

<kes>

Die Zeitschrift für
Informations-Sicherheit

special

Advanced Persistent Threats:

Unter dem
Radar

S. 20

Identity- und Access- Management: Wer bin ich? Und wie viele?

S. 22

it-sa 2014

Trends, Produkte
und Lösungen


it-sa 2014

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

SecuMedia

Schwachstellenmanagement: Mut zur Lücke – nein danke! ab S. 32



WIR HABEN NUR EINS IM SINN: IHRE BETRIEBSSICHERHEIT.

Intelligente Brandschutzlösungen für IT und EDV.

Sie können sich keine Ausfallzeiten erlauben? Dann setzen Sie auf OxyReduct®: Das aktive Brandvermeidungssystem reduziert kontinuierlich den Sauerstoffgehalt in der Raumluft. Durch dieses individuell anpassbare Schutzkonzept wird jede Brandgefahr sofort eingedämmt – ein Brand kann praktisch nicht entstehen. Der entscheidende Vorteil: Sie müssen nicht stromlos schalten, da Rückzündungen ausgeschlossen sind. Damit der Weiterbetrieb Ihres IT-Zentrums immer gesichert ist. Mehr Informationen unter www.wagner.de/edv.

WAGNER setzt Maßstäbe im Brandschutz – durch innovative Lösungen, die umfassend schützen: Brandfrüherkennung mit TITANUS®, Brandbekämpfung mit FirExting®, aktive Brandvermeidung mit OxyReduct® und Gefahrenmanagement mit VisuLAN®.

Herzlich willkommen zur it-sa 2014!

Gehackte E-Mail-Accounts, Wirtschaftsspionage oder gezielte Angriffe auf Webseiten – fast täglich erreichen uns neue Meldungen über kriminelle Machenschaften im Cyberspace.

Für Unternehmen stellt Cybercrime eine ernst zu nehmende Gefahr dar. Schließlich schreitet die Digitalisierung und globale Vernetzung der Wirtschaft unaufhörlich voran. Immer größer werden damit die Einfallstore, die Kriminellen offen stehen – wenn nicht Experten dafür sorgen, dass IT-Infrastrukturen sicher und robust sind.

CIOs, Administratoren und zahlreiche weitere Fachleute tragen hierfür ein hohes Maß an Verantwortung.

Sicherlich keine leichte Aufgabe, bedenkt man die kriminelle Energie international agierender Cyber-Verbrecher. Hinzu kommt: Die Berücksichtigung wirtschaftlicher und rechtlicher Aspekte wird beim Erstellen einer IT-Sicherheitsstrategie genauso gefordert wie Fachkenntnis zu technischen Fragen. Den Überblick über den Markt für IT-Sicherheitslösungen zu behalten, ist für IT-Sicherheitsverantwortliche deshalb von zentraler Bedeutung.



Die it-sa ist der jährliche Treffpunkt der IT-Sicherheitsfachleute. Auf der europaweit größten Fachmesse, die sich in Nürnberg exklusiv dem Thema IT-Security in allen Facetten widmet, finden sie vom 7. bis 9. Oktober einen 360-Grad-Blick über alle Bereiche des IT-Sicherheitsmarkts.

Die Messe hat eine beachtliche Entwicklung erlebt. Seit ihrer Premiere in Nürnberg vor fünf Jahren kamen zu jeder neuen Ausgabe weitere Aussteller und Besucher hinzu. Mit Congress@it-sa bietet die it-sa zum dritten Mal auch ein eigenes Kongressprogramm, das ebenfalls kontinuierlich wächst.

Diesen Trend setzt die it-sa 2014 fort. Kompakt und fokussiert auf das Thema IT-Sicherheit bietet sie eine einzigartige Plattform für Experten und Entscheider. Sie informieren sich auf der it-sa, um im Zeitalter von Cloud und Industrie 4.0 das Vertrauen in die Sicherheit digitaler Technologien zu gewährleisten.

Ihr Engagement ist heute wichtiger denn je, damit Unternehmen auch in Zukunft wettbewerbsfähig bleiben.

Wir freuen uns auf Ihren Besuch der it-sa!

Ihre Petra Wolf
Mitglied der Geschäftsleitung, NürnbergMesse



it-sa 2014:

Die Dialogplattform für IT-Sicherheitsprofis

Seite 5

Hallenplan

Seite 8

News und Produkte

Seite 10

Abhörschutz

Sichere App für Android und iPhone

Seite 19

Advanced Persistent Threats

Unter dem Radar

Seite 20

Identity- und Access-Management

Wer bin ich? Und wie viele?

Seite 22

Die Lücken schließen

Vermeintliche IT-Sicherheit

Seite 24

Schutz vor Cyberattacken

Drei Schritte für die Sicherheit

Seite 28

High-Speed-Verschlüsselung

Bodyguard für sensible Daten

Seite 30

Automatisiertes Schwachstellenmanagement

Mut zur Lücke – nein danke!

Seite 32

Öffentliches Bewusstsein

Hacker noch unterschätzt

Seite 36

Sicherer Internetzugang

Im Fadenkreuz der Hacker

Seite 38

Layer-2-Verschlüsseler SITLine ETH40G

Daten-Entführungen verhindern

Seite 40

Inhalt

Security as a Service

Schutz gegen DDoS-Angriffe

Seite 42

„Trust in German Sicherheit“

Den Überblick behalten

Seite 44

Standortübergreifende Netze schützen

VPN-Router ohne Hintertür

Seite 46

Interview

IT-Security-Trends im RZ

Seite 48

Kombinierte Sicherheit

Arbeitsentlastung für Admins

Seite 50

Vorschau auf neue ESET-Lösungen

Never change a running system?

Seite 52

Brandschutz im RZ

Mit Sauerstoffreduktion Datenverfügbarkeit sichern

Seite 56

Anwenderbericht

Die Daten sind sicher im Westerwald

Seite 58

Threat-Detection

Risiken durch Echtzeit-Analysen identifizieren

Seite 60

Data-Loss-Prevention für Unternehmen

Warum man eine Endpoint-DLP-Suite einsetzen sollte

Seite 63

Impressum

SecuMedia Verlags-GmbH

Postanschrift: Postfach 1234, 55205 Ingelheim (DE)
Hausanschrift: Lise-Meitner-Straße 4, 55435 Gau-Algesheim (DE)
Telefon +49 6725 9304-0, Fax +49 6725 5994
E-Mail: info@secumedia.de, Web: www.secumedia.de

Beteiligungsverhältnisse (Angabe gem. § 9, Abs. 4 Landesmedienges. RLP): Gesellschafter zu je 1/6 sind Gerlinde Hohl, Klaus-Peter Hohl, Peter Hohl (GF), Veronika Lauferweiler (GF), Nina Malchus (GF), Steffi Petersen

Handelsregister AG Mainz HRB 22282

Herausgeber: Peter Hohl

Anzeigenleitung: Birgit Eckert (verantwortlich für den Anzeigenteil)
Tel. +49 6725 9304-20, E-Mail: anzeigenleitung@secumedia.de

Satz: BlackArt Werbestudio,
Stromberger Straße 47, 55413 Weiler bei Bingen

Druck: Schmidt printmedien GmbH
Haagweg 44, 65462 Ginsheim-Gustavsburg

Bildnachweis Titelbild und S. 4: NürnbergMesse

Alle Rechte vorbehalten, auch die des auszugsweisen Nachdrucks, der Reproduktion durch Fotokopie, Mikrofilm und andere Verfahren, der Speicherung und Auswertung für Datenbanken und ähnliche Einrichtungen.



7. bis 9. Oktober 2014

it-sa 2014: Die Dialogplattform für IT-Sicherheitsprofis

Ihren festen Platz in der Messelandschaft hat die it-sa in Nürnberg längst eingenommen. Zur sechsten Ausgabe der IT-Sicherheitsfachmesse werden über 370 Aussteller aus dem In- und Ausland erwartet. Mit ihren Produkten und Dienstleistungen deckt sie alle Bereiche der IT-Sicherheit ab.

Von Thomas Philipp Haas, NürnbergMesse

Vom 7. bis 9. Oktober 2014 verwandelt sich das Messezentrum Nürnberg wieder zur Leistungsschau der IT-Sicherheitsbranche. Die it-sa bringt dann CIOs, CISOs und Entscheider mit internationalen Unternehmen und IT-Sicherheitsexperten zusammen. Das Veranstaltungskonzept bleibt unverändert. Die it-sa kombiniert wieder die B2B-Fachmesse mit weiteren Veranstaltungen, allen voran Congress@it-sa. „Kompakt, fokussiert und effizient“, so beschreibt Veranstaltungsleiter Frank Venjakob den Kern der it-sa. Zu den Ausstellern zählen Spezialisten aus Deutschland und Europa, aber auch Firmen aus Übersee. Sie decken die gesamte Bandbreite aktuell verfügbarer IT-Sicherheitslösungen von A wie Application Security bis Z wie Zugriffsschutz ab.

Mitten im Messegesehen finden Besucher auch dieses Jahr die Sonderflächen „Das perfekte Rechenzentrum“ und die IAM-Area. Erste informiert über Planung, Bau und Technik von Rechenzentren, während Zweite als Anlaufstelle für Fragen zu Identity- und Accessmanagement dient. Unternehmen, die neu auf dem IT-Sicherheitsmarkt sind, stellen sich auf der Fläche Startups@it-sa vor. Im Rahmen von Campus@it-sa präsentieren Hochschulen ihre Forschungsergebnisse. Mit insgesamt 21 Ausstellern aus beiden Bereichen sind Startups@it-sa und Campus@it-sa komplett ausgebucht.

Zum ersten Mal gibt es auf der Messe einen internationalen Gemeinschaftsstand. Hier präsentieren sich

diesmal tschechische Aussteller im Verbund. Gemeinsam demonstrieren sie dort das gebündelte Know-how ihrer Sicherheitsforschung und -entwicklung. Spezialisiert haben sich die tschechischen Anbieter unter anderem auf Mobile Security, Netzwerk- und SCADA-Sicherheit oder Sicherheit in der Cloud. Die Tschechische Republik zählt neben den USA und Großbritannien zu den Top-Drei-Ausstellernationen. Insgesamt sind ausstellende Unternehmen, Verbände und Institutionen aus über 20 Ländern in Nürnberg vertreten.

Fachwissen auf drei Bühnen

Wie sieht die Verschlüsselung für den mobilen Zahlungsverkehr der Zukunft aus? Oder: Wie lässt sich der „Unsicherheitsfaktor“ Mensch bei der Entwicklung eines Sicherheitskonzeptes berücksichtigen? Auf diese und weitere Fragen bieten die offenen Foren der it-sa Antworten. In den Foren Rot und Blau sowie im Auditorium erwartet die Besucher an allen drei Messtagen ein breit gefächertes Angebot von zumeist 15-minütigen Vorträgen zahlreicher Aussteller. Im Forum Rot dreht sich wieder alles um die Bedeutung umfassender IT-Sicherheitsmaßnahmen im Unternehmen.

Strategische Aspekte werden hier genauso beleuchtet wie betriebswirtschaftliche Fragen. Im Forum Blau erläutern Exper-

Alle Forenvorträge lassen sich online auswählen, weiterempfehlen und als Kalenderdatei speichern.

**Weitere Infos unter:
www.it-sa.de/foren**

it-sa – auf einen Blick



Die it-sa ist eine der führenden Spezialmessen zum Thema IT-Security und findet vom 7. bis 9. Oktober 2014 im Messezentrum Nürnberg statt. IT-Profis, Sicherheitsverantwortliche und Unternehmenslenker informieren sich auf der it-sa über Software, Hardware und Dienstleistungen, die IT-Infrastrukturen schützen. Congress@it-sa bietet vom 6. bis 9. Oktober zusätzliches Fachwissen.

Öffnungszeiten (Fachmesse):

7. und 8. Oktober 2014	9-18 Uhr
9. Oktober 2014	9-17 Uhr

Eintritt

Tagesticket:	24 €
Dauerticket:	55 €

Weitere Informationen:
www.it-sa.de



Im letzten Jahr zählte die it-sa 358 Aussteller und 6.900 Besucher.

ten vorrangig technische Lösungsansätze zur Informationssicherheit. Big Data, Intrusion Detection Monitoring oder DDoS-Attacken sind einige der Themen, die hier behandelt werden. Im bekannten Grün präsentiert sich auch zur it-sa 2014 das Auditorium, die Vortragsfläche für Sessions von Verbänden, Forschungsinstituten, Wissenschaftlern und Behörden. Hier informiert beispielsweise Brigitte Zypries, parlamentarische Staatssekretärin beim Bundesminister für Wirtschaft und Energie, über die Initiative „IT-Sicherheit in der Wirtschaft“. In Kooperation mit eco e.V., dem Verband der deutschen Internetwirtschaft, findet im Auditorium der it-sa zudem eine Vortragsreihe statt, die einen Überblick zu aktuellen Anforderungen an moderne Rechenzentren gibt. Zu den Höhepunkten im Forenprogramm zählen wieder die Live-Hacking-Vorfürhrungen. IT-Sicherheitsprofis demonstrieren hier, wie Kriminelle Zugriff auf Geräte und Anwendungen erlangen und welche Methoden helfen, die Sicherheit von IT-Systemen zu gewährleisten.

DsiN MesseCampus

Wie die Sonderfläche Campus@it-sa schlägt der DsiN MesseCampus am Donnerstag, den 9. Oktober, die Brücke in die akademische Welt. Er bringt Studierende, Professoren und Vertreter der IT-Wirtschaft zusammen. Das diesjährige Motto lautet „IT-Sicherheit als Karriereturbo“, denn Unternehmen fordern von Hochschulabsolventen heute mehr denn je tiefes Know-how in diesem Fachbereich der Informatik. Neben Kurzvorlesungen von Dozenten wie Prof. Sachar Paulus (FH Brandenburg) zum Thema IT-Sicherheit in der Informatikausbildung stehen ein Panel zu den Karriereaussichten angehender IT-Sicherheitsexperten und Karrieregespräche auf dem Programm. Veranstaltet wird der MesseCampus wieder gemeinsam von Deutschland sicher im Netz e.V. (DsiN) und it-sa Benefiz.

Mit themenorientierten Topic Routen bietet der Veranstalter vor Ort wieder ein aus den Vorjahren bekanntes Instrument zur Orientierung. Dank vorgezeichneter Wege finden Besucher wie in einem Stadtplan schnell die richtigen Ansprechpartner und Spezialisten, die zu konkreten Fragestellungen Auskunft geben.

Congress@it-sa

Zum dritten Mal findet das begleitende Kongressprogramm Congress@it-sa statt, das Gelegenheit zur vertieften Auseinandersetzung mit spezifischen Fragen der IT-Sicherheit bietet. Unter einem gemeinsamen Dach informieren Verbände und Unternehmen zwischen dem 6. und 9. Oktober zu zehn aktuellen Programmpunkten. Das Kongressprogramm startet wieder mit der Jahrestagung der

IT-Sicherheitsbeauftragten der Länder und Kommunen. Sie macht bereits zum zweiten Mal in Folge in Nürnberg Station. Gleich am Montag, den 6. Oktober, schulen sich IT-Sicherheitsbeauftragte und

Beschäftigte im IT-Sicherheitsmanagement der öffentlichen Verwaltung zu den Besonderheiten von IT-Infrastrukturen und -Verfahren in der öffentlichen Verwaltung. Ebenfalls am Montag bietet cirosec eine Einschätzung aktueller Angriffsszenarien, klärt über ihre Relevanz auf und spürt den Angriffsformen nach, die in Zukunft an Bedeutung gewinnen.

TÜViT fragt in einem praxisorientierten Workshop am Dienstag, 7. Oktober, wie mobile Endgeräte und Apps geschützt in die Unternehmens-IT integriert und verwaltet werden können. Um Cloud-Konzepte, Virtualisierung und Outsourcing oder spezielle Brandschutzlösungen für Rechenzentren geht es in der von BITKOM ausgerichteten Vortragsreihe "IT-Sicherheit und Verfügbarkeit". Sie findet ebenfalls am Dienstag statt. Application Hacking ist ein weiteres Thema am Dienstag, zu dem Experten von qSkills informieren. Außerdem geht es am ersten Messetag um die Frage, welche Herausforderungen intelligente Stromnetze, Industrie 4.0 und die zunehmende Vernetzung unseres Lebensumfelds für IT-Sicherheitsprofis mit sich bringen. Das Bayerische IT-Sicherheitscluster begrüßt die Kongressteilnehmer unter dem Motto „Safety meets Security“ zum Gespräch mit Experten, unter anderem über die IT-Sicherheit im Prozessnetzwerk eines Energieversorgers und Security Audits von vernetzten industriellen Komponenten. An Entscheider in Unternehmen jeder Größenordnung richtet sich der Bayerische Unternehmensverband Metall und Elektro bayme vbm/partnering von Dienstag bis Donnerstag mit einem umfassenden Programm. Haftungsrisiko Website, Internetsicherheit für den Mittelstand oder ganzheitliche Ansätze zur Cybersicherheit stehen hier auf der Agenda.



Der Congress@it-sa bietet zehn Vortragsreihen mit 14 Kongress-Tracks.
Bilder: NürnbergMesse

Am Mittwoch, den 8. Oktober, dreht sich bei Congress@it-sa alles um Identity- und Accessmanagement sowie Cloud-Security. Über „Authentifizierung, Vergabe und Kontrolle von Berechtigungen oder Single Sign On“ informiert FSP Software & Consulting. Ein zweiter Block, der vom Bayerischen IT-Sicherheitscluster veranstaltet wird, heißt „Cloud- und Informationssicherheit – praktisch umgesetzt in KMU“. Der Fokus liegt hier auf Überlegungen zur Daten- und Informationssicherheit für kleinere und mittlere Betriebe und Informationen zur sicheren Nutzung von Cloud-Diensten. Proofpoint zeigt den Kongressteilnehmern, wie sie sich vor gezielten Attacks und Advanced Threats schützen können. Trend Micro lädt am Mittwoch außerdem zum ersten Trend Micro Weltsicherheitsfrühstück, das den Auftakt für die Präsentation aktueller Cloud- und Mobile-Security-Lösungen bildet.

Bühne für Politik und Verbände

Die it-sa ist auch wieder Kristallisationspunkt für das Engagement von Verbänden und Institutionen im Bereich der IT-Sicherheit. Zu den begleitenden Veranstaltungen im Messezentrum Nürnberg zählt auch der vierte IT-Grundschutztag am Mittwoch, den 8. Oktober. Inhaltlich dreht sich bei der Veranstaltung des Bundesamts für Sicherheit in der Informationstechnik diesmal alles um das Thema Identitäts- und Berechtigungsmanagement. Der BITKOM nutzt – wie in den vergangenen Jahren – die it-sa als Plattform für die Ausrichtung des Executive Dinner. Hier treffen sich Vorstände und Geschäftsführer der BITKOM-Mitgliedsunternehmen.

Alle Aussteller, ihre Produkte und eine Hallenübersicht sind abrufbar unter: www.it-sa.de/aussteller-produkte

**Besuchen Sie uns
auf der it-sa 2014**

Halle 12 | Stand 310

Halle 12 | Stand 321 bei **[sysob]**



SecurITy
made
in
Germany

HSM – Datensicherheit aus einer Hand

Egal ob optische, magnetische und elektronische Speichermedien, mit Akten- und Festplattenvernichtern von HSM werden die unterschiedlichsten Datenträger zuverlässig vernichtet. www.hsm.eu



Halle 12



Besuchen Sie uns:

**HALLE
12
STAND
125**



Unsere **Sicherheitslösungen:**
für Unternehmen, Hotels, Schulen und Privatanwender

- > Arbeitsplatzschutz
- > Systemwiederherstellung
- > WLAN-Zugangskontrolle
- > Viren- und Spamschutz



**Marktführer im
Schwachstellen-
und Compliance
Management**

Halle 12, Stand 429




Die Experten für Privileged Account Security

**Besuchen Sie uns:
Halle 12, Stand 318**




ZERTIFIZIERTE DATENLÖSCHUNG

Halle 12, Stand 338
Tel. 07141-95660-25, www.blancco.com



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



Exhibitors:

- IAM-AREA certgate 12.0-516
- IAM-AREA Peak Solution 12.0-519
- ectacom 12.0-520
- Kaspersky 12.0-416
- TESIS 12.0-517
- baramundi 12.0-414
- G Data 12.0-415
- QGroup 12.0-312
- Infotecs 12.0-315
- Passwerk 12.0-313
- Desk Center 12.0-216
- elmos 12.0-214
- Juniper Networks 12.0-219
- CyProtect 12.0-114
- Czech Trade 12.0-413
- Jakob software 12.0-109
- PSW GROUP 12.0-108
- Thales 12.0-212
- SecureGUARD 12.0-309
- IKARUS 12.0-208
- Splunk 12.0-207
- Consist 12.0-205
- Akamai 12.0-104
- Checkmarx 12.0-103
- LogPoint 12.0-107
- QSC 12.0-512
- CENTRIFY 12.0-510
- protected-networks 12.0-608
- Safetica 12.0-609
- Blue Frost 12.0-604
- AirWatch 12.0-603
- Wick Hill 12.0-512
- HOB 12.0-508
- Zertificon 12.0-506
- Arrow ECS 12.0-504
- ESC 12.0-511
- CenterTools 12.0-410
- CHERRY 12.0-410
- n3k Informatik 12.0-507
- Protea 12.0-508
- noris 12.0-402
- Infinigate 12.0-403
- Westcon 12.0-202
- itWatch 12.0-301

Other areas:

- Exclusive Networks 12.0-401
- Eingang Entrance West
- Bayrisches IT-Sicherheitscluster 12.0-111

Icons: Information, Access, Wheelchair, Press Center, VIP Lounge



Hochwertige Security-Schulungen

Wir setzen auf Qualität. Setzen Sie sich zu uns.

qSkills GmbH & Co. KG
Süd-West-Park 65 D-90449 Nürnberg
Tel. +49 (0)911 80 103-31 Fax +49 (0)911 80 103-39
info@qskills.de www.qskills.de

qSkills: Stand 12.0-547



EINE SICHERE IT – IHR VERDIENST

Erfolgreiches Business geht auf Nummer sicher

**Kaspersky Lab auf der it-sa
Halle 12, Stand 416**

KASPERSKY
www.kaspersky.de

State of the Art der E-Mail-Verschlüsselung



Halle 12, Stand 506

sales@zertificon.com
www.zertificon.com

zertificon



mediaTest digital TÜV
TÜV NORD GROUP

www.appsecuritycenter.com
Sicheres App Management für Unternehmen.

Halle 12.0 Stand 739

News und Produkte

apsec: Mehr PS für die Verschlüsselung

Mit dem Release 6.2 seiner Verschlüsselungslösung fideAS file enterprise präsentiert apsec Verbesserungen, die sich besonders bei großen Firmen auswirken. „Die Geschwindigkeit in der Verwaltung von mehreren tausend Nutzern hat sich um den Faktor hundert verbessert“, freut sich Marketingleiter Dr. Volker Scheidemann. „Konnten Administratoren früher beim Aktivieren einer solchen Konfiguration schon mal in die Mittagspause gehen, so reicht es jetzt nicht mal mehr zum Kaffeeholen“, so Scheidemann weiter. Neben der deutlichen Beschleunigung wartet die Lösung des deutschen Spezialisten für sichere Daten noch mit der Freigabe der Software für Windows Server 2012 R2, sowie mit der Verschlüsselung für Microsofts Cloud-Speicher OneDrive auf.

Halle 12, Stand 538

Blanco: Daten vor unbefugtem Zugriff schützen

IT-Sicherheit ist das Hightechthema des Jahres, wie unlängst die Trendumfrage des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. ergeben hat. NSA-Datenskandal und regelmäßige, die Öffentlichkeit alarmierende Datenpannen hätten das Bewusstsein

für die IT-Security gestärkt, so die Initiatoren der Umfrage. Vor diesem Hintergrund zeigt sich, wie wichtig professionelles Datenlöschmanagement in Zeiten weltweit wachsender Datenmengen ist. Wie Unternehmen durch professionelles Datenlöschmanagement ihre IT-Security und die Einhaltung von Compliance-Regeln sicherstellen und sich zugleich vor unbefugtem Datenzugriff schützen, zeigt der Datenlöschexperte Blanco an seinem Messestand.

Halle 12, Stand 338

cirosec mit aktuellen Sicherheitsthemen

Im Mittelpunkt des diesjährigen Auftritts des Unternehmens stehen, neben dem Schutz vor gezielten Angriffen, die Sicherheit von Apps auf mobilen Endgeräten und sichere Arbeitsumgebungen auf fremden Endgeräten. Im Rahmen von congress@it-sa findet am Vortag der Messe (6. Oktober 2014) zudem eine kostenfreie cirosec-Veranstaltung zum Thema „IT-Sicherheit heute – aktuelle Angriffsszenarien und Trends“ statt. Anhand zahlreicher Beispiele wird dort die Entwicklung der auf den ersten Blick unüberschaubaren Gefahren für IT-Systeme und die daraus resultierenden Schutzmaßnahmen erläutert. Intensiv wird diskutiert werden, welche Relevanz sie heute haben. Stefan Strobel, Geschäftsführer der cirosec, wird

anschließend typische, hochaktuelle Angriffsszenarien aufzeigen und moderne Sicherheitslösungen vorstellen.

Halle 12, Stand 411

Cisco Security: Schutz vor APTs

Cisco Security zeigt Sicherheitslösungen, mit denen Unternehmen neue, intelligente Cyberattacken gezielt bekämpfen können. So wurde Cisco Advanced Malware Protection um neue Funktionen erweitert und ist nun die erste Lösung, die Indications of Compromise (IoC)-Daten aus dem Netzwerk mit denen von Endgeräten abgleicht und mit integrierter Bedrohungsabwehr kombiniert. Kunden erhalten so kontinuierlichen Schutz vor Advanced Persistent Threats. Speziell für Rechenzentren und die Cloud wurde die Cisco Adaptive Security Appliance (ASA) Firewall-Familie so erweitert, dass sie nun Software Defined Networking und Application Centric Infrastructure-Umgebungen unterstützt - für optimale Leistungsfähigkeit, Skalierbarkeit und Flexibilität.

Halle 12, Stand 624

COMPUTENT zeigt Remote-Desktop-Lösung

Auf der Messe stellt COMPUTENT die neue Desktop-Version der Verbindungssoftware COMPUTENT Secure vor, die Anwenderunternehmen jetzt auch auf den firmeneigenen Laptops

Rittal – Das System.

Schneller – besser – überall.

Die RiMatrix S Roadshow kommt auch in Ihre Nähe.
Termine: www.rittal.de



Besuchen Sie uns:
it-sa in Nürnberg
07.-09.10.2014
Halle 12.0, Stand 345



nextlevel
for data centre

SCHALTSCHRÄNKE

STROMVERTEILUNG

KLIMATISIERUNG

oder Notebooks beispielsweise der Außendienst-Mitarbeiter installieren können. Dies verringert Aufwand und Kosten im Zusammenhang mit verlorenen oder gestohlenen Sticks und erhöht den Bedienkomfort für Benutzer mit fest zugeordneten Geräten. Die Verbindung der Software mit der Festplatten-ID und Passwörter schützen vor unberechtigtem Zugriff auf die Unternehmensdaten.

Halle 12, Stand 111

Consist präsentiert Security-Konzepte und -Lösungen

Der IT-Dienstleister stellt auf der Messe als Integrationspartner seinen Security-Stack und Lösungen führender Technologieanbieter vor. Grundlage des Security-Stacks ist die Kombination und Integration von Lösungen unter Einbeziehung von Big Data. Das modular aufgebaute Angebot für Unternehmen reicht von der Beratung und Konzeption über Ad-hoc-Analysen und die Implementierung geeigneter Security-Lösungen durch zertifizierte Consultants bis zu Managed Services. Die bestehende IT-Infrastruktur von Unternehmen wird so bei Bedarf auf zukunftsichere Beine gestellt und optimiert. Auch ein kontinuierliches Compliance-Monitoring ist auf diese Weise möglich. Individuelle Expertengespräche mit Consist, Splunk, ObservIT und Lieberman Software

stehen ebenso im Fokus wie Live-Demonstrationen und erfolgreiche Praxisbeispiele. Pierre Lukas von Consist referiert zudem im „Forum Rot“ (Management) über „Compliance in der Praxis“.

Halle 12, Stand 205

IT-Notfallplanung und IT-Grundschutz

IT-Grundschutz für Unternehmen und Behörden bekommt ab sofort wieder eine solide und sichere Basis: Mit der Software INDITOR präsentieren die CONTECHNET-Experten für Notfallplanung und Notfallmanagement als Erweiterung zu INDART Professional ein Modul zur Erstellung eines ISMS auf Basis von IT-Grundschutz und der ISO 27001. Das BSI unterstützte Unternehmen und Behörden seit 1998 mit seinem sogenannten „GSTOOL“ (Grundschutztool) beim Erstellen, Verwalten und Fortschreiben von IT-Sicherheitskonzepten entsprechend dem IT-Grundschutz in der vom ihm effizient geforderten Form. Seit 2008 vom BSI extern vergeben, führte die Neuentwicklung und Verzögerung des GS-TOOLS 5.0 zum Einstellen des Supports (Ende 2015) für die Version 4.x. Für die Anwender bietet CONTECHNET nun mit INDITOR eine Alternative für IT-Leitungen von öffentlichen Einrichtungen und Unternehmen an.

Halle 12, Stand 437

CORISECIO: Verschlüsselung für SharePoint

CORISECIO ist ein Hersteller von Open Source Security Produkten. Auf der it-sa werden neue Software-Security-Lösungen gezeigt: Transparente Verschlüsselung für SharePoint und sensitive Dokumente – serverseitig und ohne Client. Weltweit einzigartig ermöglicht CORISECIO eine Volltext-Suche, innerhalb verschlüsselter Dokumente. Für unterwegs bietet die „Secure Mobile Collaboration“-Lösung einen sicheren Zugriff auf vertrauliche Dokumente und Mails im SharePoint-System des Unternehmens an. Die Produkte basieren auf den Ergebnissen langjähriger, praktischer Projekterfahrung. Die Open Source secRT stellt die Basis aller von CORISECIO entwickelten Sicherheitsprodukte dar, die gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) entworfen wurde.

Halle 12, Stand 745

dacoso: 100-G-Verbindungen plus Verschlüsselung

Verschlüsselung direkt auf der optischen Übertragungsebene – das ist die Idee hinter der Sicherheitslösung von dacoso und ADVA Optical Networking. Damit können auch extrem starke Metro-Verbindungen zum Beispiel zwischen Rechenzentren zuverlässig vor Datenspionage geschützt werden. Und zwar komplett:

RiMatrix S – das modulare standardisierte Rechenzentrum.

Die revolutionäre Alternative zum individuellen Rechenzentrumsbau – im Gebäude, Container oder Sicherheitsraum.

- Standardisierte Rechenzentrumsmodule in Serie
- Einfache Bestellung
- Kurze Lieferzeit



Verschlüsselt wird die gesamte Verbindung mit allen Datenströmen. Basis dafür ist die AES 256-bit-Encryption mit häufigem Schlüsselaustausch. Die Performance der Datenübertragung bleibt dabei nahezu identisch – bei Kosten, die im Gegenwert maximaler Sicherheit überschaubar bleiben.

Halle 12, Stand 357

DATEV präsentiert Lösungen für Internetschutz und E-Mail-Sicherheit

Ausspäh-Vorfälle, Hacker-Angriffe, Datendiebstahl – fast permanent bestimmen derartige Meldungen inzwischen die Schlagzeilen. Antworten auf die Frage, mit welchen Mitteln sich der stetig steigenden Bedrohungslage in einer vernetzten Welt begegnen lässt, liefert die DATEV eG auf der it-sa. Den Messeauftritt der Genossenschaft bestimmen in diesem Jahr die Themen Internetschutz und E-Mail-Sicherheit. Am Stand zeigt der IT-Dienstleister dazu unter anderem Lösungen zur E-Mail-Verschlüsselung sowie die Sicherheitsdienstleistung DATEVnet pro, bei der der gesamte Datenverkehr des Anwenders eine mehrstufige Sicherheitszone im DATEV-Rechenzentrum durchläuft. Als weiteren wichtigen Aspekt präsentiert DATEV Lösungen für die Absicherung des Zugriffs von mobilen Endgeräten auf das Unternehmensnetzwerk.

Halle 12, Stand 425

F-Secure mit Sicherheitslösungen für den Mittelstand

Die Wahrung der digitalen Freiheit und die kompromisslose Nutzung des Internets stellen das Leitmotiv von F-Secure auf der diesjährigen it-sa dar. Unter dem Claim „Switch on Freedom“ klärt der finnische Sicherheitsanbieter den Mittelstand darüber auf, wie die Persönlichkeitsrechte von deren Mitarbeitern und die digitale Freiheit von Unternehmen in Zeiten von NSA und Co. gewahrt werden können. F-Secure wird seinen Protection Service for Business in der neuen Version zur Schau stellen. Hierbei handelt es sich um eine webbasierte,

vollautomatische Sicherheitslösung für kleine und mittlere Unternehmen mit begrenzten IT-Ressourcen. Zu den Neuerungen gehören unter anderem younited for Business, das sichere Collaboration-Tool, sowie Freedom for Business, eine Cloud-basierte Sicherheits-App für Smartphones. Diese Lösungen sind nun in die dezentrale Sicherheitslösung Protection Service for Business implementiert.

Halle 12, Stand 434

Fujitsu zeigt Sicherheitslösungen „Made in Germany“

Das Unternehmen stellt neue End-to-End-Sicherheitslösungen und -konzepte „Made in Germany“ vor. Diese unterstützen Unternehmen und Verwaltungen sowie deren Kunden und Bürger dabei, in allen relevanten Geschäftsprozessen einen angemessenen Sicherheitsstandard bei gleichzeitig hoher Gebrauchstauglichkeit und Performance zu gewährleisten. Zudem können sich Fachbesucher einen Überblick über das umfassende Sicherheitsportfolio von Fujitsu verschaffen. Dieses reicht von biometrischen Authentifizierungsverfahren über das menschliche Handvenenmuster (PalmVein) über Virtual Client Services, bis hin zu End-to-End-Lösungen für das moderne Arbeiten in verteilten Organisationen. Auch Lösungen für die beweiswerterhaltende Langzeitspeicherung und das ersetzende Scannen werden bedient.

Halle 12, Stand 362

Genua: neuer Security Laptop „cyber-top“

Firmenmitarbeiter möchten über ihre Workstations auf sensible Daten zugreifen, gleichzeitig aber auch Mail-Programme oder Browser nutzen – ohne die IT-Sicherheit zu gefährden. Der deutsche Hersteller genua präsentiert dafür mit dem Security Laptop cyber-top eine neue Lösung: Auf dem Laptop werden mittels einer neuen Separationstechnologie strikt getrennte Bereiche erzeugt, sodass Angreifer oder Malware keinen Weg beispielsweise vom Browser zu den sensiblen Daten finden. Diese Sicherheits-Sepa-

ration läuft im Hintergrund ab, der Anwender bemerkt davon nichts. Er arbeitet mit den gewohnten Programmen und kann das Security Laptop im Büro, unterwegs oder auch im Home Office einsetzen. Auf dem cyber-top läuft das Separationssystem L4. Dieses erzeugt auf dem Laptop strikt isolierte Compartments: In einem laufen die Mail- und Browser-Programme, in einem anderen die Anwendungen zur Bearbeitung sensibler Daten. Da jedes Compartment mit einem eigenen Betriebssystem ausgestattet ist, bestehen keine Abhängigkeiten.

Halle 12, Stand 422

HSM: Speichermedien sicher vernichten

Im Mittelpunkt auf dem HSM-Messestand steht der mechanische Festplattenvernichter HSM Powerline HDS 230. Digitale Datenträger werden mit Hilfe eines robusten Vollstahl-Schneidwerks in kleinste Partikel zerschreddert, so dass eine Wiederherstellung unmöglich ist. Vernichtet werden können Festplatten und Magnetbänder, CDs/DVDs, Disketten, USB-Sticks sowie Mobiltelefone. Ebenfalls zu sehen ist das Spektrum an klassischen Aktenvernichtern, die direkt vor Ort begutachtet und getestet werden können. Die Shredder machen vertrauliche Dokumente unleserlich – und das in verschiedenen Sicherheitsstufen, die von Stufe zu Stufe ein höheres Maß an Sicherheit gewährleisten.

Halle 12, Stand 442

Infinigate: neue E-Mail-Verschlüsselungslösung

Der IT-Security-Distributor Infinigate ist neuer Vertriebspartner von Secure Messaging-Experte SEPPmail. Bei SEPPmail schickt der Nutzer die digitale Post mit seinem lokalen E-Mail-Programm ab und markiert diese als „vertraulich“; den Rest übernimmt das Sicherheitssystem von SEPPmail. Die Nachricht wird verschlüsselt und als HTML-Anhang vollständig an den Empfänger ausgeliefert. Zusätzlich kann der Mitarbeiter die Nachricht mit einer digitalen Signatur versehen.

IT-Sicherheit mit Security Information und Event Management von McAfee am Flughafen Köln Bonn

Der Köln Bonn Airport zählt mit mehr als neun Millionen Passagieren und über 740.000 Tonnen Luftfracht zu einem der größten Verkehrsflughäfen Deutschlands.

Für einen internationalen Flughafen gelten strenge Anforderungen hinsichtlich Pünktlichkeit und Sicherheit – und das geht u.a. nur mit einer ausfallsicheren IT. Dafür müssen die IT-Verantwortlichen Netzwerk, Server, Datenbanken und Steuerungssysteme wirkungsvoll, und aus Compliance-Gründen auch nachweislich, vor Angriffen schützen. Hierfür zeichnet der Geschäftsbereich Informationstechnologie des Köln Bonn Airport verantwortlich.

Sicherheit und Compliance das A und O

Ein Unternehmen dieser Komplexität und mit den besonderen Anforderungen eines Flughafens muss ganz besonders darauf achten, alle Vorgaben für IT-Sicherheit und IT-Compliance zu erfüllen. Im Falle des Köln Bonn Airport war der Nachweis der IT-Sicherheit nicht immer einfach – die IT-Infrastruktur war wie in vielen großen Netzwerken über die Jahre heterogen und unterschiedliche Systemarchitekturen mussten manuell miteinander in Einklang gebracht werden.

Aufwändige Analysen an unterschiedlichen Management-Konsolen verbrauchten dabei unverhältnismäßig viele Ressourcen, Korrelationen zu bereits bestehenden Information waren nicht möglich. Die IT musste potentielle Schwachstellen zunächst identifizieren und den betroffenen Informationssystemen manuell zuordnen. Eine Aussage zum Grad der Verwundbarkeit war nicht immer kurzfristig möglich, und damit auch die Einhaltung der

Compliance problematisch. Eine neue Lösung sollte diese Situation verbessern.

Integriertes Steuerungscockpit für die IT-Sicherheit

Diese neue Lösung musste vor allem zwei Dinge erfüllen: die Transparenz erhöhen und die IT-Landschaft zentral steuerbar machen. Auch sollten alle Informationen die IT-Sicherheit betreffend über ein integriertes „Steuerungscockpit“ teilweise automatisiert kontrolliert, beeinflusst und dokumentiert werden können.

Um dies zu realisieren, entschied sich der Köln Bonn Airport für die Security Information und Event Management (SIEM)-Lösung „McAfee® Enterprise Security Manager“. Sie erfüllte nicht nur die Vorgaben hinsichtlich des Reportings, sondern bietet der IT auch die Möglichkeit, zeitnah und fundiert auf Sicherheitsvorfälle reagieren zu können. Weil das System eine risikobasierte Priorisierung von Maßnahmen erlaubt, können nun auch Aufgaben zur Schwachstellen- und Bedrohungsbekämpfung intelligent gesteuert und nachgehalten werden.

Die protokollierten Informationen sind vollständig, fälschungssicher und unveränderbar, um die Beweiskraft der Berichte sicherzustellen. Die Lösung kann außerdem heterogene Informationen für ein Gesamtlagebild normalisieren und ermöglicht es dem Team, sehr einfach einzelne priorisierte Vorgänge

aus der Menge aller Ereignisse zu filtern. Granulare Zugriffsrechte erhöhen die Sicherheit auf ein Maximum.

Passgenaue Sicherheit durch SIEM-Individualisierung

Heute kann der Geschäftsbereich Informationstechnologie des Köln Bonn Airport relevante Ereignisse produktunabhängig und angepasst an die jeweiligen Bedürfnisse der verschiedenen Fachteams betrachten. Durch die Integration mit McAfee Vulnerability Manager und McAfee ePolicy Orchestrator® (McAfee ePO™) kann die IT nun Bedrohungen und Störungen der IT-Landschaft zielgerichtet behandeln. Und das spart Zeit im laufenden Betrieb.

Je besser integriert und intelligenter die SIEM-Lösung, desto mehr Kontrolle bietet sie den Verantwortlichen. Als Teil des McAfee „Security Connected“-Ansatzes integriert sich der McAfee Enterprise Security Manager nahtlos in McAfee ePO, McAfee Risk Advisor sowie in McAfee Global Threat Intelligence und liefert den notwendigen Kontext für eine autonome und adaptive Verwaltung von Sicherheitsrisiken.

Sie möchten mehr erfahren?

Dann besuchen Sie uns doch auf der it-sa 2014 in Nürnberg, Halle 12, Stand 403.



Der Empfänger weiß dadurch, dass die Nachricht tatsächlich vom Absender stammt und auch am Transportweg nicht verändert wurde. Im Anschluss generiert SEPPmail einmalig ein Passwort, welches der Absender dem Empfänger telefonisch oder automatisiert via SMS übermittelt. Der Empfänger muss sich einmalig am SEPPmail-System registrieren und kann die geschützte Nachricht mittels Passwort zum Lesen freischalten. Im Anschluss ist es dem Adressaten möglich, eine sichere, ebenfalls verschlüsselte E-Mail-Antwort an den Absender zu verfassen.

Halle 12, Stand 403

Infotecs zeigt ViPNet

Am Infotecs Stand können sich Interessierte von den Security-Spezialisten rund um das Thema IT-Sicherheit und Verschlüsselung beraten lassen. Im Mittelpunkt steht die ViPNet Technologie, welche in Hinblick auf Security, Connectivity und Usability sowohl für den Einsatz in KMU und Großunternehmen als auch in den Branchen Industry, Health oder Energy geeignet ist. Bei ViPNet VPN handelt es sich um eine VPN-Lösung zur sicheren und verschlüsselten Übertragung von sensiblen Daten zwischen verschiedenen Firmenstandorten und beispielsweise mobilen Mitarbeitern im Außendienst. Dabei kann das VPN-Netzwerk auf beliebig viele Endpunkte erweitert werden. Als Netzwerkknoten eignen sich alle Endgeräte, welche über einen Internetanschluss verfügen. Speziell für Administratoren stellt Infotecs den ViPNet StateWatcher vor. Dieses Incident- und Reporting-Tool überwacht das mit ViPNet aufgebaute Netzwerk und informiert unmittelbar über Ereignisse und kritische Systemzustände entsprechend im Vorfeld definierter Regeln.

Halle 12, Stand 315

ITConcepts: IDM-System für den Mittelstand

ITConcepts stellt seine vorkonfigurierte IDM-Lösung go:Identity vor, durch die sich sensible Daten sowie geschäftskritische Informationen

durch ein konsistentes Zugriffsmanagement vor unberechtigtem Zugriff schützen lassen. Die Standardlösung enthält die wichtigsten IDM-Prozesse und Funktionen und ist in kürzester Zeit einsatzbereit. So bleibt das IDM-Projekt besonders für mittelständische Unternehmen überschaubar und kalkulierbar, und gleichzeitig können sie den gesetzlichen Anforderungen an Compliance gerecht werden. Computacenter, Devoteam GmbH und die ITConcepts Professional GmbH haben zudem im Bereich "Identity und Access Management" (IAM) eine enge Zusammenarbeit vereinbart. Zusammen haben sie jetzt einen Prozess aufgesetzt, mit dem Erfahrungen aus Projekten ausgetauscht, analysiert und die Methodenkompetenz stetig weiterentwickelt wird. Erste Erfahrungen aus gemeinsam durchgeführten Projekten zeigen, dass die Kunden dadurch bis zu 53 Prozent schneller ihre Projektziele erreichen.

Halle 12.0, Stand 541

itWatch: Vertrauensketten von der Tastatur bis zu den Daten

itWatch stellt 2014 durchgehende Vertrauensketten vor. Zum einen von den Ein-/Ausgabe-Geräten des Anwenders über vertrauenswürdige Services bis zu den geschützt liegenden Daten – zum anderen ein durchgehendes Lifecycle Modell vom Risiko über die Qualität und Quantität des Angriffs zum adäquaten Schutz. Die Schutzverfahren sind alle aus nationaler Produktion. Dazu sind folgende Innovationen vorbereitet: Risiko auf Knopfdruck - RiskWatch, MalWare-Trap, die sichere Tastatur, sichere und effiziente Speicherung von (Internet)-Passworten, Kostensenkung durch virtuelle Schleusensysteme sowie das Beheben von Blinden Flecken im Lagebild / SIEM.

Halle 12, Stand 301

Im Blickpunkt: Security Consulting von KPMG

Weltweit arbeiten über 2000 Sicherheitsexperten des KPMG-Netzwerks – davon mehr als 100 in Deutschland

– an Lösungen und Konzepten, mit denen sich Unternehmen und Organisationen gegen Cyber-Angriffe und Sicherheitsbedrohungen schützen können. Die KPMG-Experten begleiten Unternehmen dabei umfassend: von der Entwicklung und Umsetzung der Sicherheitsstrategie über den Aufbau der Sicherheitsorganisation bis hin zur Auswahl, Implementierung und Konfiguration geeigneter technischer Tools und Sicherheitskomponenten. Mithilfe eigener Cyber Defense und Security Labs testet KPMG die Wirksamkeit von Maßnahmen zum Schutz der kritischen Infrastruktur, Industrieanlagen und Informationswerte der Kunden. Darauf aufbauend werden Sicherheitslösungen entwickelt, die individuell auf die Gefahren für Ihr Unternehmen ausgerichtet sind.

Halle 12, Stand 445

Kaspersky Lab: „Eine sichere IT – Ihr Verdienst“

Kaspersky Lab präsentiert sich auf der it-sa unter dem Motto „Eine sichere IT – Ihr Verdienst. Erfolgreiches Business geht auf Nummer sicher“. Am Stand informiert der IT-Sicherheitsexperte zusammen mit seinen Partnern Bücker EDV, CyProtect, NetPlans und saveITfirst in persönlichen Gesprächen, Live-Demos und Vorträgen über die zentralen Fragen der IT-Sicherheit. Im Mittelpunkt steht mit Kaspersky Endpoint Security for Business, Kaspersky Security for Virtualization und Kaspersky Fraud Prevention ein umfassendes IT-Sicherheitslösungsportfolio für kleine, mittlere und große Unternehmen. Die Experten von Kaspersky Lab halten unter anderem folgende it-sa-Vorträge: „IT Bedrohungen, Trends & Mitarbeitersensibilisierung“ (7.10., 11:30 Uhr, Forum Rot) und „Wie kann eine virtualisierte IT-Umgebung geschützt werden?“ (8.10., 13:30 Uhr, Forum Blau).

Halle 12, Stand 416

m-privacy: ReCoBS mit Rückenwind

Immer mehr Bundes- und Landesbehörden, Verwaltungseinrichtungen

und öffentliche Stellen setzen auf dedizierte Remote-Controlled-Browser-Systems (ReCoBS) zum Schutz ihrer Netze. Das Präventivkonzept gegen Angriffe über den Internetbrowser überzeugt Dienststellenleiter und IT-Verantwortliche. Die Zahl der von der m-privacy GmbH angebotenen PC-Arbeitsplätze geht mittlerweile weltweit in die Zehntausende. Zur diesjährigen it-sa präsentieren sich die TightGate-Appliances speziell zum Einsatz in ausgedehnten Infrastrukturen. Auch die Nutzung lokaler Drucksysteme und die Systemintegration mit CITRIX-Terminalservern sind weitere Highlights des „ferngesteuerten Browsers“. Details gibt es am Messestand oder im Internet unter www.m-privacy.de.

Halle 12, Stand 427

mediaTest digital und TÜViT: Launch des Application Security Center

Das Application Security Center ist eine „360° App Risk Management“-Plattform, die sich sowohl an Unternehmen als auch an App-Entwickler und Publisher richtet. Unternehmen statten Dienstgeräte mithilfe des Trusted App Directory mit sicheren Apps aus – wahlweise als eigenständige Lösung oder als Add-on zu einem bestehenden MDM-System. App-Entwickler und Anbieter lassen ihre Apps von den Experten testen und setzen nach einer erfolgreichen Auditierung das „TRUSTED APP“-Siegel als schlagkräftiges Verkaufsargument ein. Ob für unternehmensinterne oder öffentliche Anwendungen: Die Security Guidelines ermöglichen es Entwicklern, sichere Apps zu programmieren.

Halle 12, Stand 739

NCP: Secure Remote Access made in Germany

Der Nürnberger Remote Access VPN-Spezialist NCP präsentiert auf seinem Messestand hochsichere VPN-Lösungen für den Fernzugriff via Notebook, Tablet PC oder Smartphone auf Netze von Firmen, Institutionen und Behörden. Unter dem

Motto "Secure Remote Access made in Germany" dreht sich auf dem NCP Messestand alles um universelle VPN-Lösungen für Android, iOS, BlackBerry, Windows, OS X und Linux. Das Portfolio umfasst IPsec VPN Clients mit eigenem Internet Connector, 3G/4G-Kartenunterstützung, WLAN-Verwaltungstool und dynamischer Personal Firewall, ein mandantenfähiges VPN Management System, virtualisierbare VPN Serversoftware für IPsec und SSL Remote Access-VPNs sowie eine VPN-Box für sicheren Remote Access nach Geheimhaltungsstufe VS-NfD.

Halle 12, Stand 413

NetIQ: Lösungen für Identity- und Access Management

Das Unternehmen präsentiert Lösungen für Identity- und Access Management, Sicherheit und Compliance in physischen, virtuellen und Cloud-Umgebungen. Gemeinsam mit den Partnern G+H Netzwerk-Design, IPG AG und IS4IT GmbH werden Lösungen vorgestellt, die einen identitätsgesteuerten sicheren, verwaltbaren Zugriff auf kritische Dienste und Daten sowie eine schnelle Reaktion auf Bedrohungen ermöglichen. Mit den Sicherheitslösungen von NetIQ und Partnern sind Unternehmen in der Lage, interne Sicherheitsvorgaben konsequent durchzusetzen und gesetzliche Auflagen nachprüfbar zu erfüllen. Interne Kontrollsysteme und Risikofrüherkennung Management ermöglichen zudem Überwachung, Reporting und Problembehebung für alle IT-Ressourcen.

Halle 12, Stand 524

Paessler AG: PRTG Network Monitor

Die zukunftsichere Gestaltung der IT-Infrastruktur ist eine anspruchsvolle Herausforderung. Die Netzwerkexperten der Paessler AG zeigen auf der Messe, wie Unternehmen mit der Netzwerküberwachungssoftware PRTG Network Monitor alle Systeme und Geschäftsprozesse ihrer IT-Infrastruktur ausfallsicher einrichten, den kompletten Überblick über lokale

und externe Standorte bewahren und ihre Netzwerkbereiche optimieren.

Halle 12, Stand 313

PCS zeigt Handvenenerkennung

Das Unternehmen PCS präsentiert sein Spektrum zum Unternehmensschutz mit physischer Zutrittskontrolle, Kennzeichenerkennung, Zufahrtskontrolle, Videoüberwachung und -Analyse sowie Zeiterfassung. Im Umfeld der Ausstellung „Das perfekte Rechenzentrum“ präsentiert PCS die hochsichere Handvenenerkennung INTUS 1600PS als Zutrittssicherung. Die PCS On- und Offline- sowie Biometrie-Zutrittsleser und die Zeiterfassungsterminals werden zusammen mit der Zutrittskontrollsoftware DEXICON zum integrierten Schutzsystem und über die OPC-Schnittstelle an ein Leitstands- oder Gebäudemanagementsystem angebunden. Das Unternehmen zeigt außerdem eine Zutrittskontrolle mittels eines NFC-Tags an Offline-Türterminals. Neu auf der it-sa ist das leistungsstarke PCS-Besuchermanagement, das revisionssicher alle Vorgänge dokumentiert.

Halle 12, Stand 354

Ping Identity: Multi-Faktor- Authentifizierung

Die Identity Security Company Ping Identity stellt neue Lösungen für die Post-Passwort-Ära vor: PingID ist ein Ansatz zur Multi-Faktor-Authentifizierung. Dabei steht die Nutzererfahrung im Fokus, denn die Authentifizierung funktioniert über Smartphones. Mit Ping Federated Access Management können Unternehmen Identitätsregeln schnell und einfach erweitern – über Clouds, mobile Umgebungen und API hinweg und ohne Security Coding und WAM-Umbau. PingOne ist eine IDaaS-Lösung, mit der sich sowohl eine positive Nutzererfahrung als auch die notwendigen Zugangskontrollen und Sicherheitsregeln gewährleisten lassen. Außerdem unterstützt PingOne die Multi-Faktor-Authentifizierung, so dass Unternehmen ihre geschäfts-

kritischen Anwendungen noch besser schützen können.

Halle 12, Stand 514

QGroup: physikalische und logische Zutrittskontrolle

Wie sich Unternehmen vor Datenklau schützen können, welche Strategie, Vorkehrungen und Produkte geeignet sind, um unautorisierten Zugriff auf Unternehmensdaten und -applikationen zu verhindern, zeigt der IT-Sicherheitshersteller QGroup. Dort zu sehen sind neben sicheren Betriebssystemen und Security-Appliances-Lösungen zur physikalischen und logischen Zutrittskontrolle, wie beispielsweise die Multifaktor-Authentifizierungslösungen mit und ohne Biometrie QTrust 2go Life und Smart. Mit diesen Lösungen, die per Smartphone oder Smartcard unterschiedliche biometrische Merkmale abfragen, ist eindeutig sichergestellt, dass nur der autorisierte Nutzer Zugriff erlangt.

Halle 12, Stand 312

qSkills zum Schnuppern und auf dem Congress@it-sa

Das Trainingsunternehmen qSkills zeigt anlässlich der it-sa sein Fach-Know-how zu neuesten IT-Sicherheitsthemen. Kern des qSkills-Messeauftritts sind wie in den letzten Jahren rund 30-minütige Schnuppertrainings am Messestand. Die Schnuppertrainings reichen von der IT-Sicherheit über das Hacking/Digitale Forensik und Security E-Learning bis zur Prozessmodellierung (BPMN 2.0) sowie neuesten Erkenntnissen im Risikomanagement und der Normen- und Standard-Welt. Einen weiteren Höhepunkt des qSkills-Messeauftritts bilden Vortragsreihen auf dem Congress@it-sa. Im Mittelpunkt der 2-stündigen Vorträge am ersten Messtag stehen die zwei Themenfelder: „Prozesse sicher, compliant und effizient steuern - BPMN 2.0 im IT-Service-Management“ sowie „Herzlich willkommen in unserem Netz – 7 Einladungen, die Hacker gerne annehmen?“.

Halle 12, Stand 547

REDDOXX: Sicheres, ganzheitliches E-Mail-Management

Am Stand von REDDOXX dreht sich alles um sicheres E-Mail-Management. Der deutsche Hersteller präsentiert die Lösungen MailDepot (rechtskonforme E-Mail-Archivierung), MailSealer (Verschlüsselung/Signatur) und Spamfinder (Anti-Spam). Unternehmen und Organisationen können ihre E-Mail-Kommunikation damit über den gesamten Lebenszyklus absichern: Vom Spam-Schutz über vertraulichen Versand und Empfang von E-Mails per Verschlüsselung und Signatur bis hin zur gesetzlich geforderten, compliancegerechten Langzeit-Archivierung. Ältere Mails lassen sich jederzeit wiederherstellen, während lokale Systeme entlastet werden. Besucher erhalten einen ersten Einblick in die neue Version 2031 inklusive komfortablem Administratoren-Zugriff per Web-GUI.

Halle 12, Stand 321

RÜHLCONSULTING: Normen, Standards und Awareness

Das Beratungsunternehmen präsentiert die neusten Erkenntnisse aus den Bereichen Risikomanagement, Informationssicherheitsmanagement (ISMS) sowie Business Continuity Management. Konkret zeigt das Expertenteam von RÜHLCONSULTING seine Expertise rund um aktuelle Entwicklungen aus der Normen- und Standardisierungswelt. Hierzu zählen unter anderem Neuerungen zu ISO 27001 für das ISMS und 31000 im Risikomanagement sowie Gründe für den Einsatz eines Business Continuity Managements. Abgerundet werden die Inhalte durch das Thema Awareness. Denn gerade Sensibilisierungsmaßnahmen sind ein wesentlicher Schlüssel zum Erfolg jeder IT-Sicherheits- und Risikomanagementstrategie.

Halle 12, Stand 547

Secorvo: Neuauflage des T.I.S.P.-Begleitbuchs

Seit 2004 können Informationssicherheitsspezialisten ihre Kenntnisse in allen Kerngebieten der Informationssicherheit durch ein T.I.S.P.-Zer-

tifikat bestätigen lassen. Das T.I.S.P.-Begleitbuch „Zentrale Bausteine der Informationssicherheit“ ist ein auf diesen 26 Themenfeldern aufbauendes Kompendium für Fachexperten. Es eignet sich sowohl zur Vorbereitung auf eine T.I.S.P.-Prüfung als auch zum Selbststudium. Die zweite, aktualisierte Auflage wurde um die Kapitel Recht, Netzwerksicherheit (einschließlich IPv6) und Incident Management erweitert. Auch die im Jahr 2013 überarbeiteten ISO 2700x-Standards wurden berücksichtigt. Die Autoren sind Berater bei Secorvo und Referenten der T.I.S.P.-Schulung. Zusammen verfügen Sie über 250 Jahre Berufserfahrung in Informationssicherheit und Datenschutz.

Halle 12, Stand 646

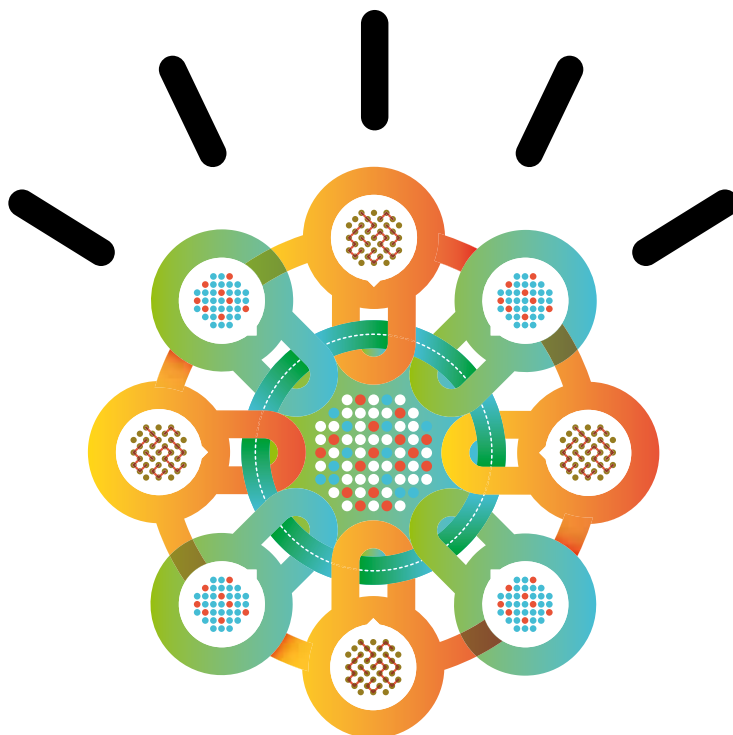
SECUDE: Datenschutz für Export aus SAP Systemen

HALOCORE ist eine Technologie, die sich direkt in die SAP-Anwendungen einfügt und sensible Daten mit minimaler Benutzerinteraktion klassifiziert und schützt. Die Lösung fungiert als Middleware zwischen SAP und ihrer Microsoft-Umgebung. Dabei erfolgt eine automatische Verschlüsselung der aus SAP exportierten Daten, bei gleichzeitiger Vergabe von Zugriffsrechten, mittels Active Directory Rights Management Services (AD RMS) von Microsoft. Die immateriellen sowie Finanz- und Mitarbeiterdaten der Unternehmen können so gesichert werden, dass nur autorisierte Personen darauf zugreifen können, ganz gleich welchen Transportweg die Daten nehmen, ob sie lokal, auf einem Server oder in der Cloud abgespeichert werden.

Halle 12, Stand 514

secunet: Penetrationstests als laufender Service

secunet stellt unter anderem PaPSS vor – mit „Penetrationstests as Permanent Security Service“ bietet secunet ein Werkzeug für vereinfachte interne Schwachstellenscans. Die Appliance wird von secunet speziell auf das Kunden-Netzwerk und seine Bedürfnisse hin konfiguriert. Die anschließende Dokumentation findet bei secunet



Security Intelligence. Think Integrated.

The threat landscape continues to challenge organizations with increases in advanced attacks resulting in more security breaches, while mobile, social and cloud initiatives create greater IT complexity and expose new vulnerabilities. To keep pace, you need a proactive, big-picture approach to protecting users, data and infrastructure in an integrated manner.

IBM Security offers a framework of integrated security intelligence capabilities, backed by industry-leading experience and supported by world-renowned IBM X-Force research and development. These capabilities and services are delivered through a comprehensive and robust set of tools and best practices, delivering distinct value through:

Intelligence

Our security portfolio is unmatched in its depth and breadth of technology and services, which ward off a wide range of threats and accelerate the detection and remediation of those that slip through.

Expertise

IBM can help you incorporate security into your new initiatives and innovations with easy-to-use offerings and strategic roadmaps that simplify the proactive adoption of security.

Integration

Our solutions and services systematically integrate both new and existing security products, providing critical visibility at a fast time to value—and enabling you to retain your existing investments.

For more information, please visit ibm.com/security or securityintelligence.com.



statt, wo die die Ergebnisse der automatischen Testläufe analysiert und hinsichtlich kritischer Schwachstellen untersucht werden. Damit bietet PaPSS einen Service, der sich nahtlos in jede spezifische IT-Infrastruktur beim Kunden integrieren lässt.

Halle 12, Stand 636

Infoblox: Appliance-basierte DNS-Lösung

Infoblox stellt zwei Produkte vor: Advanced DNS Protection, eine DNS-Appliance, die über integrierte Verteidigungsmechanismen gegen DNS-basierte Angriffe verfügt und DNS-basierte Attacken wie Amplification, Reflection, Cache Poisoning, DNS Tunneling, DDoS erkennt, alarmiert und verhindert. Die DNS-Firewall unterbindet den Protokoll-Missbrauch durch Malware und Spyware mittels einer Reputations-Prüfung, ähnlich den Methoden, die seit vielen Jahren erfolgreich im Bereich E-Mail als Schutz gegen SPAM verwendet werden.

Halle 12, Stand 526

SecuPedia: Sicherheitstipps aus der Praxis

Neben den aktuellen Sicherheitsmeldungen und dem Sicherheitslexikon bietet die Sicherheits-Plattform www.secupedia.de des SecuMedia-Verlags ab sofort auch ganz praktische Hilfen in Sachen IT-Sicherheit: Unter der Rubrik „Sicherheitstipps aus der Praxis“ gibt es konkrete Antworten und Anleitungen für mehr Sicherheit im Beruf wie im Privatleben. Autor ist Oliver Wege, im Berufsleben landesweiter IT-Sicherheitsmanager des Landes Brandenburg. Oft sind es einfache, aber wirksame Hinweise, die schnell einen großen Sicherheitsgewinn zur Folge haben. Zum Beispiel der Rat: „Zumindest der Mailaccount sollte grundsätzlich immer ein separates Passwort bekommen. Fast jeder Online-Dienst bietet ein Passwortrücksetzungsverfahren unter Beteiligung des Mail-Postfachs an. Wer also Zugriff auf das Postfach hat, kann leicht auch in alle anderen genutzten Dienste einbrechen.“ Als „Grundausrüstung“ hält SecuPedia

Antworten auf fünf besonders häufig gestellte Fragen bereit: Anonymisieren im Internet, Browser-Sicherheit, Passwortschutz für Internet-Dienste, Verschlüsselungsprogramme und Webmailerauswahl.

Halle 12, Stand 628

Sophos: Umfassende Sicherheitslösungen für KMUs

Sophos präsentiert IT-Sicherheitslösungen, die vor allem auf kleine und mittelständische Unternehmen ausgerichtet sind: Neben der neuen SG Hardware Serie stellt Sophos auch die aktuellen Versionen der UTM-, Mobile-Control-, Endpoint- oder Verschlüsselungslösungen unter fachkundiger Anleitung vor. Highlights sind die neuen Cloud-Angebote und das Sicherheitsprojekt Galileo. Mit Galileo vereint Sophos seine Endpoint-, Server- und Netzwerk-Security-Technologie unter einer Managementoberfläche und ermöglicht so miteinander kommunizierende IT-Sicherheitsmodule (Context Aware Security). Sophos Cloud, eine einfach zu administrierende Sicherheitslösung, mit der Windows-, Mac- und mobile Geräte unter einer einheitlichen Konsole verwaltet werden können. Daneben baut Sophos weiterhin auf seine On-Premise-Versionen, um IT-Profis die Wahl zwischen virtuellen oder Vor-Ort-Lösungen zu bieten.

Halle 12, Stand 426

sysob und REDDOXX: Strategien für sicheres E-Mail-Management

sysob zeigt am Stand professionelle Lösungen aus den Bereichen IT-Security, Wireless LAN sowie Serverbased Computing, Traffic Management, Storage, Cloud Computing und MSSP. Partner REDDOXX ist mit von der Partie und fokussiert in diesem Jahr das Thema sicheres E-Mail-Management. Der deutsche Hersteller präsentiert die neuen Versionen seiner Lösungen MailDepot, MailSealer und Spamfinder. Mit REDDOXX bietet sysob seinen Partnern eine Komplettlösung „Made in Germany“ für E-Mail-Archivierung, Anti-Spam, Virenschutz

und Verschlüsselung. Alle rechtlichen Anforderungen (TÜV geprüft) werden automatisiert erfüllt und es wird auch ermöglicht, firmeninterne Regelungen umzusetzen. Bei der neuen Version legten die Entwickler den Schwerpunkt vor allem auf das komfortable Management für Administratoren mittels neuer Web GUI.

Halle 12, Stand 321

SySS bietet digitale Forensik

Nicht nur Prominente kennen das mulmige Gefühl, wenn intime Bilder ohne ihre Zustimmung publik werden. Auch Firmenvorständen und Geschäftsführern wird es angst und bange, wenn sie erfahren, dass vertrauliche Daten in die Hände von Hackern gelangt sind und ihnen dadurch wirtschaftlicher Schaden droht. Die SySS GmbH hat die Forensik-Abteilung erheblich weiterentwickelt und hilft betroffenen Firmen, mit geeigneten Incident-Response-Maßnahmen angemessen auf solche Vorfälle zu reagieren. Auch bei jeglichem Verdacht von Missbrauch in der IT bietet das Unternehmen die Dienstleistung der Digitalen Forensik an.

Halle 12, Stand 342

Zertificon: Kombi für „Organizational & Personal End2End“

„Z1 SecureMail End2End“ ist die neue Entwicklung von Zertificon und realisiert zusammen mit dem Z1 SecureMail Gateway die effiziente Kombination von Server- und Client-verschlüsselung als „Organizational“ und „Personal“ Ende-zu-Ende-Verschlüsselung. Die Client-Anbindung erfolgt dabei über Z1 MyCrypt Mail, als Add-In für MS Outlook und Lotus Notes sowie als App für iOS, Android etc. Mit Z1 MyCrypt BigAttach wird auch der Z1 SecureHub zum sicheren Transfer großer Dateianhänge direkt aus dem Mailprogramm der Clients angesprochen. Die besonderen Sicherheitsansprüche der im geschäftlichen Umfeld stetig zunehmenden Kommunikation über Mobile Clients wie Smartphones, Tablets und Notebooks sind damit verlässlich erfüllt.

Halle 12, Stand 506

Vodafone „Secure Call“

Sichere App für Android und iPhone

Secusmart zeigt auf der Sicherheitsmesse it-sa 2014 mit der App Vodafone „Secure Call“, wie jedermann wirkungsvolle Abhörsicherheit ganz einfach auf sein Smartphone herunterladen kann. In der App wird die gleiche Verschlüsselung für Sprache wie in der SecuSUITE for BlackBerry 10 verwendet. Sie kann vor Ort am Messestand der Düsseldorfer Secusmart GmbH getestet werden.

*Von Swenja Kremer,
Secusmart GmbH*

Auf der CeBIT 2014 angekündigt und auf der Nürnberger it-sa für jedermann zum Anfassen und Ausprobieren: Mit der hochsicheren App Vodafone „Secure Call“ sollen künftig hochsichere Telefonate für alle möglich sein – sowohl auf Android-Devices als auch auf iPhones. Zum Ende des Jahres kann jeder die Applikation aus den bekannten App-Stores für Android und iOS downloaden. Hochsichere Kommunikation ist damit nicht mehr nur Politikern und Funktionären vorbehalten, sondern dank einem guten Preis-/Leistungsverhältnis auch für Privatpersonen sowie für Wirtschaft und Industrie erschwinglich.

Gerade für den Mittelstand ist die App interessant, um eventuellen wirtschaftlichen Schäden durch Datenklau rechtzeitig entgegenzuwirken. Schon im Jahr 2009 berichtete das Handelsblatt von horrenden Schadenssummen: Frank Hülberg, Leitung der Abteilung Forensik bei KPMG, die Computerdaten auf Spuren krimineller Handlungen durchsucht, schätzte schon damals den Gesamtschaden bundesweit auf 80 Milliarden Euro. Im Jahr 2013 berichtete der Focus



Mit Vodafone „Secure Call“ können nicht nur Politiker und Behörden, sondern auch Konzerne und Mittelständler ihr geistiges Eigentum noch besser schützen (Bild: Vodafone).

von 60 Milliarden Euro, auf die das Bundesamt für Verfassungsschutz wirtschaftliche Schäden schätzt, die durch Datenklau entstehen. Dies zeigt: Der tatsächliche Schaden ist kaum greifbar, die Dunkelziffer sehr hoch.

Abhörschutz für alle

Seit Jahren steht die Düsseldorfer Secusmart GmbH für ein umfangreiches Abhörschutz-Portfolio. Neben der mobilen Kommunikation sichern die Hochsicherheitslösungen auch Festnetztelefone und Telefonkonferenzen vor Lauschangriffen ab.

Integriert in eine App, kann durch die hochklassige Sprachverschlüsselungstechnologie das sichere Smartphone entstehen: „Bring Your Own Device“ war gestern. Der Trend heute lautet „Build Your Own Device“ mit mehr Sicherheit. Über Vodafone „Secure Call“ stellen Vodafone und Secusmart Unternehmen und Privatpersonen die Sprachverschlüsselung wie im Regierungshandy plattformunabhängig zur Verfügung. Die App ist zu Beginn für Android und iPhone einsetzbar. So wird sichere Kommunikation nicht mehr zum zufälligen Luxusgut, sondern zur Selbstverständlichkeit.

Der Markt für sichere Apps hat allerdings gerade erst begonnen, zu wachsen. Was früher nur die Branchengrößen betroffen haben soll und nur für die Großen und Mächtigen der Politik ein Problem war, das ist jetzt die Herausforderung des Mittelstandes. Damit ist Sicherheit in der Kommunikation eine Aufgabe für ganz Deutschland. Schließlich stellt der Mittelstand den Motor der deutschen Industrie und formt damit das Bruttoinlandsprodukt.

Vodafone „Secure Call“ hilft genau an dieser Stelle. Die App kostet voraussichtlich 15 Euro im Monat und macht so Sicherheit erschwinglich. Damit wird sie vom Luxusgut zum Sicherheitsgurt für die deutschen KMUs. Denn jedes Unternehmen soll sicher kommunizieren können, ohne dabei auf gewohnten Smartphone-Komfort verzichten zu müssen. Dass das möglich ist – davon können sich die Besucher der Sicherheitsmesse it-sa selbst überzeugen und die App Vodafone „Secure Call“ noch vor dem offiziellen Verkaufstart selbst testen. ■

Ansprechpartner am Stand der Secusmart GmbH in Halle 12.0-423 ist Pressesprecherin Swenja Kremer. Termine mit dem Secusmart-Team vereinbaren Interessenten mit einer E-Mail an sales@secusmart.com mit dem Betreff „Besuch it-sa 2014“.

Advanced Persistent Threats erkennen

Unter dem Radar

Komplexe Angriffsvektoren unterschiedlicher Natur machen die Erkennung von modernen Angriffen schwierig bis unmöglich.

Mit Hilfe eines konfektionierten SIEM-Systems und der Fähigkeit, sich in die Lage des Angreifers hineinzudenken, kann man jedoch auch moderne Advanced Persistent Threats (APTs) erkennen.

Von Konrad Pesch, MODCOMP, Deutschland

Die meisten Unternehmen haben viel investiert, um ihre IT-Infrastruktur und damit vorrangig ihr Datenkapital zu schützen. Firewalls überwachen den Perimeter, Intrusion-Prevention-Systeme suchen im Netzwerkverkehr nach bekannten Angriffssignaturen, um diese Verbindungen zu protokollieren und eventuell zu unterbrechen. Log- und Monitoring-Systeme überwachen den Status und Identity-Management-(IDM)-Systeme verwalten die Zugriffsrechte der Mitarbeiter. Die Laptops der Kollegen sind über Endpoint-Protection komplett verschlüsselt und mittels Anti-Viren-Software geschützt. Vielleicht sind auch Schwachstellen-Scanner im Einsatz, die Systeme ohne aktuelle Patches identifizieren oder gar Data-Leakage-Prevention-(DLP)-Systeme und Prozesse implementieren, welche den Datendiebstahl aus den eigenen Reihen verhindern. Also ist man doch auf der sicheren Seite!

Brute-Force-Attacken und Denial-of-Service-Angriffe werden erkannt und abgewehrt. Man hat IT-Administratoren für die Windows-Systeme, welche für die UNIX-Server, es gibt Firewall- und Datenbankadministratoren. Also ist man doch auf der sicheren Seite! Oder? Die klare Antwort lautet: Leider nicht!

Zielgerichtete Angriffe

Durch moderne und komplexe Angriffsmethoden gelingt es

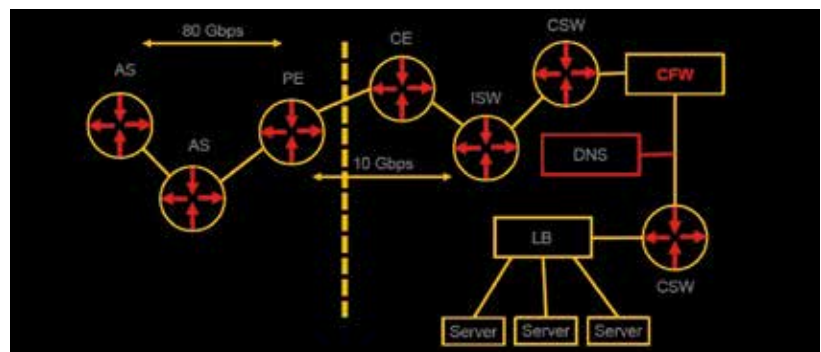
Cyberkriminellen dennoch immer wieder, in eigentlich gut geschützte Unternehmen einzudringen. Dazu führen sie zielgerichtete, dauerhafte Attacken durch, mittels deren sie versuchen, möglichst lange unentdeckt zu bleiben. Sie unterscheiden sich auch darin von gewöhnlichen Hackern, das sie viel Zeit und Handarbeit investieren. Ihr Ziel ist es, irgendein System des Opfers zu kapern, das sie dann als Sprungbrett nehmen, um weiter ins Unternehmensnetzwerk zu gelangen und dort unerkannt zu agieren.

Es handelt sich dabei um komplexe, zielgerichtete Angriffe, die sogenannten Advanced Persistent Threats. Die oben beschriebene traditionelle Sicherheits-Infrastruktur ist nicht in der Lage, diese ausgeklügelten Angriffe zu erkennen.

ATP-Angriffe laufen mehrstufig ab: Zuerst wird versucht, das Opfer auszukundschaften. Zum Zweck der Informationsbeschaffung werden beispielsweise Social-Engi-

neering-Methoden angewandt. Gibt die Bürokraft leichtsinnigerweise die Telefonnummer oder E-Mail-Adresse des Geschäftsführers heraus und erwähnt vielleicht noch, dass er schon im Feierabend auf dem Golfplatz weilt, ist es ein Leichtes, eine E-Mail maßzuschneidern und dem Opfer im Namen seines Golfplatzes ein paar Freistunden zu spendieren. Diese E-Mail markiert den Eintrittspunkt ins Unternehmen. Über E-Mails oder soziale Netzwerke werden die Opfer verleitet, auf Links zu klicken, die dann unbemerkt einen Trojaner oder andere Malware installieren.

Nach dem erfolgreichen Ausnutzen einer Schwachstelle, zum Beispiel mittels eines eigenen Zero Day Exploits, wird der Angreifer als nächstes versuchen, die Rechte auf dem System auszuweiten, um dann mittels eines Trojaners, eines Speicher-Hardhooks oder einer BIOS-Manipulation Persistenz zu erlangen und so die dauerhafte Kommunikation zu seiner Command-and-Control-(C&C)-Umgebung herzustellen. Der erste Callback zu seinem C&C-Server wäre dann das erste sichtbare Event für die IT-Security-Infrastruktur, während die vorherigen Aktivitäten im Verborgenen abgelaufen sind. Allerdings kann man auch die C&C-Kommunikation tarnen und dabei auf vorhandene SSL-Infrastrukturen wie Webmail zurückgreifen. Sobald die stetige Kommunikation in das infiltrierte Netzwerk gesichert ist, kann der Angreifer sich auf die Suche nach wertvollen Assets (Hosts) begeben, die ein lohnendes Ziel für das eigentliche Ziel der Aktion, den



Traffic Flow Beispiel

Diebstahl der Daten, darstellen. Das Abziehen der Daten ist dann über die üblichen Protokolle relativ einfach.

Gegenmaßnahmen

Was kann man also tun, um solche zielgerichteten Attacken zu erkennen? Neben der Schärfung des immer noch stiefmütterlich behandelten Sicherheitsbewusstseins der Mitarbeiter, ist ein Security-Information-and-Event-Management-(SIEM)-System eine sinnvolle Erweiterung der Sicherheitsarchitektur. Hier werden die Event-Logs der diversen Sicherheitssysteme gebündelt und korreliert. Von entscheidender Bedeutung ist es, das System so zu konfigurieren, dass auf ATP-Angriffsvektoren spezialisierte Regeln entwickelt werden. Die Qualität des SIEM-Systems hängt dabei maßgeblich von der Anzahl und Qualität der verfügbaren Quellen ab. Dieses Modell muss individuell für die zu überwachende Umgebung erstellt und kontinuierlich angepasst werden.

Unterstützen kann ein forensisches Analyseprogramm, das auch historische Daten auswertet, um den Weg einer Attacke zurückzuverfolgen. Einige moderne SIEM-Lösungen bringen diese Funktion gleich mit, andere können entsprechend erweitert werden.

Eine Möglichkeit, APT-Aktivitäten festzustellen, ist es, sogenannte Mausefallen anzulegen und den Zugriff auf diese zum Beispiel mittels File Activity Monitoring zu überwachen. Die Fallen sind vermeintlich lohnende Ziele für den Angreifer, etwa ein Sharepoint-Ordner mit dem Vermerk „Vertraulich“ oder eine Datenbank-Tabelle „Kunden-Bankverbindungen“. Nun ist es von höchstem Interesse, von wem der Zugriff erfolgt. Auf welche Systeme wurde von dieser IP-Adresse noch zugegriffen? Hier hilft die Korrelation der Log-Daten im SIEM bei der Aussortierung von „False Positives“ und der Erkennung weiterer verdäch-

tiger Aktivitäten. Die Erkennung von Anomalien ist eine ebenso wichtige Aufgabe. Finden ungewöhnlich große Dateitransfers statt? Und welche Ablenkungsmanöver können die Angreifer sich ausgedacht haben? Man muss sich also in die Lage des Gegners versetzen und ihm im Idealfall einen Schritt voraus sein.

Dienstleister unterstützen

Der Aufbau entsprechender Expertise seitens der SIEM-Analysten kann dementsprechend aufwändig, zeit- und kostenintensiv sein. An dieser Stelle kann man auf spezialisierte Dienstleister zurückgreifen, die den Aufbau des SIEM-Systems und die Feinjustierung der Regeln durchführen sowie den Wissenstransfer zu den Analysten unterstützen, deren Know-how über stattfindende Angriffe und nahende Bedrohungen somit im Betrieb bleibt. Die erzielten Synergieeffekte müssen dann noch prozess- und personaltechnisch verankert werden, da noch die Frage geklärt werden muss, wie auf entdeckte Angriffe reagiert werden soll.

Für diejenigen Unternehmen, die sich eine aufwändige SIEM-Lösung inklusive des benötigten Personals nicht leisten können oder wollen, besteht eine Alternative im Auslagern der SIEM-Lösung an einen Managed-Security-Service-Provider. Diese ist eine kostengünstigere Variante, da man auf Personal und Teile der eigenen Hardware verzichten kann.

Unabhängig von der Frage, ob man die Expertise nun im eigenen Hause behält oder von einem Dienstleister bezieht, bleibt eines sicher: Die Konfiguration der SIEM- und Analyse-Tools muss immer wieder dynamisch angepasst werden, da die Angreifer ständig neue Methoden ersinnen, um unter dem Radar der Systeme zu bleiben. Es bleibt ein Kopf-an-Kopf-Rennen. ■

MODCOMP auf der it-sa:
Halle 12, Stand 412

Zur Sicherheit: Hand auf's Herz.



INTUS 1600PS.

Hätten Sie nicht auch gerne eine biometrische Zugangskontrolle mit dem Komfort einer Fingerabdruckerkennung und dem Sicherheitsniveau einer Iriserkennung? Bei der INTUS 1600PS Handvenenerkennung halten Sie kurz die Hand vor den Sensor, und das System entscheidet hochpräzise, wer Zutritt erhält oder nicht. Hygienisch, schnell, komfortabel und dabei hochsicher. Eine typische Innovation von PCS.



Besuchen Sie uns:
it-sa 2014
07. – 09.10.2014
Halle 12, Stand 354

Tel.: +49 89 68004-550
www.pcs.com

pcs

Ein gutes Identity- und Access-Management (IAM) ist für die Sicherheit unerlässlich

Wer bin ich und wie viele bin ich eigentlich?

Unternehmen sollten sich in den kommenden Jahren verstärkt mit dem Ausbau des eigenen IAM beschäftigen. Denn mit einem gut ausgebauten IAM bietet sich die Möglichkeit, in einem Schritt die Sicherheit zu erhöhen, Produktivität zu verbessern und Kosten zu senken.

Von Franjo Majstor, CISSP

Im Identitäts- und Zugriffsmanagement liegt der Grundstein einer jeden effizienten IT-Sicherheitsarchitektur. Täglich werden unzählige Daten von Unternehmen, Institutionen und Organisationen zwischen den unterschiedlichsten Anwendern hin und her befördert. Doch die Technik, die im Laufe der letzten Jahre Kommunikations- und Arbeitsprozesse wesentlich erleichtert hat, hat auch ihre Schattenseiten. Die Schnittstellen zwischen den einzelnen Arbeitseinheiten, die erst die erhöhte Produktivität unserer heutigen Zeit ermöglichen, können sich schnell auch in Sicherheitslücken verwandeln. Um hier den Überblick zu behalten und die Ordnung der Systeme und Datenbanken aufrechtzuerhalten, ist ein gut aufgestelltes Identity- und Access-Management (IAM) unerlässlich.

Hierbei handelt es sich eigentlich um zwei unterschiedliche Komponenten der IT-Sicherheit, die voneinander sehr abhängig sind. Während „Identity Management“ Daten von Mitarbeitern verwaltet und Sicherheitsprogramme über seine Verzeichnisse zur Verfügung stellt, verwaltet das „Access Management“ die einzelnen Zugriffsrechte und Security Policies. Da hierzu ein

enger Austausch und eine starke Abhängigkeit zwischen beiden Komponenten erforderlich ist, werden sie von IT-Sicherheitsexperten schon länger als Einheit gedacht und mit dem Kürzel IAM abgekürzt. IAM ist das erste Glied in einer ganzen Reihe von Sicherheitskontrollen, die allesamt verhindern sollen, dass Unbefugte Zugriff auf relevante Datensätze erhalten. Die Zugriffsbefugnis, die ein solches System verschaffen kann, sollte möglichst minimal sein. Der Anwender oder ein Anwendungsprogramm soll nur Zugriff auf solche Daten erhalten, die er, sie oder es auch tatsächlich für die jeweilige Arbeit benötigt. Erfolgreiches Access-Management kann so daran mitwirken, mit minimalem Risiko eine maximale Produktivität zu entfalten. Es beeinflusst nicht nur die Sicherheits-, sondern auch die Arbeitsstruktur. Benutzern kann mit dem richtigen System eine individuelle Zugangsberechtigung gewährt werden, die optimal auf ihre jeweilige Funktion und Aufgabenstellung im Unternehmen zugeschnitten ist.

Flexibilität und einfache Bedienung

Die beispiellose Entwicklung, die Soft- und Hardware des

IT-Bereiches in den letzten Jahren durchlaufen haben, hat auch im IAM ihre Spuren hinterlassen. Die Ausweitung der Zugriffsmöglichkeiten auf das Internet, ob nun über einen regulären Anschluss, W-LAN oder ein Mobiltelefon, hat es ermöglicht, dass so gut wie jede Büroarbeit heutzutage von überall – ob im Homeoffice oder auf der Dienstreise – abgearbeitet und in das Unternehmensnetzwerk übertragen werden kann. Über Cloud-Networking oder Kollaboration können Projekte mittlerweile sogar gleichzeitig gemeinsam im Netz bearbeitet werden. Und wenn einmal tatsächlich kein Netz zur Verfügung stehen sollte, so kann doch immer noch auf einen USB-Stick zurückgegriffen werden, um die Arbeit mit nach Hause zu nehmen. Die Sicherheit hat hinter diesem ständigen Mehr an Mobilität und Zugriffsoptionen häufig zurückstecken müssen. Erst mit den Enthüllungen von Edward Snowden hat das Problembewusstsein unter den Anwendern und Unternehmen wieder etwas zugenommen.

Das heutige IAM hat sich diesen neuen Bedingungen angepasst. Das ständige Anwachsen der Zahl der Endgeräte – und damit auch der Nutzer – sowie der Anwendungsmöglich-

keiten hat dazu geführt, dass nicht mehr allein technische Effizienz das Wesen eines optimal aufgestellten Systems bestimmt. Skalierbarkeit, Benutzerfreundlichkeit und Transparenz sind in den Fokus seiner Entwicklung gerückt. Der richtige Umgang mit dem Endnutzer wird nun hervorgehoben. Auch auf staatlicher Seite wurde die Bedeutung dieser Weiterentwicklung mittlerweile erkannt. So hat die Europäische Union seit der Jahrtausendwende zahlreiche Projekte zur Verbesserung von IAM-Systemen, wie Privacy and Identity Management for Europe (PRIME) und Future of Identity in the Information Society (FIDIS) aufgelegt und finanziert. Doch sollte dies nicht darüber hinwegtäuschen, dass die Bedeutung eines gut ausgebauten Systems immer noch unterschätzt wird. Selbst Sicherheitsexperten bilden hier keine Ausnahme. Eine 2013 von (ISC)² veröffentlichte Umfrage unter IT-Sicherheitsexperten kam zu dem Ergebnis, dass nur 45 Prozent der Befragten eine automatische Identity-Management-Software als relevant für die System- und Netzwerksicherheit einschätzen. Die Werte für Authentifikation und Network Access Control lagen sogar bei unter einem Prozent. Dabei lässt sich doch gerade über solche Komponenten eine nicht zu unterschätzende Prävention betreiben. Weit besser schnitten dagegen Netzwerküberwachung und Informationsbeschaffung (75 %) sowie eine verbesserte Erkennung von Eindringlingen und präventive Technologien ab (72 %). Die Studie zeigt, dass das Potenzial noch lange nicht ausgereizt ist.

Selbstverständlich kann ein schlecht aufgestelltes IAM sich auch negativ auf die Produktivität eines Unternehmens auswirken. Überregulierung, zum Beispiel durch Mehrfachauthentifizierungen aller Systeme und Programme, verlangsamt Arbeitsprozesse. Im schlimmsten Fall unterbindet sie diese sogar zur Gänze. Ein Absinken der Gewinnspanne ist die Folge. Zum Problem kann ein

Access-Control-System auch werden, wenn es vom Nutzer zunehmend als Hindernis für die eigenen Arbeitsprozesse wahrgenommen wird. Hier kommt es dann häufig zu einem Sinken der Nutzerakzeptanz. Wenn sich Preis und Leistung der IT-Sicherheit dann nicht die Waage halten, kann es schnell passieren, dass Endnutzer beginnen, sich nach Möglichkeiten umzusehen, die mühevoll aufgebauten Sicherheitsbarrieren eigenmächtig zu umgehen.

Business Enabler?

Wird das IAM dagegen gut aufgestellt, kann es durchaus nicht nur einen wichtigen Beitrag zur IT-Sicherheit leisten, sondern auch neue Optionen bei der Bewältigung betrieblicher Aufgaben eröffnen. Arbeitsprozesse können mit seiner Hilfe besser skaliert und damit auch die Produktivität erhöht werden. Insofern kann IAM durchaus auch als Business Enabler verstanden werden. Zusätzlich kann IAM auch Kosten senken, da es die IT-Administration durch Automatisierung zahlreicher Prozesse erheblich vereinfacht. Prozesse, die bei der Einstellung, dem Arbeitsplatzwechsel und dem Ausscheiden von Mitarbeitern im IT-Bereich stets anfallen – wie Erstellen, Auswechseln und Sperren von Benutzerkonten – können so mit minimalem Zeit- und Arbeitsaufwand bewältigt werden. Auch ermöglicht es, Systeme nicht mehr einzeln zu administrieren, sondern zentral zu erschließen. Erhöhung der Sicherheit, Verbesserung der Produktivität und Senkung der Kosten – dies alles kann ein gut aufgestelltes IAM bewerkstelligen, wenn es sich bemüht, auf die Bedürfnisse des Endnutzers einzugehen.

Eine weitere Entwicklung liegt im technischen Bereich. Zunehmend kommen biometrische Daten zum Einsatz. Deren Erfassung und Verarbeitung sind optimal auf den für ein heutiges System so wichtigen Faktor der Benutzerfreundlichkeit

ausgerichtet. Am Endgerät ist derzeit meist eine Kamera oder ein Sensor angebracht, die mittels eines Scans der Iris oder eines Linienbildes des Fingerabdrucks, die Zugriffsberechtigung des Endnutzers ermitteln können. Weitere biometrische Erkennungsmerkmale werden in den kommenden Jahren sicherlich hinzukommen. Das Interessante an der biometrischen Erkennung ist nun, dass nicht nur die Erfassung, sondern auch die Verarbeitung der Daten eben hier – am Endgerät – und nicht im System selbst erfolgen, wodurch die Daten nicht weitergegeben und von außen auch keine Manipulation des Verarbeitungsvorgangs vorgenommen werden können.

Fazit

Die anwenderbezogenen wie die technischen Entwicklungen zeigen, dass es sich für Unternehmen, Institutionen und Organisationen durchaus lohnt, sich in den kommenden Jahren verstärkt mit dem Ausbau des eigenen IAM zu beschäftigen. Nur selten bietet sich die Möglichkeit, in einem Schritt Sicherheit zu erhöhen, Produktivität zu verbessern und Kosten zu senken. Dank der enormen CPU-Fähigkeiten von stationären und besonders mobilen Endgeräten befindet sich das IAM zur Zeit am Rande einer Übergangsentwicklungsphase, bei der die Weiterentwicklung dahingehen wird, dass noch bessere, aber auch noch transparentere IAM-Systeme geschaffen werden. ■

Auf der it-sa wird die (ISC)², Halle 12, Stand 648 am ersten Messtag, den 7. Oktober eine Panel Diskussion zum Thema Identitäts- und Zugriffsmanagement von 14 bis 15 Uhr auf dem Auditorium veranstalten. Interessenten sind herzlich dazu eingeladen die Diskussion zu verfolgen und können danach mit den Referenten weiter diskutieren.

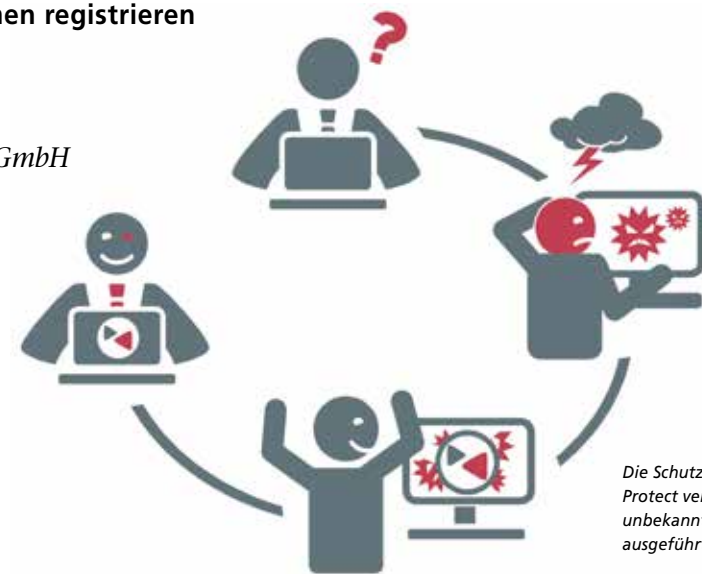
Die Lücke schließen, die Firewalls und Antivirenprogramme hinterlassen

Vermeintliche IT-Sicherheit

Knapp die Hälfte aller Unternehmen in Deutschland war schon einmal Ziel eines Spionageangriffs. Jährlich entstehen der deutschen Wirtschaft dabei Schäden in Milliardenhöhe. Entgegen der landläufigen Meinung sind jedoch nicht nur die Forschungs- und Entwicklungsabteilungen in Unternehmen Ziele der Angreifer: Auch die Bereiche IT-Administration und IT-Service sowie Vertrieb und der Bereich Fusionen und Übernahmen registrieren zunehmend Angriffe.

Von Dirk Kaiser, ReddFort Software GmbH

Der Schutz der eigenen Daten und Anwendungen ist für Unternehmen heute mehr denn je ein essenzielles Thema. Ein großes Sicherheitsproblem ist die starke Verflechtung von Laufzeitumgebung mit den eigentlichen Programmen. Da Anwendungen nicht isoliert ablaufen, sondern in einer Laufzeitumgebung, die ihnen vom Betriebssystem zur Verfügung gestellt wird, genügt bereits die Manipulation einer einzelnen Komponente, um die Umgebung einer ganzen Anwendung zu kompromittieren. Dazu gehören nicht nur die ausführbare Programmdatei, sondern auch Treiber, Bibliotheken, die interaktive Ein- und Ausgabe sowie die Kommunikation zwischen einem Betriebssystem und anderen ausgeführten Anwendungen. Gezielte Manipulationen können hier also zu schwerwiegenden Störungen führen. So kann eingeschleuste Malware beispielsweise persönliche Daten und Zugangskennwörter ausspionieren, auf wichtige und geheime Geschäftsunterlagen zugreifen, rechtsverbindliche Geschäfte durchführen oder auch weitere Angriffe mithilfe des bereits kompromittierten Rechners starten.



Die Schutzsoftware App-Protect verhindert, dass unbekannte Programme ausgeführt werden.

Besonders wenn Sicherheitskonzepte fehlen und es Sicherheitslücken im Betriebssystem gibt, haben Cyberkriminelle vielfältige Möglichkeiten, die Laufzeitumgebung bereits während des Betriebs anzugreifen und damit die Integrität ausgeführter Programme zu beeinträchtigen. Dies können auch die zurzeit häufig eingesetzten Schutzsysteme nicht verhindern, da sie oft nur reaktiv, auf bereits bekannte Angriffe reagieren. Schädlinge haben so nach dem Eindringen weitestgehend freien Zugriff auf Ressourcen wie etwa Dateien, Drucker oder Benutzerdaten.

Viele Unternehmen kennen die Problematik bereits. Vor allem in ihren Branchen führende Firmen oder auch Markenhersteller sehen sich zunehmend damit konfrontiert, sich vor diesen Angriffen besser zu schützen. „Gerade bei Markt- oder

auch Leistungsführern würden solche Angriffe unmittelbar die Innovationskraft angreifen“, so Dieter Schulz, Geschäftsführer der ReddFort Software GmbH. Viele Unternehmen sind daher verstärkt auf der Suche nach besonderen Schutzmaßnahmen für kritischen Daten und Anwendungen.

Antivirenprogramme und Firewalls stoßen an ihre Grenzen

Dabei besteht die Herausforderung darin, Lösungen zu finden, die den möglichst besten Schutz für die eigene IT bieten – Unterstützung findet man hier beispielsweise bei ReddFort. Das deutsche Unternehmen bietet mit seinen Lösungen App-Protect und S-Protect eine Kombination aus Client- und Serverschutz. Durch eine einfach zu installierende

SecurITy
made
in
Germany

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

Unser Versprechen für Ihr Netzwerk

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



ANWENDUNGEN

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



ZERTIFIZIERUNG

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



PORTFOLIO

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



SICHERHEITSVERSPRECHEN

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

www.lancom-systems.de/it-sa

Testphase können die IT-Sicherheitsexperten aus Kürten umfassenden Schutz für die sensiblen Daten und Applikationen in den Unternehmen darstellen und aufzeigen, welche Sicherheitslücken durch die ReddFort-Lösungen geschlossen werden. Auf Basis einer eigens entwickelten Technologie schützen diese Lösungen die IT-Systeme von innen heraus.

„Wir gehen einen vollkommen neuen und bisher so nie dagewesenen Weg, sicherheitskritische Daten und Anwendungen in Unternehmen zu schützen“, erläutert Dieter Schulz, Geschäftsführer bei ReddFort. Demnach würden sich die herkömmlichen Verteidigungsstrategien meist auf die Außengrenzen eines Computers konzentrieren, während die eigenen Lösungen jedoch die Ausführung schädlicher Software sowie den Zugriff auf sicherheitskritische Daten verhindern. Eine Besonderheit dabei ist ein Verfahren, das direkt im Kern des Betriebssystems integriert wird und die interaktive Ein- und Ausgabe sowie den Datenverkehr von bestimmten Anwendungen schützt.

Herkömmliche Schutzsysteme nur im Zusammenspiel erfolgreich

Laut aktuellen Studien wird es für Unternehmen letztlich sogar eine Überlebensfrage sein, wie wichtig sie den Schutz ihrer sensiblen Daten nehmen. „Wir haben die Erfahrung gemacht, dass das Thema Informations- und Datenschutz in Unternehmen zumeist Chefsache ist“, erläutert Martin Gaese, Leiter Vertrieb und Marketing bei ReddFort. Dabei stünden vor allem auch mittelständische Unternehmen im Fokus der Angreifer, da diese häufig über ein hohes technologisches Know-how und zumeist auch über eine hohe Innovationskraft verfügen würden. „Klar ist“, so Gaese, „dass die Schutzsysteme, so, wie wir sie heute kennen, bei weitem nicht mehr ausreichen. Gefragt sind Schutzsysteme, die die Ausführungsumgebung sicherheitskritischer Anwendungen

schützen und Veränderungen rechtzeitig erkennen beziehungsweise nicht zulassen.“

Bisherige Konzepte sehen ihre Aufgabe bis dato darin, Ressourcen bestehender Systeme vor Angriffen oder unberechtigten Zugriffen zu schützen. Dabei steht der Schutz der Ausführungsumgebung jedoch nicht im Vordergrund; dieser ergibt sich erst in Folge der realisierten Systeme. Zudem hängt ein wesentlicher Teil des erreichten Schutzes auch davon ab, dass die Systeme über Gesetzmäßigkeiten bereits bekannter Angriffsszenarien Kenntnis haben. Die heute vielfach vorzufindenden Kombinationen aus Anti-Virus-Programm, Firewall und IDS/IPS, sind nur schwer einem einzigen Konzept zuzuordnen und zeigen daher, dass keines der Systeme für sich allein in der Lage ist, einen ausreichenden Schutz zu realisieren.

IT-Sicherheit made in Germany

Bei ReddFort ist man sich dieser Problematik schon seit langem bewusst. Bereits seit dem Jahr 2006 arbeitet man dort an neuen Lösungen zum Schutz vor Angriffen auf die IT in Unternehmen, seit 2008 hält das Unternehmen ein Patent auf die eigens entwickelte Technologie. Diese zeichnet sich in erster Linie durch ein bewusstes „Agieren“ statt „Reagieren“ aus. „Auch wenn der Begriff schon ein wenig in Mitleidenschaft gezogen ist – wir sprechen ganz bewusst und nach wie vor von einem Paradigmenwechsel“, erläutert Dr. Adrian Spalka, Erfinder der ReddFort-Technologie. „Die Revolution liegt dabei im technologischen Ansatz“, so Dr. Spalka weiter. „Denn während marktübliche Produkte versuchen, das Eindringen schädlicher Software auf den Rechner zu verhindern – nach wie vor unterstellt der Schädling wird überhaupt erkannt –, kann unter Einsatz der ReddFort Lösungen nur im Vorfeld autorisierte Software ausgeführt werden.“

Der entscheidende Unterschied zu herkömmlichen Schutzprogrammen ist, dass ReddFort den Schutzmechanismus direkt auf der Ebene des Betreiberprogrammes implementiert. Dabei analysiert ReddFort bereits im Vorfeld die Systemebene, auf der zum Beispiel die Benutzer- und Rechtevergabe der zu betreibenden Programme autorisiert ist. Die Lücken, die gängige Antivirenprogramme und Firewalls hinterlassen, werden so eliminiert.

„Benutzer können heute nicht mehr sicher identifizieren, ob beispielsweise eine Datei oder eine E-Mail mit Schädlingen behaftet sind oder nicht“, erläutert Schulz. „Wir nehmen ihnen diese Verantwortung ab, indem unsere Lösungen unbekannte Programme gar nicht erst zur Ausführung gelangen lassen“, so Schulz weiter.

Konkret bedeutet dies, dass ReddFort App-Protect zunächst eine Art Systemscan durchführt und festlegt, welche Systemdateien erlaubt sind. Im Anschluss daran übernimmt das Programm dann selbstständig die Einschätzung, welche Fälle kritisch sind und welche nicht – denn immer dann, wenn Schädlinge nach dem Systemscan zur Ausführung gelangen wollen oder gar Veränderungen im System durchführen wollen, wird dies verhindert.

„IT-Administratoren profitieren davon, dass sie zentralisiert, auf Administratorebene, definieren können, welche Dateien und Anwendungen quasi in das „sichere, schützenswerte Paket“ gehören“, erläutert Dr. Spalka. „Damit können auch für einzelne Benutzergruppen sichere Umgebungen erzeugt werden“, so Spalka weiter. Die ReddFort Lösungen sind einfach zu handhaben und auch leicht zu monitoren. ■

**ReddFort auf der it-sa:
Halle 12, Stand 219**

Your knowledge.
Your people.
Your future.

Security Powered by HOB



**Uncle Sam Wants
YOUR Data!**

**Umfassende Remote-Access
Lösungen für alle Einsatzzwecke,
alle Betriebssysteme, alle Geräte,
auch Mobile Devices**

- Kostenersparnis durch
clientless; keine Installation
am Client
- Absolut sicher, nachgewiesen
durch Zertifizierung durch das
BSI nach **Common Criteria
EAL 4+**



HOB RD VPN

Die umfassende SSL VPN Komplettlösung



HOBLink VPN

Modulare IPsec Connectivity

Vereinbaren Sie ein unverbindliches Beratungsgespräch!

Tel.: 09103-715-3715

E-Mail: marketing@hob.de

Integration als Schlüssel zum Schutz vor Cyberattacken

Drei Schritte für die Sicherheit

Laut dem aktuellen IBM Cyber-Security-Intelligence-Index haben Cyberkriminelle allein letztes Jahr weltweit über eine halbe Milliarde persönlicher Informationen gestohlen. Ziele solcher Angriffe sind vor allem Unternehmen, deren Geschäftsgeheimnisse reiche Beute versprechen. Auf der it-sa zeigt die IBM, wie sich Organisationen jeder Größe mittels integrierter Lösungen vor gezielten Cyberangriffen schützen können.

Von Gerd Rademann, IBM DACH

Es gibt Unternehmen, die mit mehr als 50 verschiedenen Sicherheitsanwendungen von Dutzenden unterschiedlichen Anbietern versuchen, ihre Mitarbeiter, Daten, Anwendungen und Infrastruktur vor kriminellen Cyberattacken zu schützen. Eine wichtige Voraussetzung zum effizienten und effektiven Betreiben einer Security-Plattform wird dabei aber häufig übersehen: das nahtlose Ineinandergreifen der einzelnen Teile der Abwehrkette. Wie wichtig das ist, zeigt sich vor allem bei sogenannten „Advanced Persistent Threats“ (APT), also aufwändige, zielgerichtete Attacken gegen Unternehmen und Behörden. Diese Angriffsstrategie zielt darauf, unachtsame oder unzureichend ausgebildete Nutzer zu überlisten, um so die Unternehmens-IT unbemerkt und dauerhaft zu infiltrieren und sensible Informationen abzugreifen. Ein klassisches Einfallstor ist zudem noch immer der Angriff über mit Malware versehene E-Mail-Anhänge. Diese Methode erlebt laut dem aktuellen IBM X-Force Report gerade ein großes Comeback. Hier verzeichneten IBM-Forscher im März 2014 den höchsten Anstieg innerhalb der letzten zweieinhalb Jahre.

Schwachstelle Mensch

Gerade bei Angriffen, die es auf die Schwachstelle Mensch abgesehen haben, ist das effektive Zusammenspiel verschiedener IT-Komponenten wichtig. Wenn es nicht funktioniert, finden Cyberkriminelle schnell Sicherheitslücken, die mit nicht integrierten Einzellösungen nicht oder nur sehr schwer geschlossen werden können. Für Angreifer, die zum Beispiel nach einer erfolgreichen Phishing-Attacke im Besitz der Zugangsdaten von Unternehmensmitarbeitern sind, ist das Überwinden klassischer Security-Schranken – dazu zählen insbesondere Firewalls – ein Kinderspiel. Das kann für die Opfer teuer

werden und für deutsche Unternehmen sogar ganz besonders. So ergab eine aktuelle Studie des Ponemon-Instituts, dass diese zwar seltener attackiert werden, mit Kosten von durchschnittlich 4,74 Millionen US-Dollar aber mit den weltweit höchsten Verlusten rechnen müssen.

Vor solchen Szenarien können sich Organisationen jeder Größenordnung schützen: So setzt etwa das Threat-Protection-System der IBM bei der Abwehr von APTs und anderen Cyberangriffen auf den Ansatz, Gefahren zu eliminieren, noch bevor diese Schaden anrichten können. Dazu arbeitet es in drei integrierten Schritten: Vorbeugen, Erkennen, Bekämpfen.

Vorbeugen

Das Zusammenspiel der Security-Komponenten des Threat-Protection-Systems von IBM bildet eine integrierte Lösung für verschiedene Bedrohungsszenarien. So trägt die im Mai 2014 ins Portfolio der IBM aufgenommene Software Trusteer APEX mit ihrem verhaltensbasierten Erkennungsalgorithmus dazu bei, dass Attacken gar nicht erst stattfinden können. Dabei schützt sie gezielt eine der anfälligsten Stellen im System entlang der gesamten Angriffskette, also Endgeräte wie Notebooks und Desktops. Die größte Schwachstelle auf diesen Geräten wiederum sind Java-Anwendungen, die in rund der Hälfte der Fälle das Einfallstor für erfolgreiche Attacken sind. Als einziges Programm auf dem Markt kann Trusteer APEX einen automatischen Java-Shutdown auf betroffenen Geräten durchführen. Zudem bietet es einen Passwortschutz, der Mitarbeiter daran hindert, unternehmensinterne Passwörter auf Internetseiten Dritter, etwa Facebook, zu verwenden. Auch dem Öffnen gefährlicher E-Mails, die nicht im Spam-ordner gelandet sind, schiebt die Software einen Riegel vor.

Doch nicht nur auf den Endgeräten, auch im Netzwerk drohen Gefahren: Um diesen entgegenzutreten, schützt die IBM Security Network Protection (XGS) zum Beispiel vor Sicherheitsbedrohungen wie SQL-Injection und Cross-Site-Scripting und hilft durch den verhaltensbasierten Erkennungsansatz und die Erkenntnisse der IBM X-Force auch Gefahren abzuwenden, die noch gar nicht gepatcht oder gar bekannt sind (Zero-Day-Exploits).

Erkennen

Gerade APTs wurden speziell entwickelt, um punktuelle Sicherheitslösungen zu umgehen. Sobald sie sich einen Weg in die Infrastruktur gebahnt haben, können sie meist nur entdeckt werden, wenn man die einzelnen Angriffskomponenten und ihre Beziehung zueinander versteht. Auch deshalb ist ein integrierter Ansatz so wichtig. Hier kommen Analytics-Lösungen wie die IBM QRadar-Security-Plattform ins Spiel. Sie kann in Echtzeit auf mehr als 400 Datenbanken mit sicherheitsrelevanten Informationen zurückgreifen und so Gefahren schnell lokalisieren.

Um die Raffinessen von APTs erkennen zu können, bedarf es einer Analyse in allen relevanten Bereichen eines Systems: beim Zugriff auf Daten, im Bereich des Identitätsmanagements, in der Infrastruktur sowie den Anwendungen und deren Verhalten – und zwar in Echtzeit. Die QRadar-Plattform führt diese Analysen integriert und automatisiert unter Einbeziehung von Realtime-Events durch und kann Milliarden Events pro Tag auf wenige Handlungsaktionen reduzieren.

Schützen

Vor dem Hintergrund der aktuellen Bedrohungslage ist die Frage nicht, ob ein Unternehmen Opfer von Cyberangriffen wird, sondern wann es passiert oder ob es möglicherweise schon unbemerkt attackiert wurde. Betroffene Organisationen verfügen oft nicht über die Mittel, eine gründliche digitale Forensik durchzuführen und so angemessen auf Angriffe zu reagieren. Die IBM Security QRadar-Incident-Forensics-Lösung kann die Vorgehensweise eines Angreifers Schritt für Schritt zurückverfolgen sowie schnell und einfach eine umfassende Untersuchung auch von mutmaßlichen Verletzungen der Netzsicherheit durchführen. So lassen sich die Ursachen einer Sicherheitsverletzung korrigieren und ein nochmaliges Auftreten verhindern. An dieser Stelle schließt sich der Kreis. ■

IBM auf der it-sa: Halle12, Stand 331

Sicherheit zum Anfassen

Auf der it-sa veranschaulicht IBM mit einer Live-Hacking-Demo, wie raffiniert Cyberkriminelle heute vorgehen und wo Unternehmen beispielsweise Gefahr laufen, Wettbewerbsvorteile durch Spionageangriffe einzubüßen. Die Demonstration zeigt aber auch, wie sich Unternehmen mithilfe des IBM Threat-Protection-Systems wirkungsvoll schützen können. Dieser Schutz umfasst Personen, Daten, Applikationen und Infrastruktur: Was können proaktive Sicherheitslösungen leisten und wie sieht die aktuelle Bedrohungslage gemäß der neusten Erkenntnisse der IBM X-Force aus?

Peter Häufel „*Prevent. Detect. Respond*“, 8.10., 9.45-10.00 Uhr, Forum Rot (Management)

Digitaler Türsteher für Web, Mainframe, Cloud und Mobile

Zu den Themen, über die IBM auf der Messe außerdem spricht, gehört auch das Identitäts- und Zugriffsmanagement. Mit dessen Hilfe können Unternehmen unbefugten oder versehentlichen Zugriff auf Daten verhindern, indem sie Berechtigungen gezielt überwachen und steuern. Ganz gleich ob in Web- oder Mainframeumgebungen, in der Cloud oder von mobilen Geräten aus – mit dem IBM Security Identity- und Access-Management lassen sich Onlineressourcen schützen und Sicherheitsvorschriften einhalten.

Gregor Schinke „*Identity & Access Management*“, 7.10., 12.45-13.00 Uhr, Forum Blau (Technik)

360-Grad-Blick über Endgeräte

IBM präsentiert zudem eine Lösung für das Mobility-Management des kürzlich akquirierten Unternehmens Fiberlink: MaaS360 ist eine hochstabile cloudbasierte Plattform, die Geräte, Benutzer, Anwendungsprogramme, Dokumente und Kosten erfasst. Sie verwaltet die sich ständig erweiternde Palette an Endgeräten – von der Anmeldung über die Einstellung von Sicherheitsregeln bis hin zum Monitoring – über ein einziges Portal. Dadurch wird das Risiko von Datenverlust oder -spionage deutlich reduziert.

Sicherheit ein komplettes Datenleben lang

Geht es um die Absicherung aller in Unternehmenssystemen gespeicherten Daten, sollten Messebesucher sich die Enterprise-Security-Plattform IBM InfoSphere Guardium näher ansehen: Sie ist die einzige Lösung, die Datenbanksicherheit und Compliance während des gesamten Lebenszyklus von Daten verwaltet. Durch fortlaufende Überwachung erkennt sie auch potenziellen Betrug über Benutzerkonten von Unternehmensanwendungen wie Oracle E-Business Suite, PeopleSoft, SAP und internen Systemen

High-Speed-Verschlüsselung schützt Informationen auf dem Weg durch das WAN

Bodyguard für sensible Daten

Immer noch verschlüsseln viele Unternehmen ihre Daten nicht, weil sie den administrativen Aufwand fürchten oder sich vor vermeintlich hohen Investitionskosten scheuen. Heutige Verschlüsselungsmethoden ermöglichen jedoch Sicherheit ohne Verluste bei Bandbreite oder zusätzliche Latenzzeiten – und das Ganze zu vernünftigen Kosten.

Von Thorsten Krüger, SafeNet

IT-Teams, die mit der Sicherung sensibler Informationen beauftragt sind, stehen heute vor enormen Herausforderungen. Das liegt nicht nur an den gesetzlichen Rahmenbedingungen, die sich in Europa und Deutschland ändern sollen, sondern vor allem an den immer raffinierteren Methoden der Hacker. Kaum eine Woche vergeht ohne Medienberichte über neue Fälle von Datendiebstahl und -missbrauch. Unternehmen haben, so scheint es, oft keine Kontrolle mehr über ihre Daten, besonders wenn sie in einem externen Netzwerk verschickt und bewegt werden. Denn Cyberkriminelle können diese relativ einfach und ohne hohe Kosten abfangen. Die Motivation dafür reicht von Industriespionage, über den Verkauf der Daten bis zur Erpressung der betroffenen Firmen. Verschlüsselung ist deshalb eine enorm wichtige Komponente im Mix der Sicherheitstechnologien.

Viele Unternehmen gehen fälschlicherweise davon aus, dass die von ihnen verwendeten Datennetzwerke sicher sind. In der Realität besteht aber gerade bei Daten, die verschickt und bewegt werden, ein besonders hohes Verlustrisiko. Millionen von Tera- und sogar Petabytes be-

finden sich auf den Datenautobahnen und können schnell in unbefugte Hände geraten – sei es durch Cyber-Angriffe, menschliche Fehler und technische Schwachstellen.

Vernachlässigte Sicherheitsmechanismen

Obwohl es definitiv den Bedarf für Sicherheitsmechanismen in Netzwerken gibt, ergreifen die wenigsten Service Provider Maßnahmen, um die Datenintegrität zu gewährleisten. Grundsätzlich ermöglichen deren Lösungen nur die Isolation von Traffic oder bestimmten Daten. Dieser Ansatz schützt jedoch nicht gegen das Abhören von Übertragungsleitungen und Knotenpunkten oder gegen falsche Konfiguration.

Aber auch viele Unternehmen haben keine umfassenden Security-Strategien: Während sie große Mengen an Zeit und Geld in die Sicherung ihrer Informationen auf Servern und Datenbanken investieren, unterschätzen sie das Risiko bei der Übertragung. Dabei sind gerade öffentliche oder private Datennetze anfällig gegen Manipulation, da hier der klassische Perimeterschutz nicht greift.

Um die Bedrohungen für „Data in Motion“ wirkungsvoll zu bekämpfen, muss der Schutzmechanismus bei der Information selbst angesiedelt werden – unabhängig davon wo sie sich befindet. Eine solche ortsungebundene Methode ist die Verschlüsselung. Damit erlangen Unternehmen zu großen Teilen die Kontrolle über ihre Daten zurück, auch wenn sie sich in der Cloud oder auf mobilen Geräten befinden. Zukünftig gilt es, die Sicherheitsmaßnahmen so nah wie möglich an das zu schützende Objekt zu binden. Nur dann stellen IT-Verantwortliche sicher, dass sensible Geschäftsgeheimnisse auch geschützt sind, wenn die erste Sicherheitslinie im Unternehmen überwunden wurde. Aber warum investieren so wenig Unternehmen in die Verschlüsselung bewegter Daten?

High Speed-Verschlüsselung als Antwort

Verschlüsselung ist nicht neu: Regierungen und Behörden auf der ganzen Welt nutzen chiffrierte Informationen seit unzähligen Jahren. Trotzdem verschlüsseln Unternehmen bewegte Daten bisher selten, weil sie Engpässe bei der Bandbreite, hohen administrativen Aufwand und enorme Investitionen befürchten. Moderne Verschlüsselungsmethoden ermöglichen jedoch Sicherheit ohne Verluste bei Bandbreite oder zusätzliche Latenzzeiten und das Ganze zu vernünftigen Kosten.

Aktuell werden meist Layer-3-Netze zur Datenübertragung verwendet. Diese sind allerdings nicht optimal für die heutigen Ansprüche geeignet. Sie sind kompliziert zu verwalten und besonders bei größerem Bedarf nicht gut skalierbar. Bei der Verschlüsselung von Layer-3-Netzwerken greifen die IT-Verantwortlichen typischerweise auf IPsec-Encryption zurück, um die Daten zu schützen. Das führt allerdings zu Performanceverlusten von bis zu 40 Prozent und höheren Latenzzeiten.



Fakten zur
Verschlüsselung
mit IPsec

Aus diesem Grund eignet sich die Verschlüsselung auf Layer 2, auch als High-Speed-Verschlüsselung bekannt, deutlich besser für den Schutz sensibler Daten. Layer-2-Netzwerke lassen sich mit speziellen Appliances sichern und verschlüsseln, ohne an Geschwindigkeit und Bandbreite einzubüßen. Eine verlustfreie Qualität auch für Echtzeitanwendungen wie Voice over IP (VoIP) oder Video-Applikationen mit kleinen Frames ist somit garantiert.

Ein weiterer großer Vorteil ist der deutlich geringere Verwaltungsaufwand. Durch den Einsatz einer zentralen Management-Plattform lassen sich die Verschlüsselungssysteme, auch an verschiedenen Standorten, in wenigen Minuten installieren. Das Netzwerk muss dabei nicht neu konfiguriert und die Routing-Tabellen nicht aktualisiert werden. Die Verschlüsselung bleibt auch bei zukünftigen Veränderungen im Routing unberührt. Das führt verglichen mit Layer-3-Netzen zu geringeren Kosten pro Gigabyte.

Entsprechende Lösungen wie die CN-Serie von SafeNet schützen sensible Informationen inklusive Metadaten innerhalb von Wide Area Networks (WAN) und helfen Unternehmen die Kosten für Hochgeschwindigkeitsverschlüsselung um bis zu 50 Prozent zu senken. Dabei bieten sie hohe Übertragungsraten von zehn Megabit bis zehn Gigabit pro Sekunde. Damit eignet sich Netzwerkverschlüsselung heute auch für zeitkritische und sichere Kommuni-

kation, beispielsweise im Finanzsektor und bei Internetkonzernen.

Durch die Verschlüsselung auf Layer 2, können Unternehmen ihre Daten besser vor Lauschangriffen, Überwachung sowie offenen und verdeckten Eingriffen schützen – zu einem erschwinglichen Preis, ohne Abstriche bei der Leistung.

Zwischen Sicherheit und Performance

Damit Unternehmen ihre Daten ganzheitlich und nicht nur an einem isolierten Ort schützen können, müssen sie ihre Vorschriften und Sicherheitstechnologien an den gesamten Lebenszyklus anpassen. Das bedeutet, dass wichtige Informationen bereits auf der Anwendungsschicht abgesichert sind – auch während der Übertragung über das Netzwerk bis zum Speichervorgang.

Im Kampf gegen Cyberkriminalität vertrauen viele CIOs immer noch auf eine starre Verteidigungslinie am Tor des eigenen Netzwerkes. Sie soll Hacker und Industriespione davon abhalten, Zugriff auf die gespeicherten Daten zu erlangen. Der Perimeterschutz kann aber nur ein Baustein einer modernen Sicherheitsstrategie sein.

Ein weiteres Element sind Verschlüsselungslösungen, die dafür sorgen, dass geschäftliche Daten an jedem Ort des Netzwerkes geschützt sind. Keys werden mit einem Hardware-basierten Zufallsgenerator

erzeugt, in einer manipulationssicheren Umgebung aufbewahrt und automatisch in definierbaren Zeitabständen getauscht. Die Schlüsselverwaltung ist inkludiert und muss nicht extern durchgeführt werden. Jedes Verschlüsselungsgerät im Netz kann als führendes System eingerichtet werden und so automatisch die Schlüssel für alle anderen Devices im Netz erstellen. Bei der „Point to Multipoint-Konfiguration“ kann sich so ein einziger Encryptor mit hunderten Niederlassungen verbinden und eine VLAN-granulare Verschlüsselung einrichten. Darüber hinaus können Sicherheitsverantwortliche mit Zugangskontrollen festlegen, welche Mitarbeiter auf welchen Key und somit auf welche Daten im Klartext zugreifen können. Damit sind die Informationen unbrauchbar, selbst wenn sie in unbefugte Hände geraten sollten.

Das Argument, dass WAN-Verschlüsselung unwirtschaftlich ist und das Netzwerk mit zusätzlichem Overhead belastet, zählt heute nicht mehr. Moderne Hochgeschwindigkeitstechnologien ermöglichen effiziente Verschlüsselung ohne exorbitante Kosten. Damit gibt es keinen Grund mehr, wichtige Daten im Klartext zu übertragen. Nur wenn Unternehmen die Verschlüsselungsstrategie von ihrer Netzwerkarchitektur abkoppeln, sind sie den Cyberkriminellen einen Schritt voraus. ■

**SafeNet auf der it-sa:
Halle 12, Stand 308**

Mit automatisiertem Schwachstellenmanagement Sicherheitslücken schnell erkennen und schließen

Mut zur Lücke – nein danke!

Eine Schwachstelle auf einem einzigen Rechner im Unternehmen genügt, um die Sicherheit der gesamten IT-Umgebung und damit der sensiblen Firmendaten zu gefährden. Doch dem IT-Administrator ist es in der Praxis nicht möglich, alle Clients und Server laufend auf alle bekannten Lücken zu prüfen. Abhilfe schafft automatisiertes Schwachstellenmanagement mithilfe einer Client-Management-Software.

Von Armin Leinfelder, baramundi software AG

Vollkommen fehlerfreie Software gibt es nicht. Potenziell kann jeder Fehler ein Sicherheitsrisiko darstellen und eine Hintertür öffnen, die für Angriffe genutzt werden kann. Im Jahr 2013 wurden jede Woche rund 100 neue derartige Schwachstellen in Betriebssystemen und Anwendungen entdeckt und in der National Vulnerability Database des US-CERT dokumentiert.

Mut zur Lücke ist vor diesem Hintergrund für IT-Administratoren keine Tugend. Schließlich tragen sie die Verantwortung für die Sicherheit der Daten und einen störungsfreien Betrieb. Kundendaten, Geschäfts-

zahlen, Entwicklungsunterlagen – die Konsequenzen eines erfolgreichen Cyberangriffs können den Betrieb lahmlegen und Firmeninterna offenlegen. Neben finanziellen Verlusten und einem Imageschaden für das Unternehmen drohen im ungünstigsten Fall sogar staatsanwaltschaftliche Ermittlungen. Zum Beispiel wenn der Verdacht auf einen Verstoß gegen Datenschutzrichtlinien besteht.

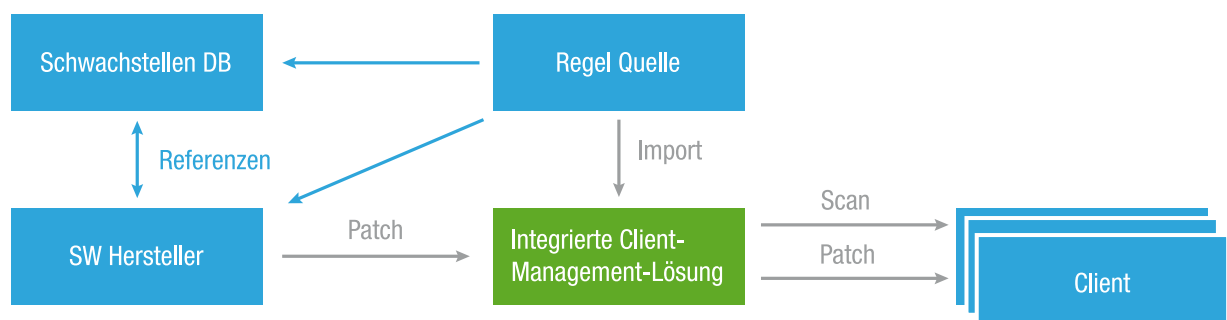
Längst sind für schadensträchtige Cyberangriffe auch keine weitreichenden Programmierkenntnisse mehr erforderlich. Viele Attacken gehen inzwischen auf das Konto von Kriminellen, die auf im Internet

verfügbare Exploits zurückgreifen. Derartige Angriffssoftware, die gezielt eine bekannte Schwachstelle ausnutzt, wird im Internet gratis oder gegen Bezahlung angeboten. Verfügbar ist sogar eine grafische Benutzeroberfläche, sodass Angriffe auch für mittelmäßig begabte Hacker kein Problem mehr darstellen.

Firewall und Virens Scanner bieten inzwischen einen sehr wirkungsvollen Schutz gegen in der Vergangenheit populäre Angriffsmethoden. Da diese Sicherheitsvorkehrungen kaum noch auszuhebeln sind, haben sich Angreifer inzwischen auf Attacken über die Hintertür verlegt. Bei diesen Reverse-Angriffen werden Firewall und Virens Scanner einfach umgangen, indem eine Sicherheitslücke in einer Software ausgenutzt wird. Ein Beispiel: Über eine E-Mail mit einem sensationell günstigen Angebot wird ein Mitarbeiter auf eine präparierte Webseite gelockt, die sich eine Lücke im Flash-Player zunutze macht und so einen Schadcode auf dem Rechner ausführen kann. Dieser lässt den Rechner eine Verbindung nach außen zum Server des Angreifers aufbauen, die ihn zum willigen Sklaven des Angreifers macht. Da die Verbindung aus dem Unternehmen heraus aufgebaut wird, greift die Firewall nicht ein.

Neben präparierten Webseiten werden auch manipulierte Dateien (z. B. Office-Dokumente, PDFs) eingesetzt. Es wurden auch bereits Angriffe über bösartige Anzeigen auf eigentlich harmlosen Internetseiten ausgeführt. Oft verwenden Angreifer auch Informationen aus sozialen

Komponenten und Abläufe einer integrierten automatisierten Schwachstellenmanagement-Lösung



Netzwerken, um ihre Opfer gezielt in die Falle zu locken und sie zum Öffnen einer bestimmten Datei oder zum Klick auf einen Link zu bewegen. Und egal wie detailliert die Verhaltensregeln des Unternehmens und die Warnungen der Admins auch sein mögen: Irgendwann macht ein Mitarbeiter vorsätzlich oder fahrlässig einen Fehler und geht einem Angreifer auf den Leim. Nötig sind daher auch technische Schutzmaßnahmen gegen solche Angriffsmethoden.

Vorsorgeuntersuchung für die IT

Solange eine Schwachstelle nicht bekannt ist und im Verborgenen zwischen Millionen Zeilen Programmcode schlummert, sind die von ihr ausgehenden Gefahren äußerst gering. Die Schwachstelle ähnelt einem offenen Fenster, das noch niemand entdeckt hat. Gefährlich wird es, sobald sie weithin bekannt sowie in einschlägigen Schwachstellenda-

tenbanken dokumentiert ist, was oft dann passiert, wenn der Softwarehersteller einen Patch bereitgestellt hat. Denn auch potenzielle Angreifer und Exploit-Entwickler lesen diese Datenbanken, analysieren die vom Hersteller bereitgestellten Patches und können daraus Rückschlüsse ziehen, wie sich die Lücke ausnutzen lässt.

Solange der Patch nicht auf allen betroffenen Geräten eingespielt wurde, sind daher über die Schwachstelle wirkungsvolle Angriffe ausführbar, gegen die kaum Gegenwehr möglich ist. Am offenen Fenster lehnt nun eine Leiter, die Zahl der Attacken unter Ausnutzung der Lücke steigt stark an. Für einen wirksamen Schutz gegen Angriffe ist es daher essenziell, Sicherheitslücken auf allen Geräten zu erkennen und alle nötigen Patches unverzüglich, flächendeckend und zuverlässig einzuspielen.

Ohne automatisierte Hilfsmittel ist diese Anforderung ange-

sichts der großen Zahl von Geräten, eingesetzter Software und Sprachversionen de facto nicht zu erfüllen. Der Administrator müsste 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. Ein automatisiertes Patch-Management für Microsoft-Produkte reicht alleine nicht aus: Es 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, die anerkannte Sicherheitsorganisationen pflegen, laufend aktualisieren und online zur Verfügung stellen. In diesen Datenbanken werden die Schwachstellen bewertet und nach Gefährdungspotenzial markiert. Ein solcher Schwachstellenscan

Die ReddFort Protection Software fängt da an, wo andere aufhören.

Die ReddFort Protection Software schützt Daten und Anwendungen in Unternehmen von innen heraus. Eine einzigartige und patentierte Technologie verhindert die Ausführung schädlicher Software sowie Zugriffe von außen. Schützenswerte Daten oder Anwendungen werden zunächst definiert und dann in einem autarken und geschützten Bereich isoliert. Mögliche Angriffe schädlicher Software können so diesen kritischen Daten nichts anhaben. Jetzt anrufen: 02204 759886 oder vertrieb@reddfort.com

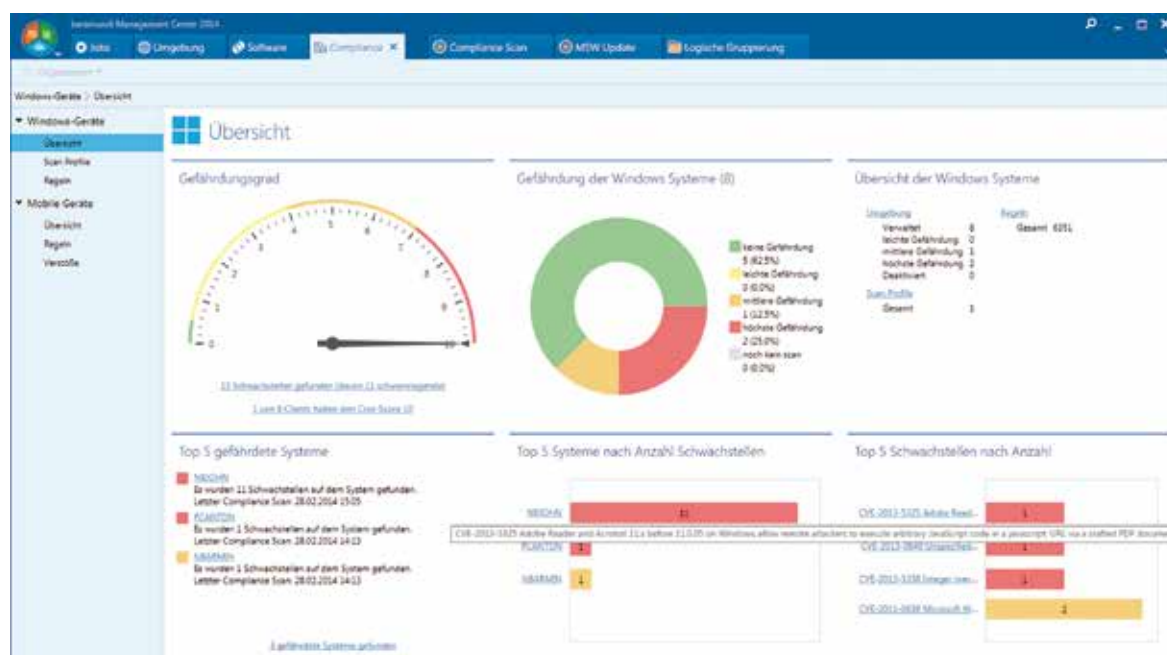
www.reddfort.com



enduring safety.
think redd.



Ein Compliance-Dashboard macht Schwachstellen in der eigenen IT-Umgebung transparent.



findet bei minimiertem Ressourcenverbrauch im Hintergrund statt und beeinträchtigt den angemeldeten Nutzer am Client nicht bei der Arbeit. Gleichzeitig nimmt er potenziellen Angreifern den Vorsprung: Der IT-Administrator erhält einen umfassenden Überblick über etwaige Lücken. Eine gute Lösung bietet eine Drill-Down-Möglichkeit, zum Beispiel nach den Clients mit den meisten oder den gefährlichsten Lücken.

Updates und Patches zentral verteilen

Für das schnellstmögliche Schließen der Lücken stehen ebenfalls automatisierte Hilfsmittel zur Verfügung. Im Idealfall sind diese mit dem Schwachstellenscanner in einer integrierten, ganzheitlichen Client-Management-Software zusammengefasst, sodass der gesamte Prozess vom Aufspüren der Lücken bis zur Patch-Verteilung in einer einheitlichen Lösung zügig ablaufen kann.

Neben Microsoft-Patches sollte eine Lösung für das Schwachstellenmanagement mindestens auch Updates für häufig genutzte Anwendungen wie Adobe Reader, Java oder Firefox zentral und automatisiert

verteilen, die aufgrund ihrer großen Verbreitung bei Angreifern besonders populär sind. Aktuelle Softwarepakete für zahlreiche Anwendungen sind auch als Managed Services von Client-Management-Herstellern verfügbar. Darüber hinaus lässt sich jede Software, die mit einer Client-Management-Lösung automatisiert nach Original-Setup-Verfahren verteilt werden kann, mit dieser automatisiert patchen.

Es genügt für ein wirksames Schwachstellenmanagement aber nicht, von einer Lücke zu wissen und eine Patch-Installation anzustoßen. Essenziell ist auch das Wissen darüber, ob das sicherheitsrelevante Update tatsächlich auf allen Clients angekommen ist. Installationen können fehlschlagen, vom Benutzer blockiert werden oder ein Notebook im Außeneinsatz könnte nicht erreichbar sein. Die eingesetzte Lösung für die Patch-Verteilung muss daher eine Rückmeldung zum Installationsstatus sowie zu etwaigen Fehlern geben.

Wichtiger Baustein Schwachstellen- management

Ein automatisiertes Schwachstellenmanagement sorgt für mehr Transparenz und eine größtmögliche

Aktualität der Client-Systeme und Server im Unternehmen. Ebenso wie eine Firewall allein, kann es 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 und automatisiertes Backup von Daten und Benutzereinstellungen, 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, die inzwischen in nahezu jedem größeren Netzwerk zu finden sind, 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.

**baramundi software AG auf der it-
sa: Halle 12, Stand 414**



Freiraum schaffen für Innovation, Kreativität, Produktivität.

Sie verantworten IT in einem Unternehmen, sind qualitätsorientiert und kostenbewusst?

Mit noris network an Ihrer Seite finden Sie **Kostenentlastung, Effizienz** und zusätzliche **Sicherheit**. In **eigenen zertifizierten Hochleistungsrechenzentren** bieten wir Ihnen individuelle **Managed IT-Services** – vom **Hosting** bis hin zum **IT-Outsourcing** mit Maßgaben nach ITIL.

Erleben Sie neue Freiheiten – www.noris.de

noris network



Studie „Hacker im öffentlichen Bewusstsein“ von Cisco Security

Deutsche unterschätzen Hacker noch immer

Jeder zweite Deutsche ist davon überzeugt, dass er noch nie privat oder am Arbeitsplatz gehackt wurde. Fast 60 Prozent sind sich zudem sicher, dass sie im Fall eines Cyberangriffs diesen schon bemerken würden. Für die Studie zum Thema „Hacker im öffentlichen Bewusstsein“ wurden 500 Deutsche Ende 2013 befragt.

Von Volker Marschner, Cisco Security

Angesichts der Tatsache, dass es heute eher unwahrscheinlich ist, im Laufe seines Lebens nicht mindestens einmal Opfer einer Cyberattacke zu werden, und die meisten Angriffe unbemerkt vonstattengehen, scheint die öffentliche Wahrnehmung beim Thema Hacking erschreckend naiv in Deutschland zu sein. Eine Studie von Cisco Security zum Thema „Hacker im öffentlichen Bewusstsein“ hat ergeben, dass ein Drittel der Deutschen beim Wort Hacker noch immer zuerst an Nerds mit zu viel Freizeit oder Teenager, die ihre Grenzen austesten wollen, denkt. Zudem ist jeder zweite Befragte davon überzeugt, dass er oder sie selbst noch nie privat oder auf der Arbeit gehackt wurde. Und es geht noch selbstbewusster: Fast 60 Prozent der Deutschen sind sich sogar sicher, dass sie im Fall eines Cyber-Angriffs diesen schon bemerken würden.

Das Bild der Deutschen von Hackern ist durch die Darstellung in der Unterhaltungsbranche stark geprägt worden. Während in Blockbustern wie beispielsweise Oceans 11 Hacking daraus besteht, ein paar Befehle einzutippen, die innerhalb von Minuten oder Stunden ein ganzes System von Unternehmen infiltrie-

ren, kann ein ernst zu nehmendes Hacking Monate oder Jahre dauern. Nur sechs Prozent der Befragten erkennen die Komplexität eines erfolgreichen Hacks an und schätzen die Dauer von einer Woche bis zu einem Monat. Mehr als 80 Prozent der Befragten glauben hingegen weiterhin, dass ein erfolgreicher Hack nur ein paar Stunden dauert. In der Realität muss die Menge an Vorbereitung, Testläufen und Überwachungsprozessen von Hackern sorgfältig geplant werden. Allein das dauert in der Regel mindestens mehrere Wochen.

Hackermotivation aus deutscher Sicht

Die deutsche Mehrheit stuft aber nicht nur die Komplexität von Hacks fehl ein, auch die Motivation von Hackern wird von einem Drittel der Befragten ziemlich unterschätzt. Neben Nerds und Teenagern betrachten 36 Prozent der Befragten Hacker als einfache Kriminelle, die ihr Handwerk digital ausüben. Dabei lässt sich ein Großteil der Angriffe auf vier typische Hackerprofile zurückführen, die sich in ihren Motiven und Zielen unterscheiden.



Digitaler Homo Oeconomicus



Der „Digitale Homo Oeconomicus“ ist der professionelle Cyberspion. Hacker dieses Typs verschaffen sich im Auftrag von Dritten, häufig Regierungen, Zugriff auf bestimmte politisch oder wirtschaftlich relevante Informationen und handeln sehr rational. Der Erfolg ist bei diesem Typ von Hacker das größte Ziel und dazu gehört auch, dass der Angriff unbemerkt bleibt.

Cyber-Dieb



Der Typ „Cyber Dieb“ wird ebenfalls vom wirtschaftlichen Erfolg angetrieben. Kennzeichnend für diesen Hackertyp ist, dass er nicht nur virtuell Konten leer räumt und sich eine Sammlung sensibler Bankinformationen beschafft, auch Phishing-E-Mails und Angriffe durch Botnetze sind bei diesem Hackertyp üblich. Dabei gehen Cyberdiebe

sehr gezielt vor, bis sie alle notwendigen Daten gesammelt haben. Im Angriffsmittelpunkt stehen Banken und Kreditkartenunternehmen, aber auch Privatpersonen und deren Kontodetails sind für diesen Angriffstypen von Interesse.

Digital Rowdys



„Digital Rowdys“ sind durch ihre erhöhte mediale Aufmerksamkeit wahrscheinlich am bekanntesten

in der Bevölkerung. Typischerweise agiert dieser Typ unter dem Deckmantel einer internationalen Hackvereinigung, die für eine bestimmte Ideologie steht und meist politische Ziele für ihre Angriffe vorschiebt. Diese Attacken werden sehr gezielt vorbereitet und treffen in der Regel Unternehmen, die entweder einen bestimmten öffentlichen Standpunkt vertreten oder die Hacker durch ihr Verhalten verärgert haben.

Amateur-Bomber



Der „Amateur-Bomber“ kommt den Klischees vom typischen, nerdigen Hacker am nächsten. Er unterscheidet sich von anderen Hacker-

typen in zwei wichtigen Punkten: Er hat erstens keinen Auftraggeber und verfolgt zweitens keine dauerhaften Ziele. Seine Motive variieren und reichen vom einfachen Beweis gegenüber anderen, dass sie einen erfolgreichen Angriff durchführen können, bis hin zu Erpressung und Voyeurismus. Viele frei verfügbare Hilfsprogramme erleichtern diesen Eindringlingen ihr Vorhaben, sodass nicht zwangsläufig professionelle Hacking-Kenntnisse vorhanden sind. Weiterhin charakteristisch für den Amateur-Bomber: Er sucht sich ganz genau aus, wann und wie er seine Hacks öffentlich macht.

In den letzten zehn Jahren gab es eine deutliche Verschiebung weg vom Hobby-Hacker hin zu großen Organisationen, die auf Cyberkriminalität spezialisiert sind. Die Angriffe werden oft weit im Voraus geplant und dauern über Monate hinweg. Die Motive sind meist wirtschaftlicher oder politischer Natur und werden oft von Auftraggebern mit erheblichen Ressourcen wie Regierungen oder Großunternehmen durchgeführt, die bestimmte Ziele verfolgen. Aber auch kriminelle Vereinigungen nutzen Hacking, um an vollständige Informationen zu gelangen.

Deutsche vertrauen weiter auf Standard-schutz

Mehr als die Hälfte der Befragten weiß, dass Cyberangriffe andauernde Prozesse sind und gemindert werden können, indem man Schwachstellen frühzeitig erkennt und beseitigt. 24 Prozent der Befragten vertrauen ihrer Malware-Schutzsoftware und denken, dass diese einen Alarm auslösen würde. 14 Prozent gaben an, dass sie einen Angriff bemerken würden, weil sich ihr Computer dann anders benehme. Was jedoch nicht bedacht wird, ist die Tatsache, dass Tarnung lebenswichtig für Hacker ist. Deshalb gilt es als oberste Priorität, von den üblichen Antivirenprogrammen eben nicht erkannt zu werden. Daher ist es für den Durchschnittsnutzer äußerst schwierig, zu erkennen, ob ein System beeinträchtigt wurde. Leider dringt diese Erkenntnis noch nicht zur breiten Bevölkerung durch. So sind nur weniger als 20 Prozent der Befragten überzeugt, dass sie einen Angriff erst merken würden, wenn es bereits zu spät ist, da gestohlene Informationen genutzt und Online-profile missbraucht wurden. ■

*Cisco auf der it-sa:
Halle 12, Stand 624*

BLACK OUT

Panikmache oder reale Gefahr?

IT-Security hautnah erleben:

**IT-Thriller als Live-Event.
München, 26.11.2014**

- // **Profi-Hacker**
- // **verblüffender Identitätsklau**
- // **IT-Crash-Szenario**
- // **Top-Abwehrspezialisten**
- // **handfeste Schutzmaßnahmen**
- // **Show Cooking**
- // **Bestsellerautor Marc Elsberg**



Erleben Sie hautnah die Gefahren, die der Autor Marc Elsberg in seinem Bestseller-Roman beschreibt. Verstehen Sie die Denkweise realer Angreifer.

Entdecken Sie mit unseren Profi-Hackern Einfallstore und Schlupflöcher.

Die besten Abwehr-Spezialisten zeigen Ihnen anschaulich die wichtigsten Schutzmaßnahmen und Wege zur Absicherung Ihres Unternehmens.

Mit: Marc Elsberg, Sebastian Schreiber, Marco Di Filippo, Bayerisches Landesamt für Verfassungsschutz, TÜV-Rheinland, TÜViT, Fink Secure, Hewlett Packard CH, ControlIT, Bundesamt für Sicherheit in der Informationstechnik (BSI)

**Jetzt informieren unter:
www.blackout-das-event.de**

SecuMedia

Der Verlag für Sicherheits-Informationen

Eine Veranstaltung von



Schutz durch zentrale Sicherheitszone
für den Internetzugang

Unternehmen im Fadenkreuz der Hacker

Das Wissen um die Notwendigkeit von Informationssicherheit ist in den Unternehmen vorhanden, nun gilt es, die Sensibilität auch in Maßnahmen umzumünzen. Praktikable Lösungen gibt es genug. DATEV zeigt Lösungswege auf.

Von Benedikt Leder, DATEV eG

Unternehmen kommen heute kaum darum herum, die Potenziale der Digitalisierung zu nutzen. Derzeit sind es Stichworte wie Server-Virtualisierung, Mobilität - beziehungsweise die sichere Anbindung mobiler Endgeräte - und Cloud Computing, mit denen sie sich beschäftigen sollten. So viel die Digitalisierung zur Rationalisierung beiträgt, sie birgt bekanntermaßen auch Angriffspoten-

ziale. Wie wichtig Datenschutz und -sicherheit insbesondere im geschäftlichen Umfeld sind, wird an diversen Stellen regelmäßig betont. Prinzipiell ist dies auch im Bewusstsein der Menschen verankert. Dennoch wird der Sicherheitsaspekt immer noch oft aus Bequemlichkeitsgründen verdrängt, wenn es um die praktische Umsetzung geht.

Eindringlicher als ein allgemeiner Appell ist natürlich der Blick auf die eigene Situation. Damit Unternehmer realistisch einschätzen können, wie ihr Betrieb in Sachen Sicherheit aufgestellt ist, bietet die DATEV einen kostenfreien und anonymen Sicherheitscheck an. Er fragt die kritischen Faktoren aus den Bereichen IT-Infrastruktur/Management, Internet- und E-Mail-Nutzung, Mobile Business sowie Datenschutz-/IT-Sicherheits-Management ab und bewertet den Ist-Zustand. Einschätzungen zu den behandelten Gefährdungsschwerpunkten erläutern, ob und welche Verbesserungsmöglichkeiten bestehen.

Auf Wunsch kann sich der Nutzer auch passende Lösungsmöglichkeiten aus dem Portfolio der DATEV aufzeigen lassen. Der Internetzugang lässt sich beispielsweise mit der Sicherheitsdienstleistung DATEVnet pro absichern. Eine zen-

trale Sicherheitszone bei DATEV schützt dabei zuverlässig vor Viren, Trojanern oder Phishing-Versuchen. Darüber hinaus werden der Zugriff auf mit Viren oder Trojanern verseuchte Webseiten blockiert und E-Mails rückwirkend auf aktuelle Virenmuster geprüft.

Über den Dienst DATEVnet pro mobil lässt sich zusätzlich der sichere Zugriff von mobilen Endgeräten auf das eigene Netzwerk realisieren. Er setzt auf eine systematische, über das Rechenzentrum abgewinkelte zentrale Verwaltung von Smartphones und Tablets sowie auf durchgängige Authentifizierungsverfahren. Über diese Infrastruktur können Unternehmer ihren Mitarbeitern auf Wunsch auch mit deren privaten Endgeräten einen abgesicherten Zugriff auf das Unternehmensnetz ermöglichen – Stichwort „Bring Your Own Device“ (BYOD).

Gegen das Ausspähen auf dem elektronischen Kommunikationsweg lassen sich sensible Daten und Informationen durch eine automatische E-Mail-Verschlüsselung schützen. Diese stellt für DATEVnet-Anwender sicher, dass jede ausgehende Mail zentral und ohne Aufwand durch den Nutzer verschlüsselt wird. Ebenso werden ankommende verschlüsselte Nachrichten zentral entschlüsselt.

Für den Schutz von Datenbeständen vor Verlust oder Zerstörung bietet DATEV mit der „Datensicherung online“ ein Backup im Nürnberger Rechenzentrum an. Dabei erfolgt die Sicherung softwaregestützt und automatisch über eine abgesicherte Internetverbindung. Darüber hinaus gehören differenzierte Beratungsleistungen zum IT-Einsatz sowie zu Sicherheit und Datenschutz zum Leistungsspektrum der DATEV. ■

Informationssicherheit: Sensible Unternehmensdaten schützen

Vortrag am Dienstag und Donnerstag im Forum Rot (Management), sowie am Mittwoch im Auditorium in Halle 12

Trotz eines insgesamt gestiegenen Bewusstseins für die Bedrohungen, ist in den Unternehmen eine Diskrepanz zwischen dem Wachstum bei der Nutzung von IT-Diensten und dem Zuwachs an Maßnahmen zur Sicherung der IT-Systeme festzustellen. Welche Maßnahmen sind für Unternehmen wichtig, um sich gegen Angriffe auf ihre Daten zu schützen? Antworten auf diese Fragestellung geben die Referenten in ihrem Vortrag.

**DATEV eG auf der it-sa:
Halle 12, Stand 425**



DIE NEUE ADRESSE FÜR IHRE IT-BEDÜRFNISSE.

2015 geht ein weiteres Hochleistungsrechenzentrum der ODN in Betrieb. Leistungsstarke IT-Infrastruktur, moderne Flächen und neueste Hardware bieten die bestmögliche Umgebung für Ihre Server, Storage-Systeme und Backup-Lösungen.

Profitieren Sie schon jetzt von unseren attraktiven Eröffnungsangeboten, exklusiv auf der it-sa 2014 in Nürnberg.

Halle 12 - Stand 433


it-sa 2014

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

ODN GmbH & Co. KG
Hermann-Glockner-Straße 7
90763 Fürth
Telefon +49 911 933877 0
www.odn.de | info@odn.de

PERSÖNLICH. INDIVIDUELL. KRAFTVOLL.



Layer-2-Verschlüsseler SITLine ETH40G

Schutz vor Daten-Entführungen

Daten werden auf ihrem Transfer auf möglichst direktem Weg zwischen den Beteiligten versandt. Immer häufiger nehmen Datenpakete jedoch unfreiwillig Umwege. Denn um Daten zu stehlen, manipulieren Angreifer die Übertragungskette und leiten den Datenstrom gezielt um. Derartige „Daten-Entführungen“ bedrohen auch deutsche Unternehmen.

Von Peter Rost, Rohde & Schwarz SIT

Um sich vor Datenumleitungen zu schützen, ist ein besonderer kryptografischer Schutz notwendig. Das gilt besonders für Datentransfers über öffentliche Netze, ein Sicherheitsrisiko sind aber auch Verbindungen, die zwar durch private Leitungen, aber über öffentlichen Grund und Boden laufen. Denn eine vorhandene Netzwerkinfrastruktur ist meist über eine lange Zeit entstanden und dadurch heutzutage mit geringem Aufwand und unverdächtigem Standardwerkzeug angreifbar.

Das Netzwerk wird allgemein als eine Schichtenarchitektur begriffen, die sich aus sieben aufeinanderfolgenden Schichten – den sogenannten OSI-Layern – zusammensetzt. Eine Verschlüsselung ist prinzipiell in jedem Layer möglich. Internet Browser bieten beispielsweise oft SSL/TLS-Verschlüsselung auf Layer 4 an, um maximal anwendungsunabhängig und interoperabel zu sein.

Wollen Unternehmen oder Behörden ihre Daten an verschiedenen Standorten verfügbar machen, stehen ihnen zwei Alternativen zur Verfügung: eine IP-basierte Ver-

schlüsselung auf OSI Layer 3 oder die Ethernet-basierte Layer-2-Verschlüsselung. Beide Varianten haben ihre Daseinsberechtigung; daher ist es sinnvoll, den Verschlüsselungs-Layer je nach Einsatzszenario und Sicherheitsanforderungen auszuwählen.

Weniger ist oft mehr

Behörden und die geheimhaltungsbetreute Industrie unterliegen im Datenschutz den höchsten Sicherheitsauflagen. Daher bedarf es eines umfassenden Schutzes des Netzwerkverkehrs. Eine Verschlüsselung auf Layer 3 ist dazu nicht ausreichend: Sie kann nur den IP-Verkehr codieren, der Rest – beispielsweise die darunter liegenden Layer-2-Protokolle – bleibt unverschlüsselt. Die sogenannte Payload, das sind jene Nutzdaten, die während der Kommunikation übertragen werden, ist damit zwar vollständig kryptografisch geschützt, jedoch bleibt der Header teilweise zugänglich. Informationen, etwa wer mit wem kommuniziert, könnten beispielsweise über eine Verkehrsfluss- oder eine Infrastrukturanalyse ausgelesen und für Angriffe genutzt werden.

Hinzu kommt, dass die IP-basierte Verschlüsselung mit einer enormen Overhead-Belastung einhergeht. Der kryptografische Protokoll-Overhead, der für die Verschlüsselung den übertragenen Paketen hinzugefügt wird, variiert abhängig von der Paketgröße, verbraucht aber bis zu 60 Prozent der Bandbreite. Mehr als die Hälfte der übertragenen Daten steht damit nicht für Nutzdaten zur Verfügung. Die Folge sind mögliche und im Vorhinein unkalkulierbare Bandbreiteneinbußen, je nach den aktuell laufenden Anwendungen. Auch darf nicht vergessen werden, dass die Auswertung und Verarbeitung der Paket-Header gemäß IPsec-Protokoll Zeit kostet. Dadurch kommt es zu einer erhöhten Latenz und einer eingeschränkten Performance gegenüber unverschlüsselter Übertragung. Die Verschlüsselung wirkt sich also negativ auf die Netzwerkperformance und damit mittelbar auf die Kosten für die Unternehmen aus. Es gibt aber auch Vorteile: IP-basierte Verschlüsselung funktioniert in allen gerouteten Netzwerken und ist daher ein weitverbreitetes Standard-Verfahren.

Die Alternative ist eine Layer-2-Verschlüsselung, die auf Ethernet-Frames angewendet wird. Ihr wesentlicher Vorteil gegenüber IPsec-basierten Verschlüsseln ist der Bandbreitengewinn durch das optimierte Overhead-Verhalten. Selbstverständlich gibt es auch auf Layer 2 Verschlüsselungsprotokolle; diese sind jedoch auf die Kommunikation zwischen den Verschlüsseln begrenzt und dadurch um bis zu 40 Prozentpunkte geringer als auf Layer 3. So wird der Datenfluss deutlich geringer ausgebremst. Mögliche Payload-Durchsatzraten von 10 bis 40 Gbit/s stehen hier den in der Praxis auf etwa 3 Gbit/s beschränkten Layer-3-Lösungen gegenüber. Eine Verschlüsselung auf Layer-2-Schicht ist aber nicht nur schneller und effizienter: Neben der Payload werden hier auch die IP-Adressen verschlüsselt und damit für Unbefugte unlesbar.

Sicherheit ist mehr als Technik

Das Vertrauen in die Wirksamkeit der Datenverschlüsselung hängt nicht ausschließlich an den technischen Aspekten. Zur Sicherheit gehören ebenfalls Zuverlässigkeit und Ausfallsicherheit einer Lösung, daher ist auch die richtige Wahl des Anbieters wichtig. Dessen finanzielle Stabilität als auch seine Herkunft und Service-Lokationen stellen erste Orientierungspunkte dar. Um sich auf die hohen deutschen Datenschutzstandards verlassen zu können, empfiehlt sich ein deutscher Anbieter für IT-Sicherheitslösungen, im Idealfall mit eigenen Entwicklungs- und Produktionsstätten im Inland.

Einen optimalen Schutz vor unberechtigtem Datenzugriff bieten zudem Verschlüsselungslösungen von Anbietern, die vom BSI zertifiziert oder sogar für die Übertragung von Verschlusssachen zugelassen sind. Ein weiterer Anhaltspunkt: Die Codierung sollte in einem separaten Gerät erfolgen – nur dann bleibt sie

im Falle eines Angriffs auf die Netzwerktechnik unangetastet.

SITLine ETH40G

Ein solcher Anbieter ist der IT-Sicherheitsexperte Rohde & Schwarz SIT. Mit dem R&S SITLine ETH40G löst das Unternehmen den Zielkonflikt von Sicherheit und Schnelligkeit: Dieser weltweit erste dedizierte Layer-2-Verschlüsseler mit 40 Gbit/s Datendurchsatz ist speziell für den codierten Austausch riesiger Datenmengen in Echtzeit konzipiert. Damit optimiert diese Lösung



Mit den Ethernet-Verschlüsseln von Rohde & Schwarz SIT ist eine sichere Datenübertragung über Festnetz, Richtfunk und Satellit für Bandbreiten von 25 Mbit/s bis 40 Gbit/s möglich.

erstmal die Performance-kritischen Faktoren Bandbreite, Latenz, Quality-of-Service, Portdichte und Energieverbrauch in einem Gerät mit der Bauhöhe nur einer Höheneinheit. Vor allem für Betreiber und Nutzer von Rechenzentren, für den Einsatz in Backbone-Netzen und zur Kopplung von Unternehmensstandorten ist diese neue Geräteklasse ideal: Sie bietet Schutz in öffentlichen und privaten Netzen, ohne deren Leistungsfähigkeit zu beeinträchtigen.

Das SITLine ETH40G setzt auf der von Rohde & Schwarz SIT eigenentwickelten Plattform-Architektur auf. Diese modulare Hard- und Softwarearchitektur bündelt die Vorteile von hochsicheren Individualentwicklungen und kostengünstigeren Standardlösungen für die Netzwerk-Kommunikationssicherung.

Die Sicherung des Datenverkehrs mit Verschlüsseln der SITLine ETH-Gerätefamilie ist mit wenig Aufwand verbunden: Außer den Sicherheitsparametern sind keine weiteren netzwerkspezifischen Konfigurationen erforderlich. Sicherheitsmanagement und Netz-

werkmanagement sind voneinander getrennt, sodass die SITLine ETH-Geräte problemlos in bestehende IT-Systeme integriert werden können. Dadurch entfällt eine aufwändige Anpassung der Netzwerkinfrastruktur.

SITLine ETH-Verschlüsseler sind aber nicht nur bei Punkt-zu-Punkt-Verbindungen oder Sternstrukturen einsetzbar. Durch die innovative Gruppenverschlüsselung kann auch die Übertragung in vollvermaschten „switched networks“ effizient abgesichert werden. Unternehmen können so die Datenströme

zwischen ihre auf mehrere Standorte verteilten Speicherlösungen absichern. Dabei spielt es sicherheitstechnisch keine Rolle, ob sie zur Vernetzung gemietete oder eigene Leitungen einsetzen.

Verschlüsselung aus „eigener Produktion“

Als 100-prozentige Tochter des unabhängigen Elektronik Konzerns Rohde & Schwarz entwickelt und produziert Rohde & Schwarz SIT in Deutschland. Das hat zwei Vorteile: Zum einen ist so eine schnelle und langfristige Verfügbarkeit der Plattformkomponenten und der darauf basierenden Produkte gewährleistet. Zum anderen können sich Kunden auf die hohen deutschen Datenschutzstandards verlassen – ein wichtiger Pluspunkt, vor allem beim Einsatz von Verschlüsselungstechnik. Die Netzwerkverschlüsseler von Rohde & Schwarz SIT sind vom BSI für die Verarbeitung von Daten der Vertraulichkeitsgrade VS-NfD und NATO Restricted zugelassen. ■

**Rohde & Schwarz SIT auf der it-sa:
Halle 12, Stand 642**



Security as a Service von T-Systems

Schutz gegen DDoS-Angriffe

Unternehmen und Organisationen sind von einer störungsfreien und verfügbaren Internetanbindung abhängig. Das nutzen Kriminelle aus und verursachen durch Distributed-Denial-of-Service (DDoS)-Angriffe große Schäden. Der Schutz vor solchen Angriffen kann heute von Unternehmen jedoch als Security as a Service ausgelagert werden.

Von Christopher Wolf, T-Systems International GmbH

Es kann jede Webseite, jeden Blog und zunehmend auch Telefonhotlines treffen. DoS-Attacken torpedieren Webserver oder auch VoIP-Server gezielt mit Verbindungsanfragen, bis der attackierte Dienst nicht mehr reagiert. Noch effektiver sind die Angriffe, wenn sie von weltweit verteilten Rechnern ausgeführt werden und Domain-Name-System-(DNS)- oder Network-Time-

Protocol-(NTP)-Verstärkungsangriffe nutzen. Solche DDoS-Attacken mit gemessenen 400 Gb/s (CloudFlare, Q1 2014) können selbst die besten Firewalls nicht abwehren.

Hohe Erfolgsquote, niedrige Preise

Die Zahl der DDoS-Angriffe stieg laut Gefährdungsbarometer

des Bundesamts für Sicherheit in der Informationstechnik (BSI) im Jahr 2013 deutlich gegenüber dem Vorjahr an. Und auch Sicherheitsanalysten von Pierre Audoin Consultants (PAC) gehen davon aus, dass es heute weltweit im Schnitt 1,4 erfolgreiche Angriffe pro Woche und Unternehmen gibt. Die Kosten durch Ausfälle betragen im Schnitt 7,2 Millionen US-Dollar pro Un-

ternehmen und Jahr. „Wir gehen davon aus, dass der Anstieg von Bedrohungen durch DDoS weiter anhält“, prognostiziert BSI-Präsident Michael Hange. Dazu tragen die Erfolgsquote der DDoS-Attacken sowie niedrige Preise der buchbaren Hacker bei, die ihre Dienste bereits für wenige Hundert Euro anbieten.

Unternehmen, die Kundendaten verarbeiten oder sicherheitskritische Aufträge erfüllen, nutzen seit jeher eine Vielzahl von Sicherheitslösungen. Dazu gehören gängige Maßnahmen wie Firewalls, Intrusion Detection Systeme (IDS), verschlüsselte Datenhaltung oder die Anwendung von Authentifizierungsmaßnahmen. Gegen eine gezielte DDoS-Attacke sind diese Vorkehrungen jedoch wirkungslos.

Wenn Bestell- oder Fertigungsprozesse komplett digital ablaufen, wird die Verlässlichkeit der Verbindung eine notwendige Voraussetzung, da sonst teure Produktionsausfälle oder unternehmensgefährdende Service-Level-Agreement-(SLA)-Verletzungen auftreten können. Gleiches gilt häufig für kritische VoIP-basierte Hotlines, zu denen auch Notrufnummern zählen können.

Eingenrealisierungen greifen zu kurz

Bestimmte Paketfilter und Application Layer Gateways können verschiedenen Arten von DDoS-Attacken zwar erkennen, allerdings können sie Angriffe nur dadurch stoppen, dass sie den Verkehr komplett unterbinden, den unternehmenskritischen Dienst so nicht nur für den unerwünschten, sondern auch für den notwendigen Verkehr unerreichbar machen. Im ungünstigsten Fall werden die Angreifer somit durch die Sicherheitsmechanismen der Unternehmen noch unterstützt.

Dabei sind die Motive der Cyberkriminellen verschieden: erpressen, bestrafen oder den Wettbewerber schädigen. Dadurch sind auch die unterschiedlichsten Unternehmen oder Vereinigungen Opfer von DDoS-Angriffen. Ende März 2014 traf es zum Beispiel die NATO, während zur gleichen Zeit die Gaming-Firma Blizzard gegen massive Angriffe auf ihre Server kämpfte.

Security as a Service

Was also tun, wenn alle implementierten Sicherheitslösungen bereits greifen? Eine effektive Maßnahme gegen die zunehmende Bedrohung durch DDoS-Attacken ist Unternehmen nur möglich, wenn zusätzliche Sicherheitsmaßnahmen vor den Grenzen ihrer Firewall eingesetzt werden. Denn dort transportiert der Internet Service Provider den Verkehr zu den Unternehmen. Neben dem reinen Transport wird der Verkehr jedoch auch hinsichtlich der Quality-of-Service und der Netzstabilität analysiert und aktiv verwaltet.

Die Deutsche Telekom als Deutschlands größter Netzbetreiber, unterhält ein eigenes Abwehrzentrum, das unter anderem den Datenverkehr des gesamten Backbone-Netzes im Blick hat – also Angriffe erkennt und abwehren kann, bevor sie auf die Firewalls der Kunden treffen. Unternehmen, die T-Systems als Internetprovider haben, können auf diese Services zurückgreifen, um die bereits seit Jahren für die Netzqualität eingesetzten, massiven DDoS-Mitigationsmöglichkeiten in Anspruch zu nehmen. ■

**T-Systems auf der it-sa:
Halle 12, Stand 12.0-546**

Keynotes und Fachvorträge von T-Systems auf der it-sa 2014

Keynotes

Dienstag, 07.10.2014,
11:00 – 11:30 Uhr

Cyber Security

Referent: Michael Uebel, Head of Executive Security Consulting, T-Systems International GmbH

Donnerstag, 09.10.2014,
11:00 – 11:30 Uhr

Neue Entwicklungen im Datenschutz

Referentin: Dorothee Schrief, Leiterin Strategy & Steering, Deutsche Telekom AG

Fachvorträge

Dienstag, 07.10.2014,
13:45 – 14:00 Uhr

Security 2.0: Tipps und Trends rund um das Security Information und Event Management (SIEM)

Referentin: Manuela Martin, Sales Consultant Security, Deutsche Telekom Technischer Service GmbH

Dienstag, 07.10.2014,
16:45 – 17:00 Uhr

Sicherheitskonzepte neu denken. Cloud und Consumerization ändern die Arbeitswelt - und Ihre Sicherheitskonzepte?

Referent: Michael Hinrichs, Leiter Produktmanagement Enterprise Mobility Services, Deutsche Telekom AG

Mittwoch, 08.10.2014,
17:00 – 17:15 Uhr

Ist die Mobilität sicherer geworden? Was hat der Abhörskandal bewirkt?

Referent: Michael Bartsch, T-Systems International GmbH

Donnerstag, 09.10.2014,
12:45 – 13:00 Uhr

Heutige Angriffsszenarios besser verstehen: Live-Hacks auf Web-Anwendungen und Kommunikationswege

Referenten: Joschka Sonneck & Markus Mielich, Security Consultants, Deutsche Telekom Technischer Service GmbH

Trust in German Sicherheit

Den Überblick behalten

Cyberangriffe auf Unternehmen haben in den vergangenen Jahren deutlich zugenommen. Die Mehrzahl der Angreifer setzt dabei auf nicht geschlossene Software-Sicherheitslücken. Ganzheitliche IT-Sicherheitslösungen schaffen hier Abhilfe.

Von Thorsten Urbanski, G DATA Software AG

Der Handel mit Informationen über bestehende Schwachstellen in Betriebssystemen, Standard- oder Branchensoftware blüht. In speziellen Untergrund-Foren werden diese zu hohen Preisen an potenzielle Angreifer und Schadcode-Schreiber verkauft. Eine Investition, die sich für Cyber-Kriminelle auszahlt, denn 90 Prozent aller erfolgreichen Schadcode-Infektionen waren im vergangenen Jahr auf Software-Sicherheitslücken zurückzuführen (Palo Alto). Interessanterweise gab es für die Mehrzahl bereits zum Zeitpunkt des Angriffs ein entsprechendes Update des jeweiligen Herstellers.

Doch warum schließen die Unternehmen bekannt gewordene

Schwachstellen nicht zeitnah? Aufgrund zunehmend heterogener Netzwerkstrukturen fehlt IT-Verantwortlichen oft der Überblick über die installierte Software und deren Update-Möglichkeiten. Verstärkt wird diese Problematik durch den Einsatz unterschiedlicher Geräte: PCs und mobile Devices und deren große Bandbreite an verschiedenen Betriebssystemversionen und Gerätehersteller-Software. Zur Ausstattung vieler Arbeitsplätze gehört heute beispielsweise ein Mobilgerät – oder den Mitarbeitern ist es erlaubt, eigene Geräte mitzubringen und am Arbeitsplatz zu nutzen. Dank umfassender Funktionen können Smartphone und Tablet auch immer mehr im Firmenalltag leisten und werden

damit immer tiefer in die Arbeitsabläufe eingebunden. So wird neben der Möglichkeit, E-Mails zu senden und zu empfangen, über den Browser oder über spezielle Apps auch auf unternehmenskritische Daten zugegriffen. Viele Außendienstler pflegen beispielsweise Bestellungen beim Kunden vor Ort direkt am Tablet ins firmeninterne Warenwirtschaftssystem ein und werden so zum potenziellen Sicherheitsrisiko. Auch die Nutzung von öffentlichen WLANs kann dazu führen, dass Schadcode über das Mobilgerät ins Firmennetz eingeschleust wird.

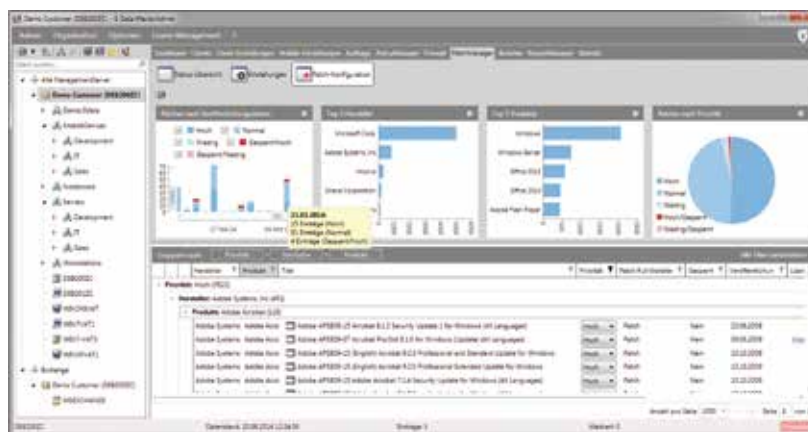
Die mangelnde Bereitschaft zu regelmäßigen Software-Updates wird durch den Umfang der in den Unternehmen eingesetzten Software noch zusätzlich verstärkt: Auf einem durchschnittlichen Computer im Netzwerk einer Organisation sind 74 verschiedene Anwendungen installiert. Viele davon sind dabei nicht integraler Bestandteil des Betriebssystems, sondern stammen von Drittanbietern (69 Prozent).

Das wiederum bedeutet, dass die jeweiligen IT-Verantwortlichen mit 30 oder mehr verschiedenen Verfahren für Updates und Patches arbeiten müssen, um die eingesetzten Anwendungen immer auf dem neuesten Stand zu halten. Zudem mangelt es in manchen Unternehmen am Problembewusstsein für die Wichtigkeit der Programm-Aktualisierungen, was Onlinekriminellen geradewegs in die Hände spielt und erfolgreiche Cyber-Attacken ermöglicht. Das Installieren von Patches und Updates ist daher ein entscheidender Baustein im IT-Security-Gerüst.

Fehlendes Device-Management

Bekanntlich erfolgen die Angriffe auf Unternehmen nicht ausschließlich über das Internet. Nicht selten gelangt Spionagesoftware mithilfe infizierter USB-Sticks

Mit G DATA PatchManagement halten Administratoren die eingesetzte Software durch zentral verteilte Updates und Patches immer auf dem neuesten Stand.



in das firmeninterne Netzwerk. Ermittlungsbehörden konnten in einzelnen Fällen von Betriebsspionage nachweisen, dass die Angreifer präparierte USB-Sticks auf Parkplätzen oder in Fahrstühlen von Unternehmen als „Fundsache“ innerhalb des Zielobjekts platzierten. Bei diesem Konzept setzen die Täter auf die Neugier des Finders, der diesen ohne Nachdenken in seinen Arbeitsplatz-PC steckt, um zu überprüfen, ob sich vielleicht interessante Daten darauf befinden.

Der installierte Schädling könnte, wie auch bei Angriffen über das Internet, nicht geschlossene Lücken in der installierten Software ausnutzen, um sich im Netzwerk zu verbreiten. Letztendlich könnten so auch Industrierechner erreicht werden, die nicht direkt mit dem Internet verbunden sind. Um Angriffe mit USB-Sticks zu vermeiden, sollten Unternehmen generell den Gebrauch privater Speichermedien in einer IT-Policy fixieren und Mitarbeiter für das Thema Datensicherheit und Cyber-Spionage sensibilisieren. Zusätzlichen Schutz schaffen Sicherheitslösungen mit integriertem Policy-Management, die den Gebrauch von USB-Speichermedien oder externen Festplatten technisch verhindern.

Gefahren von innen

Datendiebstahl erfolgt aber nicht nur durch externe Angreifer oder ist das Resultat des Befalls der IT-Infrastruktur durch Spionageprogramme. Unternehmen, die das Thema IT-Security ganzheitlich betrachten, müssen unweigerlich auch Konzepte zur Abwehr von Gefahren von innen definieren. Datendiebstahl und Datenmissbrauch sind die häufigsten Deliktarten in deutschen Großunternehmen – so das Ergebnis einer aktuellen KPMG-Studie zum Thema Wirtschaftskriminalität. 48 Prozent der Täter sind der Studie zur Folge Mitarbeiter aus den eigenen Reihen.

Die Absicherung der Firmendaten vor internem Datendiebstahl gilt es somit, ebenso zu berücksichtigen. Unternehmen sind daher gut beraten, auch hier einheitliche und verbindliche IT-Policies zu bestimmen und ein Daten-, Berechtigungs- und Device-Management-System durch entsprechende IT-Lösungen umzusetzen.

Mobilgeräte im Griff

Die zunehmende Anzahl von Smartphones und Tablets und deren Einbindung in das Firmennetzwerk bereitet IT-Verantwortlichen in puncto Sicherheit oft Kopfzerbrechen. Insbesondere beim Thema „Bring Your Own Device“ sollten Unternehmensleitung und IT-Verantwortliche genauestens die Vor- und Nachteile abwägen. Die Umsetzung und Einhaltung einer einheitlichen IT-Policy muss auf jeden Fall auch den Gebrauch von Privatgeräten im Betriebsumfeld umfassen. Dazu gehören neben restriktiven Zugangsregelungen auch eine möglichst umfassende Konsolidierung der Infrastruktur sowie klare Zugriffsrechte im Netzwerk. Wenn beispielsweise zwar neue Software an Arbeitsplätzen nur von der IT-Abteilung ausgerollt werden darf, sich aber jeder Nutzer eines Mobilgeräts danach beliebige Apps auf den Geräten installiert, gefährdet die fehlende Kohärenz der Policies das gesamte Netzwerk.

Um dabei den Überblick zu behalten, helfen beispielsweise Lösungen wie G DATA Mobile Device Management. Damit können Administratoren alle Android-Geräte als vollwertige Clients in die Security-Lösung einbinden. Egal ob es um die Absicherung vor gefährlichen Schädlingen, dem Passwortschutz für wichtige Apps und Kontakte oder die Konfiguration des Diebstahlschutzes geht, mit dem Management-Modul können IT-Verantwortliche die Sicherheit der Firmen-Mobilgeräte sicherstellen – so wird auch aus „Bring

Your Own Device“ nicht „Bring Your Own Disaster“.

Bedienkomfort reduziert Kosten

Sicherheitslösungen sollen die IT-Infrastruktur von Unternehmen effektiv schützen. Neben den eingesetzten Abwehrtechnologien, spielt hier die einfache Bedienung der eingesetzten Lösung eine nicht zu unterschätzende Rolle. Für eine umfassende und vor allem flexible Abwehrstrategie, ist es erforderlich, alle relevanten Informationen über den Sicherheitsstatus seines Netzwerkes zu erhalten. Welche Computer werden oft angegriffen - und sind bei allen PCs die Virensignaturen auf dem aktuellsten Stand? Bei G DATA Unternehmenslösungen haben Administratoren und IT-Verantwortliche dank des übersichtlichen Dashboards den Sicherheitsstatus ihres Netzwerkes und alle weiteren wichtigen Informationen jederzeit im Blick. Vorgänge wie Scan-Aufträge oder die Installation neuer Clients lassen sich mit der zentralen Management-Konsole einfach und schnell erledigen – das spart Aufwand und Zeit. Mit der Remotesteuerung G DATA MobileAdmin können IT-Verantwortliche zudem jederzeit und von jedem Ort aus auf die eingesetzte Netzwerklösung zugreifen, um den Sicherheitsstatus in Echtzeit abzufragen und so schnell und flexibel auf potenzielle Bedrohungen reagieren zu können. ■

**G Data auf der it-sa:
Halle 12, Stand 415**

Standortübergreifende Netze schützen

VPN-Router ohne Hintertür

Viele IT-Verantwortliche müssen dafür sorgen, dass die verschiedenen Standorte ihres Unternehmens sicher miteinander vernetzt sind. Das Unternehmen LANCOM Systems bietet dafür VPN-Router an, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Common-Criteria-(CC)-Stufe EAL 4+ zertifiziert sind.

Von Eckhart Traber, LANCOM Systems GmbH

Ein Jahr nach den Snowden-Enthüllungen und weiterer zahlreicher Nachrichten über Datenlecks hat sich beim Sicherheitsdenken von Unternehmen nicht viel geändert. So fragt der Sicherheitsanbieter Trend-Micro angesichts der Ergebnisse seiner Studie zur Bedrohungslage im zweiten Quartal 2014 frustriert: „Nichts Neues unter der Sonne!“ Bemerkenswert sei unter anderem, dass der mittlerweile über fünf Jahre alte Wurm Conficker im zweiten Quartal wieder einmal die Liste der Neuinfektionen mit Schadsoftware anführe, sich die Zahl der Android-Schädlinge um weitere 25 Prozent erhöht habe und Online-Gangster und -Spione klar auf Steuerungssysteme für Industrieanlagen und öffentliche Infrastrukturen zielen.

Gerade deshalb gilt weiterhin: Der heute allgegenwärtigen Gefahr durch Sabotage und Spionage müssen Unternehmen im Rahmen einer umfassenden Sicherheitsstrategie begegnen. Insbesondere der Sicherheit der eingesetzten Router sollte hier eine

hohe Priorität eingeräumt werden. So schützen VPN-Router beispielsweise standortübergreifende Netze und kritische Infrastrukturen gegen Abhören, Manipulation und Sabotage.

Bei den Anschaffungen von IT-Produkten und besonders bei der von Routern sollten IT-Verantwortliche jedoch besonderen Wert darauf legen, vertrauenswürdige Produkte zu erwerben. Denn gibt es darin eine Backdoor, ob absichtlich oder unabsichtlich, ist es für Angreifer sehr leicht, das gesamte Unternehmensnetzwerk zu infiltrieren. Aber welche Produkte sind vertrauenswürdig? Orientieren kann man sich zum Beispiel an Zertifizierungen nach dem internationalen Standard Common Criteria (CC). Auch sollten IT-Verantwortliche auf das Herstellungsland eines Produktes achten. Deutsche Produzenten müssen sich nämlich an hiesige Datenschutzgesetze halten. Einige Sicherheitshersteller haben sich darüber hinaus in der Initiative „IT Security Made in Germany“ (ITSMIG) zusammengeschlossen und verpflichten sich so selbst, in ihren Produkten keinerlei Backdoors einzubauen. Produkte, die den Anforderungen von ITSMIG entsprechen, sind mit einem Siegel gekennzeichnet.

Auch Lancom hat sich ITSMIG angeschlossen. Die VPN-Router des Unternehmens werden in Deutschland gefertigt und arbeiten mit einer eigens entwickelten Verschlüsselungstechnik. Wer es ganz sicher haben will, kann auf die „CC-Router“ des Unternehmens zurückgreifen: Diese sind durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Stufe CC EAL 4+ zertifiziert und haben damit die höchste international anerkannte Zertifizierung für ein kommerzielles Netzwerkprodukt dieser Komplexität. Die zu erfüllenden Vorgaben beinhalten unter anderem die Prüfung der Entwicklungsumgebung, des gesamten Quellcodes, der Dokumentation, des definierten Sicherheitsziels und darüber hinaus umfassende Penetrationstests durch unabhängige Experten.

In allen VPN-Routern von Lancom arbeitet das vom Unternehmen selbst hergestellte Betriebssystem „LANCOM Operating System“ (LCOS). LCOS wird unter Einhaltung höchster Sicherheits- und Datenschutzstandards am Firmensitz von Lancom in Würselen bei Aachen entwickelt. Hierdurch hat das Unternehmen die volle Kontrolle über den gesamten Quellcode und kann Manipulationen an der Firmware durch Dritte sowie Sicherheitslücken durch Fremdcode effektiv ausschließen. Auch die Hardware-Entwicklung sowie die Produktion der Lancom Router erfolgen in Deutschland.

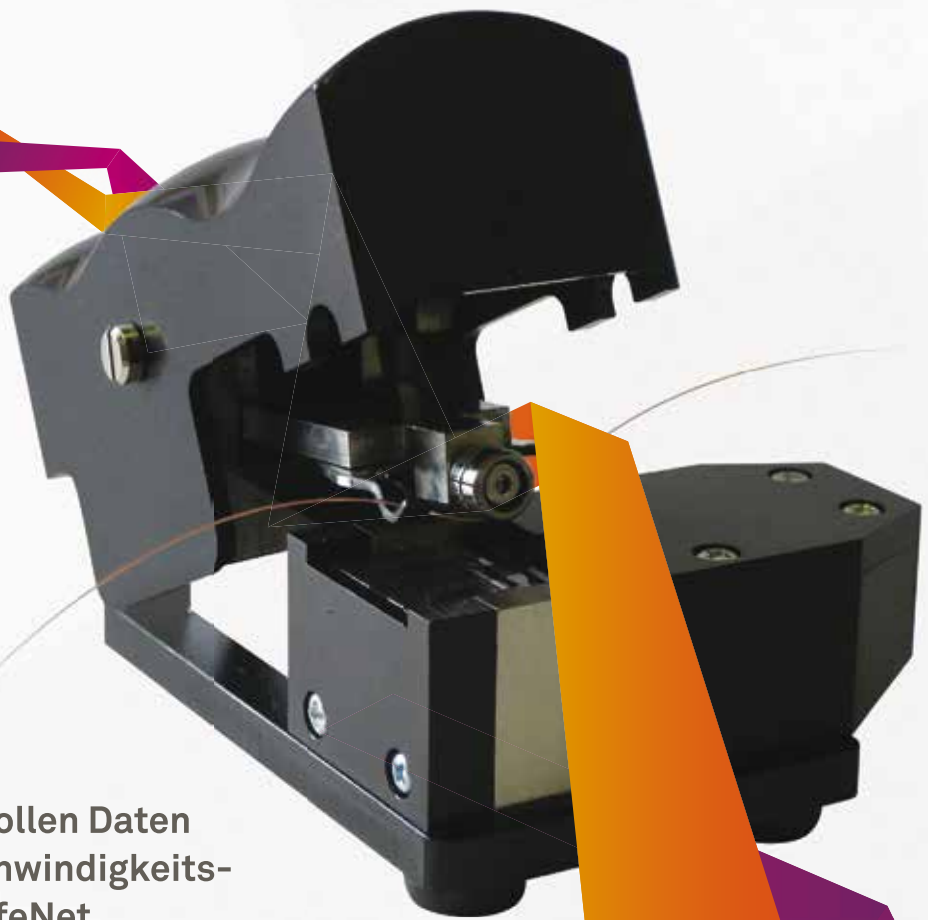
Hundertprozentige Sicherheit vor Cyberangriffen und Spionage wird es zwar nie geben. Wenn Unternehmen jedoch genau hinsehen, woher ihre IT-Produkte kommen, ist ein hohes Schutzniveau möglich. ■

Das CC-Portfolio von Lancom umfasst mittlerweile sechs VPN-Router. In der Abbildung ist der Router 9100+ zu sehen.



**Lancom auf der it-sa:
Halle 12, Stand 332**

Betriebsgeheimnisse für 250 Euro?



Schützen Sie Ihre wertvollen Daten mit Ethernet-Hochgeschwindigkeits- Verschlüsselung von SafeNet

Wir alle sind uns darüber im Klaren, dass sensible Daten im Unternehmen geschützt werden müssen. Aber wissen wir, was genau mit unseren Daten passiert, während sie an andere Niederlassungen übermittelt werden? Cyberkriminelle können, z.B. mit Clip-On-Kopplern, leicht und günstig Data-in-Transit abfangen und für ihre Zwecke weiterverwenden.

- Reduziert Kosten durch Layer2 Verschlüsselung
- Maximale Leistung: hoher Durchsatz bei Null-Latenz
- Zentrale Kontrolle und Remote-Management
- Verschlüsselt mit AES-256 und zertifiziert nach FIPS 140-2 Level 3

Informieren Sie sich über die neuen Verschlüsselungs-Appliances von SafeNet auf der it-sa 2014 oder unter www.safenet-inc.com

Trends in der IT-Security für Rechenzentren

„Wir helfen Kunden beim automatisierten IT-Security Monitoring“

Viele positive Effekte sieht Joachim Astel in der aktuellen Diskussion über IT-Sicherheit. Im Interview erläutert er, was Betreiber von Rechenzentren künftig für Kunden leisten können – und müssen.



Joachim Astel ist einer der Gründer und Eigentümer der noris network AG.

Herr Astel, wie bewerten Sie die aktuelle Diskussion um Daten- und IT-Sicherheit?

Joachim Astel: Die Diskussion ist grundsätzlich gut. Wir sehen, dass die Verantwortlichen in den Unternehmen – auch außerhalb der IT – sensibilisiert werden. Wichtig ist aber, dass diese Bewusstseinsänderung auch zu Konsequenzen führt. Nur viel guter Wille, ein deutscher Standort, ein bisschen Firewall, Spam- und Virenschutz sowie Zutrittskontrollen werden nicht reichen, um das erforderliche hohe Maß an Daten- und Betriebssicherheit zu gewährleisten.

Was ist denn in Ihren Augen zusätzlich erforderlich?

Joachim Astel: IT-Sicherheit kostet. Wir sehen das ja in unseren eigenen Rechenzentren. In den letzten Jahren haben wir enorme Investitionen getätigt, um unsere Datacenter weiter zu härten. Das sind Investitionen in spezielle Software, in die Ausbildung von Personal und in Audits und Zertifizierungen. Heute umschließen wir unsere Rechenzentren mit verschiedenen Sicherheitsringen.

Wie sieht das aus?

Joachim Astel: Da sind beispielsweise die äußeren Ringe mit Botnet Interception, unser noris network-Backbone als eigene Infrastruktur und Filter gegen Distributed-Denial-of-Service-(DDoS)-Attacken. So werden wir sehr früh über Botnets, deren Command-and-Control-Server sowie IP-Adressen infizierter Rechner informiert. Mit den DDoS-Schutzsystemen lassen sich auch komplexere Attacken erkennen und unterbinden. Danach beginnt der eigentliche Perimeterschutz mit Next Generation Firewalls und zusätzlichen, spezialisierten Filtersystemen, wie etwa Web Application Firewalls, um Kundensysteme gegen SQL-Injection, Cross-Site-Scripting oder komplexeren Gefahren zu schützen. Einen Rundumschutz in puncto Sicherheit haben wir über die Jahre durch engmaschige Monitoring-Systeme geschaffen. Der große Vorteil: Sicherheitschecks werden nicht als Projekte durchgeführt, stattdessen prüfen die Monitoring-Systeme permanent in allen Facetten der Infrastruktur. Die Techniker erhalten Hinweise über Schwachstellen und Auffälligkeiten und können gegebenenfalls sehr zeitnah darauf reagieren

und gezielt Gegenmaßnahmen einleiten. Darüber hinaus bieten wir Services wie die permanente Überprüfung der Benutzerverwaltung, bei der die Systeme auf Schwachstellen – wie etwa verwaiste Accounts oder Sonderrechte – hinweisen. Entsprechende Trust-Inkonsistenzen zwischen Active-Directory-Systemen und des Rechtemanagements werden so vermieden. Zudem lassen sich Workflows mit Freigabemechanismen etablieren. Kurz gesagt: Dank der Monitoring-Systeme und weitergehenden Compliance-Tools können sich die IT-Spezialisten auf das Schließen von Sicherheitslücken konzentrieren – während sie früher sehr viel mehr Zeit für die Suche dieser Lücken aufwenden mussten. Weiterhin erfassen wir mit Audit-Mechanismen und Auditsystemen für Systeme mit hohem Schutzbedarf alle Zugänge und Zugriffe von Systemen – sei es durch unsere Techniker oder die Techniker unserer Kunden. Mit Logging- und Korrelations-Applikationen wie Splunk oder LogStash überprüfen wir permanent die Protokollierung verschiedenartiger Systeme und können in Verbindung mit modernen Technologien Unregelmäßigkeiten und Abweichungen heute sehr bequem

erkennen. Die Systeme lösen in einer sehr frühen Security-Event-Phase Frühalarm aus und unsere Techniker können die Ursachen gleich an der richtigen Stelle prüfen.

Dieser Aufwand ist doch für normale Unternehmen und kleinere Rechenzentren und Infrastrukturen kaum darstellbar.

Joachim Astel: Der Investitionsaufwand ist wirklich erheblich. Und es braucht ja noch das kompetente Personal, das diese Systeme zielgerichtet bedient und betreibt. Wenn Unternehmen nicht wissen, wie ihr „normaler“ Betrieb aussieht, wird der Kauf eines modernen Monitoring-Systems, das auf Abweichungen von diesem Regelbetrieb reagiert, nichts bringen. Solche IT-Sicherheitsinfrastrukturen sind erst ab einer gewissen Mindestgröße wirtschaftlich darstellbar. Wir als Rechenzentrumsbetreiber müssen hier mit sehr vielen

Kunden zusammenarbeiten, müssen Schutzschirme bieten. Wir haben die kritische Masse erreicht, wo es sich lohnt, entsprechend komplexe Systeme aufzubauen und zu betreiben.

Wo ziehen Sie dort die Grenzlinien? Wie wird die Arbeits- und Aufgabenteilung zwischen Kunden und Rechenzentrumsbetreiber künftig aussehen?

Joachim Astel: Der Betrieb dieser Monitoring-Systeme und anderer Sicherheitseinrichtungen wird von den Rechenzentrumsbetreibern als Managed Service angeboten werden. Wichtig ist aber das Verständnis beim Kunden, dass sich die Unternehmen damit nicht absolut aus der Verantwortung ziehen dürfen. Wenn wir zum Beispiel auf die fehlende Awareness bei der Übermittlung ausgeschiedener Mitarbeiter im Unternehmen des Kunden oder auf offensichtlich verwaiste Accounts

hinweisen, müssen die Unternehmen durch eigene oder externe Techniker dies prüfen und zeitnah Gegenmaßnahmen einleiten. Umgekehrt müssen die Unternehmen prüfen oder durch externe Audits prüfen lassen, ob die zugesagten Services und Systeme vom Rechenzentrumsbetreiber, wie vereinbart, auf dem Stand der Technik und nach anerkannten Best Practices eingesetzt werden. Ein hohes Maß an Sicherheit wird aber auch künftig nur im Zusammenspiel zwischen Kunden und IT-Dienstleistern zu haben sein, bei denen im Projektverlauf eine regelmäßige Abstimmung zwischen Kunden und Dienstleister stattfindet – und das gerade auch im mittelständischen Umfeld. ■

**noris network AG aus der it-sa:
Halle 12, Stand 402**

Abonnieren Sie Ihre IT-Sicherheit!

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.



- liefert Ihnen strategisches Know-how, damit Sie eine solide Grundlage zur Entscheidungsfindung haben
- berichtet über Trends und Neuentwicklungen
- gibt Hilfen zum Risikomanagement
- erläutert einschlägige Gesetze im Umfeld der IT und TK
- informiert über die wichtigsten Messen und Kongresse
- ermöglicht es Ihnen durch Anwenderberichte von den Erfahrungen anderer zu profitieren
- gibt mit Marktübersichten einen Überblick über ausgewählte Produkte und Dienstleistungen



Das Abonnement enthält ein Passwort zur Nutzung des Abo-Bereichs auf www.kes.info mit allen aktuellen Beiträgen und dem **<kes>-Archiv** sowie dem Bezug des **<kes>/SecuPedia** Newsletters.

Jahresbezugspreis (6 Ausgaben) € 129,00 inkl. MwSt. und Versandkosten (Schweiz SFr 247,00 / restl. Ausland € 153,41).

Der Jahresbezugspreis wird jeweils für ein Jahr im Voraus berechnet. Eine Kündigung des Abos ist dennoch jederzeit zur nächsten nicht gelieferten Ausgabe möglich. Überbezahlte Abogebühren werden rückerstattet.

SecuMedia Verlags-GmbH, Abonnenten-Service, Postfach 12 34, 55205 Ingelheim, www.kes.info, vertrieb@secumedia.de

ABONNEMENT-BESTELLUNG: www.kes.info

Lumension Security und NetMotion Wireless bieten kombinierte Sicherheit

Arbeitsentlastung für Admins

Mit steigenden Sicherheitsanforderungen erhöht sich auch der Arbeitsaufwand für Administratoren. Unser Autor stellt den Lösungsansatz von Lumension und NetMotion Wireless vor, mit dem die Compliance- und Sicherheitsrichtlinien des Unternehmens effektiv umgesetzt werden können.

Von Andreas Müller, Lumension

BadUSB, Mobilität, Produktivität, Kostenreduktion, Personalabbau, zielgerichtete Angriffe, Softwareverteilung, Patchmanagement – das sind nur ein paar Beispiele für die Schwierigkeiten, die eine IT-Abteilung heute bewältigen muss. Während in den letzten Jahren der Fokus häufig auf Automatisierung und weitergehende Vernetzung von Unternehmen und kritischen Anwendungen gelegt wurde, kamen schleichend immer noch mehr Herausforderungen hinzu.

Ein gutes Beispiel hierfür ist die wachsende Verbreitung von mobilen Geräten. Der anfangs häufig eingeschränkte und zielgerichtete

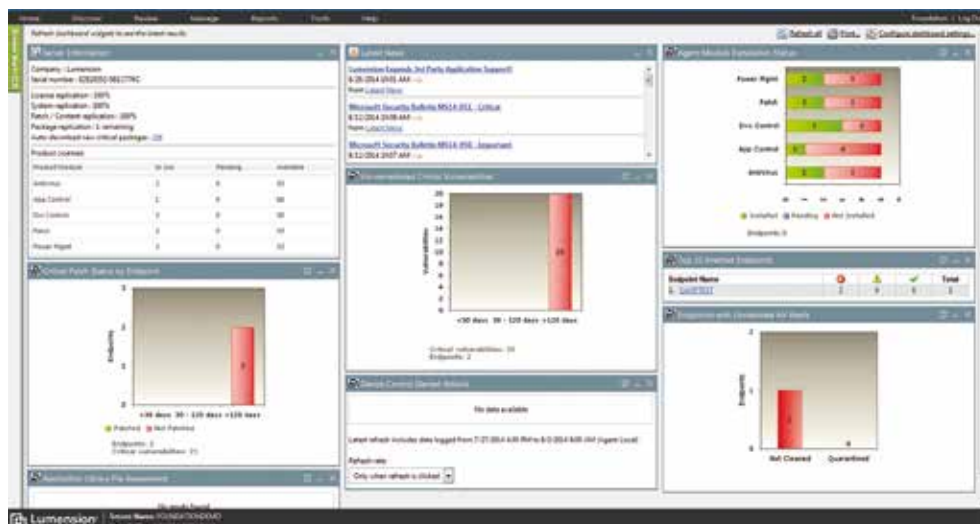
Einsatz wurde schnell aufgrund von Begehrlichkeiten von vermeintlich „vernachlässigten“ Personenkreisen aufgeweicht und führte nicht selten zu einem wahren Wildwuchs an Hard- und Software. Aktuell finden sich in vielen Umgebungen darum neben Windows, Linux, Mac OS oder RedHat auch mobile Betriebssysteme wie iOS und Android, die berücksichtigt werden müssen.

Im Gleichklang mit der damit erreichten erhöhten Produktivität, sollten die neu hinzugekommenen Tools und Geräte natürlich auch den firmenspezifischen oder allgemeinen Compliance- und Sicherheitsrichtlinien entsprechen

und den immer häufigeren und raffinierteren Angriffen widerstehen. Das brachte und bringt noch heute IT-Verantwortliche schnell an die Grenzen der verfügbaren Ressourcen. Denn zusätzlich zum sowieso schon umfangreichen und komplexen Aufgabengebiet des Lifecycle-Managements der Server, Clients und Produktivsoftware bleibt häufig einfach kein großer Spielraum dafür mehr übrig.

Kombinierter Lösungsansatz

Die Sicherheitsunternehmen Lumension und NetMotion Wireless bieten Unternehmen und Behörden daher einen kombinierten Lösungsansatz an, der einigen der häufigsten Herausforderungen in der Unternehmensinfrastruktur gerecht wird, ohne die Arbeitsbelastung der IT-Abteilungen zu erhöhen oder die Usability einzuschränken. Im Folgenden werden wichtige Punkte des Ansatzes genannt.



Screenshot der Lumension Endpoint Management and Security Suite

Mobile Geräte

Mobile Geräte befinden sich häufig nicht im firmeninternen Netzwerk und sind damit nicht durch die erweiterte Netzwerkabsicherung geschützt. NetMotion Wireless ist ein vollständig transparenter (Mobile)-VPN. Der Agent wird als Dienst ausgeführt und verbindet den Client automatisch nach dem Bootvorgang mit dem firmeninternen Netz. Das Kompromittieren des Clients über die externen Schnittstellen durch externe Software kann ebenso wie unerwünschter Datenfluss zusätzlich mit der externen Device-Control-Lösung von Lumension unterbunden werden. Sollte dennoch Schadsoftware über freigegebene Medien auf den Rechner gelangen, so wird die Ausführung durch Lumension Application Control unterbunden. Egal ob es sich dabei um eine bekannte Schadsoftware handelt oder um eine sogenannte Zero-Day-Attacke.

VIP-Nutzerrechte absichern

Einige User haben mehr Rechte auf ihren Geräten und sind durch Low-Level-Sicherheit ein Risiko für das Netzwerk, wenn sie sich wieder verbinden. Die Anforderung zur Freigabe höherer Rechte ist in einigen Fällen wie zum Beispiel bei Servicetechnikern oder Entwicklungsabteilungen durchaus angebracht. Dies betrifft je nach User alle Gerätetypen, nicht nur die mobilen. Für diese speziellen User wurde in Lumension Application Control mit der Berechtigung zur „Lokalen Selbstautorisierung“ ein komfortabler Weg eingebaut. Hier wird der User via Popup darauf hingewiesen, dass die auszuführende Datei nicht dem Firmenstandard entspricht, er aber eine lokale Ausnahme generieren kann. Diese wird danach geloggt und dem zentralen Administrator per Report zur Kenntnis gebracht. Dieser kann dann im Nachhinein die Applikation auch für andere User freigeben oder den Gebrauch per Mausklick unterbinden. Zusätzlich können Geräte,

die sich nach einer geplanten Phase der „Freiheit“ wieder mit dem Netzwerk verbinden, mit der integrierten NAC-Funktion von NetMotion Mobility auf die Sicherheitsrichtlinien des Unternehmens geprüft und erst dann ins Netzwerk gelassen werden, wenn diese auch erfüllt sind.

User Acceptance

Wenn Mitarbeiter durch zu strikte Regeln in der Produktivität eingeschränkt werden, fangen sie an, sich zu wehren. Ein Vorteil der Lösungen von NetMotion und Lumension besteht in der starken Ausrichtung auf den Aspekt der Usability. Durch die vollständige Transparenz des mobilen VPN-Clients, der die gängigen Single-Sign-On-Verfahren vom normalen Windows-Domain-Logon bis zu dedizierten PKI-Lösungen unterstützt, werden die User von der Notwendigkeit zur weiteren Eingabe eines Passwortes entlastet. Den Vorteil einer solchen automatischen Verbindung kann wohl jeder nachvollziehen, der schon mal versucht hat, auf Reisen und mobil auf Unternehmensressourcen zuzugreifen und sich nach wiederholtem Verbindungsabbruch erneut anmelden durfte. Ein weiteres Merkmal der VPN-Lösung besteht in der Priorisierung der benutzten Verbindungen und in der automatischen Wiederaufnahme am Punkt der Unterbrechung. Dabei gehen die eingegebenen Daten auch bei Online-Formularen nach Tagen nicht verloren. Nutzer mit speziellen Anforderungen können über individuelle Regeln und Freigaben in Lumension Application Control und Device Control berücksichtigt werden.

Bandbreite

Ein oft genanntes Argument gegen VPN ist, dass die Verwendung eines VPN die verfügbare Bandbreite einschränkt. NetMotion Mobility verfügt über eine integrierte Quality-of-Service-Funktion. Diese lässt sich bis auf Applikationsebene

konfigurieren, sodass die verfügbare Bandbreite in Abhängigkeit der Umgebungsvariablen optimal verteilt wird. Zum Beispiel kann SAP bei Verbindungen über 3G oder UMTS 70 Prozent der Bandbreite bekommen und Facebook auf 5 Prozent reduziert werden, während bei hohen Bandbreiten via WLAN keinerlei Einschränkungen bestehen. Applikationen können auch ganz für die Verwendung über mobile Verbindungen gesperrt werden. Zusätzlich verfügt Mobility über eine eingebaute Komprimierungsfunktion.

Schwachstellenmanagement auf mobilen Geräten

Grundsätzlich kann Lumension mit den Funktionen von „Patch & Remediation“, einer der ältesten und am weitesten entwickelten Schwachstellenmanagement-Lösung, bereits das Management der stationären Geräte erheblich vereinfachen. Der Agent überprüft hierbei selbstständig seinen Host auf das Vorhandensein von Schwachstellen im Betriebssystem und von Applikationen und meldet das dem Administrator. Dieser kann dann auf einen umfangreichen Katalog fertiger und geprüfter Installationspakete beziehungsweise Schwachstellenbehebungen zurückgreifen und diese ohne weiteren Aufwand an die Clients verteilen. Für Nutzer von Microsofts SCCM2012 stellt Lumension die Möglichkeit zum Import des Softwarekatalogs via System Center Updates Publisher (SCUP) für alle nicht MS-Software zur Verfügung. Da Systeme mit NetMotion Mobility sich quasi immer im Firmennetz befinden und sowohl der VPN als auch Patch & Remediation über eine Möglichkeit zum Bandbreitenmanagement verfügen, können also auch Patches und Policies im Hintergrund an diese Clients verteilt und sie so auf einem aktuellen Stand gehalten werden. ■

**Lumension auf der it-sa:
Halle 12, Stand 12.0-520**

Vorschau auf die neuen Business-Lösungen von ESET

Never change a running system?

Über 25 Jahre Erfahrungen im IT-Security-Bereich, mehr als hundert Millionen Nutzer und verschiedenartige Großprojekte haben wichtige Erkenntnisse für die Weiterentwicklung der ESET-Produkte hinterlassen. Eine sinnvolle Umsetzung all der sich daraus ergebenden Potenziale war ohne eine neue technische Basis nicht machbar.

Von Michael Klatte, ESET Deutschland GmbH

Es ist nicht überraschend, dass die Business-Produkte für Windows-Endpoints eine herausragende Stellung bei ESET einnehmen. Schließlich decken sie einen erheblichen Teil der gesamten Installationsbasis und Umsätze ab. Entsprechend umfassend fällt die aktuelle Überarbeitung der Version 6 des Endpoint-Schutzes aus. Dabei stehen die Verbesserung der Sicherheit und der Effizienz im Vordergrund.

Die eigentliche Abwehr von Viren & Co. erreicht ein neues Niveau, insbesondere bei erstmalig auftretenden, bisher unbekannten Bedrohungen. ESETs Scan-Engine und der Echtzeit-Dateischutz wurden weiter verbessert und um neue Techniken erweitert. So überwacht der Exploit Blocker häufig angegriffene Programme auf Auffälligkeiten. Zeigen beispielsweise ein Web-Browser, MS Office, das E-Mail-Programm oder ein PDF-Reader ungewöhnliche Verhaltensweisen, werden die damit verbundenen Prozesse automatisch analysiert und im Ernstfall unterbrochen.

Ähnlich arbeitet der erweiterte Speicherscanner. Moderne Malware ist zunehmend aufwändig getarnt und/oder verschlüsselt, um einer Erkennung durch Antiviren-Software zu entgehen.

Zum Zeitpunkt der Ausführung im Arbeitsspeicher muss der Schadcode jedoch „die Hosen herunterlassen“ und kann detektiert werden. Bei verdächtigen Verhaltensmustern kann auch hier der kritische Prozess abgebrochen werden.

Die Schwachstellen-Prüfung der ESET Endpoint Security untersucht den Datenverkehr auf Angriffe gegen Sicherheitsdefizite der verwendeten Netzwerk-Protokolle. Wird versucht, ein bekanntes Problem von SMB, RPC, RDP & Co. auszunutzen, kappt die Zwei-Wege-Firewall die Verbindung und die zugehörigen Prozesse werden gründlich analysiert.

Verbesserter Endpoint-Schutz

ESETs Produkte gehen sparsam mit Systemressourcen um und sind relativ unkompliziert zu benutzen. Das beginnt mit der Version 6 schon bei der Installation. Ersetzt der Anwender beispielsweise ein ESET Endpoint-Produkt durch eine neue Version, wird er bei der Migration der Einstellungen unterstützt. Zudem wurde in der neuen Version die Bedienoberfläche überarbeitet. Sie ist nun auch für Touchscreen-Geräte sowie hochauflösende Displays geeignet und primär auf intuitive

Bedienung getrimmt. So wurde beispielsweise die Struktur der erweiterten Einstellungen neu aufgebaut und ist auch im ESET Remote Administrator in identischer Form wiederzufinden, was dem Admin die Einarbeitung erleichtert.

Ähnlich ist es bei der Firewall. Regeln können nun auch aus Log-Files heraus erstellt werden und ein Assistent hilft bei deren Einrichtung oder der Fehlersuche. Bei besonders anspruchsvollen Topologien erweist sich die neue Gestaltung der Netzwerk-Zonen ebenso hilfreich wie die Möglichkeit, Regelsätze bestimmten Standorten sowie Netzwerk-Interfaces zuzuweisen.

Auch im Bereich der Ressourcenschonung konnten noch Fortschritte erreicht werden: Der „shared local cache“ speichert lokal Metadaten zu bereits gescannten Dateien und vermeidet somit mehrfache Scans. Innerhalb schneller Netzwerke ist der Effekt nennenswert. Bei üblichen Virtualisierungs-umgebungen werden nicht selten Reduktionen der Systembelastung durch Scans zwischen 40 bis 80 Prozent erreicht. Die Netzwerklatenz der virtuellen Maschinen (VM) untereinander spielt auf einem gemeinsamen Hypervisor eine untergeordnete Rolle und die Systeme



TOMORROW starts here.



Cisco Connect

Berlin, Station
20.-21. November 2014

Internet of Everything:
Connect the unconnected

Informieren, orientieren, entscheiden – IoE ist auch Ihr Thema!

Connect the unconnected –

Der größte Internet of Everything (IoE) Business-Kongress zeigt, wie Unternehmen in Deutschland von Industrie 4.0 profitieren können und welche IT-Infrastruktur dies ermöglicht.



Cisco Connect Kongressprogramm

- ▶ Keynotes & Power-Sessions von Top Unternehmen wie z. B. BASF Group, Daimler, SAP AG und anderen
- ▶ Networking, Erfahrungs- und Gedankenaustausch mit Experten und Teilnehmern
- ▶ Ausstellung mit über 40 Industrie-, Technologie- und Vertriebspartnern
- ▶ Cisco Connect Party am Abend des ersten Kongresstages

▶▶▶ Jetzt anmelden! www.ciscoconnect.de

Cisco auf der it-sa 2014

Wir freuen uns über Ihren Besuch am Stand 12.0-624

in den VMs weisen oft große Ähnlichkeiten auf. Zusammen mit einer Reihe weiterer Neuerungen ist der Fortschritt erheblich – insbesondere in virtuellen Umgebungen.

ESET Remote Administrator

Neben den Trends zu Cloud- und Virtualisierungslösungen hat auch die zunehmend komplexe Netzwerktopologie einen Einfluss auf das Neudesign gehabt. Die zentrale Verwaltung mehrerer Standorte mit hierarchischen Policies und abgestuften Administrator-Rechten ist immer häufiger zu beobachten, wie auch die Auftrennung von Netzwerken je nach Funktion. Das Isolieren von Netzwerken ist insbesondere bei Problemstellungen wie dem allgegenwärtigen „Bring Your Own Decice“- (BYOD)-Hype ratsam.

Um den IT-Experten in ihrer immer komplexeren Welt das Leben zu erleichtern, wurde der ESET Remote Administrator (ERA) von Grund auf neu konzipiert:

— Der ERA ist nicht mehr exklusiv an ein Windows-System gebunden, sondern kann nun auch auf einem Linux oder in Form einer VM bereitgestellt werden.

— Das Ausrollen und Verwalten der Clients erfolgt mittels eines unabhängigen ESET Remote Administrator Agents. Dieser Agent kann auch Policies und dynamische Gruppen automatisch verarbeiten, womit ein korrektes Verhalten der Clients auch bei fehlender Verbindung zum ERA sichergestellt wird. Beispielsweise können bei der Erkennung einer Bedrohung automatisch Policies oder Firewall-Regeln ersetzt, Scans gestartet, Wechseldatenträger gesperrt und Reports generiert werden.

— Der ERA-Agent erlaubt auch die Installation sowie das Entfernen von Software Dritter.

— Die Verwaltung mehrerer Netzwerke beziehungsweise Standorte kann nun auch unter Verwendung von Proxies realisiert werden. Diese koordinieren die Kommunikation der Agents beziehungsweise Clients des jeweiligen Netzwerks mit dem ERA. So benötigt man nicht überall eine vollständige ERA-Installation und die auftretende Netzwerkcommunication wird weiter reduziert.

— Die Datenbanken, der eigentliche Server und auch der Webserver können bei Bedarf auf verschiedene Systeme verteilt werden.

— Die Administrationsoberfläche kann immer und überall via Web-Interface erreicht werden. Ein Client muss nicht installiert sein.

— Deutliche Verbesserungen der Reporting-Funktionen.

— Das überarbeitete Lizenzmodell vereinfacht die Verwaltung der ESET-Lizenzen. Änderungen an den Lizenzen werden automatisch an alle Clients übertragen.

— Unbekannte und ungeschützte Systeme innerhalb des Netzwerks können besser detektiert werden.

— Die Administration wird durch Maßnahmen wie den neu gestalteten Policy-Editor, Assistenten oder Templates für Policies, Reports, Warnungen, Tasks & Co. vereinfacht.

Der Blick auf diese Liste der Neuerungen lässt leicht erahnen, dass es sich um ein größeres Projekt handelt. Umso erfreulicher ist es, dass die Entwicklung im Plan liegt und die Tests mit ersten Kunden positiv ausgefallen sind.

Verschlüsselung mit DESlock+

Der Einsatz von Verschlüsselungslösungen sollte in Unternehmen integraler Bestandteil der IT-Sicherheitsrichtlinien sein. Dass sich

bequemes Handling und eine einfache Installation bei einer solchen Software nicht ausschließen müssen, beweist die Verschlüsselungslösung DESlock+. Bei der sogenannten ESET Technology Alliance steht der sichere Datenaustausch ganz oben auf dem Programm: Von E-Mail-, über Dateien- bis hin zu Ordnerverschlüsselung, die bei teamübergreifenden Projekten und komplexen Arbeitsgruppen den notwendigen Schutz vor fremden Blicken bietet. Auf Knopfdruck kann die Verschlüsselung ganzer Festplatten vorgenommen werden. Zudem lassen sich über den DESlock+ Enterprise Server alle Konfigurationen und Policies bequem umsetzen und verwalten.

Verschlüsselungslösungen sind schön und gut, sollten aber natürlich auch benutzt werden. Und das werden sie nur dann, wenn die Handhabung einer solchen Software die Mitarbeiter nicht von der täglichen Arbeit abhält oder letztere gar verkompliziert. Neben umfassender Datensicherheit liefert die benutzerfreundliche Oberfläche von DESlock+ ein Argument mehr, den Schutz im Unternehmen nicht mehr zu vernachlässigen.

Auch wenn es keine 100-prozentige Sicherheit gegen Schnüffelnasen wie NSA & CO. gibt, legt beispielsweise der eco Verband deutschen Unternehmen einen breiten Einsatz von Verschlüsselungslösungen ans Herz. Denn auf die Weise legt man den Geheimdiensten entscheidende Hürden in den Weg und vertrauliche Informationen können nicht ohne Weiteres mal eben ausgelesen werden. Das Abhören von Firmen- und Privatrechnern wird für die Spionageabteilung weitaus schwieriger, teurer und zeitaufwändiger. Schon allein das ist es wert. ■

itsa 2014

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

Punktlandung für Ihre IT-Sicherheit

Nürnberg, Germany, 7. – 9.10.2014



Stets bestens informiert: it-sa.de/newsletter



Congress@it-sa – bereits vom 6.–9.10.2014

Expertenwissen hautnah – kompakt, relevant und aktuell.

Mehr Informationen und Anmeldung unter:
it-sa.de/congress

NÜRNBERG MESSE

Moderne Brandschutzkonzepte für hochtechnisierte Rechenzentren

Mit Sauerstoffreduktion Datenverfügbarkeit sichern

Hochtechnisierte Rechenzentren sind das Herzstück vieler Unternehmen. Damit Daten und Informationen ohne Unterbrechung verarbeitet und weitergeleitet werden können, bedarf es entsprechender Sicherheitsvorkehrungen. Dazu gehört auch das passende Brandschutzkonzept.

Von Katharina Bengsch, WAGNER Group GmbH

Störungen der IT-Infrastruktur kann sich heute kaum noch ein Unternehmen leisten – insbesondere, wenn sowohl interne als auch externe Abläufe über den IT-Server oder ein Rechenzentrum gesteuert werden. Bei Unterbrechungen sind negative Auswirkungen auf den Geschäftsbetrieb vorprogrammiert. Dafür muss noch nicht einmal das gesamte Rechenzentrum betroffen sein. Bereits Ausfälle einzelner Serverschränke oder IT-Komponenten können dazu führen, dass wichtige Daten nicht oder nur eingeschränkt verfügbar sind. Arbeitsstillstände, Umsatzeinbußen und eine beschädigte Reputation sind die Folgen. Ein 10-tägiger Ausfall eines Schlüsselsystems der IT könne ein Unternehmen so nachhaltig schädigen, dass es mit 50 % Wahrscheinlichkeit innerhalb der nächsten drei bis fünf Jahre vom Markt verschwindet, heißt es im Leitfaden „Betriebssichere Rechenzentren“ vom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM).

Um einen störungsfreien Betrieb an 365 Tagen im Jahr gewährleisten zu können, sind gewisse Sicherheitsvorkehrungen notwendig. Redundanzen in der Klimatechnik und eine unterbrechungsfreie Stromversorgung sowie regelmäßige Wartungen ohne den Betrieb zu unterbrechen haben sich mittlerweile

als Standard in hochverfügbaren IT-Strukturen etabliert. Ein modernes Brandschutzkonzept gehört ebenfalls dazu. Mit einer Kombination aus beispielsweise aktiver Brandvermeidung durch Sauerstoffreduktion sowie einem Ansaugrauchmeldesystem bietet das Langenhagener Unternehmen WAGNER individuelle Brandschutzlösungen an, mit denen auf ein Stromlosschalten im Brandfall verzichtet werden kann.

Erhöhtes Brandrisiko in RZs

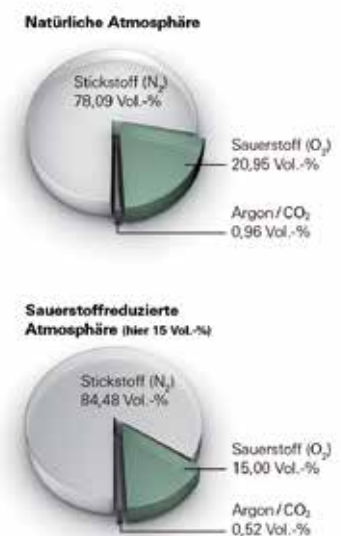
In IT-Zentren bestünde aufgrund der Vielzahl elektrischer Komponenten wie Leiteranschlüsse und -verbindungen und Kabelleitungen ein erhöhtes Risiko für durch technische Mängel ausgelöste Brände, so das VdS-Merkblatt VdS 2837. Ein Schmelzbrand, der nicht frühzeitig erkannt wird, findet beispielsweise durch die im Rechenzentrum vorhandenen Kunststoffe wie Kabelummantelungen, Platinen, Servergehäuse und dergleichen ausreichend „Nahrung“, um sich weiter auszubreiten.

Damit ein Brand überhaupt entstehen kann, müssen grundsätzlich Energie, Sauerstoff und Brennstoff in ausreichend großer Menge vorhanden sein. Wird einer dieser Faktoren verändert, ändert sich damit auch das Brandverhalten. Genau

da setzt das Prinzip der Brandvermeidung mittels Sauerstoffreduzierung an, das sich speziell in sensiblen IT-Bereichen bewährt hat.

Brandvermeidung durch Sauerstoffreduzierung

Mittels der OxyReduct-Brandvermeidungsanlage wird die Sauerstoffkonzentration innerhalb eines Schutzraumes von den in der normalen Umgebungsluft enthaltenen 20,9 Vol.-% auf ein reduziertes



Beim Prinzip der aktiven Brandvermeidung wird kontrolliert Stickstoff in den Schutzbereich eingeleitet und somit die Sauerstoffkonzentration gesenkt. Das Maß der Sauerstoffreduzierung wird in Abhängigkeit der Entzündungsgrenzen der zu schützenden Stoffe festgelegt. In der Regel reichen bereits einige Vol.-% weniger aus, um das Brandrisiko erheblich zu reduzieren.

Niveaugesenkt. Das geschieht, indem dem Bereich kontrolliert Stickstoff zugefügt wird. Der dafür benötigte Stickstoff wird umweltschonend und kosteneffizient direkt vor Ort aus der Umgebungsluft gewonnen. So wird eine weitere Brandentwicklung verhindert. Auf ein Stromlosschalten der gesamten IT-Infrastruktur, wie es bei herkömmlichen Brandschutzsystemen im Brandfall erforderlich ist, kann somit verzichtet werden.

Wie stark die Sauerstoffkonzentration gesenkt werden muss, wird im Hinblick auf die vorherrschenden Materialien und deren unterschiedlichen Entzündungsgrenzen entschieden. Im IT-Bereich werden die Entzündungsgrenzen der vorhandenen Stoffe und die erforderliche Auslegungskonzentration der Sauerstoffreduzierungsanlage in der VdS 3527 geregelt. In anderen Schutzbereichen wird die benötigte Sauerstoffkonzentration durch Brandversuche von WAGNER bei Bedarf individuell ermittelt. Zudem muss beachtet werden, ob eine freie Begehrbarkeit für das Personal jederzeit gewährleistet sein muss oder nicht. So kommen unterschiedliche Brandschutzkonzepte – teils mit mehrstufigen Sauerstoffreduzierungen – zum Einsatz.

In zahlreichen Anwendungen wird durch die Brandvermeidungsanlage die Sauerstoffkonzentration in dem Schutzbereich zunächst auf ein Niveau mit deutlich verringertem Brandverhalten abgesenkt, zum Beispiel auf 17 Vol.-%. Die Bereiche bleiben dabei von autorisiertem Personal weiterhin begehbar. In der Regel wird eine Brandvermeidungsanlage mit einer Brandfrüherkennung kombiniert, wie etwa mit den TITANUS Ansaugrauchmeldern von WAGNER. Diese erkennen Brände bereits während ihrer Entstehungsphase. Dafür entnehmen sie der Luft aktiv Proben und analysieren diese auf Pyrolysepartikel. Bereits zwei Gramm stoffliche Umsetzung reichen in der Regel

aus, damit das System anschlägt. Rauch ist während dieser frühen Entwicklung eines Brandes mit dem bloßen Auge nicht zu erkennen. Im Vergleich zu konventionellen Punktmeldern sind Ansaugrauchmelder der TITANUS-Familie daher bis zu 2.000-mal sensibler. So wird ein entscheidender Zeitvorteil für das Ergreifen von Maßnahmen geschaffen.

Ergänzende Maßnahmen

Die neueste Generation der TITANUS Ansaugrauchmelder ermöglicht zusätzlich zur normalen Detektion eine besondere Brandmustererkennung. Mit TITANUS MULTI-SENS können Brandmuster und Störgrößen dem Ansaugrauchmeldesystem kundenspezifisch angelernt werden. Die neue Technik erkennt diese und bewertet sie dann automatisch. Die Rauchaerosole einer Zigarette oder auch Nebel klassifiziert das System beispielsweise als unkritisch und sendet statt eines Brandalarms nur eine entsprechende Infomeldung.

Das Ziel der Neuentwicklung ist nicht nur Täuschungsalarme auszuschließen. Durch die genaue Analyse darüber was brennt, können auch gezieltere Gegenmaßnahmen ergriffen werden. Wird in einem Bereich des Rechenzentrums, in dem der Sauerstoffgehalt bereits durch eine OxyReduct-Anlage abgesenkt wurde, ein Brand detektiert, sieht ein Schutzkonzept von WAGNER vor, mithilfe einer Schnellabsenkung den Sauerstoffgehalt weiter auf eine löschfähige Konzentration abzusinken. Der dafür benötigte Stickstoff wird dafür aus Flaschen bereitgestellt. Das stark reduzierte Sauerstoffniveau kann danach über die OxyReduct-Anlage so lange wie nötig gehalten werden, bis beispielsweise der Stickstoff in der Flaschenbatterie wieder aufgefüllt wird. Denn die Batterie wird für die Schnellabsenkung in der Regel vollständig entleert.

Durch die genaue Detektion, welcher Stoff innerhalb des



Der Ansaugrauchmelder TITANUS MULTI-SENS analysiert Brandmuster und Störgrößen und stuft diese kritisch und unkritisch ein.

Schutzraumes brennt, kann das Ansaugrauchmeldesystem die Information weiterleiten, wie viel Stickstoff tatsächlich benötigt wird und ob die vorhandene Menge ausreicht. Erkennt das System beispielsweise einen Kabelschmelzbrand, müsste der Sauerstoffgehalt nur bis kurz unter dessen Entzündungsgrenze gesenkt werden. Mit dem Einsatz von TITANUS MULTI-SENS kann die Löschmittelmenge brandspezifisch angepasst und somit gezielter bestimmt werden. Die OxyReduct-Anlage hält anschließend das erneut verminderte Sauerstoffniveau so lange wie nötig. Ein Auslösen der gesamten Flaschenbatterie ist in diesem Fall nicht mehr notwendig.

Fazit

Eine Kombination aus aktiver Brandvermeidung und frühestmöglicher Branderkennung schützt IT- und Rechenzentren nachhaltig vor den Auswirkungen eines Feuers. Dabei wird jedes Brandschutzkonzept individuell auf die Gegebenheiten vor Ort zugeschnitten und den Bedürfnissen der Betreiber angepasst. Datenverluste, die über den direkten Brandschaden hinausgehen, können vermieden werden. Ein Stromlosschalten der IT im Brandfall gehört damit der Vergangenheit an, die ständige Datenverfügbarkeit bleibt erhalten. ■

Verbandsgemeinde Selters setzt auf ein
Micro Data Center von Rittal

Die Daten sind sicher im Westerwald

Die IT-Infrastruktur der Verbandsgemeinde Selters im Westerwald war in einem separaten EDV-Raum untergebracht, der jedoch die Anforderungen an Datensicherheit und Verfügbarkeit nicht mehr erfüllte. Mit dem Rittal Micro Data Center Level E sind die Server der Verbandsgemeinde nun sicher vor physischen Gefahren wie zum Beispiel Feuer oder Fremdzugriff.

Von Patricia Späth und Bärbel Müller, Rittal

Eine sichere Verwahrung aller Einwohnerdaten ist für öffentliche Verwaltungen ein Muss. Die IT-Infrastruktur der Verbandsgemeinde Selters war in die Jahre gekommen und konnte den Anforderungen



Das Rittal Micro Data Center Level E ist ein Umhausungssystem, das einen vollständigen Sicherheitsbereich um ein Server-Rack einrichtet. (Bilder: Rittal)

des IT-Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) nicht mehr standhalten. Die Server der Gemeinde beherbergen neben dem Meldewesen über Ausweis-, Verkehrs- und Gewerbeangelegenheiten auch die Meldedaten der 16800 Einwohner. Alle Daten waren in einem separaten Server-Raum untergebracht, den man bereits 1998 von einer lokalen Firma übernommen hatte. Zusätzlich unterstützen die IT-Systeme die Eigenbetriebe der Verbandsgemeinde, insbesondere deren IT-gestützte Abrechnungen sowie Auswertungen.

Auch wenn die IT-Komponenten der Verbandsgemeinde in einem separaten Raum mit Brandschutztür untergebracht waren, bot diese Lösung nur unzureichende Sicherheit. Neben den Servern befanden sich im Raum beispielsweise andere Geräte, die eine zusätzliche Brandlast und somit eine Gefahr für das IT-Equipment darstellten. Eine lückenlose Überwachung des Raumes und somit ein frühzeitiges Erkennen einer Gefahr war nicht sichergestellt.



Ein Blick in den BSI-Grundschutzkatalog öffnete den IT-Verantwortlichen in der Verbandsgemeinde Selters die Augen. „Wir mussten unsere IT konsolidieren und wollten die Anzahl der Server verringern“, sagt Udo Köth, verantwortlich für die EDV der Verbandsgemeinde. „Uns war aber auch klar, dass wir im Zuge der Konsolidierung unsere IT sicherer und verfügbarer auslegen mussten. Ein eigener Sicherheitsraum für die Abwehr von physischen Gefahren wäre allerdings überdimensioniert gewesen.“

Auslagerung der Daten zu unsicher

Nachdem 2012 die Gelder im Haushalt für eine neue IT-Infrastruktur bereitgestellt wurden, begannen die IT-Verantwortlichen 2013 mit der Suche nach einer Lösung. „Wir hatten auch überlegt, die IT-Prozesse auszulagern“, beschreibt Köth den Entscheidungsprozess. „Jedoch müssen wir für unsere Bürger maximale Datensicherheit garantieren, die Auslagerung der Daten war uns zu unsicher.“ Eine

bauliche Veränderung des Raumes für maximale Sicherheit wäre für ein einziges Server-Rack ebenfalls zu aufwändig und zu teuer gewesen. Auf einer Kundenveranstaltung wurden die IT-Verantwortlichen auf das Rittal Micro Data Center Level E aufmerksam. „Wir hatten bereits Rittal Komponenten in unserem EDV-Raum im Einsatz. Außerdem kennen wir das Unternehmen natürlich durch dessen Produktionsstandort in Hof. Das Konzept der Rittal Lösung sowie die regionale Nähe zum Hersteller überzeugten uns sofort“, unterstreicht Köth die Entscheidung.

Das Rittal Micro Data Center Level E ist ein Umhausungssystem, das einen vollständigen Sicherheitsbereich um ein Server-Rack einrichtet. Darin findet IT-Hardware auf 42 oder 47 Höheneinheiten sicheren Platz. „Als wir die Lösung das erste

Der „Tresor“ für die IT bietet außerdem systemgeprüfte Sicherheit und eine hohe Schutzwertigkeit. So wird beispielsweise ein Feuerwiderstand über 90 Minuten nach DIN 4102 (F90) eingehalten. Im Brandfall steigt die Innentemperatur des Micro Data Centers innerhalb der ersten 30 Minuten um nur maximal 50 Kelvin und die relative Luftfeuchte bleibt bei kleiner gleich 85 Prozent. Darüber hinaus widersteht das Rechenzentrum Staub, Rauch sowie starkem Strahlwasser und bietet einen bis zu Widerstandsklasse 4 wählbaren Einbruchschutz, der in Anlehnung an DIN V ENV 1627 getestet wurde.

Die Abwärme der Server wird durch das Kühlgerät direkt nach außen abgeführt. Die Ausführung als „Splitgerät“ mit separatem Innen- und Außenkreislauf verhindert, dass Staub und Rauch aus der Umgebung in den Safe gelangen.

Optional hat sich die Verbandsgemeinde für das Monitoring-System CMC III (Computer Multi Control) entschieden. Dieses überwacht die physischen Parameter wie die Temperatur oder Feuchtigkeit im Micro Data Center und gibt entsprechend Alarm, wenn die einstellbaren Schwellwerte über- oder unterschritten werden.

„Wir haben die Rittal Lösung nun seit knapp einem Jahr im Einsatz. Das Rittal Micro Data Center Level E erfüllt unsere Ansprüche an Sicherheit und Verfügbarkeit“, zieht Udo Köth Resümee. ■

Optional hat sich die Verbandsgemeinde für das Rittal Monitoring-System CMC III (Computer Multi Control) entschieden. Dieses überwacht die physischen Parameter wie die Temperatur oder Feuchtigkeit im Micro Data Center und gibt entsprechend Alarm, sollten die Messwerte von der Norm abweichen.

Mal sahen, fragten wir uns, wie wir den tresorähnlichen Schrank durch unsere Tür zum EDV-Raum bekommen sollten“, beschreibt Köth die ersten Gedanken. Der modulare Aufbau der Rittal Lösung ermöglicht eine Installation an schwer zugänglichen Stellen und sorgt zudem für eine hohe Zukunftssicherheit, denn er kann jederzeit abgebaut, an anderer Stelle wieder aufgebaut und bei zunehmendem Platzbedarf erweitert werden.

**Rittal auf der it-sa:
Halle 12, Stand 345**

Schutz vor Malware und Cyberangriffen

Sorgen Sie mit automatisiertem Schwachstellen- und Patchmanagement für eine aktuelle und sichere IT-Umgebung!



Besuchen Sie uns auf der
IT-Security Messe in Nürnberg

it-sa 2014

Jetzt kostenfreies Ticket anfordern!

➔ www.baramundi.de/itsa-info

Threat-Detection

Sicherheitsrisiken durch Echtzeit-Analysen identifizieren

Bei den heutigen Sicherheitsanforderungen muss die IT-Sicherheit intelligenter werden, um potenziellen Angreifern immer einen Schritt voraus sein. Hersteller von Sicherheitslösungen haben dies erkannt und setzen zunehmend auf Verfahren wie Threat-Detection und Threat-Intelligence.

Von Frank Irnich und Sebastian Beckert, SAP Deutschland SE & Co. KG

In vielen IT-Abteilungen herrscht der Glaube vor, durch eine strenge Absicherung von Endgeräten, Servern und weiteren Elementen der IT-Infrastruktur, könne man eine lückenlose IT-Sicherheit erzielen. Leider ist das eine Illusion. Eine lückenlose IT-Sicherheit gibt es schlichtweg nicht, da die heutigen Infrastrukturen zu komplex sind. Zudem wird die Betrachtung der Wirtschaftlichkeit von gängigen IT-Sicherheitsmaßnahmen immer wichtiger, denn ein vermeintlich sicheres Vorgehen, welches versucht, keine Lücken zu lassen, schränkt Benutzer möglicherweise unnötig ein und kann so immense Kosten verursachen.

Eine Lösung ist hier ein Verfahren, das vielfältige Informationen aus diversen Stellen der IT-Landschaft sammelt, um mögliche Bedrohungen oder gar Einbrüche zu erkennen. Diese Threat-Detection- und Threat-Intelligence-Lösungen bewerten in Sekundenbruchteilen, ob eine Attacke oder eine Gefahrenlage vorliegt, und reagieren umgehend darauf. Dabei sind die Quantität der Echtzeit-Analyse sowie die Qualität der in der Infrastruktur verteilten

Sensoren (Log-Daten) entscheidend. Die größten Herausforderungen von IT-Sicherheitsabteilungen liegen darin, die Menge an angefallenen Daten schnell zu verarbeiten, welche ihre Sicherheitssysteme und Komponenten aus der Hard- und Softwarelandschaft produzieren. Neben den Bestandteilen einer Netzwerk-Infrastruktur wie Firewalls, Router, et cetera müssen sowohl Applikationen, Workflows, Datenbanken als auch mobile Endgeräte und deren Zugriffe überwacht werden. Das ist für die IT-Verantwortlichen fast nicht machbar und so kommt es zu einer unzureichenden Performance bei der Analyse von Dateien, was zu hohen Wartezeiten bei der Erkennung von Angriffen führt. Oft mangelt es auch an der Unterstützung bei der Auswertung von großen Datenbeständen (Extraktion und Analyse) durch die jeweiligen Hersteller. Darüber hinaus findet häufig keine beziehungsweise nur eine eingeschränkte Integration von Meta-Informationen statt. Gelingt es jedoch nicht, über eine geeignete Methode oder geeignete Algorithmen, einen Angriff oder Anomalien zeitnah zu erkennen, ist der zu erwartende Schaden möglicherweise bereits eingetreten.

Massendaten in Echtzeit auswerten

Abhilfe schaffen hier sogenannte ereignisgesteuerte Verarbeitungssysteme (engl. Event Streaming Processor). Dabei handelt es sich um Infrastrukturkomponenten oder IT-Systeme, die in der Lage sind, Massendaten aus eingehenden Datenströmen zu verarbeiten. Solche Systeme verarbeiten und analysieren sehr hohe Datenmengen aus diversen Quellen in Bruchteilen von Sekunden. Anders als bei herkömmlichen Datenhaltungssystemen, werden Ergebnisse von Korrelationen kontinuierlich berechnet. Sobald ein neuer Wert oder ein neues Datum aus einer Datenquelle in einen Event-Stream-Processor gelangen, steht somit sofort das Ergebnis zur Verfügung und kann entweder einen Alarm auslösen, für weitere Berechnungen zur Verfügung stehen oder für spätere Analysen gespeichert werden. Die Möglichkeit der kontinuierlichen Analyse resultiert aus der Tatsache, dass solche eventorientierten Verarbeitungssysteme ausschließlich den Hauptspeicher eines Rechnersystems nutzen und eine Speicherung auf Datenträgern aus Geschwindig-



DEM METIER DER INFORMATIONSSICHERHEIT GEHÖR VERSCHAFFEN

AUSBILDUNG UND ZERTIFIZIERUNG

Was die Ausbildung und Zertifizierung von Fachleuten in der Informationssicherheit anbelangt, ist (ISC)² als weltweit führende gemeinnützige Organisation anerkannt. Durch unser Renommee sind unsere Zertifizierungen und Weltklasse-Ausbildungsprogramme als Gold-Standard der Industrie anerkannt.

SCHUTZ FÜR UNSERE ZUKUNFT

Wir unterhalten ein Elitenetzwerk mit mehr als 100.000 Fachleuten in der Informationssicherheit in über 135 Ländern, die sich mit Hilfe der besten und hellsten Köpfe der Branche vernetzen, lernen, lehren und sich entwickeln. Diese Mitglieder engagieren sich z. B. für:

Programme für Staatstätigkeit & Öffentlichkeit

Die Mitglieder des (ISC)² EMEA Advisory Council beeinflussen die Regierungspolitik, agieren als Botschafter für Ausbildungs- und Gemeindegruppen und sorgen dafür, dass es nicht an Nachwuchs auf diesem Gebiet mangelt. Außerdem gibt es weltweit 100 offizielle Chapter, die Wissen und Ressourcen teilen und gemeinsame Projekte mit anderen Informationssicherheitsexperten durchführen.



DER GEMEINSCHAFT ETWAS ZURÜCKGEBEN

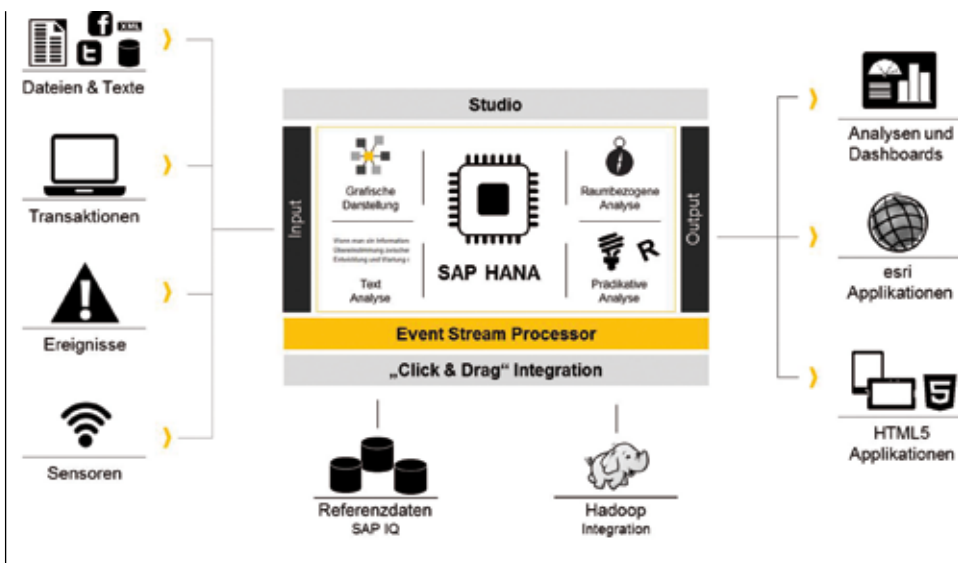
Die (ISC)² Foundation erreicht die Gesellschaft durch ihre Mitglieder, indem sie Schüler, Lehrer und die Allgemeinheit auf dem Gebiet der Cyber-Sicherheit schult, um deren Online-Tätigkeiten abzusichern. Sie führt auch Forschungen hinsichtlich aktueller Entwicklungstendenzen, Mitarbeiterprofilen und kritischer Angelegenheiten durch, welche die Entwicklung der Informationssicherheitsindustrie betreffen, und sie gewährt Stipendien, um Berufsanfänger für die Industrie zu begeistern. Weitere Informationen erhalten Sie unter www.isc2cares.org.

So können Sie **MITMACHEN**: www.isc2.org

Besuchen Sie (ISC)² auf der it-sa 2014. Halle 12 Stand 648



INSPIRATION FÜR EINE SICHERE CYBER-WELT.



Architektur der SAP zur Echtzeit-Daten-Analyse.

keitsgründen von vornherein nicht vorgesehen ist. Somit ist die bisher unmögliche Informationsauswertung von Massendaten in Echtzeit, in Korrelation von Streamdaten sowie historisch, meist redundant gespeicherten Daten zur Erkennung von Cyber-Angriffen erst möglich.

SAP HANA für die Echtzeitanalyse

Das Produkt SAP HANA ermöglicht durch eine neuartige Kombination von Hardware- und Software eine übergreifende Informationsauswertung von Massendaten in Echtzeit, in Korrelation mit Streamdaten (SAP Event Stream Processor) sowie historischen Daten. In SAP HANA stehen umfangreiche Funktionen und Werkzeuge für die gezielte Auswertung von großen Datenmengen in Echtzeit zur Verfügung. Klassische Anwendungen und Datenbanksysteme arbeiten meist in der 3-Tier-Architektur. Ein großer Teil der Laufzeit wird in den verschiedenen Verarbeitungszyklen verbraucht, bei denen die Daten aus der Datenbank gelesen, in die Applikationsschicht zu den Programmen transportiert, dort verarbeitet und dann wieder zurück in die Datenbank oder nach oben zu den Frontends übertragen werden. Jeder Lesezugriff erfordert Zeit und

wird bei aufwändigen Programmschleifen schnell zum Flaschenhals der gesamten Anwendung. Anders bei SAP HANA, bei der eine umfangreiche und komplexe Analyse direkt im Kontext der Daten erfolgen kann, ohne den sonst üblichen Datentransport. Basis hierfür ist eine In-Memory-Appliance: Sie umfasst eine Kombination aus unterschiedlichen SAP-Software-Komponenten und entsprechend konfigurierter Hardware. Im Kern besteht die Appliance aus einer zeilen- und spaltenbasierten In-Memory-Datenbank für OLTP- und OLAP-Anwendungen, flankiert von einer sehr schnellen Planungs- und Berechnungsmaschine (Calc-Engine) direkt auf der Datenbankebene. Die Calc-Engine beinhaltet ganze Bibliotheken von mathematisch-statistischen Funktionen, Prognosetools, Funktionen zur Textanalyse und Recherche, Hadoop-Integration und Sicherheitsfunktionen. Der schnelle Datenzugriff durch die In-Memory-Technologie und die Möglichkeit, die Daten direkt in der Datenschicht durch die integrierte Calculation-Engine verarbeiten zu können, erlaubt ganz andere Verarbeitungszyklen, als es in traditionellen Rechnerarchitekturen möglich war.

Optional können die historischen Daten auch für einen

längeren Zeitraum vorgehalten werden. Das kann insbesondere dann nützlich sein, wenn eine schnelle Risikobewertung einer Bedrohungslage über verschiedene Zeiträume hinweg erfolgen muss. Ferner ist es durch einen historischen Datenbestand möglich, neue Algorithmen für die Angriffsprävention zu finden und zu testen. Diese Art des Prozesses wird auch bei ähnlichen Anwendungsfällen mit Echtzeit-Charakter, wie automatischer Aktienhandel oder Fraud Management verwendet. Technisch wird dies durch eine Kombination von SAP HANA und SAP IQ realisiert. SAP IQ ist als hochperformante, diskbasierte Analysedatenbank optimal geeignet, die In-Memory-Plattform SAP HANA zu erweitern, wenn es um die Verwaltung sehr großer Datenbestände geht, die nur gelegentlich ausgewertet werden und damit nicht unbedingt im relativ teuren Hauptspeicher ständig vorgehalten werden müssen. In diesem Zusammenhang spricht man vom Einsatz von „multitemperatur Data“, da je nach Alter oder Temperatur (neue Daten sind heiß, historische eher kalt) der Daten, verschiedene Speicherbereiche verwendet werden, um die Massendaten kosteneffizient zu speichern. SAP IQ ist damit vor allem dann sinnvoll, wenn sehr große Datenmengen bis in den Petabyte-Bereich für gelegentliche Analysen vorgehalten werden sollen.

Fazit

Die Vorteile von SAP HANA und korrespondierenden Komponenten können im Kontext Cyber-Security verwendet werden, sodass SAP seinen Kunden damit einen sehr guten Schutz der Infrastrukturen bieten kann. Cyberangriffe auf IT-Systeme können so in Echtzeit erkannt und entsprechende Gegenmaßnahmen eingeleitet werden. ■

**SAP auf der it-sa:
Halle 12, Stand 461**

Warum Unternehmen eine Endpoint-DLP-Suite einsetzen sollten

Firewalls, komplexe Passwörter und Verschlüsselungslösungen schützen die Daten innerhalb des Netzwerks. Dennoch sind Unternehmen nicht sicher vor Datenverlust. Benutzer kopieren – bewusst oder unbewusst – vertrauliche Informationen auf USB-Sticks, Smartphones, Kameras oder andere Speichergeräte. Eine Data-Loss-Prevention-(DLP)-Lösung schützt vor solchen Datenlecks.

Von Thomas Tuckow, DeviceLock Europe GmbH

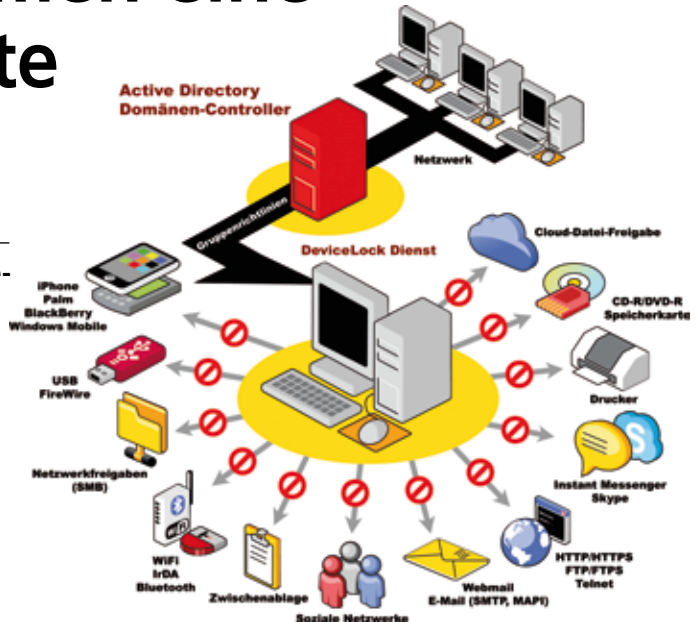
Durch die steigende Mobilität der IT, zahlreiche neue Geräteformen und kabellose Schnittstellen wie Bluetooth oder WLAN steigen die Möglichkeiten des Datenaustauschs und damit die Gefahr eines ungewollten Datenabflusses. Um sich davor zu schützen, können Unternehmen zahlreiche organisatorische und technische Maßnahmen ergreifen, die beispielsweise in den IT-Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beschrieben sind. Dort wird auch empfohlen, ein Tool zur Data-Loss-Prevention einzusetzen, um Datenbewegungen zu kontrollieren und den unerwünschten Datenabfluss zu verhindern. Solch ein Tool sorgt gleichzeitig dafür, dass interne Sicherheitsrichtlinien durchgesetzt werden, und es stellt die Einhaltung gesetzlicher Vorgaben nach dem Bundesdatenschutzgesetz (BDSG), dem Sarbanes-Oxley-Act (EURO/SOX) oder eben den ISO/BSI-Normen sicher. Da sich eine richtig umgesetzte DLP auf alle Arbeitsprozesse im

gesamten Unternehmen auswirkt, sollten Unternehmen diese auch in ihr Information-Security-Management-System (ISMS) einbetten.

Soweit die Theorie. In der Praxis sind heute viele Geschäftsführer – vor allem aus dem Mittelstand – durch die Medienberichterstattung über die NSA-Affäre zwar stärker für Informationssicherheit sensibilisiert als vorher. Erste Studien von Herstellern in diesem Bereich deuten jedoch darauf hin, dass sich dies nicht unbedingt in Handlungen niederschlägt. Jeder weiß heute, es gibt Cyberkriminelle und Wirtschaftsspionage – man fühlt sich jedoch trotz der zahlreichen Medienmeldungen davon nicht betroffen. Manchmal weil man das eigene Unternehmen für zu klein hält, manchmal weil das Mantra der IT-Sicherheitsindustrie von vor zehn Jahren noch nachhallt: Programme auf dem neuesten Stand, Firewall und Virenschutz reichen, um die meisten IT-Gefahren abzuwehren. Das ist sicher richtig und

damit lässt sich auch heute noch vieles verhindern, es hilft jedoch nur bedingt gegen ungewollten Datenabfluss, zum Beispiel durch einfaches Herausragen eines vorher gut gefüllten USB-Sticks. Ein weiteres Problem ist, dass sich eine effektive DLP stark auf die Arbeitsprozesse in den Unternehmen auswirkt. So müssen sich Geschäftsführer und IT-Verantwortliche zum Beispiel darüber Gedanken machen, was welcher Mitarbeiter genau darf. Auch müssen die Daten klassifiziert werden und einige befürchten ganz pauschal, dass eine DLP-Software die Mitarbeiter bei der Arbeit behindert. So bestehen schon vor der Einführung (unberechtigte) Vorbehalte hinsichtlich des Aufwands und der späteren Prozesse.

Daher gibt es heute in den Unternehmen immer noch – und oft trotz besseren Wissens – zahlreiche Lücken, die einen ungewollten Datenabfluss ermöglichen. Manchmal sogar noch, wenn bereits DLP-Tools eingesetzt werden, diese jedoch



Die Endpoint-DLP-Suite von DeviceLock kontrolliert alle Datenströme im Unternehmen und blockiert sie bei Bedarf.

nicht korrekt konfiguriert sind oder einfach nicht die passenden Funktionen für die Organisation bieten. Unternehmen sollten daher darauf achten, eine auf DLP spezialisierte Lösung einzusetzen, die wirklich alle Datenströme kontrollieren und bei Bedarf blockieren kann. Das Blockieren von USB-Schnittstellen durch Zusatzfunktionen anderer Sicherheitsprodukte reicht zum Beispiel nicht. Deshalb umfasst die Endpoint DLP-Suite von DeviceLock die Kontrolle aller lokalen Schnittstellen und der gesamten Web- und Netzwerkkommunikation, ein Event-Logging und die Datenspiegelung für alle Datenkanäle.

Kontext- und Inhaltsanalyse

Ein wichtiger Baustein dafür ist eine Kontextkontrolle aller lokalen Schnittstellen. Diese erfasst auch Gerätetypen, wie Wechseldatenträger, verbundene Smartphones, optische Laufwerke, Drucker und die Zwischenablage. Die Kontrolle dieser Typen kann zudem innerhalb einer RDP/Terminal-Session auf einem Thin-Client durchgesetzt werden. Durch das in die DLP-Suite integrierte sogenannte NetworkLock wird die Kontextkontrolle auf die Web- und Netzwerkkommunikation ausgedehnt. Die verwendeten Protokolle und Anwendungen werden portunabhängig erfasst und wahlweise gesteuert.

Außerdem prüft und bewertet ein Content-Filter ergänzend zum Kontext den Inhalt der Datenbewegungen. Das bedeutet, dass der Datenfluss blockiert oder erlaubt wird, und zwar in Abhängigkeit davon, welcher Mitarbeiter, was, über welches Interface, Gerät oder Protokoll, mit welchem Ziel, mit welchem Inhalt und zu welchem Zeitpunkt bewegt. Alle Wege des potenziellen Datenverlusts, wie Ausdrucke oder Smartphones werden dabei kontrolliert. Neben einer binären Inhaltsanalyse zur Bestimmung des

Dateityps und der Auswertung von Dokumenteneigenschaften, wird sensibler Textinhalt mithilfe von Wortübereinstimmungen, Mustern regulärer Ausdrücke und booleschen Kombinationen („und/oder/nicht“-Kriterien) dieser Varianten erkannt. Die entsprechende Datenbewegung wird in Abhängigkeit der Berechtigungen eines Benutzers zugelassen oder verhindert. Die inhaltliche Analyse und Filterung kontrolliert jeden Datenaustausch mit Wechseldatenträgern, PnP-Geräten und Netzwerkverbindungen. Damit wird sichergestellt, dass nur die zuvor geprüften Daten mit für den Benutzer freigegebenen Informationen ihre Ziele erreichen.

Die Endpoint-DLP-Suite von DeviceLock bietet zudem Werkzeuge für ein umfassendes DLP-Management und wendet zentral definierte DLP-Richtlinien an. Für die Konfiguration der verteilten physischen sowie virtuellen Endpoint-Agenten können Administratoren die Windows-Active-Directory-Gruppenrichtlinienobjekte (GPOs) verwenden oder die in der DLP-Suite integrierten Konsolen. Eine Konsole ist unmittelbar in die Microsoft-Management-Console (MMC) der Active-Directory-(AD)-Gruppenrichtlinien-Verwaltung integriert. Dadurch wird die Steuerung beispielsweise über die Gruppenrichtlinienkonsole (GPMC) ermöglicht. Administratoren binden die Konfiguration der DeviceLock-Zugriffsrechte in ihre allgemeinen Systemmanagement-Aufgaben ein. Zusätzlich ermöglicht eine Web-Konsole die Steuerung der Komponenten über jeden Webbrowser. Dadurch kann der Datentransfer von Benutzern auf Peripheriegeräte, über lokale Schnittstellen und Netzwerk-/Webverbindungen zentral gesteuert, protokolliert, gespiegelt, analysiert und mit einer Alarmierung verbunden werden. Zusätzlich werden Hardware-Keylogger erkannt und ihre Benutzung blockiert, um den Verlust von Passwörtern und anderen proprietären Daten zu verhindern.

Um Datenverluste zu unterbinden und Compliance mit regulatorischen und unternehmerischen Datensicherheitsrichtlinien zu erreichen, können IT-Verantwortliche zusätzlich die Funktion „Discovery“ einsetzen, die sich mit den „ruhenden Daten“ befasst. Sie scannt automatisch Daten auf Netzwerkfreigaben, Speichersystemen und Windows-basierten Computern innerhalb und außerhalb des Unternehmensnetzwerks und sucht Dateien mit sensiblen Inhalten. Wird eine solche gefunden, bietet Discovery Optionen an, um sie durch Korrekturmaßnahmen zu schützen und Incident-Management-Verfahren einzuleiten, indem Echtzeit-Alarmierungen zu einem in der Organisation verwendeten Security-Information- und-Event-Management-(SIEM)-System gesendet werden.

Fazit

Wie das Beispiel der DLP-Suite von DeviceLock zeigt, haben die Programme zu Data-Loss-Prevention in den letzten Jahren einen enormen technischen Sprung gemacht. Heute ist deren Einführung und Nutzung durch die unterstützenden Funktionen relativ einfach umsetzbar. Was bei aller Technik jedoch nicht vernachlässigt werden darf ist, die Mitarbeiter mit in den Prozess einzubinden. Denn wenn diese unvorbereitet vor technischen Einschränkungen stehen, kommt schnell Unmut auf und sie versuchen, die Schranken aktiv zu umgehen. Daher sollte ihnen der Grund der Maßnahmen transparent gemacht werden, indem ihnen zum Beispiel durch einen Hinweis angezeigt wird, warum es nicht erlaubt ist, Daten auf einen mitgebrachten USB-Stick zu kopieren. Auch hier unterstützt die DLP-Software mit entsprechenden Nachrichtenfenstern. ■

**DeviceLock auf der it-sa:
Halle 12, Stand 325**

Unternehmen bedroht durch Wirtschaftsspionage

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. HOB GmbH & Co. KG unterstützt mit seinen eigen-entwickelten Security-Lösungen made in Germany Unternehmen bei der Planung und Implementierung sicherer Zugriffsszenarien für Mitarbeiter auf Unternehmensdaten.

Von Reinula Böcker, HOB GmbH & Co KG

IT-Security Lösungen aus Deutschland wie die von HOB, unterliegen nicht dem Einfluss der Geheimdienste und haben somit keine Backdoors. HOB nutzt darüber hinaus eine eigene SSL-Implementierung. Das Kernprodukt von HOB, die Secure Remote Access Suite HOB RD VPN ist vom BSI zertifiziert nach Common Criteria EAL 4+.

Anlässlich der it-sa 2014 können sich Fachbesucher ein eigenes Bild von den vielen Security-Lösungen von HOB machen. HOB stellt seine ganze Produktreihe für den sicheren, performanten Fernzugriff vor. Viele besondere Konzepte in den HOB Produkten unterstützen die Nutzer dabei, flexibel und dennoch sicher mit Unternehmensdaten zu arbeiten.

Secure Remote Access

HOB RD VPN ist die umfassende Secure Remote Access Lösung mit vielen Vorteilen. So sind client-seitig weder Installationen noch Administratorrechte erforderlich. Die zentrale Administration senkt Administrationsaufwand und damit Kosten und erhöht die Flexibilität. HOB RD VPN sorgt durch seinen benutzerfreundlichen Aufbau für eine hohe Akzeptanz bei den Anwendern.

Security

HOB RD VPN enthält Bestandteile für die sichere Kommunikation und Authentifizierung auf Basis von SSL Version 3 und TLS. Es ermöglicht u.a. die Erstellung und Verwaltung von Zertifikaten, sowie den Aufbau einer eigenen Public Key Infrastructure.

Sichere Verschlüsselung durch starke Algorithmen

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. Diese wird gewährleistet für die CC EAL 4+ zertifizierten Komponenten, bei den anderen Komponenten werden vergleichbare Algorithmen verwendet.

Erweiterte Sicherheit durch moderne Authentifizierungsmethoden

HOB RD VPN unterstützt die Microsoft CryptoAPI und damit den Einsatz von Authentifizierungstechnologien wie z. B. Smartcards. Zudem wird auf Java-Clients der PKCS#11 Standard unterstützt.

nologien wie z. B. Smartcards. Zudem wird auf Java-Clients der PKCS#11 Standard unterstützt.

Unterstützung von Sicherheitsstandards

HOB RD VPN unterstützt Sicherheitsstandards und Algorithmen wie Methoden zum Schlüsselaustausch mit RSA, DH (Diffie-Hellman), DHE (Diffie-Hellman ephemeral) und Verschlüsselungsalgorithmen wie u.a. AES mit 256 Bit und 128 Bit, RC4 mit 128 Bit und 40 Bit, 3DES.

Eigenes Zertifikatsmanagement

HOB RD VPN unterstützt, mithilfe der Softwarekomponente HOBLink Security Manager, die Verwendung von Zertifikaten nach dem X.509 Standard. Dieses Tool erlaubt zudem die Erstellung von eigenen Zertifikaten, die Verwendung von CA-Zertifikaten und das Importieren von Wurzelzertifikaten. Die Softwarekomponente bietet die Möglichkeit Zertifikat-Requests zu erstellen. Die daraus generierten, von einer offiziellen Zertifizierungsstelle signierten Zertifikate, können wieder importiert werden. Dadurch können Zertifikate erzeugt werden, deren private Schlüssel von keinen Dritten einsehbar

sind, da nur der öffentliche Teil des Zertifikates an die Zertifikatsstelle gesendet wird.

Hohe Sicherheitsstufe durch zertifizierten Zufallszahlengenerator

Der zertifizierte Zufallszahlengenerator von HOB RD VPN arbeitet mit einer Zufälligkeit (Entropie) von mindestens 50 Bit. Um sich diesen Wert besser zu veranschaulichen, kann zum Vergleich eine Lotterziehung herangezogen werden. Beim Lotto gibt es für eine „6 aus 49“ Ziehungen knapp 14 Millionen Kombinationsmöglichkeiten, um garantiert 6 Richtige zu treffen. Diese Kombinationsmöglichkeiten haben lediglich ungefähr eine Entropie von 20 Bit, dabei ist die Trefferquote mit 6 Richtigen ganz gering. HOB RD VPN verfügt im Vergleich dazu über mindestens 50 Bit Entropie.

Zentrale Server Komponente als zentrales Sicherheitselement

Der HOB WebSecureProxy (WSP) ermöglicht als zentrale Sicherheitskomponente in HOB RD VPN die SSL-gesicherte Kommunikation der Client-Anfragen zu firmeninternen Servern und Applikationen und unterstützt alle gängigen Verschlüsselungsverfahren inklusive AES mit bis zu 256 Bit Schlüssellänge. Zusätzliche Sicherheit kann durch die Verwendung von Authentifizierungssystemen, wie Zwei-Faktor bzw. RADIUS-Authentifizierung erreicht werden. Die Kerberos-Implementierung ermöglicht Secure Single Sign-on. HOB RD VPN unterstützt auch die Verwendung von Client-Zertifikaten, die beim SSL-Verbindungsaufbau genutzt werden. Der Administrator kann unterschiedliche Domänen für Kerberos/LDAP definieren, so dass auch komplexe Netzwerke unterstützt werden. Ein differenziertes Rollen- und Rechtssystem erhöht die Sicherheit durch ausgeklügelte Zugriffslogik. Z. B.: Abhängig vom Status der Antivirensoftware erhält der

Anwender unterschiedliche Rollen und Rechte. Zur Erhöhung der Ausfallsicherheit ist eine Zusammenfassung mehrerer HOB WebSecureProxies zu einem Cluster möglich. Jede aktive Session ist jedem Proxy bekannt, so dass im Fehlerfall eines Proxys der weitere Betrieb störungsfrei gewährleistet ist. Für die Remote Anwender ist das Cluster als eine Einheit sichtbar. Zur Steigerung der Verbindungsqualität wurden Optimierungen für den gesamten Datenstrom implementiert. Die End-to-End Flow Control bringt eine höhere Stabilität und Performanz der Netzverbindungen. Um Anwender im internen Netzwerk besser identifizieren zu können, kann für jeden eine persönliche IP-Adresse definiert werden, die für die internen Netzverbindungen verwendet wird. Der HOB WebSecureProxy kann auch zur Abschottung eines E-Mail-Servers vor dem direkten Zugriff aus dem Internet dienen. Die Kommunikation zwischen E-Mail-Client und HOB WSP erfolgt dabei über POP3S, IMAPS und/oder SMTPS. Mit HOB Anti Split Tunneling kann verhindert werden, dass ein Benutzer auf andere Netzwerke zugreift, während er mit HOB RD VPN arbeitet. Dadurch wird die Sicherheit des Systems deutlich erhöht. Über die ICAP-Schnittstelle im HOB WebSecureProxy ist es möglich, übertragene Dateien innerhalb von Remote Desktop Sessions zu scannen und die übertragenen Dateien auf potentielle Gefahren geprüft. Somit werden übertragenen Dateien schon an zentraler Stelle auf potentielle Gefahren geprüft.

HOBLink VPN Gateway

Das neue HOBLink VPN Gateway, die grundlegend überarbeitete Version 2, bietet als reine Software-Lösung neben Sicherheit auch gute Skalierbarkeit. Das Gateway unterstützt eine beliebige Anzahl von Site-to-Site und Client-to-Site Verbindungen und 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 im Unternehmen 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 mitgelieferte HOB Zertifikatmanager ermöglicht die Bearbeitung des HOB Keystore. Damit kann eine Zertifikatsstruktur aufgebaut werden aus eigenen Zertifikaten oder mit Zertifikaten von externen Certificate Authorities. HOBLink VPN Gateway ermöglicht die Benutzerauthentifizierung mit RADIUS 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 Gateway ist kompatibel mit VPN-Clients unterschiedlicher Hersteller auf verschiedenen Plattformen und dem HOBLink VPN Anywhere Client.

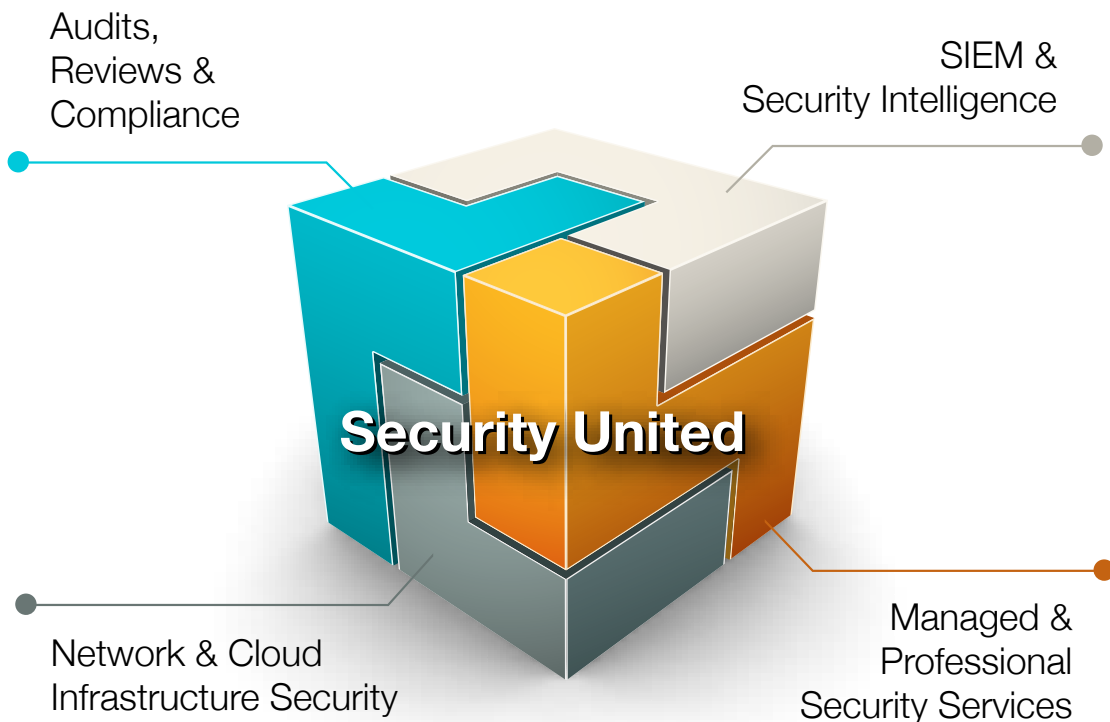


**HOB auf der it-sa:
Halle 12, Stand 508**



Security United – MODCOMP

Your Trusted IT Security Partner



Security United - Sicherheit aus einer Hand

Die Basis für eine effektive IT-Sicherheit ist die ganzheitliche Betrachtung. MODCOMP Deutschland unterstützt seit über 20 Jahren bedeutende große Unternehmen aus der Telekommunikation und Energiewirtschaft bei der Vermeidung und Verhütung von Geschäftsrisiken. Dabei decken wir die gesamte Bandbreite der Security Produkte und Dienstleistungen ab von der Beratung über Audits und Penetrationstests bis hin zum Managed Service eines gesamten SOC (Security Operation Center). MODCOMP steht dabei immer für innovative, kundennahe und ganzheitliche Security Lösungen. Nutzen Sie unsere Erfahrung aus zahlreichen Großprojekten für Ihre...Security United.

Besuchen Sie uns auf der it-sa 2014 in Halle 12, Stand 420.

Modular Computer Systems GmbH

Oskar-Jäger-Str. 50
D-50825 Köln, Germany
Tel: +49 (0) 221 954466-0
Fax: +49 (0) 221 954466-99
info@modcomp.de
www.modcomp.de

