medialer Breite wird ausgerollt, welche Mechanismen US-Unternehmen zur Kooperation mit den „Diensten" zwingen können (Patriot Act, Geheimgerichtsbeschlüsse). Kein Wunder, dass US-amerikanischen IT-Firmen inzwischen vielerorts so etwas wie ein Generalverdacht entgegenschlägt. Denn Vertrauen ist eine binäre Größe. Entweder man vertraut jemandem – sei es eine Person, ein Produkt oder eine Firma – oder nicht.

Hier geht es nicht nur um rein rationale Überlegungen, sondern in hohem Maße um Bauchentscheidungen. Und meldet das Bauchgefühl Zweifel an, dann werden die schönsten Return-on-Investment-Berechnungen, gedruckt auf Hochglanzpapier obsolet.

Tendenzen im Markt

Was die Spionage-Affäre angeht: Zu viel ist im Dunkeln abgelaufen. Und zu erkennbar war die Salami-Taktik – zugegeben oder nicht bestritten wurde stets nur das, was Edward Snowden enthüllte. Entscheidend ist aber: Es ist nicht ⇨

Selbstbedienungsladen Deutschland

Über Jahre haben sich die Geheimdienste fremder Staaten hemmungslos an den Daten deutscher Bürger und Unternehmen bedient, schrieb der Bundesverband IT-Mittelstand e.V. (BITMi). „Der Schaden für die Wirtschaft ist überhaupt nicht abzusehen, das Vertrauen in die Aufrichtigkeit unserer Freunde und europäischen Nachbarn nachhaltig beeinträchtigt."

Michaela Merz, IT-Sicherheitsexpertin des Verbandes findet klare Worte: „Deutschland ist besonders anfällig für solche Spionage-Aktionen. Unsere Wirtschaft ist sehr stark von ausländischen Technologien abhängig, und wir wissen nicht, ob und welche Hintertüren noch in häufig benutzten Soft- und Hardware-Produkten eingebaut sind."

Wirtschaftsspionage seitens der Geheimdienste ist keine "Verschwörungstheorie" mehr.

erkennbar, dass Weichen anders gestellt werden. Das Gegenteil ist der Fall. Die meisten Fragen zur Geheimdienstaffäre bleiben offen. Aber der Markt hat Antworten auf offene Fragen parat. Es gibt bereits ganz konkrete Auswirkungen auf das Marktgeschehen durch die Bespitzelungsproblematik und die Frage nach Vertrauen oder Skepsis.

Das Kredo der Skeptiker lautet von der Tendenz her Private statt Public Cloud, interne statt externe Datenhaltung, verschlüsselter statt unverschlüsselter Datenverkehr und Zertifizierungen für Backdoor-freie Geräte. Dieser Ansatz ist sicherlich sehr sinnvoll. Allerdings gibt es auch Stimmen, die warnen, dass es für elektronische Daten niemals vollständige Sicherheit geben könne.

Die beschriebenen Marktentwicklungen zeigen sich in vielen der angeblich boomenden Segmente, die davon betroffen sind, insbesondere bei der vieldiskutierten Cloud-Problematik. So boomen Dokumenten-Management-Systeme hierzulande beispielsweise, ohne dass der Cloud-Ansatz hierbei eine nennenswerte Rolle spielt. Laut einer Befragung von Techconsult setzt sich Cloud Computing hierzulande im Mittelstand nur zögerlich durch. Besonders beim Beispiel „Social Business" gelte diese Aussage, denn ein Großteil der Befragten sieht laut Forschungsinstitut durch „Social Business" keinen direkten Mehrwert. Lediglich 18 Prozent der Befragten glauben, dass sich durch die Integration von Social-Networking-Lösungen Geschäftsprozesse effizienter gestalten lassen. 62 Prozent sehen durch Cloud-basierte Social-Business-Dienste keinen Mehrwert.

Deutsches Internet?

Die Deutsche Telekom will es ausländischen Geheimdiensten künftig schwerer machen, systematisch Daten aus dem „deutschen Internet" auszuspähen. Dazu will der Provider ein innerdeutsches Internet auf die Beine stellen, wie die Nachrichtenagentur dpa verlauten lässt. Die Idee dabei ist, dass der Datenverkehr zwischen Punkten in Deutschland oder Europa nicht die regionalen Grenzen verlassen soll.

Die Liste der negativen Auswirkungen des NSA-Skandals ließe sich weiter fortsetzen. Vor diesem Hintergrund haben sich zentrale Player der US-amerikanischen IT-Wirtschaft zusammengetan. AOL, Apple, Facebook, Google, Linkedin, Microsoft, Twitter und Yahoo fordern auf einer gemeinsamen Website (http://reformgovernmentsurveillance.com/) Reformen der Überwachungsprogramme. □

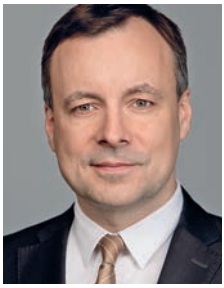
Deutschland als Vertrauensraum ausbauen

Dr. Holger Mühlbauer, Geschäftsführer von TeleTrusT – Bundesverband IT-Sicherheit e.V. reflektiert im Gespräch mit IT-BUSINESS über IT-Sicherheit in Deutschland.

IT-BUSINESS / Das Interview führte Petra Adamik

Was unterscheidet deutsche IT-Sicherheitsunternehmen vom internationalen Wettbewerb?

Dr. Mühlbauer: Deutsche IT-Sicherheitsunternehmen sind führend bei der Herstellung hochspezialisierter Produkte, die im Hinblick auf Vertrauenswürdigkeit und Informationssicherheit höchsten Ansprüchen genügen. Sie unterliegen nicht von vornherein dem Verdacht, auf Druck staatlicher Stellen verdeckte Backdoors implementieren zu müssen. Dies ist auch der wesentliche Aussagegehalt des TeleTrusT-Qualitätszeichens „IT Security made in Germany".



Dr. Holger Mühlbauer
Geschäftsführer von TeleTrusT – Bundesverband IT-Sicherheit e.V.

Was sind für Sie in den kommenden Monaten die zentralen Themen?

Dr. Mühlbauer: TeleTrusT begrüßt zentrale Festlegungen zur „IT-Sicherheit" im aktuellen CDU/CSU/SPD-Koalitionsvertrag, wie sie auch in der „Digitalen Agenda" und im künftigen „IT-Sicherheitsgesetz" reflektiert werden. Die jetzige Legislaturperiode bietet die Chance, verlorenes Terrain in der IT-Sicherheitstechnologie wiederzugewinnen und Deutschland im internationalen Kontext wegweisend aufzustellen. Die Liste der Absichtserklärungen in diesem Papier ist lang. Besonders erwähnen möchte ich den Ausbau der Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Zu den für unseren Verband wichtigen Punkten gehören auch die Initiierung eines Spitzenclusters „IT-Sicherheit und kritische IT-Infrastruktur" sowie das Eintreten für eine europäische Cybersicherheitsstrategie. IT-Sicherheit erfordert auch die Entwicklung und Realisierung vertrauenswürdiger IT- und Netz-Infrastrukturen. Dazu gehören neben sicherer Soft- und Hardware auch sichere Cloud-Technologien.

Wie wird sich TeleTrusT einbringen, um die IT-Welt sicherer zu machen?

Dr. Mühlbauer: Wir haben in Zusammenhang mit Konsultationen im BMWi und BMI beiden Ressorts bereits einen umfassenden Ansatz für eine „IT-Sicherheitsstrategie für Deutschland" vorgeschlagen. Anders als die zahlreichen allgemeinen und teilweise redundanten öffentlichen Verlautbarungen anlässlich der Verabschiedung der „Digitalen Agenda", ist unser Ansatz bereits von beträchtlicher Konkretisierung und Detailschärfe geprägt.

Darüber hinaus sind wir sehr nah am Markt und können daher nicht nur klassische Themen fortschreiben, sondern auch zeitnah auf aktuelle Entwicklungen reagieren. □

gateprotect: Firewall-Schutz aus Deutschland

Die Nachfrage nach verlässlichen IT-Sicherheitslösungen „Made in Germany“ steigt nach den jüngsten Skandalen rund um Cyberspionage und Datendiebstahl ungebrochen an. Experten schätzen, dass im Jahr 2014 weltweit ein wirtschaftlicher Schaden von 375 bis 575 Milliarden US-Dollar durch Cyberkriminalität entsteht.

Security made in Germany

Nahezu jedes dritte Unternehmen in Deutschland wurde in den vergangenen zwei Jahren Opfer von Hackerangriffen. Vor allem mittelständische Unternehmen sind betroffen. Die Bundesregierung handelt und hat jüngst einen Entwurf für ein IT-Sicherheitsgesetz vorgelegt.

Wirtschaftsspionage und der damit einhergehende Verlust von Know-how, das oft durch langjährige Investition in Forschung und Entwicklung erarbeitet wurde, kann für Unternehmen existenzbedrohend sein. Bei Unternehmen mit wichtiger Bedeutung für das staatliche Gemeinwesen, wie z.B. im Energiesektor, kann ein Hackerangriff Versorgungsengpässe und erhebliche Störungen der öffentlichen Sicherheit zur Folge haben.

Unternehmensnetzwerke und mobile Endgeräte müssen deshalb nachhaltig vor Cyberspionage und Datendiebstahl geschützt werden. Viele Unternehmen denken dabei verstärkt über neue innovative Sicherheitssysteme aus Deutschland nach.

Innovativer High-Tech-Schutz aus Deutschland

Die gateprotect GmbH entwickelt seit mehr als zehn Jahren Sicherheitslösungen, um Netzwerke, mobile Endgeräte und Kunden-

daten verlässlich zu schützen. Regelmäßige Updates und Patches sorgen für effektiven Schutz vor den neuesten Bedrohungen und Angriffen aus dem Netz. Die gateprotect UTM-Appliances sind mehrfach international ausgezeichnet und zertifiziert.

eGUI Technologie: Komplexe Systeme einfach und schnell managen

Die patentierte eGUI-Bedieneroberfläche der gateprotect UTM-Firewalls ermöglicht es durch die visuelle Darstellung, jedes Netzwerk und Betriebssystem übersichtlich, schnell und sicher zu administrieren. Der mehrfach ausgezeichnete Usability-Ansatz macht komplexe IT-Sicherheitssysteme erheblich übersichtlicher, reduziert Bedienerfehler und führt kostengünstig zu verlässlicher Sicherheit.

„Complete Security“ für Netzwerke und Endpoints: Echtzeitschutz zu jeder Zeit an jedem Ort

Cyber-Kriminelle konzentrieren sich zunehmend auf Mitarbeiter, um auf das geistige Eigentum von Unternehmen zugreifen zu können. Da auf den mobilen Geräten von Mitarbeitern viele vertrauliche Unternehmensdaten gespeichert sind, müssen Firmen ihre Sicherheits-Anforderungen um eine Strategie für BYOD-Schutz erweitern. gateprotects leicht zu bedienende „Complete Security“-Lösung kombiniert die Sicherheitsfeatures der gateprotect Firewall Appliances mit effektivem Endpoint-Schutz. Das Ergebnis: Perfekter Malware-Schutz und Datensicherheit für alle Geräte in Echtzeit – an jedem Ort und zu jeder Zeit.

Persönlicher Support und umfassende Tech-Trainings

Bei gateprotect sprechen Sie nicht mit einer Hotline. Als Partner profitieren Sie von der Möglichkeit, persönlich mit dem deutschen gateprotect-Support Kontakt aufzunehmen. In umfassenden Technik-Trainings und Schulungen werden Sie zudem bestens mit den Produkten vertraut gemacht.

Effektiver Schutz kritischer Infrastrukturen

Hervorragenden Schutz großer Unternehmensnetzwerke, auch als zweite Verteidigungsstufe für das erweiterte Sicherheitsbedürfnis kritischer Infrastrukturen, bietet die Next Generation Firewall Network Protector von gateprotect. Über feingranulare Applikationserkennung wird ein Whitelisting-Ansatz realisiert, der über Deep-Packet-Inspection sogar innerhalb der Applikation filtert und bewertet. Dieser Ansatz der sogenannten vollständigen Positivvalidierung sorgt dafür, dass jeglicher Verkehr, der die Firewall passieren möchte, eindeutig identifiziert und für valide befunden werden muss. Unbekannte Datenströme, ja sogar unbekannte Komponenten in bekannten Daten, werden zuverlässig geblockt.

www.gateprotect.de ■

Zertifizierte Sicherheit

Mit der Vergabe des Qualitätszeichens „IT Security made in Germany“ an deutsche Anbieter versteht sich TeleTrusT – Bundesverband IT-Sicherheit e.V. auch als offizieller Garant für vertrauenswürdige IT-Sicherheitslösungen.

Von Petra Adamik und Jürgen Paukner

Zertifizierte Anbieter müssen sowohl mit dem Hauptsitz als auch mit den Forschungs- und Entwicklungsabteilungen in Deutschland ansässig sein. Außerdem verpflichtet sich ein Träger des Qualitätszeichens, den Anforderungen des deutschen Datenschutzrechtes zu genügen.

Den nachstehenden Unternehmen wurde die Nutzung des TeleTrust-Qualitätszeichens eingeräumt. Die Liste der zertifizierten deutschen Unternehmen wächst beständig und ist deshalb tagesaktuellen Änderungen unterworfen (Stand 11.09.2014). □

Zertifizierte Anbieter des TeleTrusT-Qualitätszeichens „IT Security made in Germany“

- 2VizCon GmbH
- ads-tec GmbH
- ANMATHO AG
- Antago GmbH
- antispameurope GmbH
- Applied Security GmbH
- astiga GmbH
- Avira GmbH & Co. KG
- BCC Unternehmensberatung GmbH
- Brainloop AG
- Bundesdruckerei GmbH
- CBT Training & Consulting GmbH
- CenterTools Software GmbH
- Certgate GmbH
- Chiffry UG
- Cognitec System GmbH
- commocial GmbH
- Consultix GmbH
- CORISECIO GmbH
- CSO GmbH
- cv cryptovision gmbh
- DATAKOM GmbH
- DATUS AG
- DERMALOG Identification Systems GmbH
- DFN-CERT Services GmbH
- DIGITTRADE GmbH
- digitronic computersysteme gmbh
- DocRAID - digital asset protection GmbH i.Gr.
- ecsec GmbH
- eperi GmbH
- exceet Secure Solutions AG
- FSP GmbH
- gateprotect GmbH
- G Data Software AG
- Giegerich & Partner GmbH
- genua Gesellschaft für Netzwerk und Unix-Administration mbH
- Glück & Kanja Consulting AG
- Governikus GmbH & Co. KG
- GROUP Business Software AG
- HOB GmbH & Co. KG
- IBS Schreiber GmbH
- if(is) - Institut für Internetsicherheit
- Inlab Software GmbH
- Innominate Security Technologies AG
- innovaphone AG
- INVIAS GmbH & Co. KG
- isits AG
- International School of IT Security
- ISL Internet Sicherheitslösungen GmbH

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

- itWatch GmbH
- KOBIL Systems GmbH
- LANCOM Systems GmbH
- limes datentechnik gmbh
- Link11 GmbH
- Linogate GmbH
- media transfer AG
- MESH GmbH
- MindMatics Secure Messaging GmbH
- NCP engineering GmbH
- NEOSULTING GmbH
- Net at Work GmbH
- net-files GmbH
- Nexis GmbH
- Nimbus Technologieberatung GmbH
- OTARIS Interactive Services GmbH
- Pix Software GmbH
- PRESENSE Technologies GmbH
- procilon IT-Solutions GmbH
- protected-networks.com GmbH
- PSW GROUP GmbH & Co. KG
- Pyramid Computer GmbH
- QGroup GmbH
- retarus GmbH
- Secardeo GmbH
- secucloud GmbH
- secunet Security Networks AG
- Securepoint GmbH
- secusmart GmbH
- Secomba GmbH
- sys4 AG
- Sirrix AG
- SOFTPRO GmbH
- Steganos Software GmbH
- TESIS SYSware Software Entwicklung GmbH
- tetraguard systems GmbH
- Trust2Core GmbH
- T-Systems Multimedia Solutions GmbH
- Tutao GmbH
- TÜV Informationstechnik GmbH
- UBIN AG
- Unicept GmbH
- Unify GmbH & Co. KG
- Uniscon universal identity control GmbH
- WMC Wüpper Management Consulting GmbH
- ZenGuard GmbH
- Zertificon Solutions GmbH

Ein Quantensprung im Security-Universum

„Der IT-Weltraum – unendliche Weiten. Wir befinden uns in einer nahen Zukunft. Dies sind die Abenteuer der neuen ESET-Produkte, die im Labor entwickelt wurden, um fremde Welten zu entdecken, unbekannte Virenformen und neue Mutationen. Die Produkte dringen dabei in Galaxien vor, die nie ein Mensch zuvor gesehen hat."

Das Motto NEVER CHANGE A RUNNING SYSTEM hat gerade im IT-Umfeld eine gewisse Tradition, könnte man meinen. Dass jedoch Veränderungen bei einem „running system" zu Erfolgskatalysatoren werden können, zeigt das neueste Verteidigungssystem der ESET-Business-Produkte.

Mit WARP-Antrieb am Puls der Zeit

Das Kraftfeld der IT-Security-Branche besteht vor allem aus einem: Innovation. „Wenn eine Idee am Anfang nicht absurd klingt, dann gibt es keine Hoffnung für sie", pflegte Albert Einstein zu sagen. Als Dinosaurier der Antiviren-Industrie haben wir bei ESET 25 Jahre lang in Sachen Technologie ähnliche Erfahrungen gemacht. Ein Impulsantrieb mehr, nicht den Weg des geringsten Widerstands zu gehen, sondern immer wieder die Grenzen des Gewohnten zu durchbrechen. Damit alles später in geordneten Umlaufbahnen verläuft, werden ESET-Produkte von unseren Kunden vorher einem Härtetest unterzogen.

Beam me up, ESET!

Die Sternenflotte der ESET-Business-Produkte für Windows-Endpoints deckt einen erheblichen Teil der gesamten Installationsbasis und Umsätze ab. Die Optimierung alter und die Entwicklung neuer Funktionen liegt daher ganz deutlich auf und in unserer Hand, um Viren & Co. bereits im Anflug auszumerzen.

Fester Bestandteil der schildbasierten Technologie sind die verbesserte ESET Scan-Engine und der Echtzeit-Dateischutz. Spezialfunktionen wie der Exploit Blocker halten gegnerischen Angriffen auf unsicher geltende Programme wie Java, Web-Browser, Microsoft Office, E-Mail-Programme oder PDF-Reader ohne Probleme stand. Bei ungewöhnlichen Verhaltensweisen werden die damit verbundenen Prozesse automatisch analysiert und im Ernstfall unterbrochen.

Zwei-Wege-Firewall sichert den Datenverkehr

Auch Schwachstellen hat ESET auf dem Radar und untersucht den Datenverkehr auf Attacken gegen Sicherheitslücken der verwendeten Netzwerk-Protokolle. Bei Auffälligkeiten kappt die Zwei-Wege-Firewall schnellstens die Verbindung.

Formwandler oder Viren im Tarnmodus haben keine Chance, denn dem Erweiterten Speicherscanner entgeht nichts. Diese Funktion bringt den Schadcode vielmehr dazu, seine Logarithmen preiszugeben und führt bei verdächtigen Symptomen die richtige Operation durch.

Geringere Systembelastung, erhöhte Mitarbeitereffizienz

Ressourcenknappheit ist nicht nur ein Problem des globalen Wachstums, sondern auch im IT-Bereich. Die Lösung liegt in einer geringen Systembelastung und erhöhten Mitarbeitereffizienz durch die relativ unkomplizierte Handhabung. Damit Software und System auf einer Wellenlänge liegen, werden bereits bei der Installation Wettbewerbsprodukte automatisch erkannt und entfernt.

Mit der überarbeiteten Benutzeroberfläche, die primär auf intuitive Handhabe getrimmt wurde, sind nun auch Touchscreen-Geräte sowie hochauflösende Displays an Bord. In Lichtgeschwindigkeit können zum Beispiel Firewall-Regeln einfach aus Log-Dateien heraus erstellt werden. Ein Assistent hilft bei der Einrichtung und Fehlersuche. Hinzu kommen weitere Möglichkeiten, Standorten oder Netzwerk-Interfaces Regelsätze zuzuweisen.

Die Kommandobrücke: zentrale Verwaltung

Mit dem Management-Tool ESET Remote Administrator wird jeder Admin zur Führungskraft und kann auch bei Abwesenheit glänzen. Denn egal, wo er sich gerade befindet, ist er in der Lage, von überall auf Netzwerke zuzugreifen. Damit alles noch leichter von der Hand geht, wurde auch das zentrale Kontrollzentrum von Grund auf neu gestaltet. So ist es nicht mehr exklusiv an ein Windows-System gebunden, sondern auch für Linux-Systeme oder in Form einer Virtual Machine verfügbar. Über den ESET Remote Administrator Agent lassen sich die Sicherheitslösungen ausrollen, verwalten, Policies erstellen, Scans starten, Wechseldatenträger sperren oder Reports generieren – das volle Programm also.

Freisetzung zusätzlicher Kraftreserven

Die einfache Verwaltungsabwicklung von mehreren Netzwerken bzw. Standorten über Proxies setzt beim Admin weitere Kraftreserven frei. Durch Beschleunigungsfaktoren wie dem neuen Policy-Editor, Assistenten oder den Templates für Policies, Reports, Warnungen u.v.m. wird das Arbeitspensum um ein Vielfaches verringert. Hinzu kommt, dass Datenbanken, der eigentliche Server sowie der Webserver auch auf verschiedene Systeme verteilt werden können. Nicht einmal ein Client ist nötig, um die Administrationsoberfläche von überall aus zu erreichen – dies geschieht über das Web-Interface.

Mit der weiterentwickelten Technologie von ESET bewegen sich Anwender und Unternehmen bei ihrer Reise durchs Netz mit voller Kraft voraus in sicheren virtuellen Welten. Die neu integrierten Schutzschilde in den neuen Business-Versionen werden auch zukünftig T(r)ekkie-Herzen höher schlagen lassen. Faszinierend! ■

Zusätzlicher Schutz durch Entwicklung und Produktion in Deutschland

Technik Made in Germany hat seit jeher einen guten Ruf. Seit Edward Snowden enthüllt hat, dass Produkte ausländischer Hersteller bewusst eingebaute Sicherheitslücken enthalten, um Geheimdiensten den Zugriff zu erleichtern, dürfte der Ruf noch besser geworden sein. Was in Deutschland entwickelt und produziert wird, gilt als sicher. Aktuelle Studien belegen, dass Firmen ihre Kaufentscheidungen danach ausrichten. Von Sabine Baehre, NCP


© matisse - Fotolia.com

Sicherheit ist ein Prozess und kein Produkt. Dieses Mantra kennt jeder IT-Sicherheits-Consultant, der seinen Kunden erklärt, dass eine Firewall und Anti-Virus-Software nicht ausreichen, um ein Netz und die Daten darin zu schützen. Es ist wichtig, ein Gesamtkonzept aufzustellen und bei der Umsetzung immer im Auge zu behalten. Dazu gehört, die schützenswerten Daten zu klassifizieren, ihren Speicherort zu kennen, Risiken zu bewerten und danach Schutzmaßnahmen zu priorisieren. Natürlich sind auch die zur Firmenumgebung und zum Schutzkonzept passenden Sicherheitsprodukte wichtig. In der Vergangenheit wurde bei der Auswahl selten

Laut einer repräsentativen Studie planen zwei Drittel der IT-Entscheider in deutschen Unternehmen, verstärkt IT-Lösungen „Made in Germany" zu nutzen.

auf die Herkunft des Gerätes geachtet. Ob es sich um IT made in USA, Israel oder Deutschland handelte, hatte keine Auswirkungen auf den Entscheidungsprozess. Die Veröffentlichungen von Edward Snowden, der direkte Verbindungen des amerikanischen Geheimdienstes – ob freiwillig oder nicht – mit den Produkten einiger Hersteller belegt hat, haben die Situation verändert. Router und VPN-Gateways aus den USA werden jetzt mit anderen Augen gesehen. Und natürlich kann niemand glauben, dass die USA als einzige zu solchen Mitteln greifen, auch China, UK, Israel und Russland verfügen über aktive Nachrichtendienste.

Konkrete Folgen der Aushorchversuche

Selbst wenn die öffentliche Reaktion bislang überraschend verhalten ausfiel, ist die Besorgnis in den Vorstandsetagen der Unternehmen durchaus spürbar. Mittlerweile zeigt auch eine Untersuchung von Pierre Audoin Consultants greifbare Folgen der NSA-Schnüffelversuche. Laut der repräsentativen Studie „IT Made in Germany – Was wollen deutsche Unternehmen?“ planen zwei Drittel der IT-Entscheider in deutschen Unternehmen, infolge der anhaltenden Sicherheits-Skandale im Umfeld der NSA-Abhöraffäre verstärkt IT-Lösungen „Made in Germany“ zu nutzen. Dabei wollen 44 Prozent ganz sicher entsprechende Lösungen implementieren, während 21 Prozent darüber nachdenken. Die Verteilung ist über alle Unternehmensgrößen praktisch homogen, erstaunlicherweise sind Großunternehmen mit mehr als 500 Mitarbeitern etwas zurückhaltender. Das kann natürlich auch an den meist langfristig abgeschlossenen Wartungs- und Lieferverträgen mit den Herstellern liegen.

Sicherheit und führende Technik

Deutsche Technologiefirmen wie die NCP engineering GmbH waren schon lange vor Edward Snowden und der dadurch gesteigerten Aufmerksamkeit eine gute Adresse für IT-Sicherheit. Das Nürnberger Unternehmen gilt als einer der weltweit führenden Remote-Access-Anbieter. Für die Befragten der Pierre-Audoin-Studie ist vor allem der Aspekt des durchgängig deutschen Firmenstandorts wichtig. 94 Prozent der Befragten legten Wert darauf, dass der Hauptsitz des Unternehmens in Deutschland liegt und kein Near- oder Offshoring betrieben wird.

Für NCP ist der deutsche Standort ein Garant für hervorragend ausgebildete Mitarbeiter. Sie sichern die Führungsposition des Herstellers durch innovative Technik, die gleichzeitig solide und zuverlässig ist. So sind VPN-Clients für alle gebräuchlichen Betriebssysteme, darunter auch Windows 8.1 und Android verfügbar. Die Managementlösung für VPNs wurde mit den speziellen Anforderungen des Administrators im Blick entwickelt, sie kann mit 50 Clients ebenso schnell und effizient umgehen wie mit 10.000. Dementsprechend sind kleine wie große Firmen beim Nürnberger VPN-Spezialisten gut aufgehoben. Erst kürzlich schloss die deutsche Telekom, langjähriger OEM- und Vertriebspartner, einen Vertrag über die Nutzung der VPN-Lösung für die eigenen Mitarbeiter ab. Das Management und die einfach zu bedienende Client-Software wurden dabei besonders hervorgehoben. Dass die VPN-Lösung auch frei von Hintertüren ist, versteht sich bei „Sicherheit Made in Germany“ ohnehin von selbst. □

Die Autorin

Sabine Baehre
Leiterin Presse & Events
NCP engineering GmbH

Neue Ansätze „Made in Germany“ für die „Digitale Souveränität“

In den vergangenen Monaten ist in Deutschland ein neuer politischer und gesellschaftlicher Diskurs über die Chancen und Risiken der Digitalisierung entstanden. Dabei wird auch die Frage gestellt, wie in einer digitalen Welt ein angemessener Schutz der (Grund-)Rechte aller Bürgerinnen und Bürger gewährleistet und wie Unternehmen und wissenschaftliche Einrichtungen effizient vor Wirtschafts-und Industriespionage geschützt werden können. Diese Fragestellungen werden häufig unter dem Begriff „Digitale Souveränität“ diskutiert.

Von Thorsten Höhnke und Jochen Michels, Fujitsu

Ganzheitliche Ansätze gefragt

Möchte man dem Thema IT-Sicherheit umfassend gerecht werden, dann muss man es vom Anfang bis zum Ende betrachten. Hierzu zählen unter anderem:

- Rechenzentren, die für herkömmliche Angriffsmethoden nicht sichtbar und somit nicht attackierbar sind (Stealth Data Center).
- Daten, die der Benutzer zu beliebiger Zeit wieder löschen kann – im Original und mitsamt sämtlicher Kopien.

Sichere Authentifizierung mittels Fujitsu PalmSecure

- Geräte, die abhörsicher sind – und zeigen, wenn jemand sie attackiert.

Auf diese Weise kann eine benutzerfreundliche „transparente Sicherheit“ erreicht werden. Der Nutzer arbeitet wie gewohnt, aber entsprechend der jeweiligen Anwendung, mit den damit verbundenen Sicherheitsanforderungen.

Sichere und benutzerfreundliche Authentifizierung

Ein entscheidender Aspekt beim Thema Sicherheit ist die Authentifizierung. Hier sind Biometrie-Lösungen zukunftsträchtig, da sie höchste Sicherheit bieten und zugleich anwenderfreundlich sind. Fujitsu hat diesbezüglich die Lösung PalmSecure entwickelt, die weltweit im Einsatz ist, etwa im Gesundheitswesen der Türkei, im Bankensektor in Brasilien oder in zahlreichen Flughäfen in Deutschland. PalmSecure ist technisch robuster und sicherer als andere biometrische Lösungen: 10-mal sicherer als ein Scan der Iris im menschlichen Auge, 100-mal sicherer

als die Authentifizierung über einen Fingerabdruck und 1.000-mal sicherer als die Gesichtserkennung.

Ganzheitlich ausgerichtete Ansätze für künftige Sicherheitskonzepte

Angesichts der zahlreichen potenziellen Bedrohungen und der Vielzahl der möglichen Angriffspunkte können Informationen nur dann angemessen geschützt werden, wenn schutzbedürftige Programme und Inhalte vom Rest der IT-Infrastruktur vollständig und mit höchst möglicher Sicherheit abstrahiert werden. Diese „Kapselung" ermöglicht sichere Anwendungen und sichere Datenübertragung selbst in einer unsicheren IT-Umgebung.

Ende-zu-Ende-Verschlüsselung von Daten mit erhöhter Verschlüsselungstiefe

Die sichere Übertragung zwischen Endgerät und Server ist ein weiterer Schlüsselfaktor, weil es hier eine Vielzahl möglicher Angriffspunkte gibt. Gefragt sind daher Sicherheitskonzepte, die auf bestehenden Infrastrukturen aufsetzen können, das gesamte Spektrum abdecken und auch die sichere Anbindung mobiler Endgeräte vereinfachen. Die zentrale Eigenschaft ist die umfassende Verschlüsselung vom einen Ende der Verbindung bis zum anderen – und zwar als homomorphe Ende-zu-Ende-Verschlüsselung.

Bedeutung des Standortes Deutschland

Die deutschen Datenschutz-Gesetze regeln Zugriffe auf sensible Daten eindeutig und verlässlich. Zudem sind sie strenger sowie verbraucher- und wirtschaftsfreundlicher als die Normen in vielen anderen Ländern. Daraus kann ein entscheidender Standortvorteil für IT-Dienstleistungen entstehen, die aus Deutschland heraus erbracht werden. Viele Firmen aus dem europäischen Ausland werden künftig ihre sensiblen Daten explizit in Deutschland gehostet haben wollen. „Made in Germany" wird damit auch zu einem Qualitätsmerkmal für den Standort von Rechenzentren – und ein wichtiger Faktor, den IT-Verantwortliche beim Entwickeln ihrer Sicherheitskonzepte wieder deutlich stärker berücksichtigen.

Forschungsprojekt bei Fujitsu: Digitale Souveränität

Seit rund zehn Jahren arbeiten Fujitsu-Spezialisten an den deutschen Entwicklungsstandorten in Augsburg, Paderborn und München an einem umfassenden Ansatz, der für besonders schutzbedürftige Daten eine bislang nicht erreichte, höchstmögliche Sicherheit bieten soll – durchgängig vom Endgerät über den Transportweg bis hin zum Rechenzentrum. Dabei haben die Entwickler und Ingenieure mögliche Einbruchstellen identifiziert und technische und organisatorische Maßnahmen entwickelt, um diese schließen zu können, z. B.:

- Beim Endgerät: Abstraktion von Hardware und Betriebssystem, Kapselung der Einfallsstellen, Monitoring der Schnittstellen und des Speichers.
- Auf dem Transportweg: homomorphe Ende-zu-Ende-Verschlüsselung, gesteigerte Verschlüsselungsstärke („äußerer" und „innerer" Schlüssel).
- Auf Rechenzentrumsseite: Neuartige Mehrfaktorenabsicherung gegen interne Angriffe, durchgehendes Monitoring und Auditierbarkeit, durchgängige, automatisierte Verschlüsselung, verbesserter Schutz gegen verteilte Angriffe von außen, Absicherung gegen Seitenkanalangriffe. ■

TÜV Rheinland expandiert zum Security-Riesen

Der TÜV Rheinland ist nach eigenen Aussagen der „führende unabhängige Anbieter für Informationssicherheit auf dem deutschen Markt". Olaf Siemens, unter anderem Geschäftsführer der TÜV Rheinland i-sec, erklärt die IT-Security-Strategie.

IT-BUSINESS / Das Interview Dr. Andreas Bergler

Bild: obs/TÜV Rheinland

Weltweit beschäftigt die TÜV Rheinland Group 10.400 Menschen. Seinen Kunden bietet das Unternehmen 2.500 Dienstleistungen rund um Qualität und Sicherheit für Mensch und Umwelt.

ITB: Nach der Akquisition des Security-Dienstleisters Secaron wurde gerade die US-amerikanische OpenSky Corp. übernommen. Damit arbeiten jetzt 270 Spezialisten für IT-Security beim TÜV Rheinland. Welche Rolle spielt das Thema jetzt bei Ihnen?

Siemens: Eine große. Für TÜV Rheinland ist Informationssicherheit eines der wichtigsten strategischen Geschäftsfelder der Zukunft, weil sie für Unternehmen und Organisationen einer der erfolgsentscheidenden Faktoren ist. Wir gehen davon aus, dass die Nachfrage nach externem Know-how angesichts der dynamischen Risikolage noch zunehmen wird. TÜV Rheinland hat seine Gesellschaft für Informationssicherheit bereits 2000 gegründet, seitdem investieren wir in den Ausbau unserer Position in diesem Markt, 2013 haben wir dies noch einmal verstärkt. Seit 2014 sind wir der führende unabhängige Anbieter für Informationssicherheit auf dem deutschen Markt. Auch international streben wir eine führende Rolle an. In den kommenden vier Jahren wollen wir den Umsatz in diesem Bereich noch deutlich steigern.

ITB: Welche Schwerpunkte werden Sie innerhalb der Information Security Business Unit bei TÜV Rheinland setzen?

Siemens: Unsere Spezialisten decken das komplette Spektrum ab: von der Analyse über

Konzeption und Implementierung bis hin zur operativen Unterstützung oder Zertifizierung von Unternehmen. Zu unseren Kerngeschäftsfeldern zählen die Strategische Informationssicherheit, Qualität und Sicherheit für Applikationen und Portale, Mobile und Network Security sowie die IT-Sicherheit in Industrieanlagen und kritischen Infrastrukturen. Das aktuelle Kompetenz- und Leistungs-Portfolio beinhaltet Governance, Risk und Compliance Management, die Konzeption und Implementierung technischer Sicherheitsarchitekturen und -lösungen sowie die Überprüfung von Sicherheitsinfrastrukturen, darunter Penetrationstests und Analysen sowie Audits. Außerdem bieten wir die Zertifizierung von Systemen und Anwendungen an, allerdings nur, wenn wir zuvor keine Beratung geleistet haben. Im laufenden Jahr werden wir uns vor allem auf die Abwehr gezielter komplexer Angriffe, so genannter APTs, konzentrieren, daneben werden Qualität und Sicherheit in der Cloud sowie Application Security und die Absicherung von kritischen Infrastrukturen und Produktionsanlagen für uns eine wesentliche Rolle spielen.

ITB: Wie hat sich das Beratungs- und Zertifizierungsgeschäft in der Informationssicherheit seit den Enthüllungen von Snowden verändert? Sind deutsche Lösungsanbieter jetzt gefragter als vorher?

Siemens: Wir von TÜV Rheinland verzeichnen eine steigende Nachfrage nach Informationssicherheit „Made in Germany". Ob deutsche Lösungsanbieter insgesamt gefragter sind als ausländische Dienstleister, vermag ich nicht zu beurteilen. Es lässt sich allerdings feststellen: Der Begriff „Made in Germany", der im Bereich Produkte für hochwertige Verarbeitung und lange Lebensdauer steht, etabliert sich in der Informationssicherheit immer mehr als Synonym für durchdachte Managementsysteme und Lösungen, die konform sind mit der deutschen Datenschutzgesetzgebung. Und die gilt ja als eine der striktesten der Welt. Viele deutsche Unternehmen wollen und müssen auch auf internationalem Parkett ihre hohen Standards in Datenschutz und Datensicherheit halten, schon aus Gründen der Compliance und natürlich um ihr geistiges Eigentum vor unautorisiertem Zugriff zu schützen. Aber das ist ja kein typisch deutsches Problem, das haben ausländische Unternehmen ja auch.

ITB: Welche Garantien und Sicherheiten kann eine Zertifizierung den Unternehmen geben? Was bringt ihnen ein TÜV-Zertifikat in Bezug auf Informationssicherheit?

Siemens: Anders als ein CE-Zeichen, das auf freiwilligen Angaben des Unternehmens selbst beruht, hat ein Prüfsiegel seitens eines unabhängigen Dritten wie TÜV Rheinland eine ganz andere Aussagekraft: Es stellt Seriosität, Qualität und Sicherheit von Produkten und Dienstleistungen unter Beweis, das gilt auch für die Bereiche Datenschutz und Datensicherheit. Mit einem Zertifikat von TÜV Rheinland demonstrieren Unternehmen gegenüber ihren Kunden, dass ihnen Qualität, Vertrauenswürdigkeit und Transparenz im Business und im Umgang mit den Daten ihrer Kunden wichtig sind und dass sie sehr hohe Anforderungen an Informationssicherheit erfüllen. Im Rahmen der Audits schauen wir uns gründlich um im Unternehmen. Wir prüfen Technologien, Prozesse und Compliance und identifizieren auch mögliche technische Risiken. Und welche Dinge wir jeweils geprüft und zertifiziert haben, kann jeder ⇨

> **Wir verzeichnen eine steigende Nachfrage nach Informationssicherheit Made in Germany.**

nachlesen: Über den Certipedia-Online-Datenbank-Service von TÜV Rheinland sind die Prüfaussagen anhand der Zertifikatsnummer transparent nachvollziehbar.

ITB: Dieses Jahr soll der Handel von IaaS-Ressourcen an der „Deutschen Börse Cloud Exchange" (DBCE) starten. Das Zulassungsverfahren für die Anbieter konzipiert die Deutsche Börse gemeinsam mit TÜV Rheinland. Mit welchem Aufwand ist eine solche Zulassung verbunden und welche Sicherheiten gibt dieses Zertifikat der Zielgruppe mittelständischer Unternehmen?

Siemens: Das Zulassungsverfahren für Provider bei der DBCE ist keine Zertifizierung der Provider, so wie sie TÜV Rheinland etwa mit „Certified Cloud Services" anbietet. Dieses Zertifikat gehört zu den weltweit weitreichendsten Prüfstandards für Qualität in der Datenwolke, entwickelt auf Basis von ISO 27001, BSI-Grundschutz und ITIL.

Natürlich kann man nicht erwarten, dass alle Anbieter der DBCE zertifiziert sind. Aber Provider werden sich um Qualitätssicherung und deren Nachweis bemühen müssen, wenn sie dauerhaft Erfolg am Markt haben wollen. Für das Vertrauen in den Handelsplatz ist es wichtig, dass sich ein unabhängiger, sachverständiger Dritter bestimmte Schlüsselfragen der IT-Sicherheit zuvor gründlich angesehen hat. Im Standard-Verfahren werden die wichtigsten Kriterien aus allen Bereichen wie Technik, Organisation und Compliance abgeprüft. Das sind die Punkte, die wir auch im Rahmen einer Zertifizierung im Fokus haben. Wenn es um den Einsatz von Cloud Services in kritischen Enterprise-Umgebungen geht, sehen wir mit der Deutschen Börse Cloud Exchange ein detailliertes Prüfverfahren vor, das dann auch eine technische Sicherheitsanalyse sowie eine Prüfung von Architektur und Prozessdetails vorsieht.

Unternehmen können auf dem Cloud Marketplace also ein hohes Maß an Sicherheit, Qualität und Zuverlässigkeit beim jeweiligen Provider voraussetzen, wenn er das Zulassungsverfahren durchlaufen hat. Und daran haben sie schließlich auch ein berechtigtes Interesse, denn sie müssen ihren gesetzlichen Pflichten gegenüber dem Provider und ihren Kunden nachkommen, wenn sie die Cloud nutzen. □

Zur Person

Bild: Lothar Wels 2014

Olaf Siemens will mit der TÜV Rheinland i-sec das komplette IT-Security-Spektrum aus einer Hand abdecken.

Olaf Siemens ist Global Vice President Information Security beim TÜV Rheinland und Geschäftsführer der TÜV Rheinland i-sec, der auf Informationssicherheit spezialisierten Gesellschaft bei TÜV Rheinland.

TÜV Rheinland i-sec

TÜV Rheinland bietet Beratung und Lösungen in allen wichtigen Schlüsselbranchen an, darunter Finanzdienstleistungen, Industrie, Logistik, Automotive, Luft- und Raumfahrt, außerdem IT-Dienstleister und Telekommunikation. Zu seinen Kunden gehören Unternehmen wie zum Beispiel die Deutsche Börse Cloud Exchange, die Commerzbank, die Sparkassen-Finanzinformatik, Siemens oder Vodafone sowie eine Reihe weiterer großer und mittelständischer Unternehmen, die auf internationalen Märkten tätig sind. TÜV Rheinland begleitet bereits heute zwei von drei DAX-30-Unternehmen. Außerdem unterstützen die Experten für Informationssicherheit Einrichtungen des Bundes und der Länder in Datenschutz und Datensicherheit sowie der Einhaltung von Compliance.

Selbsttest zum Datenschutz für Unternehmen

Mit Hilfe des Datenschutzindikators von TÜV Süd können Unternehmen selbst prüfen, wie gut sie in Sachen Datenschutz aufgestellt sind und an welchen Stellen Verbesserungspotenzial besteht.

SECURITY-INSIDER / Elke Witmer-Goßner

Bild: Doc Rabe Media - Fotolia.com

Bereits 2011 und 2012 haben Studien des TÜV Süd in Zusammenarbeit mit der Ludwig-Maximilians-Universität München (LMU) gezeigt, dass gerade bei kleinen und mittelständischen Unternehmen noch Handlungsbedarf besteht. Daher stellt die TÜV Süd Sec-IT GmbH jetzt, unterstützt durch die LMU, die Plattform TÜV Süd Datenschutzindikator (DSI) vor. Unter www.datenschutzindikator.de können Unternehmen selbst einen ersten Test vornehmen, wie sie in Sachen Datenschutz aufgestellt sind.

Der Fragebogen des TÜV Süd DSI berücksichtigt die wesentlichen Grundaspekte des Datenschutzmanagements. Die Fragestellungen sollen den Unternehmen bei der Selbsteinschätzung helfen, damit sie sich ein Bild davon machen können, in welchen Bereichen des Datenschutzes sie noch Nachholbedarf haben.

Die Ergebnisse geben einen ersten Überblick über den Status Quo des implementierten Datenschutzes, weisen auf Umsetzungsdefizite hin und identifizieren Handlungsbedarf. Unternehmen erlangen so eine erste Einschätzung, ob risikobehaftete Abweichungen zu gesetzlichen Vorgaben bestehen.

Anhaltspunkte für Schwachstellen

Mit TÜV Süd DSI aktuell wird zusätzlich in regelmäßigen Abständen ein aktuelles datenschutzrelevantes Thema aufgegriffen und eine Einschätzung dazu abgefragt. Die Kurzumfrage kann unabhängig von der Selbstbewertung ausgefüllt werden. Teilnehmer können so ihre Meinung zum Thema in eine Gesamtbewertung mit einfließen lassen. Weitere Informationen zum Thema Datenschutz erhalten Interessenten unter www.tuev-sued.de/sec-it oder unter der kostenlosen Rufnummer 0800/5791-5005.

„Die Fragestellungen des TÜV Süd DSI haben eine hohe Praxisrelevanz, da unsere Erfahrungen aus der Beratung und Prüfung mit eingeflossen sind. Unternehmen können damit Defizite identifizieren und erste Verbesserungen vornehmen“, erklärt Rainer Seidlitz, Prokurist der TÜV SÜD Sec IT GmbH. „Langfristig ist es unser Ziel, auch einen Benchmark anzubieten, der eine Positionierung des eigenen Datenschutzes im Vergleich zu anderen Unternehmen erlaubt. Allerdings ist das Ergebnis nur als erster Anhaltspunkt zu sehen und ersetzt in keinem Fall eine umfassende Ist-Analyse“, betont Seidlitz. □

Net at Work enQsig:
E-Mails einfach und sicher auf dem Gateway verschlüsseln

www.netatwork.de

Seit Edward Snowden wird das Thema E-Mail-Verschlüsselung wieder heiß diskutiert: Täglich tauchen im Netz neue Kommentare, Threads und FAQs mit Tipps zum sicheren E-Mail-Versand auf. So unterschiedlich die Meinungen dabei sind, ist der Tenor der Diskussionen meist der gleiche: Ja, Verschlüsselung ist wichtig und richtig – aber auch aufwändig und unflexibel. Also verzichtet man darauf und riskiert sehenden Auges das Wohl seines Unternehmens. Dabei muss E-Mail-Verschlüsselung gar nicht kompliziert sein: Mit dem Verschlüsselungs-Gateway enQsig von Net at Work lässt sich die E-Mail-Kommunikation des Unternehmens einfach und transparent auf einem vorgelagerten E-Mail-Gateway verschlüsseln – ohne dass die Anwender eingreifen müssten.

Schlüsselverwaltung sicher und flexibel

Spricht man mit Security-Administratoren, wird schnell klar, dass diese nicht etwa die eigentliche E-Mail-Verschlüsselung, sondern vor allem die Schlüsselverwaltung als herausfordernd ansehen: Immerhin muss für eine sichere Verschlüsselung auf jedem Client-PC zum einen der private Schlüssel des Absenders verfügbar sein, um eine Signatur erstellen und eingehende E-Mails entschlüsseln zu können. Zum anderen benötigt der Absender auch den öffentlichen Schlüssel des Empfängers, damit die E-Mail verschlüsselt werden kann. Selbst in der einfachsten Ausbaustufe ist eine solche client-seitige Verschlüsselung relativ aufwändig zu implementieren und zu betreiben. Hinzu kommt, dass viele Benutzer mehrere Geräte für den Empfang und Versand ihrer E-Mails nutzen – und der Einsatz mobiler Endgeräte im Hinblick auf das Handling der privaten Schlüssel ohnehin Fragen aufwirft.

enQsig vermeidet diese unnötige Komplexität, indem Verschlüsselung und Schlüsselverwaltung auf einem zentralen Gateway zusammengeführt werden. Die Lösung vereint damit ein Höchstmaß an Sicherheit mit hoher Flexibilität: Da alle Schlüssel im geschützten Schlüsselspeicher des Gate-

ways liegen, können Benutzer ohne Zusatzinstallation von jedem beliebigen Endgerät aus die Verschlüsselungs- und Signaturfunktion nutzen. Auch bei der Wahl des Verschlüsselungsstandards setzt enQsig auf prinzipielle Offenheit: Die Lösung unterstützt sowohl S/MIME als auch PGP. Dabei können für jeden Benutzer ein S/MIME-Zertifikat und ein PGP-Schlüssel hinterlegt werden. enQsig wählt dann automatisch das passende Verfahren.

Wichtig im Hinblick auf die Durchsetzung Ihrer Unternehmensrichtlinien: Das Regelwerk von enQsig garantiert, dass diese zuverlässig durchgesetzt werden. So lässt sich zum Beispiel sicherstellen, dass E-Mails, die zwingend verschlüsselt werden müssen, das Unternehmen auch freitags um 18:30 Uhr nicht unverschlüsselt verlassen.

PDF-Mail und Large File Transfer

Falls ein Kommunikationspartner weder S/MIME noch PGP einsetzt, bietet enQsig alternativ ein zertifikatsloses Verfahren an. Dabei wird die E-Mail in ein PDF-Dokument konvertiert und mit einem Passwort verschlüsselt, das der Empfänger auf dem Web Portal von enQsig hinterlegt hat. Das Web Portal kann darüber hinaus auch für eine Antwort auf die PDF-Mail verwendet werden.

Des Weiteren ermöglicht das Web Portal auch die einfache Übertragung großer Dateien. Beim „Large File Transfer“ wird die zu übertragende Datei einfach mit Hilfe eines Outlook Add-Ins aufs Portal übertragen. Der Empfänger erhält einen verschlüsselten Link zur Datei auf dem Web Portal und kann sie über eine verschlüsselte Verbindung herunterladen. Dies entlastet sowohl den Mailserver des Empfängers als auch die eigene Infrastruktur.

Fazit

Mit den Net at Work Gateway Solutions bietet Net at Work nicht nur einen umfassenden Schutz Ihrer E-Mail-Infrastruktur, sondern darüber hinaus eine einfache und sichere Möglichkeit, E-Mail-Verschlüsselung flächendeckend zu implementieren.

S/MIME vs. PGP

Im Bereich E-Mail-Verschlüsselung haben sich die Standards S/MIME und PGP durchgesetzt. Beide verwenden größtenteils dieselben Blockchiffren wie AES oder 3DES. Ausschlaggebend für die Qualität der Verschlüsselungslösung ist in der Praxis vor allem die sachgemäße Implementierung dieser Standards: Auch eine AES256 verschlüsselte E-Mail ist leicht zu knacken, wenn AES unsachgemäß implementiert wurde. Dies fängt bereits beim Zufallszahlengenerator an.

Der entscheidende Unterschied zwischen S/MIME und PGP liegt in der Vertrauenswürdigkeit der verwendeten Schlüssel. Bei PGP muss jeder Schlüssel einzeln auf die korrekte Identität überprüft werden. S/MIME hingegen basiert auf X.509 Zertifikaten und einem hierarchischen System. Dabei übernehmen Zertifizierungsstellen (CA's) die Überprüfung der Identität. Vertraut man einer solchen CA, vertraut man automatisch allen Zertifikaten, die von ihr signiert wurden. Im deutschsprachigen Raum hat sich im Unternehmensumfeld das S/MIME Verfahren deutlich stärker durchgesetzt, da PGP nur zum Teil in RFCs standardisiert wurde.

Net at Work GmbH
T +49 5251 304-600 www.netatwork.de
F +49 5251 304-650 info@netatwork.de

Die „gefühlte IT-Sicherheit“ in Zeiten der Rundumüberwachung

Wem schenke ich Vertrauen? Wie ermittle ich Vertrauenswürdigkeit? Fragen wie diese sind in der IT-Security-Branche aktueller denn je. Ralf Nitzgen, Chef der Allgeier IT Solutions, ist auch auf das Vertrauen seiner Kunden angewiesen. IT-BUSINESS sprach mit ihm über die Zeit nach Snowden.

IT-BUSINESS / Das Interview führte Dr. Stefan Riedl

Wie sicher sind die Daten dieser Welt?

ITB: Spähprogramme wie Prism und Tempora sind in aller Munde. Und vieles deutet darauf hin, dass neben dem Ausspähen durch die Geheimdienste auch Wirtschaftsspionage betrieben wird. Wie beurteilen Sie die Situation?

Nitzgen: Letztendlich ist diese Gesamtsituation nicht grundsätzlich neu, denn auch das Spionagenetz Echelon, das seit über zehn Jahren unter anderem von den USA, Großbritannien, Australien und Kanada betrieben wird, hat die Massendatenspeicherung und das Abhören von Kommunikationskanälen zur Aufgabe. Der Verwendungszweck dieses Netzes ist bereits 2004 öffentlich bekannt gegeben worden. Auch ist das Recht zur Wirtschaftsspionage einiger Staaten seit jeher in der Verfassung verankert. Vor dem Hintergrund ist mit den aktuellen Enthüllungen in Verbindung mit einer hohen medialen Aufmerksamkeit dieses Thema in das öffentliche Bewusstsein gelangt, das an und für sich schon seit vielen Jahren auf breiter Basis praktiziert wird. Gleichwohl stellen diese Spähprogramme für die hiesige Wirtschaft eine ernsthafte Bedrohung dar. Unternehmen sind daher spätestens heute gefordert, geeignete Sicherheitsmaßnahmen zu betreiben.

ITB: Zu den Snowden-Enthüllungen zählt auch das sogenannte „Project Bullrun“, das offenbar sogar SSL-Verschlüsselung knacken kann. Wie ist dazu Ihre Einschätzung?

Nitzgen: Man muss an der Stelle etwas differenzieren. In den meisten öffentlich gewordenen Fällen sind die Angriffe auf Schwächen bei der Umsetzung der Sicherheitsmechanismen und nicht auf Schwächen des zugrundliegenden Verfahrens zurückzuführen.

Das Verfahren der SSL- beziehungsweise der asymmetrischen Verschlüsselung ist nach dem heutigen Stand der Kryptografie-Wissenschaft nach wie vor nicht ohne weiteres „knackbar". Es gibt zwar die Möglichkeit einer sogenannten Man-in-the-Middle-Attacke. Dieser Zugriff kann allerdings nicht unbemerkt erfolgen – es sei denn, dass der Herausgeber des jeweiligen SSL-Zertifikats seinerseits Schlupflöcher zur Manipulation des Authentifizierungsvorgangs eingebaut hat. Sofern die Art und Weise, wie die Schlüsselpaare zufällig erzeugt werden, nicht manipuliert wird oder die Parteien vor einem unbefugten Zugriff geschützt sind, sind SSL- beziehungsweise TLS-Verschlüsselungen weiterhin sicher. Das Gebot der Stunde lautet daher hier nach wie vor, auf eine möglichst starke Verschlüsselung – auch hiesiger Zertifikatshersteller – zu setzen und die ordnungsgemäße Umsetzung des Verfahrens zu gewährleisten.

ITB: Wie wird es in den nächsten Monaten und Jahren weitergehen im Hinblick auf die Datenschnorchelei?

Nitzgen: Die Umsetzung geeigneter politischer Maßnahmen ist in großem Maße von der Sensibilität und dem Druck der Wirtschaft gegenüber der Datenschnorchelei abhängig. Viele Unternehmen sind erst durch die jüngsten Enthüllungen sensibilisiert worden, über Compliance und Anforderungen des Datenschutzgesetzes nachzudenken und geeignete Maßnahmen zum Schutz der eigenen Datenhoheit zu ergreifen. Andere Unternehmen hingegen stehen den Spähprogrammen gelassen gegenüber, da sie über ihre kritischen Unternehmensdaten hinaus vermeintlich nichts zu verbergen haben. Hier wird letztlich die Datensicherheit zugunsten des eigenen Komforts geopfert.

Solange also keine klaren gesetzlichen Schutzmechanismen oder politischen Einschränkungen bestehen, ist jedes Unternehmen für sich gefordert, entsprechende Schutzmaßnahmen gegen die Wirtschaftsspionage zu ergreifen – je nachdem, wie wichtig ihnen die Compliance und der Schutz ihrer Daten sind. Ich bin jedoch der Meinung, dass die heutige Gesetzeslage Unternehmen geradezu dazu zwingt, über geeignete Sicherheitsstrukturen nachzudenken, um ihr geistiges Eigentum vor Zugriffen Dritter zu schützen.

ITB: US-Anbieter können dazu gezwungen werden, mit Geheimdiensten zu kooperieren. Vor diesem Hintergrund scheint sich vielerorts ein Generalverdacht gegenüber US-Anbietern zu etablieren. Ist das aus Ihrer Sicht gerechtfertigt, und was bedeutet das für Anbieter mit Rechtsstand in Deutschland?

Nitzgen: Ob dies gerechtfertigt ist oder nicht, darüber möge sich jeder selbst ein Bild verschaffen. Tatsache ist jedoch, dass es so etwas wie „gefühlte Sicherheit" zu geben scheint. Und in diesem Zusammenhang haben viele, auch international aufgestellte Kunden bereits in der Vergangenheit europäischen Sicherheitslösungen den Vorzug gegenüber Lösungen von US-Anbietern oder von Anbietern aus anderen Ländern gegeben, denen gegenüber es ähnliche Vorbehalte zu geben scheint. Deswegen glaube ich, dass sich diese Faktoren durchaus positiv für die Vermarktung europäischer Security-Lösungen auswirken werden. □

Zur Person

Bild: Allgeier IT Solution

Ralf Nitzgen ist Geschäftsführer der Allgeier IT Solutions GmbH aus Bremen. Das 1977 gegründete Unternehmen ist Teil der börsennotierten Allgeier SE und hat sich unter anderem auf Lösungen in den Bereichen Cloud Solutions sowie Compliance & Security spezialisiert.

LANCOM Systems

Standort Deutschland: Tragende Säule in der IT-Sicherheit

Mit Snowdens Enthüllungen der Überwachung durch US-amerikanische Geheimdienste erfuhr das Thema IT-Sicherheit im Jahr 2013 eine bisher unbekannte Brisanz. Insbesondere deutsche Unternehmen suchen seitdem verstärkten Schutz vor Gefahren aus dem Internet. Vertrauenswürdige Kommunikations- und Netzwerktechnik „Made in Germany“ hat somit einen völlig neuen Stellenwert gewonnen.

Diese Philosophie verfolgt der führende deutsche Netzwerkhersteller für Geschäftskunden und den öffentlichen Sektor, LANCOM Systems, bereits seit der Gründung im Jahre 2002. Das Credo „Made in Germany“ gilt für den gesamten Entwicklungs- und Produktionsprozess. Die VPN-Router und Wireless LAN-Lösungen von LANCOM werden in Deutschland entwickelt und gefertigt. Beratung, Support und Service kommen ebenfalls aus Aachen. LANCOM ist damit ein Exot im positiven Sinne: Der Netzwerkmarkt an sich ist stark asiatisch und US-amerikanisch geprägt.

Für LANCOM-Kunden ist „Made in Germany“ daher viel mehr als nur ein Qualitätsmerkmal. „Made in Germany“ steht für Produkte, die nach höchsten Sicherheits- und Datenschutzstandards in Deutschland entstehen. Von der Hardware bis zum eigenen Betriebssystem, das vollständig von LANCOM entwickelt wurde und frei von externer Einflussnahme und fremdem Quellcode ist. Nicht zuletzt hierdurch kann LANCOM seinen Kunden garantieren, dass LANCOM VPN- und Wireless LAN-Lösungen frei von versteckten Zugangsmöglichkeiten – sogenannten Backdoors – sind. Diese Hintertüren können von Cyber-Kriminellen und Geheimdiensten missbraucht werden, um auf fremde Netze zuzugreifen.

LANCOM ist darüber hinaus der einzige Router-Hersteller, der ein Sicherheitszertifikat des Bundesamtes für Sicherheit in der Informationstechnik (BSI) besitzt. 2013 ließ das Unternehmen einen Teil seines VPN-Portfolios erfolgreich nach den Common Criteria überprüfen. Setzen Unternehmen und Institutionen diese Lösungen verstärkt ein, wird die digitale Souveränität Deutschlands erhöht. „Made in Germany“ entwickelt sich zum neuen Gütesiegel. ■

LANCOM
Systems

Unser Versprechen für Ihr Netzwerk

- ✓ Höchste Sicherheit
- ✓ Maximale Zuverlässigkeit
- ✓ Volles Vertrauen

it sa 2014

Die IT-Security Messe und Kongress
The IT Security Expo and Congress

Besuchen Sie uns vom
7. – 9. Oktober 2014
auf der **it-sa** in Nürnberg:
Halle 12, Stand 332

ANWENDUNGEN
- VPN-Standortvernetzung / -Filialvernetzung
- Sicherer Internetzugang
- Anbindung mobiler Mitarbeiter

PORTFOLIO
- Kompakte VPN-Router
- Performante zentralseitige VPN-Gateways
- Für Ethernet, Glasfaser, ADSL, LTE etc.

ZERTIFIZIERUNG
- BSI-Zertifizierung nach Common Criteria EAL 4+
- Umfang: IPSec VPN, Firewall, Virtualisierung, Routing, Backup & Redundanz, Management

SICHERHEITSVERSPRECHEN
- Eigens entwickeltes Betriebssystem LCOS
- Hard- und Software entwickelt und gefertigt in Deutschland
- Garantiert Backdoor-frei

www.lancom-systems.de/**it-sa**

LANCOM Systems GmbH | Würselen | Deutschland | Telefon +49 (0)2405 49936 0 | Fax +49 (0)2405 49936 99 | info@lancom.de

Hochsensibel wird hoc
Mit secunet in KRITIS.

Kritische Infrastrukturen (KRITIS) wie beispielsweise Wasser- und Energieversorgung sind für eine Gesellschaft von existenzieller Bedeutung. Gleichzeitig sind sie mehr denn je von einer reibungslosen Informations- und Kommunikationstechnik abhängig. secunet schützt diese Infrastrukturen vor Cyberangriffen nachhaltig und ganzheitlich mit professionellen IT-Sicherheitsstrategien und Produkten wie SINA. Damit aus kritisch nicht dramatisch wird!

Klingt unmöglich? Testen Sie uns!
www.secunet.com/kritis

hsicher.

secunet

IT-Sicherheitspartner der Bundesrepublik Deutschland

Elektronische Post vor unerwünschten Blicken schützen

Die Möglichkeiten der E-Mail-Verschlüsselung sind vielfältig.

Bild: Andrea Danti - Fotolia.com

Ohne Verschlüsselung lässt sich jede E-Mail durch Dritte mitlesen. Vor dem Hintergrund der aktuellen Diskussion um Spionagefälle wie PRISM wird es höchste Zeit, das zu verhindern. Dieser Beitrag nennt die unterschiedlichen Verfahren und passende Lösungen.

Von Oliver Schonschek

Die Diskussion um PRISM und andere Geheimdienst-Aktivitäten gibt den Bemühungen um die Verschlüsselung von E-Mails neuen Auftrieb. Initiativen wie „E-Mail made in Germany“ werden zum Beispiel vom Bundesamt für Sicherheit in der Informationstechnik begrüßt.

Die Web-Mail-Dienste von T-Online, gmx.de und web.de bieten nun im Standard eine SSL-Verschlüsselung an. Betrachtet man aber E-Mail insgesamt, wird deutlich, dass für sichere E-Mails mehr erforderlich ist. Zum einen gibt es noch weitaus mehr Mail-Provider als die bisherigen Mitglieder der Initiative. Zum anderen bietet SSL nur eine Transport-Verschlüsselung der elektronischen Nachrichten.

De-Mail: Datenschützer empfehlen zusätzliche Verschlüsselung

Auch die Verschlüsselung bei De-Mail alleine reicht Sicherheitsexperten z.B. von NIFIS und den Datenschützern nicht. So werden De-Mails vor der Weiterleitung an den Empfänger kurzfristig automatisch entschlüsselt, da die De-Mail-Diensteanbieter verpflichtet sind, De-Mails auf Schadsoftware zu prüfen. Eine durch-

gehende Ende-zu-Ende-Verschlüsselung ist nur dann möglich, wenn Versender und Empfänger eine Verschlüsselungssoftware benutzen, mit der die De-Mail ver- und entschlüsselt wird.

E-Mail-Verschlüsselung mit Hindernissen

Für die fehlende Verschlüsselung von E-Mails gibt es verschiedene Gründe: Rund zwei Drittel (65 Prozent) der Internetnutzer geben in der genannten BITKOM-Umfrage an, sich mit Programmen zur E-Mail-Verschlüsselung nicht auszukennen. Bei 59 Prozent setzt der Kommunikationspartner keine entsprechende Software ein. Ein Viertel (24 Prozent) hält Verschlüsselung grundsätzlich für zu aufwändig.

Viele Wege führen zur E-Mail-Verschlüsselung

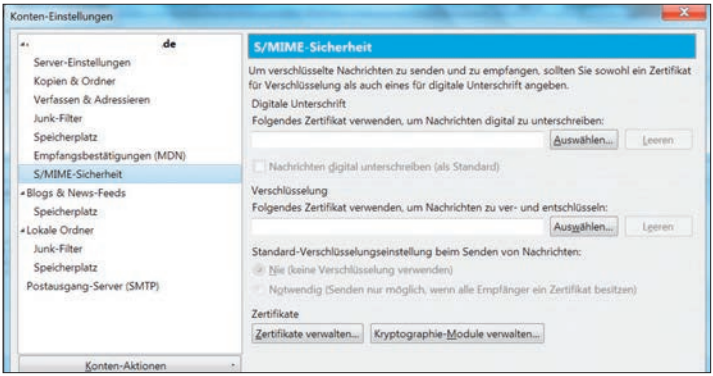
In Anbetracht der Möglichkeiten muss man erst einmal feststellen, dass es nicht die E-Mail-Verschlüsselung als solches gibt, sondern verschiedene Verfahren. Ein Grund für die geringe Verbreitung von E-Mail-Verschlüsselung liegt auch in der Mannigfaltigkeit der Verschlüsselungsmethoden begründet, denn Absender und Empfänger einer verschlüsselten E-Mail müssen jeweils das Verfahren des anderen beherrschen und unterstützen.

OpenPGP zum Beispiel nutzt zur Verschlüsselung und Entschlüsselung von E-Mails vom Nutzer erstellte Schlüsselpaare. Der öffentliche Schlüssel muss ausgetauscht werden, damit der Absender diesen zur Verschlüsselung nutzen kann. Möglich ist auch eine Veröffentlichung des Public Keys auf der Firmen-Webseite oder in zentralen Verzeichnissen. Der Empfänger verwendet seinen geheimen Private Key zur Entschlüsselung.

S/MIME hingegen setzt bei der E-Mail-Verschlüsselung auf X.509-Zertifikate, die durch Zertifizierungsstellen ausgegeben werden, und ist nicht mit OpenPGP kompatibel. Sender und Empfänger müssen also beide das gleiche Verfahren nutzen, OpenPGP oder S/MIME.

Schlüsselverwaltung

Zur Verwaltung der Schlüssel oder Zertifikate betreiben Unternehmen oft eine PKI (Public Key Infrastructure), mit der ein nicht unerheblicher Aufwand verbunden ist. Bei der identitätsbasierten E-Mail-Verschlüsselung (Identity Based Encryption, IBE) wird die E-Mail-Adresse des Empfängers als öffentlicher Schlüssel genutzt, ein Schlüsselaustausch zwischen Sender und Empfänger ist deshalb überflüssig. Dafür müssen beide Kommunikationspartner aber die gleiche Lösung im Bereich IBE unterstützen.



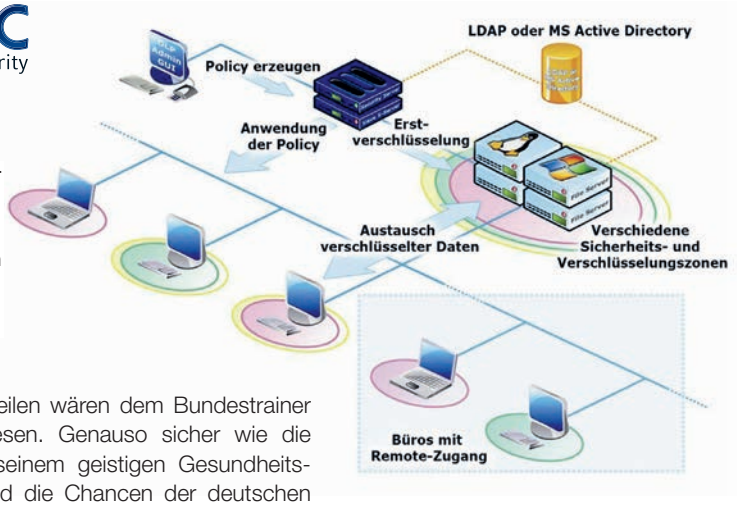
Ein E-Mail-Client wie Thunderbird oder Outlook und ein digitales Mail-Zertifikat reichen, um mit der E-Mail-Verschlüsselung (S/MIME) zu beginnen. Doch viele Nutzer scheuen den Aufwand oder wissen nicht, wie es funktioniert.

Bild: Screenshot

Daten ohne Verschlüsselung ist wie Fußball ohne Torwart

Die FIFA WM™ 2014 ist Geschichte und bescherte Deutschland den ersehnten vierten Stern. Ein Garant des Erfolges war Torwart Manuel Neuer. Jetzt stelle man sich einmal vor, der Bundestrainer hätte vor der WM verkündet, dass Deutschland ganz ohne Torwart zur Weltmeisterschaft fahre mit der Begründung, man habe ja schließlich genug Abwehrspieler!

apeec applied security



Moderne Verschlüsselungssysteme wie fide*AS*® file enterprise schützen Daten unternehmensweit.

Die Schlagzeilen wären dem Bundestrainer sicher gewesen. Genauso sicher wie die Zweifel an seinem geistigen Gesundheitszustand. Und die Chancen der deutschen Fußballnationalmannschaft auf den WM-Titel wären gleich Null gewesen.

Wie ist es aber dann zu erklären, dass bei einem ganz anderen Thema, nämlich dem der Sicherheit vertraulicher Daten, oft ganz ähnlich argumentiert wird? Hier verzichten nämlich viele Betriebe darauf, wichtige Dokumente zu verschlüsseln mit dem Hinweis, man sei durch Firewall und Virenscanner bereits gut genug gegen Hacker und Spione geschützt.

Zwei Verteidigungslinien sind besser als eine

Eine Firewall dient bekanntlich dem Schutz eines Netzwerks gegen Eindringlinge von außen. In der Fußball-Analogie ist die Firewall das, was die Abwehrmauer beim Freistoß des Gegners ist. Beim Fußball ist die zweite wichtige Verteidigungslinie der Torwart, in der IT sollte das die Verschlüsselung der Daten sein. Sie ist nur allzu oft nicht vorhanden. Besonders selten wird über den Schutz

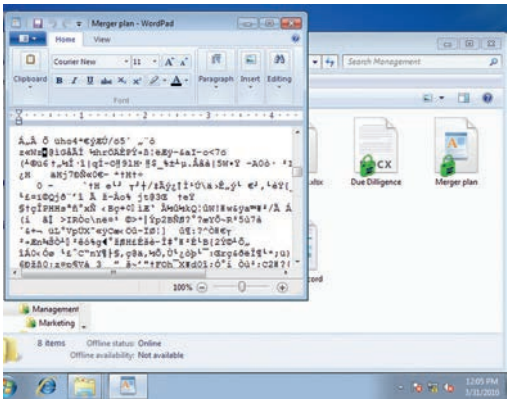
von Fileservern, Backupsystemen oder fest installierten Arbeitsplätzen nachgedacht. Darauf angesprochen, reagieren viele IT-Verantwortliche mit dem altbekannten Irrglauben, bei ihnen käme schon kein Hacker rein, man brauche so etwas wie interne Verschlüsselung nicht. Diese IT-Verantwortlichen spielen ohne Torwart!

Eigentore

Gelegentlich kommt es vor, dass ein Fußballer versehentlich ins eigene Tor trifft. Sogar Franz Beckenbauer kann in seiner glanzvollen Karriere auf nicht weniger als vier Eigentore zurückblicken. Trotzdem kommt ein solches Missgeschick beim Fußball relativ selten vor. Viel häufiger kommt es jedoch vor, dass ein eigener Mitarbeiter eines Unternehmens vertrauliche Daten versehentlich verliert oder in die falschen Hände spielt, bildlich gesprochen also ein Eigentor erzielt. Es ist eine statistisch erwiesene Tatsache, dass vier von fünf IT-Sicherheitsverletzungen auf menschliche Fehler innerhalb des Unternehmens zurückzuführen sind. Sind vertrauliche Unternehmensdaten erst einmal in die falschen Hände geraten, lässt sich das Rad nicht mehr zurückdrehen. Je nach Art der Daten können dem Unternehmen finanzielle Verluste, Imageverlust oder schwere rechtliche Konsequenzen drohen. Hier bietet eine Verschlüsselung von Daten mit einem zentralen Zugriffsrechtemanagement wie fide*AS*® file enterprise von apsec auch eine Schutzfunktion für die eigenen Mitarbeiter.

Geschlossene Mannschaftsleistung

Die deutsche Fußball-Nationalmannschaft verdankt ihren Erfolg, neben dem Torwart, vor allem einer geschlossenen Mannschaftsleistung. Auch IT-Sicherheit ist ganzheitlich zu betrachten. Der Schutz vor Hackern ist genauso wichtig, wie der Schutz gegen unabsichtliche Fehler, der Schutz gegen den Verlust von Daten auf Laptops und USB Sticks genauso wichtig wie der gegen den Verlust von Daten im Rechenzentrum oder in der Cloud. Überall hier kann fide*AS*® file enterprise helfen.



Mit fide*AS*® file enterprise verschlüsselte Daten sind für Datendiebe wertlos.

„Fußball ist wie Schach ohne Würfel“

Möglicherweise hat der Zitatengeber Lukas Podolski diese Aussage getätigt, nachdem die Anweisung des Trainers etwas zu kompliziert ausgefallen war. Zu komplexe Systeme sind nicht beherrschbar, weder auf dem grünen Rasen, noch in der IT. Diesem Grundsatz folgt auch fide*AS*® file enterprise. Einfache Administration bei der Verschlüsselung, klare verständliche Anweisungen beim Fußball, so gewinnt man das Spiel. ■

Der Autor Dr. Volker Scheidemann ist Direktor Marketing & Produktmanagement bei der Applied Security GmbH (www.apsec.de)

Zentrale Verschlüsselungs-Gateways helfen dabei, verschiedene Verschlüsselungsarten und Nutzertypen in die E-Mail-Verschlüsselung einzubinden.

↪ Alternativ können E-Mails auch auf Basis von Passwörtern ver- und entschlüsselt werden, ohne dass eine PKI notwendig ist. Allerdings muss das Passwort dann auf einem separaten, sicheren Weg übermittelt werden. Zudem entscheidet die Passwortstärke über die Sicherheit der E-Mail-Verschlüsselung.

Die genannten Verfahren werden in verschiedenen Verschlüsselungsprodukten umgesetzt, die dabei unterschiedliche Ansätze verfolgen: wie eine Verschlüsselung im Mail-Client, eine serverbasierte Verschlüsselung oder eine Verschlüsselung als Cloud-Dienst.

1. Verschlüsselung im E-Mail-Client

Die meisten E-Mail-Programme, darunter Microsoft Outlook und Mozilla Thunderbird, unterstützen eine Verschlüsselung mit S/MIME und können E-Mail-Zertifikate importieren. Zusatzprogramme wie GnuPG, Enigmail und das vom BSI beauftragte Gpg4win ergänzen die S/MIME-Funktionen der E-Mail-Clients um eine Verschlüsselung nach OpenPGP. Trotzdem tun sich viele Anwender erfahrungsgemäß damit schwer und halten den Aufwand für die Einrichtung für zu hoch. Alternativ bieten zahlreiche Anwendungsprogramme wie zum Beispiel Office-, PDF- und ZIP-Lösungen eine Passwortverschlüsselung an. Diese Verschlüsselung betrifft dann aber nur den Dateianhang und nicht die komplette E-Mail, mit der die verschlüsselte Datei verschickt wird.

Auch für Smartphones und Tablets gibt es Apps zur E-Mail-Verschlüsselung, zum Beispiel my Secure Mail als separaten E-Mail-Client oder totemomobile PushedPDF Reader, mit dem Empfänger die E-Mails entschlüsseln und bearbeiten können, die über das totemomail Encryption Gateway als verschlüsselte PDF-Datei verschickt wurden.

2. Verschlüsselung bei Web-Mail

Web-Mail-Dienste wie die Outlook Web App unterstützen keine Verschlüsselung mittels S/MIME, sondern verschlüsseln mit TLS/SSL. Deshalb können zum Beispiel Outlook-Anwender und Nutzer von Outlook Web App keine S/MIME-verschlüsselten E-Mails austauschen.

Bereits vor der eingangs genannten Initiative „E-Mail made in Germany“ haben Web-Mail-Anbieter wie Gmail.com eine Verschlüsselung über SSL angeboten bzw. automatisch aktiviert. Bei Web-Mail handelt es sich allerdings um Cloud-Lösungen, bei denen nicht nur der

Transport der E-Mail, sondern auch die E-Mail-Speicherung in der Cloud gesichert und dem deutschen oder europäischen Datenschutz entsprechend behandelt werden muss.

T-Online, Gmx.de und Web.de verweisen auf ihre Rechenzentren in Deutschland und damit auf die Anwendung des Bundesdatenschutzgesetzes. Da kaum ein Unternehmen nur Web-Mail-Dienste einsetzt, kann diese Form der E-Mail-Verschlüsselung nur eine Ergänzung sein.

3. Zentrale Verschlüsselung am Gateway

Unternehmen, die die E-Mail-Verschlüsselung zentral auf ihren Servern oder mit einer selbst betriebenen Appliance durchführen, müssen zwar in die E-Mail-Sicherheit investieren. Sie entlasten aber die einzelnen Nutzer von den Verschlüsselungsaufgaben, die Administratoren von lokalen Installationen und stellen durch eine automatische Verschlüsselung sicher, dass die Nutzer nicht doch vertrauliche E-Mails ungeschützt versenden.

Lösungen wie Reddox Mail-Sealer, XnetSolutions SX-Mail-Crypt, Zertificon Z1 Secure-Mail Gateway, SeppMail Secure E-Mail Gateway, GBS iQ.Suite Crypt, totemomail Encryption Gateway und XiTrust Business Server helfen Unternehmen dabei, verschiedene Nutzergruppen in die E-Mail-Verschlüsselung zu integrieren: Nutzer mit S/MIME-Verschlüsselung, solche mit OpenPGP-Verschlüsselung, Web-Mail-Nutzer und mobile Nutzer.

Je nach Gateway-Lösung gibt es zusätzliche Module, um die Strecke zwischen zentralem Verschlüsselungsdienst und dem einzelnen Mail-Client und innerhalb des Firmennetzwerks abzusichern, wie zum Beispiel totemomail Internal Encryption.

4. E-Mail-Verschlüsselung aus der Cloud

Unternehmen, die ein eigenes Verschlüsselungs-Gateway aus Personalgründen nicht betreiben können oder eine externe Lösung aus anderen Gesichtspunkten bevorzugen, finden entsprechende Cloud-Lösungen für die E-Mail-Verschlüsselung.

Gerade kleine und mittlere Unternehmen finden durch Cloud-Lösungen einen leichteren Zugang zur E-Mail-Verschlüsselung, da die Administrationsaufwände reduziert werden können. Beispiellösungen sind der E-Mail-Verschlüsselungsservice von Antispameurope, Secure Cloud MailEncryption, Gateguard Encryption Service und Ubique Technologies IntelliSecure.

Bild: Totemo

Für Smartphones und Tablets gibt es spezielle Apps zur E-Mail-Entschlüsselung wie zum Beispiel totemomobile PushedPDF Reader. Damit lassen sich auch mobile Kommunikationspartner ohne eigene Verschlüsselungslösung einbinden.

Ganz ohne Administrator geht es aber auch bei der E-Mail-Verschlüsselung aus der Cloud nicht, denn die Nutzer müssen in jedem Fall eingerichtet, Nutzerkonten vergeben und gepflegt werden. Wie bei allen Cloud-Lösungen kommen Anwenderunternehmen zudem um die sogenannte Auftragskontrolle nicht herum, insbesondere um die Prüfung des Sicherheits- und Datenschutzkonzeptes des Cloud-Anbieters. □

Abhörsicherheit per App „Made in Germany“

Vodafone „Secure Call“ ist die neue, plattformunabhängige App für die abhörsichere mobile Kommunikation. Hinter ihr stecken neben dem Telekommunikationsunternehmen Vodafone die Düsseldorfer Abhörschutzexperten der Secusmart GmbH.

CEO Jens Schulte-Bockum, Vodafone, und Geschäftsführer Dr. Hans-Christoph Quelle von der Secusmart GmbH

Bild: Vodafone

Unternehmen zahlen lediglich einen niedrigen zweistelligen Betrag im Monat pro aktivem Zugang. Darüber hinaus fallen keine zusätzlichen Kosten an. Vom Provider Vodafone werden keinerlei Kündigungsfristen vereinbart. Mit der App Vodafone „Secure Call“ bestimmt das Unternehmen selbst und ohne weitere Verpflichtungen, wie lange wie viele Mitarbeiter sicher telefonieren – ohne dass zusätzlich Smartphones innerhalb der Firma angeschafft werden müssen.

Geistiges Eigentum schützen

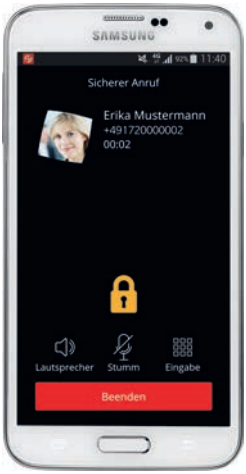
Vorgestellt wurde Vodafone „Secure Call“ zum ersten Mal im Frühjahr 2014. Sichere Telefonate über die App sind durch die gleiche Sprachverschlüsselung geschützt, die auch der SecuSUITE for BlackBerry 10 zugrunde liegt, mit der Bundesbehörden und Bundesministerien hochsicher telefonieren. Nicht zuletzt aufgrund enormer finanzieller Schäden durch Lauschangriffe ist sich vor allem der Mittelstand der drohenden Gefahr

von Spähattacken sehr bewusst und meldete noch vor dem offiziellen Verkaufsstart großes Interesse an der Sprachverschlüsselungs-App an.

Und dieser Schutz ist mehr als notwendig. Die aktuelle Studie von Corporate Trust „Industriespionage 2014“ schätzt den wirtschaftlichen Schaden alleine in Deutschland auf knapp 12 Milliarden Euro. Spionagegefährdet seien dabei vor allem innovationsstarke Branchen wie die Automobil- und Luftfahrtindustrie, der Schiffs- und der Maschinenbau. Bei einem Großteil der Firmen wird der finanzielle Schaden auf zwischen 10.000 und 100.000 Euro beziffert, bei einigen Unternehmen betrug der Schaden in den vergangenen Jahren sogar mehr als 1 Million Euro. Unternehmen ist bewusst, dass Gefährdung und Kosten durch Industriespionage in Zukunft noch deutlich zunehmen werden. Lediglich ein Viertel glaubt, dass die Bedrohung durch Spionage gleich bleiben wird. Aus diesem Grund steigt auch das Interesse an Lösungen zur Sprachverschlüsselung stetig an.

Build Your Own Device

Vodafone „Secure Call“ ermöglicht die gewünschte Sprachverschlüsselung und macht damit aus dem Smartphone ein abhörsicheres Smartphone für den Arbeitsalltag. Um die qualitativ hochwertige Technologie „Made in Germany“ zu nutzen, kann der Nutzer für sichere Gespräche sein eigenes Smartphone behalten. Dieses erhält einfach über die App plattformunabhängig das Zusatz-Modul „Abhör-Sicherheit“. Unternehmen, die mehr Sicherheit in ihrer Kommunikation möchten, können das Smartphone ihrer Mitarbeiter durch Sicherheitslösungen aufrüsten. Kosten entstehen erst, nachdem die App aktiviert wurde. Damit kommt Bring Your Own Device auf das nächste, das



sichere Level. Die Zukunft der Kommunikation lautet: Build Your Own Device.

Schon seit Jahren bietet Secusmart unterschiedliche Abhörschutzlösungen für die mobile Kommunikation und für Festnetzgespräche an. Mit der Hochsicherheitslösung SecuSUITE for BlackBerry 10 telefonieren Bundesministerien und Bundesbehörden bereits abhörsicher. Die gleiche Sprachverschlüsselung schützt jetzt auch im Rahmen der App Vodafone „Secure Call“. Flexibel und plattformunabhängig sorgt sie für sichere Sprache auf jedem Smartphone. Nach Android und iOS ist die Nutzung weiterer Plattformen für Vodafone „Secure Call“, wie etwa das BlackBerry-Betriebssystem, bereits geplant. Neben der sicheren Sprache soll ab dem ersten Quartal 2015 auch Secure Messaging zum Funktionsumfang gehören. So soll bei optimalem Preis-Leistungs-Verhältnis der Mittelstand als Motor der deutschen Industrie geschützt werden. Auf Basis erschwinglicher Sicherheit für alle. ■

Bild: freshidea - Fotolia.com

Die drei Stufen zur Cloud-Verschlüsselung

Die Verschlüsselung von Daten, die in die Cloud ausgelagert werden, ist nicht nur Aufgabe des Cloud-Betreibers. Unternehmen und Anwender müssen auch selbst aktiv werden.

Von Oliver Schonschek

Untersuchungen der Stiftung Warentest zeigten, dass es bei der Datensicherheit vieler Cloud-Dienste deutliche Mängel gibt. Cloud-Nutzer sollten deshalb die Cloud-Verschlüsselung nicht nur dem Cloud-Betreiber überlassen, sondern selbst aktiv werden.

Die Cloud-Verschlüsselung kann nur dann wirklich das Schutzziel der Vertraulichkeit erfüllen, wenn sie durchgehend umgesetzt wird: also vor der Übertragung der Daten, während des Transfers und innerhalb der Cloud.

1. Verschlüsselung vor der Übertragung in die Cloud

Vertrauliche Daten, die über einen Cloud-Dienst ausgetauscht oder in einem Cloud-Backup gesichert werden sollen, sollten an jedem Speicherort nur in verschlüsselter Form vorliegen. Dies gilt also auch für die lokalen Kopien beim Nutzer oder im Netzwerk des Anwenderunternehmens.

Verschiedene Verschlüsselungslösungen ermöglichen nicht nur diese lokale Verschlüsselung, sondern können auch dafür sorgen, dass die Daten vor dem Cloud-Transfer bereits geschützt sind. So bietet zum Beispiel der IndependenceKey von Quantec eine hardwarebasierte Verschlüsselung von Daten, die danach in einen Cloud-Speicher übertragen werden können. Alternativ lassen sich auch direkt die Daten in einem angebundenen Cloud-Dienst verschlüsseln. Boxcryptor, Cloudfogger, Drive-

Lock File Protection, Protectorion PC, Cloud Protection, CloudCockpit, OmniCloud, ShareCrypt und Wuala Desktop beispielsweise verschlüsseln die Daten vor dem Hochladen in die Cloud. Dazu werden die zu verschlüsselnden Dateien in einem bestimmten Ordner abgelegt, der mit dem Cloud-Dienst verknüpft wird. Die Verschlüsselung erfolgt dann automatisch vor dem Datentransfer.

Selbst wenn der Cloud-Transfer unzureichend gesichert wäre, könnten mögliche Lauschangriffe die Vertraulichkeit der Daten nicht gefährden, wenn diese bereits vor dem Hochladen in die Cloud verschlüsselt werden.

2. Verschlüsselung beim Transfer in die und aus der Cloud

Ein verschlüsselter Cloud-Zugang auf TLS/SSL-Basis sollte selbstverständlich sein. So fordert es jede Cloud-Sicherheitsempfehlung, wie zum Beispiel das Eckpunktepapier des BSI oder die Leitlinie der Cloud Security Alliance. Zudem können Unternehmen die Cloud-Zugänge und den Datentransfer in die und aus der Cloud über VPN-Lösungen absichern.

Viele Cloud-Nutzer überschätzen allerdings die reine Verschlüsselung der Datenübertragung. Ohne zusätzliche Verschlüsselung innerhalb der Cloud und die zuvor erwähnte lokale Datenverschlüsselung ist nur der Datentransfer geschützt, nicht aber die Datenspeicherung. Deshalb bietet Google zum Beispiel inzwischen neben der SSL-verschlüsselten Übertragung bei Google Cloud Storage auch eine automatische Verschlüsselung in der Cloud selbst an.

Verschlüsselungslösungen wie z.B. FideAS File Enterprise oder AWS Storage Gateway bieten sich an, um die verschlüsselte Datenübertragung in die Cloud zu übernehmen.

3. Verschlüsselung in der Cloud

Cloud-Dienste wie Secure Data Space oder IDGard bieten im Standard die Verschlüsselung innerhalb der Cloud an. Dabei wird der Zugriff auf die Schlüssel auf die Anwenderunternehmen selbst beschränkt. Würde auch das Schlüsselmanagement durch einen Cloud-Betreiber übernommen, könnten unbefugte Zugriffe auf die Cloud-Daten durch Mitarbeiter des Cloud-Providers nicht sicher ausgeschlossen werden.

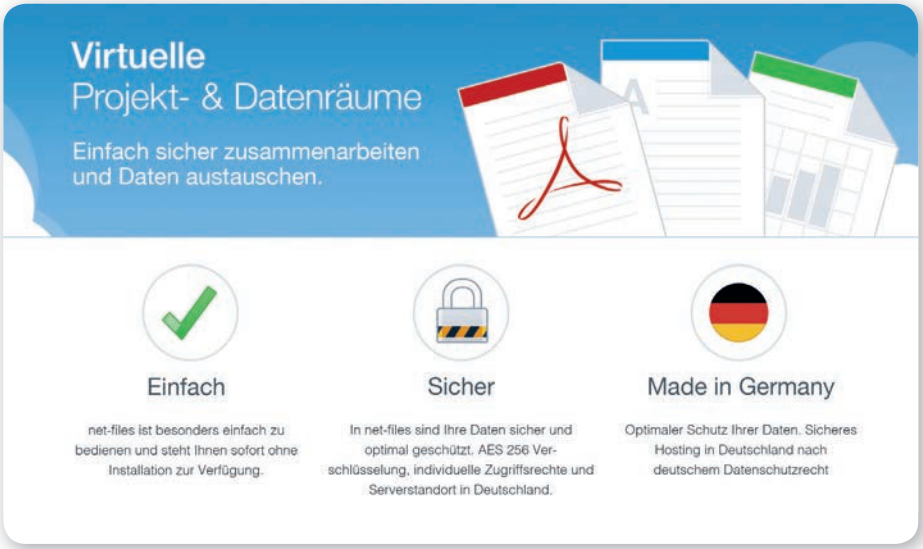
Anwenderunternehmen sollten deshalb nur Verschlüsselungslösungen in Erwägung ziehen, die unabhängig vom Cloud-Betreiber sind. Zahlreiche Lösungen zeigen, dass Anwenderunternehmen auch die Verantwortung für die Verschlüsselung in der Cloud selbst übernehmen können: HiCrypt zum Beispiel verschlüsselt neben Netzlaufwerken auch „Online-Festplatten“ und damit Cloud-Speicherplätze und bietet auch Apps für Android sowie für Apple iOS, um den mobilen Cloud-Zugriff zu ermöglichen. Da die mobile Nutzung von Cloud-Diensten weiter an Bedeutung gewinnt, sollten Unternehmen generell Lösungen nutzen, die den mobilen Zugriff auf verschlüsselte Clouds sicherstellen. Entsprechende Apps wie die DriveLock App for iPhone/iPad, die Secure Data Space App für iPhone/iPad und Android und Wuala Mobile sowie mobile Zugriffsmöglichkeiten bei OmniCloud helfen dabei.

Fazit: Selbst ist die Verschlüsselung

Sicherheitsmängel bei Cloud-Diensten und die rechtliche Verantwortung des Cloud-Nutzers für den Datenschutz (vgl. Auftragsdatenverarbeitung) machen deutlich, dass die Cloud-Verschlüsselung nicht alleine in die Hände des Cloud-Anbieters gegeben werden sollte.

Lösungen zur Verschlüsselung durch den Nutzer sind zahlreich auf dem Markt vorhanden. Allerdings kommt der Anwender um eine Datenschutzkontrolle nicht herum, wenn Verschlüsselungsdienste als Dienstleistung bezogen werden. Hier sollte insbesondere auch auf eine Trennung zwischen Cloud-Betreiber und Verschlüsselungsdienstleister geachtet werden. □

Virtuelle Projekt- und Datenräume – Made in Germany



Die net-files GmbH gehört zu den ersten und führenden Anbietern von Projekt- und Datenräumen im Internet. netfiles bietet Unternehmen und verteilten Projektteams einen geschützten Datenraum für effiziente Zusammenarbeit und den sicheren Datenaustausch über Unternehmens- und Standortgrenzen hinweg.

Made in Germany

Die net-files GmbH ist ein deutsches Unternehmen mit Sitz, Entwicklung und Hosting in Deutschland. Das Unternehmen ist inhabergeführt und arbeitet nach den strengen Anforderungen der Datenschutzrichtlinien der EU und Bundesrepublik Deutschland. Das Hosting erfolgt ausschließlich in hochsicheren, zertifizierten Rechenzentren in Deutschland.

Einfach zu bedienen

Die Nutzung der Anwendung erfolgt ausschließlich über einen Web-Browser. netfiles zeichnet sich insbesondere durch seine Anwenderfreundlichkeit aus und kann ohne Einführung und Installation von Software sofort genutzt werden kann.

Sicherheit und Schutz für sensible Daten

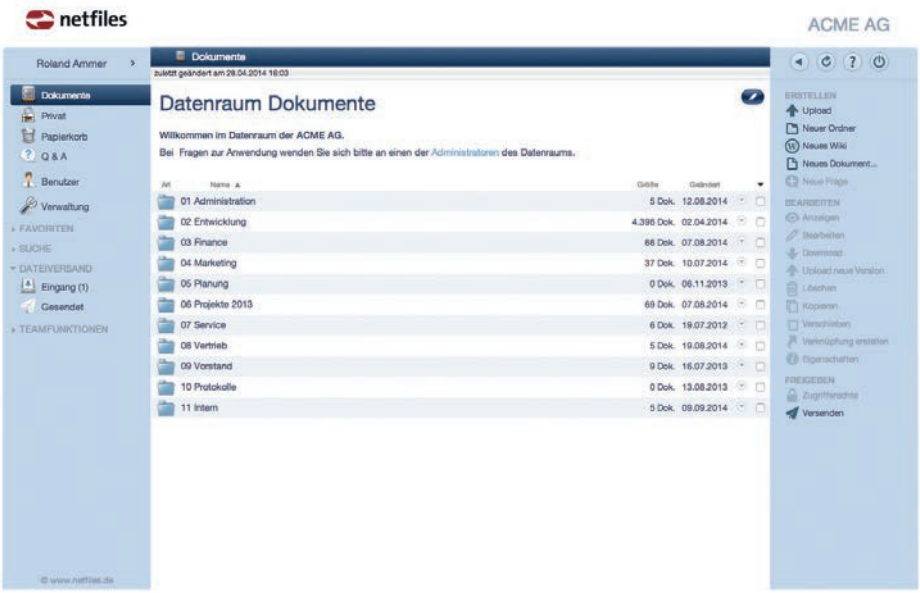
Detaillierte Zugriffsrechte regeln im Datenraum, wer welche Dateien sehen, bearbeiten und downloaden kann. Höchste Sicherheits-

standards gewährleisten dabei den Schutz und die Vertraulichkeit der Dokumente. Sowohl für die Datenübertragung als auch Datenablage werden hochsichere 256-Bit-Verschlüsselungsverfahren eingesetzt. Ein revisionssicheres Aktivitätsprotokoll dokumentiert alle Aktionen der Benutzer im Datenraum.

Die wichtigsten Einsatzbereiche von netfiles sind:

- Virtueller Datenraum für Due Diligence Prüfungen, Fusionen & Übernahmen (M&A), Immobilienverkäufen und anderen hochvertraulichen Transaktionen
- Flexibler Projektraum für die Zusammenarbeit in verteilten Teams innerhalb eines Unternehmens oder über Unternehmensgrenzen hinweg
- Intranet/Extranet für die sichere, rollenbasierte Verteilung von Dokumenten an Mitarbeiter, Partner, Lieferanten und Kunden
- Einfacher Datenaustausch für Dokumente beliebiger Größe als zuverlässige und sichere Alternative zu E-Mail oder FTP

Unter www.netfiles.de können sich interessierte Unternehmen informieren und einen kostenlosen, unverbindlichen Testzugang für 14 Tage bestellen. ■



Höchste Sicherheitsstandards gewährleisten den Schutz und die Vertraulichkeit der Dokumente.

Speichermedien verschlüsseln

Festplatten und andere Speichermedien lassen sich auf unterschiedliche Arten verschlüsseln. Doch die Anwender scheuen allzu oft den vermeintlichen Aufwand.

Von Oliver Schonschek

Verschlüsselung verursacht Kosten – und ein Großteil davon lässt sich tatsächlich auf den Aufwand der IT-Abteilungen und der Anwender beim Betrieb verschlüsselter Festplatten zurückführen. Damit die gespeicherten Daten auch tatsächlich verschlüsselt werden, reicht es meist nicht aus, die Nutzer zu motivieren oder zu ermahnen. Entscheidend sind Verschlüsselungslösungen, die ohne Zutun des Nutzers verfügbar sind und so weit wie möglich automatisch arbeiten. Hierfür stehen sowohl die Bordmittel der Betriebssysteme als auch spezielle software- oder hardwarebasierte Lösungen zur Verfügung.

Verschlüsselung über das Betriebssystem

Unter Windows 7 Ultimate/Enterprise sowie Windows 8 Pro/Enterprise können Anwender die Laufwerksverschlüsselung BitLocker nutzen. Dieses interne Verschlüsselungstool lässt sich über den Laufwerkverschlüsselungs-Assistenten von BitLocker oder einfach in den Systemeinstellungen aktivieren. Auch mobile Datenträger wie USB-Sticks können mit BitLocker verschlüsselt werden (BitLocker to Go). Unternehmen sollten es allerdings nicht den Nutzern überlassen, die Windows-Funktion zu aktivieren. Die Konfiguration von BitLocker sollte mit entsprechenden Skripts automatisiert werden. Zudem lassen sich Gruppenrichtlinieneinstellungen aktivieren, so dass Laufwerke durch BitLocker geschützt werden müssen, bevor ein durch BitLocker geschützter Computer Daten auf die Laufwerke schreiben kann. Im Falle älterer Windows-Versionen und NTFS-Dateisysteme kann EFS (Encrypted File System) zur Verschlüsselung genutzt werden.

Apple liefert Mac OS X Lion oder Mountain Lion mit FileVault 2 aus. Damit ist es möglich, sowohl die komplette Festplatte eines Apple-Endgerätes als auch einen Wechseldatenträger zu verschlüsseln. Auch FileVault 2 muss erst ak-

Im Unternehmen sollte die Festplattenverschlüsselung zum Pflichtprogramm gehören.

Bild: Alex Po - Fotolia.com

tiviert werden, so dass Unternehmen dies in der Basiskonfiguration vorsehen sollten.
Ubuntu und viele andere GNU/Linux-Distributionen bieten mit Full Disk Encryption (FDE) ebenfalls eine Möglichkeit zur verschlüsselten Datenspeicherung.
Die Verschlüsselungsfunktionen der Betriebssysteme unterstützen jeweils die dem OS untergeordneten (virtuellen) Laufwerke. Bei Endgeräten, die nicht über die Betriebssysteme und damit die genannten Funktionen für das Verschlüsseln verfügen, können andere Lösungen die Vertraulichkeit der Daten schützen.

Verschlüsselung mit Software-Lösungen

Viele Anwendungen bieten integrierte Verschlüsselungsfunktionen, dies sind allerdings Insellösungen für spezielle Dateiformate. Um interne Festplatten und mobile Datenträger zu verschlüsseln, gibt es spezielle Verschlüsselungslösungen wie Steganos Safe, SecurStar DriveCrypt, DriveLock Full Disk Encryption, Secude FinallySecure Enterprise und fideAS file enterprise. Diese verschlüsseln Partitionen bzw. (virtuelle) Laufwerke und Datenträger.
Unternehmen sollten darauf achten, dass von der Verschlüsselungssoftware der Wahl alle eingesetzten Betriebssysteme unterstützt werden. Im Idealfall läuft die Verschlüsselung automatisiert ab und bietet bei erhöhtem Schutzbedarf auch eine Zwei-Faktor-Authentifizierung. Secude FinallySecure Enterprise unterstützt beispielsweise auch Mac OS X, fideAS file enterprise bietet einen File Encryptor für Linux und DriveLock Full Disk Encryption erlaubt die Verwendung von Security-Tokens und Single-Sign-On (SSO). Securstar DriveCrypt wiederum kann mit der DriveCrypt Plus Pack Enterprise Edition zentral administriert werden.
Für USB-Speichermedien gibt es spezialisierte Programme wie Protectorion To Go oder Easy-Lock von Endpoint Protector. Solche Verschlüsselungslösungen werden vom Anwender direkt z.B. auf dem USB-Stick installiert. Alternativ gibt es Datenspeicher, die bereits ab Werk mit einer Verschlüsselungslösung bestückt sind.

Vorkonfigurierte Speicher und hardwarebasierte Verschlüsselung

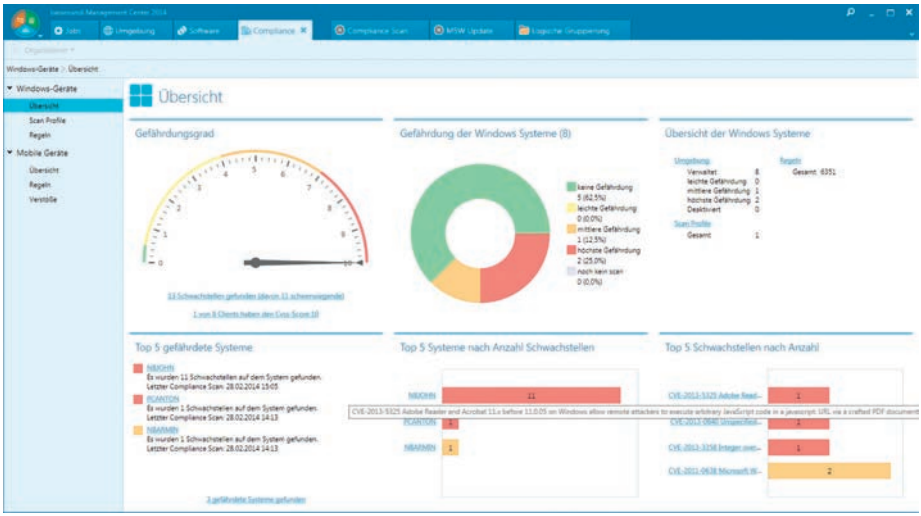
Mobile Festplatten und USB-Sticks, die bereits mit einer integrierten Verschlüsselungssoftware ausgeliefert werden, erleichtern den Anwendern die Arbeit. Beispiele für derartige Datenträger sind Safe To Go von Prosoft und G&D, USB-Speicher von LaCie mit LaCie Private-Public und Speichermedien von Digittrade. Solche Lösungen bieten zum Teil ebenfalls die Möglichkeit, den Schlüssel um weitere Schutzfaktoren zu ergänzen. Der IndependenceKey von Quantec verfügt über einen Krypto-Chip und kann als Verschlüsselungselement zum Beispiel mit USB-Speichermedien verbunden werden. Die Daten auf den USB-Speichern können dann nur mittels IndependenceKey und Kennworteingabe entschlüsselt werden.
Je nach Endgerät kann auch eine interne, hardwarebasierte Verschlüsselung zum Einsatz kommen, wenn ein TPM-Chip vorhanden ist. In dem Trusted Platform Modul (TPM) werden dann die für das Entschlüsseln notwendigen Schlüssel verwahrt.

Fazit: Verschlüsselung ist kein Aufwand, sondern Pflicht

Verschlüsselungslösungen sollten dem Anwender möglichst vorinstalliert und konfiguriert bereitgestellt werden. Wenn der User nur ein sicheres Passwort wählen muss, sinkt der Aufwand für die Datenverschlüsselung deutlich. Bleibt noch der geringe zeitliche Aufwand durch die Ver- und Entschlüsselung. Dieser ist sollte gar nicht erst zur Debatte stehen: Rechtlich gesehen ist Verschlüsselung bei entsprechendem Schutzbedarf Pflicht, wie zum Beispiel das Bundesdatenschutzgesetz betont. □

Safety First: Automatisiertes Schwachstellenmanagement

Eine Sicherheitslücke auf einem einzelnen Rechner bringt die Sicherheit der gesamten Unternehmens-IT in Gefahr. Doch einem IT-Administrator ist es in der Praxis nicht möglich, alle Clients und Server fortwährend zu prüfen und zu patchen. Abhilfe schafft automatisiertes Schwachstellenmanagement, integriert in eine Client-Management-Software.



Übersicht über den Zustand der IT-Umgebung im Compliance-Dashboard der baramundi Management Suite

Auf jedem Windows-Rechner und Server lauern potentiell tausende Schwachstellen – Tendenz steigend: 2013 wurden jede Woche rund 100 neue Sicherheitslücken in der National Vulnerability Database des US-CERT dokumentiert. Jede könnte als Einfallstor für Angreifer dienen. Schwachstellen werden für sogenannte Reverse-Angriffe genutzt, die etablierte Sicherungen wie Firewall und Virenscanner aushebeln. Ein Beispiel: Einem Mitarbeiter wird eine manipulierte Datei zugespielt, die sich eine Lücke im PDF-Reader zunutze macht und so einen Schadcode auf dem Rechner ausführen kann. Dieser macht den Rechner zum willigen Sklaven des Angrei-

baramundi software AG

fers. Da die Verbindung aus dem Unternehmen heraus aufgebaut wird, greift die Firewall nicht ein. Neben korrumpierten Dateien werden auch manipulierte Webseiten oder bösartige Online-Anzeigen eingesetzt.
Im Rahmen eines wirkungsvollen IT-Sicherheitskonzepts ist es daher essentiell, Sicherheitslücken auf allen Geräten zu erkennen und alle nötigen Patches unverzüglich, flächendeckend und zuverlässig einzuspielen.

Automatisierte Schwachstellenanalyse

Dazu müsste der Administrator laufend Datenbanken und Blogs auf Meldungen über Schwachstellen durchsuchen, diese bewerten, die eigenen Rechner prüfen, Updates paketieren, testen, verteilen und erfassen, ob die Verteilung erfolgreich war. Ohne automatisierte Hilfsmittel ist dies de facto nicht möglich. Ein automatisiertes Patch-Management für Microsoft-Produkte schließt zwar einige Lücken, deckt aber längst nicht jede Software ab. Hilfreich ist ein Scanner, der die Rechner im Unternehmensnetzwerk regelmäßig auf die Einträge in den Schwachstellendatenbanken prüft. Der IT-Administrator erhält so einen umfassenden Überblick. Sinnvoll ist dabei eine Drill-Down-Möglichkeit, zum Beispiel nach den Clients mit den meisten oder den gefährlichsten Lücken.

Integration in Client-Management

Für das schnellstmögliche Schließen der Lücken stehen ebenfalls automatisierte Hilfsmittel zur Verfügung. Neben Microsoft-Patches sollten diese zumindest Updates für weit verbreitete und daher bei Angreifern populäre Anwendungen anderer Hersteller abdecken. Aktuelle Softwarepakete für zahlreiche Applikationen sind auch als Managed Software von Client-Management-Herstellern verfügbar. Essentiell ist dabei, die Verteilung nicht nur anzustoßen, sondern auch eine Rückmeldung, ob diese erfolgreich war. Im Idealfall sind diese Lösungen mit dem Schwachstellenscanner in einer ganzheitlichen Client-Management-Software zusammengefasst, so dass der gesamte Prozess zügig ablaufen kann.
Ein derartiges automatisiertes Schwachstellenmanagement sorgt für eine größtmögliche Aktualität der Client-Systeme und Server im Unternehmen. Es kann allein aber keinen umfassenden Schutz bieten, sondern muss Teil einer umfassenden Sicherheitsstrategie sein. In einer größeren Umgebung sollte diese automatisiert umgesetzt werden, um einheitliche Standards an allen Geräten durchzusetzen. Dazu gehören standardisierte Abläufe ebenso wie ein zentrales Backup, das Verschlüsseln von Datenträgern oder der Schutz vor nicht autorisierten Anwendungen. Flankierend müssen auch die Endanwender für Gefahren sensibilisiert und darüber informiert werden, welche Verhaltensweisen zum Schutz vor Angriffen beitragen.
In ein derartiges Sicherheitskonzept sollten auch Smartphones und Tablets eingebunden werden. Es bietet sich an, auch diese Aufgabe über eine integrierte Lösung für Client- und Mobile-Device-Management abzudecken, um einheitliche Standards auf allen Geräten im Unternehmen durchzusetzen. ■

Der Autor Armin Leinfelder ist Produktmanager bei der baramundi software AG.

Daten auf Smartphone und Tablet schützen

Mobilgeräte können schnell verloren gehen oder gestohlen werden. Deshalb sollten die Daten auf Smartphone und Tablet nach Möglichkeit verschlüsselt sein.

Von Oliver Schonschek

Zwar gehen 83 Prozent aller Unternehmen von einer hohen Schadenswahrscheinlichkeit durch den Verlust eines Mobilgerätes aus, doch nur 68 Prozent aller befragten Firmen setzen eine Sicherheitslösung für ihre Smartphones ein. Dies ist das Ergebnis der „G Data Mobile Device Management Studie 2013". Fehlt aber die Datenverschlüsselung, könnte dem Geräteverlust ein Datenmissbrauch folgen.

Werden Smartphones für private und betriebliche Zwecke eingesetzt, gilt es, die betrieblichen Daten vor den Zugriffen privater Anwendungen und bei Geräteweitergabe auch vor anderen Nutzern zu schützen. Eine Verschlüsselung der betrieblichen Daten sollte deshalb zwingend vorgeschrieben werden. Entsprechende Sicherheitsrichtlinien bei BYOD-Programmen fehlen in vielen Unternehmen aber noch, wie z. B. die Studien „Acronis 2013 Data Protection Trends Research" und „Global Corporate IT Security Risks: 2013" von Kaspersky Lab zeigen.

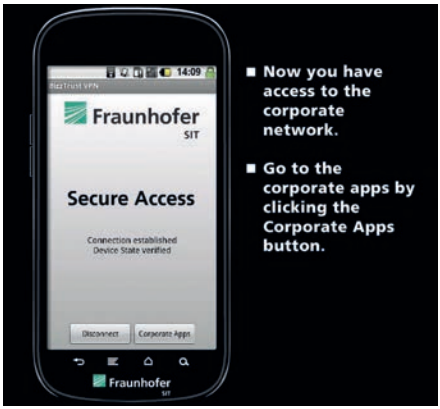


Bild: Fraunhofer SIT

BizzTrust unterstützt nicht nur die Trennung privater und betrieblicher Apps und Daten, sondern ermöglicht auch den Aufbau mobiler VPN-Verbindungen.

Möglichkeiten zur mobilen Verschlüsselung gibt es reichlich, ob mit Bordmitteln der mobilen Betriebssysteme oder per Security-App. Dabei sollte die Verschlüsselung jedoch nicht nur den gespeicherten Daten auf Smartphones gelten, sondern auch den vielfältigen Datenverkehr und die Kommunikation berücksichtigen.

Verschlüsselung über das Betriebssystem

Apple iOS, Android OS und Windows Phone OS bieten integrierte Verschlüsselungsfunktionen, die sich allerdings unterscheiden. So sieht iOS eine automatische Hardware-Verschlüsselung und eine Verschlüsselung von Flash-Speichern vor, unterstützt SSL/TLS, VPNs und WPA2 Enterprise für verschlüsselte Verbindungen sowie eine E-Mail-Verschlüsselung (S/MIME). Auch iMessage und FaceTime-Verbindungen werden automatisch verschlüsselt.

In den Sicherheitseinstellungen von Android OS findet sich die Option, die Daten auf dem

Smartphone zu verschlüsseln. Dabei dient das Passwort, das für die Display-Sperre gewählt wurde, als Schlüssel. Windows Phone 8 bietet bei Aktivierung der BitLocker-Funktion ebenfalls eine automatische Geräteverschlüsselung.

Verschlüsselung mithilfe von Security-Apps

Je nach mobilem Betriebssystem besteht folglich der Bedarf, die Datei- und Ordner-Verschlüsselung mittels zusätzlicher Security-App zu ergänzen oder zu automatisieren. Generell ist eine automatische Verschlüsselung zu bevorzugen. Umfragen unter Smartphone-Nutzern zeigen, dass die mobile Datenverschlüsselung sonst in Vergessenheit geraten könnte. So nutzen laut einer Kaspersky-Umfrage nur knapp 28 Prozent der Tablet- und Smartphone-User in Deutschland eine mobile Datenverschlüsselung.

Verschlüsselung der mobilen Kommunikation

Die mobile Verschlüsselung würde allerdings zu kurz greifen, wenn sie nur die gespeicherten Daten auf internem Gerätespeicher und ggf. der Speicherkarte umfassen würde. Smartphones werden immerhin auch für den Empfang und Versand von E-Mails, SMS und MMS, für Chats und bei entsprechender Bandbreite auch für mobile Videotelefonate genutzt. Nicht zu vergessen ist die Telefonie-Funktion, die auch vertrauliche Inhalte transportieren kann. Zudem gilt es natürlich auch, den mobilen Zugriff auf das Firmennetzwerk angemessen abzusichern.

Lösungen zur Verschlüsselung der mobilen Kommunikation sind vielfach auf dem Markt zu finden, zum Beispiel etaPhone Secure VoIP für verschlüsselte Telefonate, GSMK CryptoPhone zur mobilen Daten-, SMS- und Sprachverschlüsselung, Secure Cloud Mobile VME zur Verschlüsselung von Sprache, SMS und E-Mail sowie Adisoft KaiKrypt zur mobilen Sprachverschlüsselung.

Bild: Secusmart

Die Secusmart SecuSuite enthält u. a. die mobile Sprachverschlüsselung SecuVoice, unterstützt aber z. B. auch verschlüsselte E-Mails und SMS.

SiMKo3 von T-Systems und Secusmart SecuSUITE for BlackBerry 10 bieten sowohl Transportverschlüsselung (E-Mail, Sprache, SMS, Secure Browsing) als auch Ablageverschlüsselung (Daten, Kontakte, Notizen). TopSec Mobile und SecurStar PhoneCrypt erlauben abhörsichere Handy-Telefonate, totemomobile Transcoder for BlackBerry dient der verschlüsselten Datenkommunikation mit Blackberry-Geräten. Der totemomobile PushedPDF Reader ist derweil für den mobilen Empfang verschlüsselter E-Mails gedacht. BizzTrust bietet E-Mail-Verschlüsselung, optionale Sprachverschlüsselung und die verschlüsselte Kommunikation mit dem Firmennetzwerk. Weitere Lösungen erlauben den Aufbau einer mobilen, abgesicherten VPN-Verbindung.

Fazit: Smartphones brauchen eine Rundum-Verschlüsselung

Die vielfältigen Funktionen eines Smartphones machen eine entsprechend vielfältige Verschlüsselung notwendig, um vertrauliche Firmendaten und personenbezogene Daten zu schützen. Gegenüber der Verschlüsselung bei PCs dürfen keine Abstriche gemacht werden. Das Gegenteil ist der Fall, denn Smartphones unterliegen einem hohen Verlust- und Diebstahlrisiko. Unternehmen sollten sich also umgehend auf dem breiten Markt der mobilen Verschlüsselungslösungen umsehen, denn nicht nur Regierungsstellen brauchen eine sichere mobile Kommunikation. □

BSI-geprüfte IT-Security-Lösungen für den flexiblen Fernzugriff

Wissen und Daten von Unternehmen sind zunehmend Ziele von Wirtschaftsspionage, die insbesondere von Geheimdiensten verübt wird. Der daraus entstehende Schaden für Unternehmen ist enorm und kann existenzgefährdend sein. IT-Security-Lösungen aus Deutschland, wie die der HOB GmbH, unterliegen nicht dem Einfluss der Geheimdienste und haben somit keine Backdoors. HOB nutzt zudem eine eigene SSL-Implementierung.

Secure Remote Access mit HOB RD VPN

HOB RD VPN ist die ganzheitliche Secure-Remote-Access-Lösung mit vielen Vorteilen. Nutzer können von überall, zu jederzeit und von nahezu jedem Endgerät auf zentrale Unternehmensdaten zugreifen. Clientseitig sind weder Installationen noch Administratorrechte erforderlich. Die zentrale Administration senkt den Administrationsaufwand und damit die Kosten und erhöht die Flexibilität. HOB RD VPN enthält Bestandteile für die sichere Kommunikation und Authentifizierung auf Basis von SSL Version 3 und TLS. Es erlaubt u.a. das Erstellen und Verwalten von Zertifikaten. Der Aufbau einer eigenen Public Key Infrastructure wird so auch möglich.

HOB RD VPN unterstützt Methoden zum Schlüsselaustausch mit RSA, Diffie-Hellman und Diffie-Hellman ephemeral.
Die Verschlüsselung mit HOB RD VPN kann mit verschiedenen Algorithmen erfolgen, wie z.B. mit dem symmetrischen Verschlüsselungsstandard AES bis zu 256 Bit Schlüssellänge, dem asymmetrischen Verschlüsselungsstandard RSA bis zu 4096 Bit und mit kryptografisch starken Zufallszahlen mit mindestens 50 Bit Entropie. Im Vergleich dazu ergibt sich aus den Kombinationsmöglichkeiten einer Lottoziehung „6 aus 49" lediglich eine Entropie aus 20.

HOBLink VPN Gateway 2.1

Die grundlegend überarbeitete Version des HOBLink VPN Gateways bietet als reine Software-Lösung – auf Basis von wahlweise Linux, BSD oder Windows – neben Sicherheit auch ideale Skalierbarkeit. Das Gateway unterstützt eine beliebige Anzahl von Site-to-Site- und Client-to-Site-Verbindungen und ebenso eine beliebige Anzahl von VPN-Tunneln. Durch die Möglichkeit, für jede Benutzergruppe eine eigene Gruppe von Authentifizierungsservern zu konfigurieren, wird Mandantenfähigkeit erreicht. Für jeden VPN-Tunnel kann der Traffic-Selector konfiguriert werden, d.h., Source-IP, Destination-IP, Source-Port, Destination-Port bzw. -Protocol sind individuell bestimmbar. Zusätzliche Sicherheitsfunktionen sind die Überprüfung der Gruppenmitgliedschaft und die Zuordnung einer virtuellen IP für Clients. Der Schutz der gesamten Datenkommunikation wird gewährleistet auf Basis der Standards IPsec und IKE/ISAKMP (RFC 2401-ff) und L2TP über IPsec (L2TP/IPsec) mit starker Verschlüsselung und Authentifizierung. HOBLink VPN Gateway bietet umfassende Unterstützung von Zertifikaten und digitalen Signaturen. Der im Lieferumfang enthaltene HOB Zertifikatmanager ermöglicht die Bearbeitung des HOB Keystore. Damit kann eine Zertifikatsstruktur aufgebaut werden aus eigenen Zertifikaten oder mit Zertifikaten von externen Certificate Authorities. Weiterhin ermöglicht HOBLink VPN Gateway die Benutzerauthentifizierung mit RADIUS (z.B. RSA Authentication Manager/ACE-Server mit Challenge) und LDAP. Die Verbindungsstabilität wird durch den Einsatz von Standards wie NAT-T (Traversal) / UDP Encapsulation über beliebige Router, Firewalls und WLAN Hotspots verbessert.
Das HOBLink VPN Gateway ist kompatibel mit VPN-Clients unterschiedlicher Hersteller, VPN-Clients unterschiedlicher Hardware (PC, Laptop, Mobile Device wie Apple iOS oder Android) und dem HOB-eigenen Produkt HOBLink VPN Anywhere Client. ■

Besuchen Sie uns auf der it-sa

Das HOB Kernprodukt, die Secure Remote Access Suite HOB RD VPN wurde kürzlich vom BSI nach Common Criteria EAL 4+ zertifiziert. Im Rahmen der it-sa 2014 können sich Fachbesucher ein eigenes Bild von den HOB Security-Lösungen machen (Halle 12, Stand 508).

Netzwerke, VPN und WLAN richtig absichern

Bild: Nmedia - Fotolia.com

Lauschangriffe auf Netzwerke lassen sich nur verhindern, wenn sämtliche Verbindungen angemessen verschlüsselt sind. Nicht nur bei der SSL-Verschlüsselung im Internet gibt es Nachholbedarf, auch andere Kommunikationswege sind oft nicht umfassend abgesichert. Dieser Beitrag beleuchtet die wichtigsten Traffic-Baustellen. Von Oliver Schonschek

Als Sicherheitsverantwortlicher kann man schon froh sein, wenn IT-Nutzer vertrauliche Daten nur dann an Webapplikationen übermitteln, wenn die Verbindung per SSL/TLS gesichert ist. Leider kann man aber selbst in diesem Fall nicht davon ausgehen, dass Lauschangriffe ausgeschlossen sind. Zum einen wurden bereits SSL-Zertifikate gestohlen bzw. gefälscht, nachdem einzelne Zertifizierungsstellen erfolgreich angegriffen wurden. Zum anderen wird die SSL-Verschlüsselung im Internet häufig unzureichend implementiert.

So meldete TeleTrust, dass bei der Hälfte der schutzwürdigen Internetkommunikation möglicherweise unsichere Algorithmen verwendet werden (PDF, 140 KB). Serverseitig werde automatisiert ein Profil ausgewählt, das Verschlüsselungsalgorithmen wie RC4 oder DES-Varianten nutzt, die eine Entschlüsselung durch unbefugte Dritte nicht ausreichend verhindern. Auch der Online-Dienst SSL Pulse (Trustworthy Internet Movement) liefert Statistiken zu überprüften SSL-Verbindungen, die die Verbindungssicherheit in Frage stellen: Nicht einmal ein Viertel der mehr als 160.000 geprüften Webseiten wurde als sicher eingestuft.

Netzwerkverschlüsselung bleibt kritisch

Auch andere Verschlüsselungsmethoden für Netzwerke werden in der Praxis nicht immer so eingesetzt, wie es erforderlich wäre: Ob Virtual Private Networks (VPNs), Wireless LAN (WLAN) oder Layer-2-Verschlüsselung, Unter-

Bild: Secunet

Mobile Nutzer benötigen eine verschlüsselte Verbindung, wenn sie auf das Firmennetzwerk zugreifen wollen. Möglich wird dies zum Beispiel mit SINA Business. Das Bild zeigt einen VPN-Stick am Laptop.

nehmen sollten prüfen, wie die Verschlüsselung umgesetzt ist, und bei Bedarf nach passenden Lösungen suchen.

VPN: An jeden Nutzertyp denken

Wenn mobile oder externe Mitarbeiter auf das Firmennetzwerk zugreifen, sollte dies nicht über das offene Internet geschehen. VPNs bieten sich für sichere Verbindungen an und bilden einen Tunnel zwischen Mitarbeiter und internem Netzwerk. Jedoch sollte dabei die Komplexität der VPN-Verbindung nicht unterschätzt werden: Die anzubindenden Mitarbeiter nutzen zum Teil private Smartphones oder Tablets für den Netzwerkzugriff (Bring Your Own Device), wollen neben dem Firmennetzwerk auch betriebliche Cloud-Dienste verwenden und haben Endgeräte im Einsatz, die sich auch im Betriebssystem unterscheiden.

Insellösungen für verschiedene VPN-Nutzer sollten vermieden werden, erhöhen sie doch den Administrationsaufwand und das Risiko für Konfigurationsfehler. Deshalb sind VPN-Lösungen gefragt, die sich als App oder über mobile Browser nutzen lassen, die flexibel mehrere Netzwerke parallel unterstützen und die für verschiedene Betriebssysteme angeboten werden.

Gerade bei mobilen Geräten und dem damit verbundenen Verlustrisiko sollte an Sicherheitsfunktionen wie Zwei-Faktor-Authentifizierung gedacht werden, damit die VPN-Verbindung nicht zur Hintertür ins Firmennetzwerk wird. Beispiele für VPN-Lösungen, die Clients für mehrere Betriebssysteme bieten, sind ViPNet OFFICE 4.0 oder die NCP Secure Entry Client Suite. Möglichkeiten zur VPN-Anbindung von Smartphones und Tablets sehen zum Beispiel HOBLink Mobile und NCP Mobile VPN vor.

Der Bedarf an erhöhtem Zugangsschutz über Zwei-Faktor-Authentifizierung lässt sich ebenfalls abdecken, unter anderem mit dem ECOS VPN-Client und den VPN-Lösungen von NCP. Eine schnelle VPN-Einführung unterstützen VPN-Appliances wie genua genucrypt, SecureGUARD UAG Appliances, secunet SINA Business, Sirrix TrustedVPN, Securepoint Black Dwarf VPN-Gateway und Gateprotect Extended VPN.

Bild: Securepoint

Wer sein Netzwerk auf Außenstellen ausweiten möchte, sollte zu einer VPN-Lösung greifen. VPN-Gateways wie das Securepoint VPN-Gateway Black Dwarf ermöglichen einen schnellen Einstieg.

Layer 2: Glasklare Sicherheit für alle Standorte

Unternehmen mit mehreren Standorten wollen mit ihren Niederlassungen am liebsten so schnell und sicher kommunizieren, als ob alle Einheiten in der Zentrale angesiedelt wären. Um dies zu ermöglichen, kommen Ethernet-Services zum Einsatz, die meist auf Glasfaserverbindungen basieren, entweder als „Hub and Spoke"- oder Any-to-Any-Vernetzung.

Ohne entsprechende Verschlüsselung sind die Verbindungen zwischen den Niederlassungen ⇨

Die VPN-Lösung der Wahl sollte alle Nutzertypen unterstützen, die im Unternehmen vorkommen, zum Beispiel auch Mac-Nutzer, für die ggf. ein eigener VPN-Client benötigt wird. Das Bild zeigt den NCP Enterprise Secure Client für Mac-Nutzer.

Bild: NCP

↪ und der Zentrale (Hub and Spoke) bzw. zwischen allen angeschlossenen Standorten (Any-to-Any) allerdings ungeschützt. Hier setzen Lösungen im Bereich Layer-2-Verschlüsselung an, die schnelle Datentransporte auf der Data-Link-Schicht absichern, darunter InfoGuard Layer 2 Encryption, secunet SINA L2 Box, der CE-Infosys PowerCryptor und der atmedia 100M Ethernet-Verschlüsseler.

WLAN: Fehler aus dem Home-Office nicht wiederholen

Bei WLAN-Verbindungen besteht die Gefahr, dass der drahtlose Teil des Firmennetzwerkes genauso unsicher konfiguriert wird, wie dies in vielen Privathaushalten und Home-Offices der Fall ist.

Umfragen zeigen, dass deutschen Nutzern die Sicherheit von WLAN-Hot-Spots sehr wichtig ist. Gleichzeitig besteht aber Nachholbedarf bei der WLAN-Verschlüsselung am eigenen Hot Spot. Für Unternehmen konzipierte Produkte helfen dabei, die Verschlüsselung für WLAN- und VPN-Verbindungen einzurichten, und vermeiden so die häuslichen Fehler. Beispiellösungen sind Teldat bintec W2003n-ext, LANCOM L-452agn dual Wireless und die FRITZ!Box 7490 für das Home-Office. Allerdings sollte nicht vergessen werden, dass auch WLAN-Router Sicherheitslücken haben können, die die Verschlüsselung gefährden, wie zum Beispiel die Eingabe des Suchbegriffs „WLAN“ bei CERT-Bund zeigt.

Bild: Secunet

Die Standortvernetzung über Glasfaserleitungen bedarf einer sicheren Verschlüsselung, um Lauschangriffe abwehren zu können. Eine Layer-2-Verschlüsselung bietet zum Beispiel die secunet SINA L2 Box.

Fazit: Keine Vernetzung ohne Verschlüsselung

Ganz gleich, ob nun mobile und externe Mitarbeiter, verteilte Standorte oder der WLAN-Drucker in der Firma vernetzt werden sollen: Ohne die passende Verschlüsselungslösung geht es nicht. Dabei sollte die jeweilige Verschlüsselung natürlich auch dem Stand der Technik entsprechen, wie das Beispiel der unsicheren SSL-Verbindungen zeigt. Bei der Prüfung der Verschlüsselung hilft auch die BSI-Richtlinie „TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen“. □

Bild: Teldat

Werden WLAN-Verbindungen im Unternehmen oder Home-Office genutzt, sollte auf Sicherheitsfunktionen geachtet werden, die die notwendige Verschlüsselung einrichten und VPN-Verbindungen unterstützen. Auf dem Markt gibt es spezielle Business-Geräte wie Teldat bintec W2003n-ext.

secunet PaPSS: Penetrationstests als laufender Service

IT-Systeme und -Netzwerke sind das „Gehirn“ eines Unternehmens: Hier werden alle wichtigen Informationen und Daten zu Kunden, Mitarbeitern, Produkten und Aufträgen erfasst, bearbeitet und gespeichert. Umso wichtiger ist es, die zugrundeliegende Infrastruktur zu schützen. Oft wissen Unternehmen allerdings gar nicht, dass ihr Netzwerk Schwachstellen aufweist oder wo danach zu suchen wäre. Mit einer technischen Sicherheitsanalyse können diese möglichen Angriffspunkte aufgedeckt werden.

secunet

Technische Sicherheitsanalysen sind schon seit Jahren ein probates Mittel, um mit wenig Aufwand Systeme, Systemverbünde und Netzwerke zu überprüfen. Dabei werden aktuell bekannte Schwachstellen und Angriffstechniken ausgenutzt – daher müssen die Analysen immer als Betrachtung zu einem Stichtag aufgefasst werden. Ein System, bei dem keine Schwachstelle gefunden wurde, kann bereits einen Tag später durch eine neu entdeckte Schwachstelle angreifbar sein.

Mit PaPSS – „Penetrationtest as Permanent Security Service“ bietet secunet ein Werkzeug für vereinfachte interne Schwachstellenscans, die laufend durchgeführt werden können. So lassen sich jederzeit übersichtlich Informationen darüber gewinnen, welche Schwachstellen existieren und welche der intern getroffenen Maßnahmen Einfluss auf die IT-Sicherheit haben.

Für PaPSS wird beim Kunden vor Ort eine Appliance installiert, die speziell auf das jeweilige Netzwerk hin konfiguriert ist. Die anschließende Dokumentation findet bei secunet statt, wo die Ergebnisse der automatischen Testläufe analysiert und hinsichtlich kritischer Schwachstellen untersucht werden. Damit geht secunet PaPSS weit über die Möglichkeiten üblicher automatisierter Schwachstellenscans hinaus und bietet gleichzeitig einen IT-Sicherheitsservice, der sich nahtlos in jede spezifische IT-Infrastruktur beim Kunden integrieren lässt.

Mehr zu secunet PaPSS erfahren Sie unter www.secunet.com und auf der it-sa 2014, Halle 12, Stand 636. ■

Impressum

Vogel IT-Medien GmbH
August-Wessels-Str. 27, 86156 Augsburg
Tel. 0821/2177-0, Fax 0821/2177-150
eMail redaktion@vogel-it.de

IT-BUSINESS

Redaktion: Wilfried Platten/pl (-106) – Chefredakteur, Dr. Andreas Bergler/ab (-141) – CvD/ltd. Redakteur, Dr. Stefan Riedl/sr (-135) – ltd. Redakteur

Co-Publisher: Lilli Kos (-300)
(verantwortlich für den Anzeigenteil)

Account Management:
Besa Agaj/International Accounts (-112),
Stephanie Steen (-211),
Hannah Lamotte (-193)
eMail media@vogel-it.de

SECURITY-INSIDER.DE

Redaktion: Peter Schmitz/ps (-165) – Chefredakteur, Stephan Augsten/aus (-132) – Redakteur, Jürgen Paukner/jp (-166) – CvD, Elke Witmer-Goßner (-283) – Redakteur

Co-Publisher: Markus Späth (-138), Tobias Teske (-139)

Key Account Management: Brigitte Bonasera (-142)

Anzeigendisposition: Dagmar Schauer (-202)

Grafik & Layout: Brigitte Krimmer, Johannes Rath, Udo Scherlin, Carin Böhm (Titel)

EBV: Carin Böhm, Brigitte Krimmer

Anzeigen-Layout: Johannes Rath

Adressänderungen/Vertriebskoordination: Sabine Assum (-194), Fax (-228)
eMail vertrieb@vogel-it.de

Abonnementbetreuung: Petra Hecht, DataM-Services GmbH, 97103 Würzburg
Tel. 0931/4170-429 (Fax -497)
eMail phecht@datam-services.de

Geschäftsführer: Werner Nieberle – Geschäftsführer/Publisher

Druck: deVega Medien GmbH, Anwaltinger Straße 10, 86156 Augsburg

Vogel Business Media

Vogel IT-Medien, Augsburg, ist eine 100prozentige Tochtergesellschaft der **Vogel Business Media**, Würzburg, einem der führenden deutschen Fachinformationsanbieter mit 100+ Fachzeitschriften, 100+ Webportalen, 100+ Business-Events sowie zahlreichen mobilen Angeboten und internationalen Aktivitäten. Seit 1991 gibt Vogel IT-Medien Fachmedien für Entscheider heraus, die mit der Produktion, der Beschaffung oder dem Einsatz von Informationstechnologie beruflich befasst sind. Dabei bietet er neben Print- und Online-Medien auch ein breites Veranstaltungsportfolio an.

Die wichtigsten Angebote des Verlages sind **IT-BUSINESS, eGovernment Computing, IP-Insider.de, Security-Insider.de, Storage-Insider.de, CloudComputing-Insider.de, DataCenter-Insider.de** und **BigData-Insider.de.**

Inserenten

Applied Security GmbH (apsec)	Großwallstadt	http://www.apsec.de/	36, 37
Arrow ECS GmbH	Fürstenfeldbruck	http://www.arrowecs.de/	59
baramundi software AG	Augsburg	http://www.baramundi.de/	48, 49
Eset Deutschland GmbH	Jena West	http://www.eset.de/	16, 17
Fujitsu Technology Solutions GmbH	München	http://www.fujitsu.com/de/	22, 23
gateProtect AG Germany	Hamburg	http://www.gateprotect.de/	12, 13
HOB GmbH & Co. KG	Cadolzburg	http://www.hob.de/	52, 53
LANCOM Systems GmbH	Würselen	http://www.lancom-systems.de/	30, 31
NCP engineering GmbH	Nürnberg	http://www.ncp.de/	6, 7, 60
Net at Work GmbH	Paderborn	http://www.netatwork.de/	27, 28
net-files GmbH	Burghausen	http://www.netfiles.de/	44, 45
secunet Security Networks AG	Essen	http://www.secunet.com/	32, 33, 57
Secusmart GmbH	Düsseldorf	http://www.secusmart.com/de/	2, 40, 41

Arrow | Data Center

Security Insider

it sa 2014
Die IT-Security Messe und Kongress
The IT Security Expo and Congress

Mitmachen & Quadro-Copter gewinnen!

> Arrow-Stand 504

Auf der it-sa vom 07.10. - 09.10.2014

Halten Sie Ausschau nach uns in Halle 12 ...

Gewinnspielkarte erhalten Sie direkt auf der it-sa.

... und so erkennen Sie uns! >>

Five Years Out

Security-Insider.de

arrowecs.de

NCP
SECURE COMMUNICATIONS

OUT: Sicherheit aus der Dose
IN: Sicherheit made in Germany

Remote Access VPN-Lösungen für Profis: Läuft es gut, steht NCP drauf. Sicherheit made in Germany setzt auch in Sachen Mobility auf Benutzerfreundlichkeit und Wirtschaftlichkeit.

SecurITy made in Germany

Next Generation Network Access Technology

www.ncp-e.com