

TEC CHANNEL COMPACT

IT IM MITTELSTAND

GRUNDLAGEN ■ RATGEBER ■ PRAXIS

IT-Sicherheit

Daten schützen

- Hacker-Angriffe verhindern
- Identitätsdiebstahl erschweren
- E-Mail-Verkehr absichern

Security planen

- Sicherheitskonzepte für Ihr Unternehmen
- Empfehlenswerte Security-Lösungen
- Mehr Sicherheit durch Cloud-Services

Mobile Sicherheit

- Smartphones und Tablets richtig absichern
- iOS- und Android-Security auf dem Prüfstand
- Gratis-Apps: Vorsicht vor Datensammlern

TecChannel Silber-Paket

Print + iPad-Ausgabe + Premium-Zugang

nur
14,- €
monatlich
+ Prämie



- ▶ 40% Ersparnis gegenüber den Einzelpaketen
- ▶ TecChannel Compact kostenfrei auf Ihrem iPad
- ▶ 8 Ausgaben versandkostenfrei
- ▶ Alle Artikel im PDF-Format
- ▶ Exklusive Beiträge
- ▶ Eine hochwertige Prämie Ihrer Wahl



0711-72 52 276



www.tecchannel.de/silber



Editorial

IT-Sicherheit im Unternehmen: ein Fass ohne Boden



Die Sicherheitsanforderungen an die IT in einem Unternehmen wachsen von Jahr zu Jahr. Einerseits reicht es längst nicht mehr aus, Standardmaßnahmen wie Virens Scanner und Firewalls zu installieren, um damit das Gros der Angriffe abzuwehren. Denn es gilt auch, die Hochverfügbarkeit der IT zu gewährleisten, Nutzeridentitäten zu schützen oder Datenverlust im Unternehmen zu vermeiden sowie lokale oder Cloud-basierte Informationen zu schützen. Andererseits ist es auch nicht sinnvoll, in Panik zu verfallen und auf gut Glück wahllos irgendwelche Sicherheitsmaßnahmen einzurichten. Das richtige Maß an IT-Sicherheit ist gefragt.

Im ersten Schritt sollte eine detaillierte Sicherheitsanalyse der vorhandenen IT-Infrastruktur inklusive der Arbeitsprozesse erfolgen. Dabei ist es ganz wichtig, Aspekte wie Social Media, Cloud-Services und Mobile Computing in das Sicherheitskonzept miteinzubeziehen. Der zweite Schritt wäre, entsprechende, auf die Unternehmens-IT zugeschnittene Security-Lösungen zu finden. Allerdings sollten diese Sicherheitslösungen auf das vorher definierte Sicherheits-Level und das vorhandene Budget abgestimmt sein. Erst dann erreicht man einen maximalen Schutz seiner Unternehmens-IT zu einem angemessenen Preis.

In diesem Compact gehen wir ausführlich auf aktuelle und zentrale IT-Sicherheitsaspekte wie sichere E-Mails, Verschlüsselung, Identitätsdiebstahl oder Ausfallsicherheit ein. Auch die Themen Mobile- und Cloud-Security behandeln wir detailliert. Neben fundierten Grundlagenbeiträgen über mögliche Sicherheitsrisiken speziell in kleinen und mittelständischen Unternehmen helfen unsere Ratgeber, Praxisbeiträge und Tools, aktuelle Bedrohungen zu erkennen und mögliche Angriffe zu verhindern.

Viele nützliche Erkenntnisse bei dieser Lektüre wünscht Ihnen

Bernhard Haluschak
Redakteur TecChannel

Inhalt

	Editorial	3
1	Ratgeber und Praxis	9
1.1	Das richtige Maß an IT-Sicherheit	9
1.1.1	Nicht zu viel und nicht zu wenig IT-Sicherheit	9
1.1.2	Kontextsensitive Sicherheit: Auf das Umfeld kommt es an	10
1.1.3	Berücksichtigung der Datenkategorie	10
1.1.4	Unterscheidung Arbeitszeit und Privatnutzung	11
1.1.5	Verschiedene Risiken der Anwendungen	12
1.1.6	Eine Frage des Standortes	13
1.1.7	Fazit: nicht übertreiben und nichts riskieren	14
1.1.8	Vergleichstabelle	14
1.2	IT-Risiko-Management ist eine juristische Pflicht	16
1.2.1	Spektakuläre Pleiten	16
1.2.2	Was ist gesetzlich gefordert?	17
1.2.3	Risiko für den Vorstand	17
1.2.4	Risikoanalyse und Maßnahmenkatalog	18
1.2.5	Die Cloud als Herausforderung	19
1.2.6	Bring Your Own Device	20
1.3	Wie Unternehmen ihr DNS schützen	21
1.3.1	Massive Angriffe	21
1.3.2	DDoS-Attacken erkennen und vorsorgen	22
1.3.3	Komplize wider Willen	24
1.4	So merken Sie, dass Ihr Notebook oder PC gehackt wurde	25
1.4.1	Gefälschte Antivirenmeldungen	25
1.4.2	Unerwünschte Browser-Toolbars	26
1.4.3	Umgeleitete Websuchen	26
1.4.4	Häufige Popup-Fenster	27
1.4.5	Freunde empfangen Fake-Mails mit Ihrem Namen	27
1.4.6	Online-Passwörter ändern sich plötzlich	28
1.4.7	Software installiert sich selbstständig	28
1.4.8	Die Maus arbeitet, ohne dass Sie sie benutzen	29
1.4.9	Security-Software, Taskmanager, Registry-Editor sind deaktiviert	30
1.4.10	Auf dem Bankkonto fehlt Geld	30
1.4.11	Mahnbescheide wegen nicht bezahlter Ware	30
1.4.12	Allgemeine Hinweise	31
1.5	Identitätsdiebstahl schwer gemacht	32
1.5.1	Massenidentitätsdiebstahl	32
1.5.2	Gezielter Identitätsdiebstahl	32
1.5.3	Der Schaden	32
1.5.4	Vorgehen bei einem Datenleck	34
1.5.5	Täterprofile	35
1.5.6	Fazit	36

1.6	Vier Patch-Management-Lösungen im Test	37
1.6.1	Das Testfeld	37
1.6.2	Die bewerteten Funktionen	39
1.6.3	Die Hürden im Test	39
1.6.4	Wer erkennt die Software?	39
1.6.5	Falsche Sprache wird passend gemacht	40
1.6.6	Wie schnell wird gepatcht?	40
1.6.7	Was passiert, wenn das Update schief läuft?	41
1.6.8	Stolpersteine bei Updates	41
1.6.9	Sicherheitslücken durch Add-ons	42
1.6.10	Auto-Updates können querschießen	42
1.6.11	Nutzerlizenzen sollten einsehbar sein	42
1.6.12	Integration des Update-Support von Microsoft	42
1.6.13	Gute Steuerung der Neustarts	42
1.6.14	Fazit: Patch-Management sichert Systeme und entlastet Admins	43
1.7	Cloud- und Social-Media-Daten richtig verschlüsseln	44
1.7.1	Vielfältige Verschlüsselungsmöglichkeiten	44
1.7.2	Verschlüsselung für Speichermedien	44
1.7.3	Verschlüsselung für mobile Endgeräte	46
1.7.4	Verschlüsselung für E-Mail	46
1.7.5	Verschlüsselung für Netzwerke	47
1.7.6	Verschlüsselung für Clouds	47
1.7.7	Verschlüsselung für Social Media	48
1.7.8	Wichtig für alle Verschlüsselungslösungen	48
1.7.9	Beispiele für Verschlüsselungs-Tools	49
1.8	Tools zur Anonymisierung von Daten	50
1.8.1	Anonymisierung erleichtert Datensicherheit	51
1.8.2	Nicht immer, aber öfter anonymisieren	51
1.8.3	Anonymes Big Data ist möglich	52
1.8.4	Datenmaskierung	53
1.8.5	Webanalysen: IP-Adresse verkürzen	54
1.8.6	Datenbanken: anonyme Datenfelder	54
1.8.7	Marktforschung: anonyme Umfragen	55
1.8.8	Business Analytics: der anonyme Kunde	55
1.9	Das bieten Security-Assessment-Tools	56
1.9.1	Mit dem Browser fängt es an	56
1.9.2	Websites im Blick	57
1.9.3	Systemanalyse auf Knopfdruck	58
1.9.4	Der Fehler steckt im Quellcode	58
1.9.5	Den Nutzer nicht vergessen	58
1.9.6	Befragung statt Angriff	59
1.9.7	Fazit	60
1.10	Was mit den Online-Daten Verstorbener geschieht	61
1.10.1	Neue Dienstleistungen	61
1.10.2	Rechtliche Unsicherheit	62
1.10.3	Streitthema E-Mail	63
1.10.4	Sie beißen nicht	64
1.10.5	Was die Anbieter sagen	65

2	Sicherheit im Unternehmen	68
2.1	Intranator Business Server – Groupware- und Security-Lösung für kleine Unternehmen	68
2.1.1	Funktionen von Intranator Business Server	68
2.1.2	Der Groupware Server im Detail	70
2.1.3	Outlook- und Smartphone-Unterstützung	70
2.1.4	Fazit, Pro und Contra	71
2.1.5	Pro und Contra Intranator Business Server	71
2.2	SSL – beliebt, aber gefährlich	72
2.2.1	Funktionsweise des Protokolls	72
2.2.2	Heartbleed zeigt: SSL ist verletzlich	73
2.2.3	Abhilfe schaffen	74
2.3	Sichere E-Mail – bessere und vertrauenswürdige Kommunikation	76
2.3.1	Wie sicher ist der Inhalt einer E-Mail?	76
2.3.2	Reicht eine AV-Lösung auf dem System zum Schutz der E-Mail?	76
2.3.3	Wie kann ich E-Mail-Nachrichten sicherer versenden?	77
2.3.4	Security auch für Thunderbird	78
2.3.5	Warum sollte man keine HTML-Nachrichten verwenden?	79
2.3.6	Welche Sicherheitseinstellungen sind bei Outlook sinnvoll?	79
2.3.7	Ist vom Einsatz einer Web-Mail-Lösung grundsätzlich abzuraten?	80
2.3.8	Last but not least: sichern, sichern, sichern...	81
2.4	Single-Sign-On statt Login-Marathon	84
2.4.1	Identity Provider – das zentrale Steuerelement	84
2.4.2	One-Klick-Access mit SAML	85
2.5	Cyber-Kriminalität: Wann zahlt die Versicherung?	87
2.5.1	Das Krisenmanagement entscheidet	88
2.5.2	Wo die Versicherung ins Spiel kommt	88
2.5.3	Beispiel: Cyber Risk Management by Hiscox	88
2.5.4	Im Ernstfall	90
2.5.5	Und danach?	90
2.6	IT-Ausfällen vorbeugen	91
2.6.1	Verantwortlichkeiten nicht klar geregelt	91
2.6.2	Workflow-gestützte Dokumentation	92
2.6.3	Entwicklung des Notfallplans	92
2.6.4	Der Faktor Mensch	93
2.6.5	Krisen-, Prozess- und IT-Service-Management integriert abwickeln	94
2.7	Neue Trends im Identitäts- und Access-Management	95
2.7.1	Aktuelle Entwicklungen	95
2.7.2	Die Authentifizierung wird vielfältiger	96
2.7.3	Mobile Endgeräte	96
2.7.4	Biometrie	97
2.7.5	Neue Token und Smartcards	98
2.7.6	Single-Sign-On und Federation	99
2.7.7	Nutzerzentrierung	99
2.7.8	Fazit	100

3	Mobile Security	101
3.1	Mobile Daten effizient schützen	101
3.1.1	Fehlerhafte Mobile-Security-Strategien	102
3.1.2	Die Nein-Sager	102
3.1.3	Einfach mal ein MDM-System kaufen	102
3.1.4	Alle dicht	102
3.1.5	Private Endgeräte	103
3.1.6	Problemfall IT-Abteilung	103
3.1.7	Restriktives Vorgehen	103
3.1.8	Technische Lösungen: von Containern bis hin zu Spaces	104
3.1.9	App Wrapping: Anwendungen werden eingepackt	105
3.1.10	Virtualisierung: Desktops und Anwendungen im Rechenzentrum	106
3.1.11	Virtualisierung als App oder im Betriebssystem	107
3.1.12	Spezielle Ansätze: Samsung KNOX und Mobile Spaces	107
3.1.13	Ein Trend: Mobile Application Management	108
3.1.14	Eine weitere Entwicklung: über MIM zu Mobile Risk Management	108
3.2	Schutz vor Spionage und Datenmissbrauch	110
3.2.1	Gefahren durch Apps auf Tablets und Smartphones im Unternehmen	110
3.2.2	Beispiele für Bedrohungen	111
3.2.3	MAM: für eine sichere mobile Infrastruktur	112
3.2.4	Weitere Disziplinen des Enterprise Mobility Managements	113
3.3	So sichern Sie mobile Systeme richtig ab	114
3.4	iOS und Android – was taugt die eingebaute Sicherheit?	116
3.4.1	Wirtschaftliche Schäden und Datenschutzrisiko	117
3.4.2	Apples Sicherheitskonzept beginnt mit dem Booten	118
3.4.3	iOS ständig am Senden in Richtung Apple	119
3.4.4	Android orientiert sich am klassischen PC	119
3.4.5	Dem Entwickler auf die Finger schauen	120
3.4.6	Fazit: keine hundertprozentige Sicherheit	121
3.5	Samsung KNOX 2.0 – Sicherheit für Android	122
3.5.1	KNOX nur auf bestimmten Galaxy-Geräten	122
3.5.2	Ablauf bei der Anbindung von KNOX	123
3.5.3	Privates und Geschäftliches auf einem Smartphone	124
3.5.4	KNOX und das Rooten	124
3.5.5	Private und berufliche Daten nutzen	125
3.5.6	MDM und mehr mit KNOX	126
3.5.7	KNOX 2.0 mit zusätzlichen Features	127
3.5.8	Fazit	127
3.6	Vorsicht: die raffinierten Geschäftsmodelle der Gratis-Apps	128
3.6.1	Auf welche persönlichen Daten greifen Apps zu?	130
3.6.2	Praxis-Tipp: Welche App darf was auf meinem Smartphone?	132
3.6.3	Grundlegende Tipps zur Verwendung von Gratis-Apps	132
3.6.4	Eine besonders dreiste Geschäftsidee: Bazuc	133
3.6.5	Zum Abschluss: kostenpflichtige App, die nichts tut	134

3.7	Android-Rooting: Vorzüge und Gefahren	135
3.7.1	Gefahren und Probleme beim Rooting	136
3.7.2	Kein Support bei Rooting-Problemen	136
3.7.3	Vorteile des Rootings	137
3.7.4	Custom-ROMs versus Rooting	138
3.7.5	Wann lohnt sich das Rooten am meisten?	139
3.7.6	Stable, Nightly Build, AOSP und Stock	140
3.7.7	Gerootete Geräte sichern	140
3.7.8	Fazit	141
4	Security aus der Cloud	142
4.1	Ratgeber: mehr Sicherheit für Unternehmensdaten in der Cloud	142
4.1.1	Die Cloud gibt es nicht als Standardlösung	142
4.1.2	Security-Services: auf den individuellen Bedarf zugeschnitten	143
4.1.3	„Schatten-IT“ schadet der Sicherheit – und wird dank der Cloud überflüssig	144
4.1.4	Unternehmen müssen Cloud-ready sein, bevor sie die Services nutzen	144
4.1.5	Zertifizierungen als Hinweis auf die Verlässlichkeit des Providers	145
4.1.6	Herstellerzertifizierungen bedeuten einfache Implementierung	145
4.1.7	Die rechtlichen Grundlagen im Hinterkopf	146
4.1.8	Kunden können entscheiden, wo ihre Daten liegen	146
4.2	Kalkulierbares Risiko – Schatten-IT in Unternehmen	147
4.2.1	Verschlüsselung ja – aber wo?	147
4.2.2	Verschlüsselung ja – aber womit?	148
4.2.3	Die Schlüssel unter der Fußmatte sind auch virtuell keine gute Idee	149
4.2.4	AGB – ich verstehe nur Bahnhof ...	150
4.3	Ratgeber: Threat-Monitoring-Services aus der Cloud	151
4.3.1	Frühwarnsysteme fehlen gerade im Mittelstand	151
4.3.2	Threat Monitoring gibt es aus der Cloud	152
4.3.3	Zahl und Art der Sensoren hinterfragen	152
4.3.4	Schnittstellen prüfen	154
4.3.5	Reporting, Alarming und Dashboards müssen passen	156
4.3.6	Datenschutz nicht vergessen	156
4.4	Sieben Tipps für Ihren sicheren Weg in die Cloud	157
4.4.1	Vertrauen in den Servicepartner	158
4.4.2	Gewissheit, wo die Daten sind	158
4.4.3	Ist die Servicequalität geprüft?	158
4.4.4	Zertifizierte Qualitätsstandards	158
4.4.5	Exakt definierte Zugriffsrechte und -sicherheit	159
4.4.6	Sichere Zusammenarbeit	159
4.4.7	Gewissheit, was mit den Daten passiert	160
4.4.8	Fazit	160
5	Anhang: Die beliebtesten Sicherheits-Artikel (QR-Codes)	161
	Impressum	162

1 Ratgeber und Praxis

Der Schutz der eigenen IT-Infrastruktur, der gespeicherten Daten und der eingesetzten Anwendungen ist eine der vordringlichsten Aufgaben von Administratoren und Systemverantwortlichen. Neben optimalen Abwehrstrategien kommt es vor allem auf das richtige Handwerkszeug an. Dieses Praxiskapitel enthält umfangreiche Anleitungen, Tipps und Software-Empfehlungen zum Absichern von Netzwerken, Servern, Clients und Cloud-Diensten.

1.1 Das richtige Maß an IT-Sicherheit

Entwicklung und Umsetzung von IT-Sicherheitsrichtlinien, die zu den aktuellen IT-Risiken wirklich passen, bereiten vielen Unternehmen Probleme. Wie die PwC-Studie „Defending yesterday – Key findings from The Global State of Information Security Survey 2014“ zeigt, befassen sich die Security-Policies oftmals noch mit den Sicherheitsrisiken vergangener Tage und gehen nicht auf die aktuellen Herausforderungen beispielsweise durch mobile Endgeräte ein. Zu einem ähnlichen Ergebnis kommen die Studie „Global Corporate IT Security Risks: 2013“ von Kaspersky Lab oder die Untersuchung „Acronis 2013 Data Protection Trends Research“.

1.1.1 Nicht zu viel und nicht zu wenig IT-Sicherheit

Ohne eine Ausrichtung der IT-Sicherheitsrichtlinien auf die jeweils aktuelle Bedrohungssituation besteht jedoch die Gefahr, dass die ergriffenen Sicherheitsmaßnahmen entweder lückenhaft oder aber überzogen sind.

Beides führt zu Schwachstellen in der Risikoabwehr. So belasten übertriebene Sicherheitsmaßnahmen das IT-Budget und senken die Akzeptanz bei den Nutzern, wenn beispielweise grundsätzlich eine Mehr-Faktor-Authentifizierung für die Netzwerkanmeldung vorgesehen wird. Umgekehrt können zu schwache Sicherheitsvorgaben dazu führen, dass Nutzer mit unsicheren, mobilen Endgeräten auf das Firmennetzwerk zugreifen.

Es kommt auf das richtige Maß an, wie unter anderem die gesetzlichen Datenschutzvorgaben betonen: Es sind nur die Maßnahmen gefordert, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht – nicht mehr und nicht weniger. Kontextsensitive Security-Policies und Sicherheitslösungen sorgen für diese Verhältnismäßigkeit, indem sie bei der dynamischen Risikobewertung helfen. Die jeweils bereitgestellten Sicherheitsfunktionen hängen von den aktuellen Risiken ab und nicht von einer starren Voreinstellung. Im Folgenden sollen das Konzept der kontextsensitiven Security-Policies sowie entsprechende Sicherheitslösungen näher betrachtet werden.

1.1.2 Kontextsensitive Sicherheit: Auf das Umfeld kommt es an

Betrachtet man die Risiken, die zum Beispiel mit dem Netzwerkzugriff über mobile Endgeräte verbunden sind, ist es insbesondere die Einsatzsituation und das jeweilige Umfeld, die für die Bedrohung sorgen:

- Smartphones und Tablets werden insbesondere für das Internet genutzt, aber nicht entsprechend geschützt. Dadurch könnten sie mit Malware infiziert werden und Schadprogramme ins Netzwerk einschleusen (Risiko durch unzureichende Sicherheitsausstattung).
- Die mobilen Betriebssysteme und Anwendungen (Apps) werden nicht regelmäßig aktualisiert (Risiko durch veraltete Versionen).
- Die Mobilgeräte werden unterwegs und an Orten ohne jede Zutrittskontrolle verwendet und können deshalb leichter verloren gehen oder gestohlen werden. Unbefugte könnten sie als Hintertür ins Netzwerk missbrauchen (Risiko durch Mobilität und mangelnde Zugangskontrolle).
- Auf den Tablets und Smartphones werden auch geschäftsrelevante Daten genutzt, auf die aus der Ferne zugegriffen wird. So können auch vertrauliche Daten in die Hände Unbefugter gelangen, wenn die mobilen Geräte unzureichend geschützt werden (Risiko durch Art der Datenzugriffe).
- Die mobilen Endgeräte werden häufig sowohl privat als auch betrieblich genutzt und setzen so die betrieblichen Daten, Anwendungen und Netzwerke Gefahren aus, die innerhalb der Unternehmensumgebung nicht oder nicht in dem Ausmaß bestehen (Risiko durch Nutzer und Einsatzzweck).

Wie riskant der Netzwerkzugriff durch mobile Endgeräte oder andere IT-Systeme ist, hängt jeweils von bestimmten, sich ändernden Parametern ab: von dem jeweiligen Nutzer, dem genutzten Gerät, den betroffenen Datenkategorien, der gewählten Anwendung, der aktuellen Sicherheitsausstattung des Gerätes, dem Standort von Nutzer und Gerät, dem privaten und betrieblichen Einsatzzweck und damit verbunden auch dem Zeitpunkt des Netzwerkzugriffs.

Kontextsensitive Sicherheitsrichtlinien und -lösungen bestimmen dynamisch die entsprechenden Risikoparameter, werten diese aus und fordern oder aktivieren automatisch passende Sicherheitsfunktionen. Auf dem Markt sind verschiedene kontextsensitive Lösungen verfügbar, die zeigen, wie mit unterschiedlichen Risikoparametern umgegangen werden kann.

1.1.3 Berücksichtigung der Datenkategorie

Wenn ein Nutzer zum Beispiel mit seinem Tablet von unterwegs auf Daten im Firmennetzwerk zugreifen möchte, sollte in zwei Bereiche unterschieden werden. Zum einen ist es möglich, dass der Datenzugriff allgemein verfügbaren Daten wie

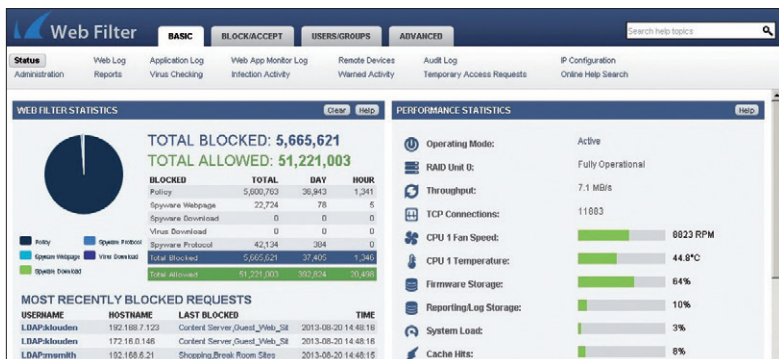
der aktuellen Produktliste gilt, die zum Beispiel bereits auf der Webseite des Unternehmens veröffentlicht wurde. Zum anderen kann es sein, dass es sich um vertrauliche Daten handelt, etwa um ein neues Produktkonzept.

Kontextsensitive Lösungen analysieren die Datenkategorie, auf die zugegriffen werden soll, und gewähren oder verweigern den Zugriff auf Basis der Security-Policies. Die dynamische Zugriffssteuerung von Windows Server 2012 (<http://tech.net.microsoft.com/de-de/library/hh831717.aspx>) oder HP ControlPoint (www.autonomy.com/products/control-point) zum Beispiel nimmt eine automatische Dateiklassifizierung vor und unterstützt die manuelle Einstufung des Schutzbedarfs verschiedener Datenarten.

Abhängig vom Schutzbedarf werden so bei Windows Server die vertraulichen Dateien mittels Rights Management Services (RMS) verschlüsselt und können von Nutzern, die kein Recht zur Entschlüsselung erhalten, nicht eingesehen werden. Berechtigte Nutzer hingegen erhalten Zugriff auf die automatisch entschlüsselten Dateien. Eine generelle Verschlüsselung aller Daten kann damit ebenso vermieden werden wie der unerlaubte Zugriff auf zu schützende Dateien. Auch der wenig praxisnahe Ansatz, generell den Datenzugriff von außen auf die Dateien zu erlauben oder zu blockieren, wird vermieden.

1.1.4 Unterscheidung Arbeitszeit und Privatnutzung

Der Zugriff auf das Netzwerk kann auch von der jeweiligen Zugriffszeit abhängig gemacht werden. So kann es einem Nutzer während der Arbeitszeit erlaubt sein, auf einen bestimmten Server mit seinem Smartphone zuzugreifen. Nach Feierabend aber und am Wochenende soll es nicht erlaubt sein. Eine solche Regelung kann zum Beispiel bei BYOD-Programmen (Bring Your Own Device) oder der erlaubten Privatnutzung betrieblicher Geräte wichtig sein.

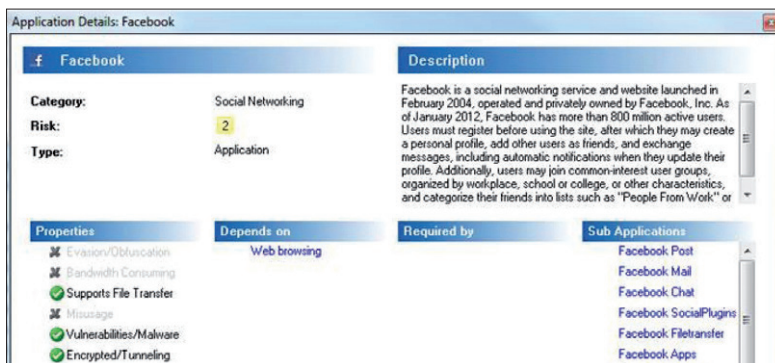


Multitalent: Webfilterdienste wie der Barracuda Web Security Service bieten die Möglichkeit, bestimmte Internetadressen 24-Stunden lang zu erlauben oder zu blockieren. (Quelle: Barracuda Networks)

Möglich wird solch eine zeitabhängige Zugriffskontrolle unter anderem dank BeyondTrust PowerBroker Servers Enterprise (www.beyondtrust.com/content/pdfs/DS_PBSE.pdf). Mit dieser Lösung kann der Zugriff nach Datum, Uhrzeit oder Zeitspanne definiert und entsprechend erlaubt oder verboten werden. Webfilterlösungen wie Barracuda Web Security Service (www.barracuda.com/products/websecurityflex/features) erlauben unter anderem die zeitabhängige Sperrung und Freigabe von Internetadressen und Online-Diensten für die Internetnutzer im Unternehmen. Ein generelles Verbot würde in der Regel keinen Sinn ergeben, eine zeitlich unbefristete Zugriffserlaubnis aber ein mögliches Risiko darstellen. Mit einer kontextsensitiven Lösung lässt sich der Schutzbedarf genauer fassen, ohne dass die Produktivität leidet. Gefahren durch Serverzugriffe außerhalb der Arbeitszeit werden trotzdem verhindert beziehungsweise Zugriffe auf bestimmte private Online-Dienste während der Arbeitszeit blockiert.

1.1.5 Verschiedene Risiken der Anwendungen

Eine dynamische Risikobewertung und Zugriffskontrolle kann auch die unterschiedlichen Gefahren berücksichtigen, die von verschiedenen Anwendungen ausgehen: Eine generelle Blockade der Internetzugriffe eines Nutzers ist in den meisten Unternehmen kaum sinnvoll. Trotz der bekannten Online-Risiken werden die meisten Nutzer zu bestimmten Zeiten einen Zugang zum Internet benötigen.



Spurensucher: Sogenannte Next-Generation-Firewalls wie die Barracuda NG Firewalls verfügen über Funktionen zur Applikationserkennung und liefern den Administratoren zu zahlreichen Anwendungen Hinweise zur Risikoeinstufung. (Quelle: Barracuda Networks)

Deshalb sollte ein Unternehmen den Internetzugriff nicht nur auf der Ebene von Nutzern, Rollen oder Abteilungen regeln. Selbst für Nutzer und Abteilungen, die ständig Internetzugang benötigen, müssen nicht alle Internetangebote am Arbeitsplatz oder über betriebliche Geräte erreichbar sein.

So kann es aus Sicherheitsgründen sinnvoll sein, bestimmte soziale Netzwerke, Cloud-Speicherdienste sowie andere als riskant eingestufte Online-Dienste und -Anwendungen zu verbieten und technisch zu blockieren. Möglich ist dies zum Beispiel mit den Cisco-ASA-5500-X-Series-Next-Generation-Firewalls. Diese Art von Firewall unterstützt die Unterscheidung von mehr als 1000 gebräuchlichen Anwendungen und erlaubt jeweils die Definition von Regeln, welcher User mit welchem Gerät an welchem Ort eine bestimmte Anwendung nutzen darf oder nicht. Dazu werden neben den Anwendungen auch die aufgerufenen Internetadressen und die dazu genutzten Geräte analysiert, um dem Risiko entsprechend mit einer Blockade und einer Zugriffserlaubnis zu reagieren.

Eine Lösung wie Afore CypherX (www.aforesolutions.com/products/cloud-security-management/cypherx-overview) unterstützt applikations- und nutzerabhängige Policies zum Beispiel bei der Regelung des Zugriffs auf Cloud-Dienste. So wird beim Zugriff auf verschlüsselte Cloud-Daten insbesondere geprüft, ob der jeweilige Nutzer die Berechtigung dazu hat (Authorized User), eine zugelassene Maschine dafür nutzt (Validated Machine) und eine der dafür zertifizierten Apps (Certified Apps) verwendet. Erst dann werden die Cloud-Daten für den entsprechenden Zugriff entschlüsselt.

1.1.6 Eine Frage des Standortes

Ob ein Netzwerkzugriff ein besonderes Risiko darstellt oder nicht, kann auch vom aktuellen Standort des Gerätes und damit des Nutzers abhängen. Geht das mobile Gerät verloren oder wird es gestohlen, ohne dass der Verlust bereits bekannt geworden ist, kann es für die Netzwerksicherheit entscheidend sein, zwischen erlaubten und unerlaubten Standorten zu unterscheiden.

Findet in der Regel zum Beispiel von einem bestimmten Land aus kein Mitarbeiterzugriff statt, könnte ein entsprechender Zugriffsversuch bedeuten, dass ein Unbefugter das Gerät gestohlen hat und es nun für einen Angriff nutzen will. Oder aber die Privatnutzung eines Gerätes ist verboten, sodass alle Zugriffsversuche außerhalb der verschiedenen Unternehmensstandorte abgelehnt werden sollen.



Ortskundig: Policy-Manager wie F5 Networks Big-IP APM können den Standort eines Gerätes ermitteln, von dem aus ein Netzwerkzugriff erfolgen soll. (Quelle: F5 Networks)

In solchen Fällen hilft eine standortabhängige Zugriffskontrolle, die zum Beispiel die IP-Adresse (datenschutzgerecht) auswertet oder die GPS-Koordinaten (ebenfalls datenschutzgerecht) analysiert, die zu dem zugreifenden Gerät gehören. Möglich ist dies unter anderem mit Lösungen wie den Stonesoft Next Generation Firewalls (www.stonesoft.com/en/products/technologies/context_awareness/) oder mit dem Geolocation Agent der F5-Networks-Big-IP-APM-Plattformen (www.f5.com/products/big-ip/big-ip-access-policy-manager/).

1.1.7 Fazit: nicht übertreiben und nichts riskieren

Kontextsensitive Sicherheitslösungen helfen Unternehmen dabei, die Verhältnismäßigkeit bei der Datensicherheit zu wahren, ohne vermeidbare Risiken einzugehen. Damit schonen sie das IT-Budget, helfen bei der Mitarbeitermotivation für die IT-Sicherheit und sorgen für dynamische Sicherheitsrichtlinien anstelle von schnell veralteten, starren Sicherheitsmodellen.

Unternehmen sollten bei ihrer Lösungssuche die jeweiligen Parameter hinterfragen, die bei der Risikoanalyse berücksichtigt werden, und dabei auch den Datenschutz für die Nutzer nicht vergessen. So sollen zum Beispiel die abgefragten Standortdaten bei der Risikobewertung helfen und nicht zu Bewegungsprofilen der Beschäftigten führen. Auch hier gilt der Grundsatz: Die IT-Sicherheit muss sich am Schutzzweck orientieren und das Verhältnis wahren zwischen dem Recht auf Privatsphäre und der möglichst hohen Netzwerksicherheit.

1.1.8 Vergleichstabelle

Die folgende Tabelle gibt eine zusammenfassende Übersicht, welche Risikofaktoren bei kontextsensitiven Security-Lösungen ausgewertet werden, wie die unterschiedlichen Sicherheitsmaßnahmen aussehen und welche Lösungen zum Beispiel das entsprechende Konzept unterstützen.

Kontextsensitive Security-Lösungen		
Risikofaktor	Kontextsensitive Sicherheitsfunktion	Beispiellösung
Zugriff auf vertrauliche Daten	z.B. Verschlüsselung abhängig von der Datenkategorie	Windows Server 2012, HP ControlPoint
Zugriff außerhalb der Dienstzeit	Zeitabhängige Zugriffsregeln pro Nutzer	BeyondTrust PowerBroker
Zugriffe auf private Online-Dienste	Zeitabhängige Blockade während der Arbeitszeit	Barracuda Web Security Service

Zugriff auf verbotene Anwendungen	Blockade des Internetzugriffs abhängig von der genutzten Anwendung oder aufgerufenen Internetadresse	Cisco-ASA-Next-Generation-Firewalls, gateprotect Appliance GPZ
Zugriff mit verbotenen Anwendungen	Entschlüsselung nur bei Verwendung erlaubter Anwendungen für den Dateizugriff	Afore CypherX
Zugriff von verbotenen Standorten	Zugriffskontrolle abhängig vom aktuellen Gerätestandort (IP-Adresse, GPS-Koordinaten)	Stonesoft Next Generation Firewalls, F5 Networks Big-IP APM Plattformen
Zugriff mit einem unsicheren Gerät	Zugriffskontrolle abhängig vom aktuellen Gerätestatus, verglichen mit den internen Sicherheitsrichtlinien	Trustwave Network Access Control, NCP Network Access Control, Dell SonicWall End Point Control

Oliver Schonschek



Oliver Schonschek ist freier IT-Fachjournalist und IT-Analyst in Bad Ems.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

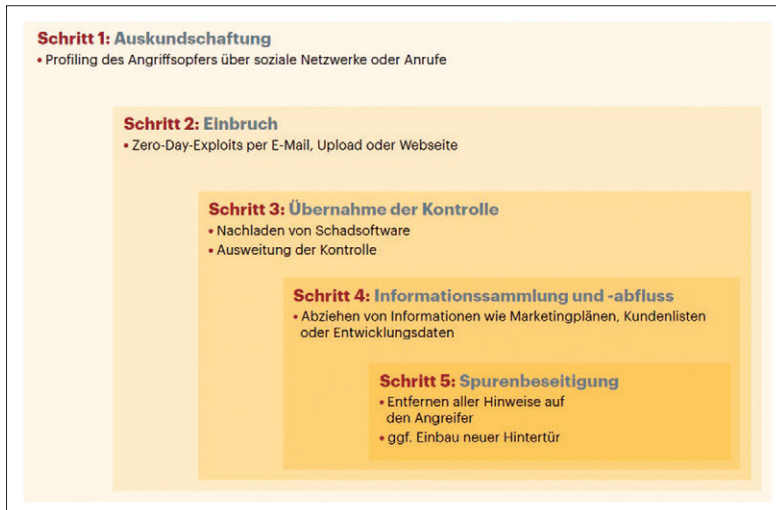
- **IT-Risiko-Management ist eine juristische Pflicht**
(www.tecchannel.de/2048166)
- **Log-Management als Unternehmensstrategie**
(www.tecchannel.de/2040047)
- **Wie verwaltet man Risiken in Projekten?**
(www.tecchannel.de/2047087)
- **Empfehlungen für ein intelligenzbasiertes Risikomanagement**
(www.tecchannel.de/2046793)
- **Sicherheitsrisiken in virtualisierten Umgebungen minimieren**
(www.tecchannel.de/2045345)
- **Security- und Risikomanagement in 15 Schritten**
(www.tecchannel.de/2046308)
- **Security-Risiko – Virtualisierung im Data Center**
(www.tecchannel.de/2040291)
- **In vier Schritten zu mehr Informationssicherheit**
(www.tecchannel.de/2040725)

1.2 IT-Risiko-Management ist eine juristische Pflicht

Neben den Vorteilen, die vernetzte IT-Systeme mit sich bringen, bergen sie auch erhebliche Gefahren. Existenzbedrohende Schäden entstehen insbesondere durch den Verlust von relevanten Daten oder durch unvorhergesehene Störungen der IT. Unternehmen haben deshalb ein großes Eigeninteresse an einer sicheren IT. Darüber hinaus sind die Betriebe aber auch gesetzlich verpflichtet, IT-Risiko-Management zu betreiben. Bei Verstößen drohen empfindliche Geldbußen und Schadensersatzforderungen sowie eine persönliche Haftung des Managements. Was ist zu tun?

1.2.1 Spektakuläre Pleiten

Schlechtes oder fehlendes Risiko-Management wird vor allem im Zusammenhang mit spektakulären Bankenpleiten oder gar drohenden Staatsinsolvenzen genannt. In der Wirtschaft wächst die Erkenntnis, dass ein effizientes und unternehmensbezogenes Risiko-Management unverzichtbar ist.



Wie Angriffe ablaufen: Wie A.T. Kearney beobachtet, laufen Angriffe typischerweise in fünf Schritten ab. Zunächst wird das Opfer über soziale Netzwerke oder Anrufe identifiziert, um ihm dann Schadsoftware unterzuschieben. In Schritt drei übernimmt der Angreifer die Kontrolle. Er lädt Malware nach und kann seinen Machtbereich dadurch ausweiten. In Schritt vier zieht der Angreifer Informationen des Opfers ab, etwa Kundenlisten, Entwicklungsdaten oder anderes. Im fünften und letzten Schritt schließlich beseitigt er seine Spuren – und baut sich nicht selten noch eine Hintertür für neue Angriffe ein. (Quelle: A.T. Kearney)

Wo sind die Risiken in der IT? Konkret droht den Unternehmen die Veränderung beziehungsweise der Verlust von Daten. Das geschieht beispielsweise durch technische Defizite, menschliches Fehlverhalten, interne Sabotage, Whistleblowing, Datenklau oder externe Angriffe (zum Beispiel Viren und Trojaner). Der Einsatz von Cloud-Computing-Lösungen, mobilen Endgeräten sowie drahtlosen Übertragungstechniken wie WLAN, LTE, HSDPA und UMTS erhöht die Gefahr.

1.2.2 Was ist gesetzlich gefordert?

Durch ein effizientes IT-Risiko-Management lassen sich die IT-Risiken naturgemäß nicht vollständig ausschließen, aber zumindest eindämmen. Das unterstreicht einmal mehr, warum Unternehmen ein eigenes Interesse am IT-Risiko-Management haben. Aber sie sind auch gesetzlich dazu verpflichtet.

Der Gesetzgeber definiert IT-Sicherheit als die Einhaltung bestimmter Sicherheitsstandards, die die Schutzgüter Verfügbarkeit, Unversehrtheit beziehungsweise Vertraulichkeit von Informationen durch Sicherheitsvorkehrungen in oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen betreffen, so nachzulesen in Paragraph 2 Absatz 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Darüber hinaus schreibt der Gesetzgeber den Unternehmen vor, technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu treffen, vergleiche Paragraph 9 des Bundesdatenschutzgesetzes (BDSG). Die Schutzmaßnahmen müssen nach Vorgabe des Gesetzgebers „erforderlich“ sein. Das sind solche Maßnahmen nur dann, wenn der damit verbundene Aufwand in einem angemessenen Verhältnis zum Schutzzweck steht. Ob das so ist, muss im Einzelfall bestimmt werden.

1.2.3 Risiko für den Vorstand

Durch die Einführung des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wurden unter anderem die Anforderungen an das Risiko-Management für Kapitalgesellschaften verschärft. So hat der Vorstand einer Aktiengesellschaft „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“, so Paragraph 91 Absatz 2 Aktiengesetz (AktG).

Der Vorstand muss also für ein umfassendes und wirksames Risiko-Management sorgen. Eine Verletzung dieser Pflicht kann die Mitglieder teuer zu stehen kommen. Sie sind der Gesellschaft nach Paragraph 93 Absatz 2 AktG persönlich zum Schadensersatz verpflichtet. Für andere Kapitalgesellschaften (zum Beispiel die GmbH) gelten ähnliche Regelungen (Paragraph 43 Absatz 1, 2 GmbH-Gesetz). Die Verletzung der Pflicht zum Risiko-Management kann einem Urteil des Landgerichts Berlin zufolge ein Grund zur fristlosen außerordentlichen Kündigung eines Vorstandsmitgliedes sein.

1.2.4 Risikoanalyse und Maßnahmenkatalog

Ein unternehmensbezogenes IT-Risiko-Management wird in der Praxis schrittweise implementiert: Zunächst erfolgt eine Risikoanalyse (Risk Assessment) zum Zweck der Ermittlung und Definition von Risikofeldern. Im Anschluss werden die Risikoquellen strukturiert und systematisiert. Dabei ist jeweils der Grad der Gefährdung in Relation zu den Kosten zu setzen, die durch die Gefahrenvermeidung entstünden. Die Ergebnisse der Risikoanalyse dienen als Grundlage für eine Risikostrategie (Kontrolle und Steuerung). Dafür müssen konzeptionelle und strategische Maßnahmen getroffen werden, zum Beispiel die Ernennung eines Chief Information Security Officer (CISO) oder der Erlass verbindlicher Unternehmensregelungen (Code of Conduct). Zudem empfiehlt es sich zumindest in größeren Unternehmen, eine unternehmensweite Sicherheitsrichtlinie (Security Policy) zu formulieren, zu erlassen und zu etablieren.



Zyklus der Informationssicherheit: Informationssicherheit sollte dem Plan-Do-Check-Act-Zyklus nach ISO 2700x folgen. Die erste Stufe (Plan – Planung und Konzeption) beinhaltet Risikoanalyse, Strategieentwicklung und die Auswahl der Sicherheitsmaßnahmen. Stufe zwei (Do – Umsetzung und Betrieb) umfasst den Realisierungsplan und die Umsetzung der Maßnahmen sowie Notfallpläne und Schulungen. Auf Stufe drei (Check – Überwachung und Kontrolle) erfolgen das Erkennen von Vorfällen und die Kontrolle der Wirksamkeit der gewählten Maßnahmen. Stufe vier (Act – kontinuierliche Verbesserung) sieht Fehlerbehebung und die Optimierung der Maßnahmen vor. (Quelle: A.T. Kearney)

Anschließend müssen operative Schritte unternommen werden. Hierzu gehören die Einrichtung von Virenschutz, Firewalls, Content-Filtern, Verschlüsselungen sowie Einbruchs- und Brandschutzvorrichtungen in den eigenen Rechenzentren, weiter Zugangsregelungen zu Systemen und Räumen sowie Sicherheitsüberprüfungen bei der Personalauswahl. Ein wichtiger Bestandteil der Risikostrategie ist auch die vertragliche Absicherung der Verfügbarkeit durch Service Level Agree-

ments (SLAs). Darüber hinaus ist eine wirksame Fall-Back-Strategie für Systemausfälle empfehlenswert. Die Funktionsfähigkeit des Risiko-Management-Systems muss ständig überwacht werden, um auf eventuell entstehende Sicherheitslücken schnell und flexibel reagieren zu können. Dafür wird ein Risiko-Monitoring-System installiert. Darüber hinaus ist eine fortwährende Anpassung der Sicherheitsmaßnahmen an die veränderten Rahmenbedingungen erforderlich.

Vorstandsbüro Oft unzureichend vor physischem Zugriff etwa durch Reinigungspersonal oder Handwerker geschützt.	
F&E Meist größter Schutzbedarf in den Unternehmen, aber oft nicht besser geschützt als andere Bereiche.	Rechenzentrum Zuverlässiger Ort für die private Cloud. Herausforderung: Der sichere Betrieb unzähliger Server inklusive der darauf laufenden Applikationen.
Lieferanten-Netzwerk Immer enger Vernetzung mit Lieferanten als Risiko, denn kleinere Lieferanten sind meist schlechter geschützt.	Cloudcomputing Eine externe Cloud ist grundsätzlich sicher. Probleme: Datenschutz außerhalb der EU, Geheimdienstzugriffe.
Produktion Viele alte Spezialsysteme. Vermehrt vernetzt, aber schwer kontrollierbar. Bei Angriffen droht Produktionsausfall bis hin zur Zerstörung.	Datenbanken Hier liegen wichtige Daten gut gesichert. Schwachstelle: als Angreifer instrumentalisierte Administratoren.
Endprodukt mit IT Zunehmend vernetzte Endprodukte ermöglichen IT-Angriffe. Erpressungspotential durch von Hackern ferngesteuerte Produkte, die Unfälle provozieren. Reputationsverluste und Ansprüche der Opfer drohen.	Büro-Netzwerk Zunehmend digitale Anbindung an fast alle Systeme. Wer einmal drin ist, hat viele Möglichkeiten.
Vertrieb Marketingpläne, Preise und Kundenkontaktdaten sind hochsensibel. Ihr Verlust zieht große Reputationsschaden nach sich und kann einen Vorsprung am Markt zerstören.	Mobile Endgeräte Handelsübliche Smartphones: Oft voll mit sensiblen Daten, immer leicht zu hacken und zu stehlen. BYOD stellt bewährte Sicherheitskonzepte in Frage.
Onlineshop Kreditkarten- und Kundendaten werden für Betrugsdelikte, gestohlene Identitäten für IT-Angriffe genutzt.	Telefonate Dank menschlicher Hilfsbereitschaft ein leichtes Einfallstor zur Informationsbeschaffung.

Die Angriffsmöglichkeiten in den Unternehmen: Vom Büro-Netzwerk bis zum Rechenzentrum – es lässt sich nicht verhindern, dass Unternehmen viele Angriffspunkte bieten. A.T. Kearney weist nicht nur auf digitale Kriminalität wie etwa Angriffe durch Cloud Computing hin, sondern auch auf ganz Handfestes: Vorstandsbüros seien häufig wenig gegen physischen Zugriff durch Reinigungspersonal oder Handwerker gesichert. (Quelle: A.T. Kearney)

1.2.5 Die Cloud als Herausforderung

Angesichts der fortschreitenden technischen Entwicklung ist gerade der letzte Punkt unerlässlich. Das wird am Beispiel Cloud Computing deutlich: Der physische Standort der Rechenzentren, in denen die Daten gespeichert werden, muss ermittelbar sein – gerade bei der Verarbeitung personenbezogener Daten –, da je

nach Standort unterschiedliche gesetzliche Regelungen gelten. Es sollte geklärt sein, wer Zugriff auf die Daten erhält und wie die Rechenzentren gesichert sind. Zudem muss sichergestellt sein, dass die Daten in der Cloud nach Vertragsende gelöscht werden. Im Zweifel muss eine Vereinbarung zur Auftragsdatenverarbeitung gemäß den Anforderungen nach Paragraph 11 BDSG geschlossen werden, in der insbesondere ein Katalog der einzuhaltenden technischen und organisatorischen Maßnahmen zum Datenschutz definiert ist.

1.2.6 Bring Your Own Device

Ein weiteres Beispiel für den ständigen Anpassungsbedarf des Risiko-Managements bietet das Thema „Bring Your Own Device“ (ByoD). Die Unternehmen müssen sich darüber im Klaren sein, dass auf den privaten Geräten relevante Unternehmensdaten verarbeitet werden. Vor dem Einsatz von BYOD sind daher unter anderem Regelungen zu folgenden Themen zu treffen: Der Einsatz muss datenschutzrechtlichen Anforderungen gerecht werden. Hierbei empfiehlt sich eine strikte Trennung von privaten und Unternehmensdaten, da Firmen grundsätzlich für dienstliche Daten, insbesondere personenbezogene Daten, die volle Verantwortung tragen. Unbedingt sollten Regelungen für den Fall des Ausscheidens aus dem Unternehmen getroffen werden. Der Einsatz muss lizenzrechtlichen Erfordernissen entsprechen. Oft ist auf den Geräten Software vorinstalliert, die ausschließlich für private Zwecke genutzt werden darf. In solchen Fällen ist eine gesonderte Lizenzvereinbarung mit dem Softwareanbieter zu schließen.

Das Arbeitsrecht ist ausreichend zu berücksichtigen. In der Regel geht es um das Mitbestimmungsrecht des Betriebsrats nach Paragraph 87 Absatz 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG).

Kevin Holleben, Fabian Winters



Dr. Kevin Max von Holleben ist Fachanwalt für Informationstechnologierecht bei Lexton Rechtsanwälte in Berlin.

Fabian Winters ist Rechtsanwalt in der Kanzlei Lexton Rechtsanwälte in Berlin.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Wie verwaltet man Risiken in Projekten?**
(www.tecchannel.de/2047087)
- **Security- und Risikomanagement in 15 Schritten**
(www.tecchannel.de/2046308)

1.3 Wie Unternehmen ihr DNS schützen

DNS-basierte DDoS-Angriffe haben sich in Ausmaß und Raffinesse innerhalb kurzer Zeit rasend schnell weiterentwickelt. Wie erklären die technischen Hintergründe und mögliche Schutzmaßnahmen.

Glaubt man einer Umfrage des DDoS-Abwehrspezialisten Arbor Networks (<http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf>), wurde im vergangenen Jahr ein Drittel aller befragten Unternehmen Opfer einer DDoS-Attacke (Distributed Denial of Service) auf ihre DNS-Server (Domain Name System Server). 2012 war es noch nur ein Viertel der Befragten. Auch der Cisco-Sicherheitsreport 2014 zeigt das steigende Risiko (www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf) – so haben die Sicherheitsexperten festgestellt, dass jedes einzelne in Augenschein genommene Unternehmen bereits von DDoS-Angriffen betroffen war.

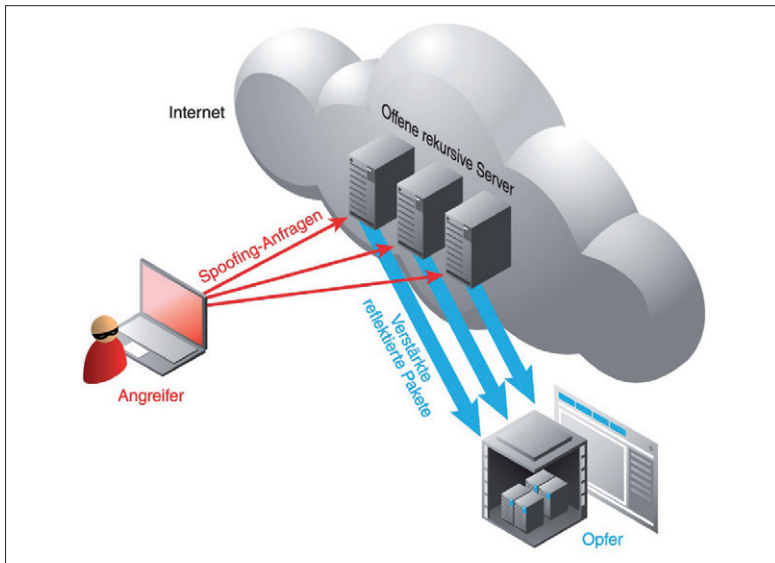
Aber: Trotz der stetig wachsenden Gefahr treffen Unternehmen nicht die notwendigen Vorkehrungen, um einen wichtigen Teil ihrer IT-Infrastruktur zu schützen. Nur wenige haben spezielles Personal, das sich intern um das Thema DNS-Sicherheit kümmert und aktive Vorsorge betreibt. Dieser Beitrag soll aufzeigen, wie DNS-basierte DDoS-Attacken funktionieren und was Unternehmen dagegen tun können.

1.3.1 Massive Angriffe

Es ist erstaunlich einfach, die DNS-Infrastruktur eines Unternehmens einzusetzen, um eine DDoS-Attacke auszuführen. Dafür nutzen die Angreifer die IP-Adresse ihres Opfers und senden darüber Anfragen an viele verschiedene Name-Server – die dann wiederum ihre Antworten zurückschicken.

Das Ganze wäre kein allzu großes Problem, wenn diese Antworten in etwa die gleiche Größe hätten wie die Anfragen selbst. Allerdings nutzen Angreifer hier oft eine sogenannte DNS Amplification Attack, einen „verstärkten“ Angriff, bei dem die Name-Server sehr große Datenmengen auf eine vermeintlich kleine Anfrage zurückschicken. Dieses Verfahren hat sich besonders verbreitet, seit es den Standard Domain Name Security Extensions (DNSSEC) gibt, mit dem DNS-Einträge digital signiert werden.

Ein Beispiel: Eine Anfrage, die gerade einmal 44 Byte groß ist, wird von einer gekaperten IP-Adresse an eine Domain geschickt, die den DNSSEC-Standard nutzt – und eine mehr als 4.000 Byte große Antwort auslöst. Mit einer Internetverbindung von einem Mbit/s hätte ein Angreifer also die Möglichkeit, 2.830 je 44 Byte große Anfragen pro Sekunde zu verschicken. Die Antworten an den Zielservers könnten sich allerdings in einer Größenordnung von 93 Mbit/s bewegen. Diese Zahlen lassen sich sogar leicht multiplizieren, wenn ein Botnetz mit Tausenden von Rechnern Anfragen an den gleichen Zielservers schickt. Zehn Komplizen könnten so schnell Antworten mit einer Größe von einem Gbit/s verursachen und den Zielservers komplett handlungsunfähig machen.



In der Praxis: So läuft ein Distributed-Reflection-DDoS-Angriff. (Quelle: Infoblox)

Viele Name-Server lassen sich so konfigurieren, dass sie erkennen, wenn sie wiederholt Anfragen für dieselben Daten von der gleichen IP-Adresse bekommen. Aber es gibt auch offene rekursive Server – schätzungsweise 33 Millionen weltweit. Diese akzeptieren dieselbe Anfrage von derselben gekaperten IP-Adresse – und zwar immer und immer wieder.

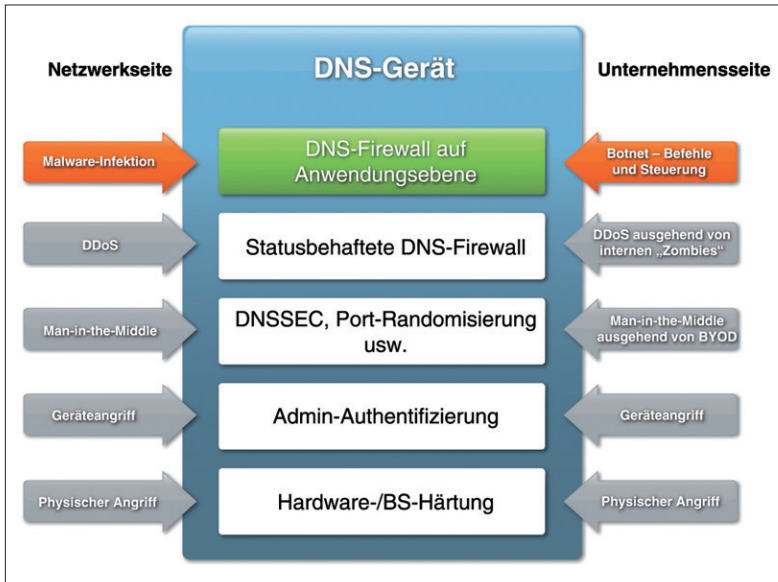
Was kann ein Unternehmen tun, um sich gegen solche Angriffe zu schützen?

1.3.2 DDoS-Attacken erkennen und vorsorgen

Als Erstes muss es registrieren, wenn (und wann) sich ein solcher Angriff ereignet. Viele Unternehmen wissen nicht, wie groß ihre reguläre Anfragemenge ist. So merken sie dann auch nicht, wenn der Normalfall deutlich überschritten wird und sie angegriffen werden. Dafür gibt es die DNS-Software BIND, mit der Statistiken eben dazu abgerufen werden können. Administratoren können also genau analysieren, wie viele Anfragen durchschnittlich über die eigenen IP-Adressen gestellt werden – und darüber auch erkennen, wenn es ungewöhnliche Ausschläge gibt, die durch einen DDoS-Angriff hervorgerufen worden sind. Auch wenn nicht immer ganz klar ist, wie ein solcher Angriff aussehen könnte, hilft die Statistik dabei, einen Durchschnitt festzulegen und Anomalien schnell zu erkennen.

Zudem sollten Unternehmen auch jede Komponente ihrer Infrastruktur ganz gezielt und aktiv auf Schwachstellen überprüfen – vor allem jene, die direkt mit dem

Internet verbunden sind. Dazu zählen nicht nur die externen autoritativen Name-Server, sondern auch Interaktionen von Switches und Routern, Firewalls und generelle Verbindungen zum Internet. Sobald Schwachstellen entdeckt werden, kann ein Unternehmen entscheiden, wie damit umgegangen werden soll.



Unüberwindbar: DNS-Sicherheit muss sowohl externen als auch internen Angriffen standhalten.
(Quelle: Infoblox)

Externe autoritative Name-Server sollten sich an möglichst vielen unterschiedlichen Standorten befinden. Das hilft nicht nur dabei, Schwachstellen zu vermeiden, sondern auch, die Antwortgeschwindigkeiten zu verringern, indem immer derjenige Name-Server antwortet, der sich räumlich am nächsten zum Kunden befindet. Um sich nicht von großen Antwortmassen außer Gefecht setzen zu lassen, sollten Unternehmen außerdem überlegen, ob sie nicht mehr Ressourcen vorhalten, als eigentlich notwendig sind (Overprovisioning). Im Vergleich zu den Konsequenzen einer DDoS-Attacke wäre das möglicherweise eine günstigere Alternative. Cloud-basierte DNS-Anbieter betreiben eigene Name-Server in ihren Rechenzentren weltweit. Die können als Ersatz für die unternehmenseigenen Name-Server konfiguriert werden – und zwar mit Daten von einem Master-Name-Server, der wiederum intern verwaltet wird. Aber Vorsicht: Viele dieser Anbieter rechnen auf Basis der erhaltenen Anfragen ab, sodass die Kosten während einer DNS-Attacke signifikant steigen.

1.3.3 Komplize wider Willen

Die richtige Konfiguration der DNS-Infrastruktur ist ein Weg, sich gegen DDoS-Attacken zu schützen. Gleichzeitig sollten Unternehmen aber auch sicherstellen, dass sie nicht unwissentlich zu Komplizen bei DDoS-Attacken gegen andere werden. Gehört ein Unternehmen nicht zu der kleinen Gruppe, die offene rekursive Name-Server betreiben, können sie die DNS-Anfragen begrenzen, die IP-Adressen in einem internen Netzwerk adressieren. So haben nur autorisierte Nutzer Zugriff auf diese sensiblen rekursiven Name-Server. Für diejenigen, die tatsächlich auch autoritative Name-Server betreiben, gibt es das sogenannte Response Rate Limiting (RRL), das in die BIND-Name-Server integriert ist. Das macht es Angreifern schwer, Anfragen zu verstärken, indem die Anzahl der Antworten, die an eine einzige IP-Adresse geschickt werden, gedeckelt wird.

Unternehmen müssen als Erstes verstehen, wie DDoS-Attacken DNS-Server nutzen, und die Zeichen für einen Angriff erkennen. Dann können sie Maßnahmen ergreifen, um sowohl die Gefahr zu mindern, dass die eigene Infrastruktur angegriffen wird, als auch zu vermeiden, dass sie wider Willen zu einem Mittäter bei Angriffen auf andere werden.

Rainer Singer



Rainer Singer ist Systems Engineering Manager Central Europe bei Netzwerk-Sicherheitsanbieter Infoblox.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Tipps & Tricks zur Absicherung der Unternehmens-IT**
(www.tecchannel.de/2047480)
- **So sichern Sie mobile Systeme richtig ab**
(www.tecchannel.de/2056373)
- **Security-Lösungen für kleine und mittelständische Firmen**
(www.tecchannel.de/2047480)
- **Security-Konzepte für Smartphone, Tablet und Co.**
(www.tecchannel.de/2040698)
- **Empfehlungen für ein intelligenzbasiertes Risikomanagement**
(www.tecchannel.de/2046793)
- **In vier Schritten zu mehr Informationssicherheit**
(www.tecchannel.de/2040725)
- **Log-Management als Unternehmensstrategie**
(www.tecchannel.de/2040047)

1.4 So merken Sie, dass Ihr Notebook oder PC gehackt wurde

Gefälschte Virenwarnungen, selbstständige Mauszeiger, merkwürdige Suchergebnisse: Hier kommen elf Anzeichen dafür, dass Ihr Rechner gehackt worden ist.

In allen genannten Szenarien ist eine Neuinstallation des Betriebssystems die beste Lösung. Das muss gar nicht die Formatierung der Festplatte bedeuten – Funktionen zu Systemwiederherstellung beispielsweise unter Windows oder regelmäßige Backups sorgen für den Ernstfall oft ausreichend vor. Eines muss jedoch klar sein: Ist ein Rechner einmal unterwandert gewesen, darf ihm nie wieder vollständig vertraut werden. Wie in welchem Fall am besten vorgegangen werden sollte, ist unter den einzelnen Punkten detailliert dargestellt.

Sie sind unter uns: Die meisten Cyber-Criminellen sind keine schwarz gekleideten Männer mittleren Alters mit Sonnenbrille und Mütze, sondern Menschen wie Du und Ich – das macht sie so gefährlich. Passen Sie auf verdächtiges Verhalten Ihres Systems auf, ignorieren Sie Spam-Mails, surfen Sie keine zwielichtigen Websites an und vor allem: Halten Sie Ihre Software auf dem neuesten Stand und lassen Sie den gesunden Menschenverstand walten. (Quelle: Alina Isakovich – Fotolia.com)



1.4.1 Gefälschte Antivirenmeldungen

Fake-Warnmeldungen des Virenschanners gehören zu den sichersten Anzeichen dafür, dass das System kompromittiert wurde. Vielen Anwendern ist nicht bewusst, dass in dem Moment, in dem eine derartige Meldung aufkommt, das Unheil bereits geschehen ist. Ein Klick auf „Nein“ oder „Abbrechen“, um den Fake-Virus-Scan aufzuhalten, genügt natürlich nicht – die Schadsoftware hat sich bestehende Sicherheitslücken bereits zunutze gemacht und ist ins System eingedrungen. Beliebte Einfallstore sind die Java Runtime Environment und die Adobe-Produkte. Bleibt die Frage: Warum löst die Malware diese „Viruswarnung“ überhaupt aus? Ganz einfach: Der vorgegebliche Prüfungsvorgang, der immer Unmengen an „Viren“ aufzut, wird als Lockmittel für den Kauf eines Produkts eingesetzt. Wer auf den dargestellten Link klickt, gelangt auf eine professionell anmutende Website,

die mit positiven Kundenbewertungen und Empfehlungen zugespflastert ist. Dort werden Kreditkartennummer und andere Rechnungsdaten abgefragt – und immer noch viel zu viele Nutzer fallen auf diese Masche herein und geben ihre Identität freiwillig an die Kriminellen ab, ohne etwas davon zu bemerken.

Was zu tun ist: Computer ausschalten, sobald die gefälschte Antivirenmeldung aufschlägt. (Achtung: Sie müssen natürlich wissen, wie eine „echte“ Meldung Ihres Virencanners aussieht.) Wenn noch etwas zu sichern ist und das problemlos geschehen kann: Machen. Und je schneller der Rechner hinuntergefahren wird, desto besser. Anschließend im „abgesicherten Modus“ neustarten (ohne Netzwerkverbindung) und die vormals neuinstallierte Software deinstallieren (was häufig klappt). Wie auch immer – wichtig ist, das System in einen Zustand zu bringen, der dem vor der Kompromittierung entspricht. Wenn das gelingt, sollte sich das System wieder normal starten lassen und keine Fake-Meldungen mehr ausstoßen. Was nun noch bleibt, sind ein umfassender Systemtest und ein kompletter Virens캔, um die letzten Reste der Malware zu entfernen.

1.4.2 Unerwünschte Browser-Toolbars

Wahrscheinlich das zweithäufigste Zeichen einer Unterwanderung: Der Browser kommt mit verschiedenen neuen Toolbars daher, die allesamt Hilfe versprechen. Solange es nicht das Produkt eines bekannten Anbieters ist (und selbst dann), sollten diese Erweiterungen entfernt werden.

Was zu tun ist: Die meisten Browser lassen es zu, sich alle installierten Toolbars anzeigen zu lassen. Entfernen Sie alle, die Sie nicht unbedingt behalten möchten. Wird die verdächtige Toolbar nicht aufgelistet oder lässt sie sich nicht ohne Weiteres löschen, sollte der Browser auf seine Standardeinstellungen zurückgesetzt werden. Klappt auch das nicht, gehen Sie so vor wie beim oben aufgeführten Punkt „Gefälschte Antivirenmeldungen“. Die meisten mit Schadcode behafteten Toolbars lassen sich schon allein dadurch verhindern, dass alle installierten Applikationen auf dem neuesten Stand sind. Und auch dadurch, dass Sie bei der Installation kostenloser Software während des Einrichtungsvorgangs ein wenig darauf achten, was alles mitinstalliert werden soll, und entsprechende Toolbars deaktivieren.

1.4.3 Umgeleitete Websuchen

Cyber-Kriminelle verdienen daran, dass Internetnutzer woanders „landen“, als sie eigentlich wollen. Die Klicks auf einer bestimmten Website werden für sie direkt in Bares umgewandelt – oft ohne dass die jeweiligen Seitenbetreiber überhaupt wissen, dass der Traffic aus einer Besucherumleitung resultiert.

Aufzufinden ist dieser Typ Malware bei infizierten Browsern schnell per Suchmaschine: einfach einige sehr generische Wörter wie „goldfish“ oder „puppy“ eintip-

pen und prüfen, ob mehrmals die gleichen Websites in den Ergebnislisten aufschlagen – diese haben meist kaum einen belastbaren Bezug zu den gesuchten Begriffen. Leider sind viele der heutigen Websuchumleitungen mithilfe diverser Proxy-Server aber so getarnt und gut versteckt, dass die gefälschten Ergebnisse für betroffene Nutzer selten direkt sichtbar sind. Häufig sind es auch Toolbars, die die Redirects auslösen. Technisch versierte Anwender, die sichergehen wollen, können auf Tools zur Überwachung des Netzwerkverkehrs zurückgreifen. Der Traffic, der auf einem kompromittierten Computer aus- und eingeht, unterscheidet sich signifikant von dem auf einem sauberen Rechner.

Was zu tun ist: Das Gleiche, das bereits erwähnt wurde. Das Entfernen von Toolbars und sonstiger Malware sollte genügen.

1.4.4 Häufige Popup-Fenster

Aufpoppende Fenster nerven. Sie sind aber auch ein Beleg dafür, dass der Rechner gehackt wurde. Liefern Websites, die für ein solches Verhalten in der Regel nicht bekannt sind, zufällige Browser-Pop-ups aus, wurde das System unterwandert. Es ist immer wieder spannend zu sehen, welche Seiten den Anti-Popup-Mechanismus des Browsers aushebeln können. Es ist wie ein Kampf gegen Spam – nur schlimmer.

Was zu tun ist: Typischerweise werden derartige Popup-Fenster durch einen der drei bereits geschilderten Fälle erzeugt. Auch hier hilft das Entfernen von Toolbars und anderen Schadprogrammen.

1.4.5 Freunde empfangen Fake-Mails mit Ihrem Namen

In diesem Fall gilt es Ruhe zu bewahren. Es ist nicht mehr außergewöhnlich, dass Adressbuchkontakte Schadcode-Mails von gefälschten Absendern empfangen. Vor knapp zehn Jahren graste die Malware noch das gesamte Adressbuch ab und schickte jedem darin befindlichen Kontakt eine böse Botschaft. Heute sind die Schadprogramme wählerischer geworden und suchen sich nur noch einzelne Opfer aus. Wenn es nur ein paar wenige Kontakte betrifft und nicht die komplette Kontaktdatenbank, ist der Rechner sehr wahrscheinlich nicht kompromittiert (zumindest nicht durch eine Malware, die E-Mail-Adressen sammelt). Viel wahrscheinlicher ist, dass die Adressen aus sozialen Netzen abgezogen wurden – wenn nicht wirklich klar erkennbar ist, dass die E-Mail von Ihrem E-Mail-Konto aus (Adresse auf Richtigkeit prüfen!), sondern nur in Ihrem Namen versendet wurde, sollte der Rechner sicher sein.

Was zu tun ist: Wenn einer oder mehrere Ihrer Kontakte von solchen Fake-E-Mails berichten, sollten Sie einen kompletten Virenscan vornehmen. Zusätzlich ist eine Prüfung angebracht, ob nicht doch unerwünschte Programme oder Toolbars installiert wurden.

1.4.6 Online-Passwörter ändern sich plötzlich

Wenn sich eines oder mehrere Ihrer Online-Passwörter von einem auf den anderen Moment ändern, ist entweder das gesamte System oder zumindest der betroffene Online-Dienst kompromittiert. Für gewöhnlich hat der Anwender zuvor auf eine authentisch anmutende Phishing-Mail geantwortet, die ihn um die Erneuerung seines Passworts für einen bestimmten Online-Dienst gebeten hat. Dem nachgekommen, wundert sich der Nutzer wenig überraschend, dass sein Passwort nochmals geändert wurde, und später, dass in seinem Namen Einkäufe getätigt, beleidigende Postings abgesetzt, Profile gelöscht oder Verträge abgeschlossen werden.

Was zu tun ist: Sobald die Gefahr besteht, dass mit Ihren Daten handfest Schindluder getrieben wird, informieren Sie unverzüglich alle Kontakte über den kompromittierten Account. Damit kann zumindest der durch Sie mit verursachte Schaden für andere reduziert werden. Danach kontaktieren Sie den betroffenen Online-Dienst und melden die Kompromittierung. Die meisten Services kennen derartige Vorfälle zur Genüge und helfen Ihnen mit einem neuen Passwort, das Konto schnell wieder unter die eigene Kontrolle zu bekommen. Einige Dienste haben diesen Vorgang bereits automatisiert. Wenige bieten sogar einen klickbaren Button „Mein Freund wurde gehackt!“ an, über den Dritte diesen Prozess für Sie anstoßen können. Das ist insofern hilfreich, als Ihre Kontakte oft von der Unterwanderung Ihres Kontos wissen, bevor Sie selbst etwas davon mitbekommen.

Werden die gestohlenen Anmeldedaten auch auf anderen Plattformen genutzt, sollten sie dort natürlich schnellstmöglich geändert werden. Und seien Sie beim nächsten Mal unbedingt vorsichtiger! Es gibt kaum Fälle, in denen Webdienste E-Mails versenden, in denen die Log-In-Informationen abgefragt werden. Im Zweifelsfall manuell den Service aufsuchen (nicht den Link in der E-Mail nutzen) und abwarten, ob der gleiche Hinweis auch erscheint, wenn Sie sich über den herkömmlichen Weg anzumelden versuchen. Sie können den Dienst auch per Telefon oder E-Mail direkt kontaktieren und sich die Echtheit der E-Mail bestätigen lassen.

Grundsätzlich ist es immer besser, ausschließlich Online-Dienste zu nutzen, die eine Zwei-Faktor-Authentifizierung verlangen – das macht es wesentlich schwieriger, Daten zu entwenden.

1.4.7 Software installiert sich selbstständig

Ungewollte und unerwartete Installationsprozesse, die aus dem Nichts starten, sind ebenfalls ein starkes Anzeichen dafür, dass das System gehackt wurde.

In den frühen Tagen der Malware waren die meisten Programme simple Computerviren, die die „seriösen“ Anwendungen veränderten – einfach um sich besser verstecken zu können. Heutzutage kommt Malware meist in Form von Trojanern und Würmern daher, die sich wie jede x-beliebige Software mittels einer Installationsroutine auf dem Rechner platziert. Häufig kommen sie huckepack mit sau-

beren Programmen – also besser immer fleißig Lizenzvereinbarungen lesen, bevor eine Installation gestartet wird. In den meisten dieser Texte, die niemand liest, wird haarklein aufgeführt, welche Programme wie mitkommen.

Was zu tun ist: Es gibt eine Menge kostenlose Programme, die alle installierten Applikationen auflisten und sie verwalten. Ein Windows-Beispiel ist Autoruns, das zudem aufzeigt, welche Software beim Systemstart mitgeladen wird. Das ist gerade in Bezug auf Schadprogramme äußerst aussagekräftig – aber auch kompliziert, weil nicht jeder Anwender weiß, welche der Programme notwendig und sinnvoll und welche überflüssig und schädlich sind. Hier hilft eine Suche im Web weiter – oder die Deaktivierung von nicht zuordenbarer Software. Wird das Programm doch benötigt, wird Ihnen das System das schon mitteilen ...

1.4.8 Die Maus arbeitet, ohne dass Sie sie benutzen

Springt der Mauszeiger wie wild über den Bildschirm und trifft dabei Auswahlen oder vollführt andere Aktionen, für deren Ausführung im Normalfall geklickt werden müsste, ist der Computer definitiv gehackt worden. Mauszeiger bewegen sich durchaus schon einmal von selbst, wenn es Hardwareprobleme gibt. Klick-Aktionen jedoch sind nur mit menschlichem Handeln zu erklären.

Stellen Sie sich das so vor: Der Hacker bricht in einen Computer ein und verhält sich erst einmal ruhig. Nachts dann, wenn der Besitzer mutmaßlich schläft (der Rechner aber noch eingeschaltet ist), wird er aktiv und beginnt, das System auszuspiionieren – dabei nutzt er dann auch den Mauszeiger.

Was zu tun ist: Wenn Ihr Rechner des Nachts von selbst „zum Leben erwacht“, nehmen Sie sich kurz Zeit, um zu schauen, was die Eindringlinge in Ihrem System treiben. Passen Sie nur auf, dass keine wichtigen Daten kopiert oder Überweisungen in Ihrem Namen getätigt werden. Am besten einige Fotos vom Bildschirm machen (mit der Digitalkamera oder dem Smartphone), um das Eindringen zu dokumentieren. Anschließend können Sie den Computer ausschalten – trennen Sie die Netzverbindung (wenn vorhanden, Router deaktivieren) und rufen Sie die Profis. Denn nun brauchen Sie wirklich fremde Hilfe.

Anschließend nutzen sie einen anderen (sauberen!) Rechner, um alle Log-In-Informationen und Passwörter zu ändern. Prüfen Sie Ihr Bankkonto – investieren Sie am besten in einen Dienst, der Ihr Konto in der folgenden Zeit überwacht und Sie über alle Transaktionen auf dem Laufenden hält. Als Betroffener dieser Art von Angriff können Sie nicht vorsichtig genug sein. Um das unterwanderte System zu säubern, bleibt als einzige Möglichkeit die komplette Neuinstallation. Ist Ihnen bereits finanzieller Schaden entstanden, sollten IT-Forensiker vorher eine vollständige Kopie aller Festplatten machen. Sie selbst sollten die Strafverfolgungsbehörden einschalten und Anzeige erstatten. Die Festplattenkopien werden Sie später noch benötigen, um den Schaden belegen zu können.

1.4.9 Security-Software, Taskmanager, Registry-Editor sind deaktiviert

Stellen Sie fest, dass Ihre Security-Software deaktiviert ist, ohne dass Sie das veranlasst haben, ist das System wahrscheinlich infiziert. Ganz besonders gilt das, wenn Sie daraufhin versuchen, den Taskmanager oder den Registry-Editor aufzurufen und diese gar nicht starten, starten und sofort wieder verschwinden oder nur in abgespekter Form starten.

Was zu tun ist: Hier ist ebenfalls eine komplette Wiederherstellung des Systems anzuraten, weil sich nicht genau nachvollziehen lässt, was genau die Probleme verursacht. Wer erst einmal die „leichte Tour“ versuchen möchte, findet im Internet eventuell Hilfe für die auftretende Funktionsstörung – hier gibt es oft zahlreiche Möglichkeiten. Findet sich ein Lösungsvorschlag, starten Sie das System im abgesicherten Modus und probieren Sie es aus. Planen Sie jedoch ein, dass viele Ideen nicht auf Anhieb funktionieren.

1.4.10 Auf dem Bankkonto fehlt Geld

Hier ist nicht das notorische Problem gemeint, das fast jeder ab und zu hat – gerade am Monatsende. Wir sprechen von viel Geld. Cyber-Kriminelle geben sich selten mit Kleckerbeträgen zufrieden – höchstens um auszutesten, ob ein Konto oder eine Kreditkarte existiert, also auch hier Vorsicht!. Sie transferieren gerne große Summen ins Ausland. In der Regel löst eine Phishing-Mail Ihrer Bank das Prozedere aus – fallen Sie darauf rein und verraten geheime Informationen wie PINs oder TANs, müssen Sie sich nicht wundern ...

Was zu tun ist: Die meisten Banken sind nach wie vor kulant und erstatten die gestohlenen Beträge zurück – gerade dann, wenn sich die Transaktion noch in der Verarbeitung befindet. Hier ist Eile angesagt! Trotzdem gab es schon einige Fälle, in denen die Kontobesitzer wegen Dummheit per Gerichtsbeschluss auf dem Schaden sitzen geblieben sind – zur Kulanz gezwungen sind die Banken nicht. Deshalb gilt auch hier: Lassen Sie sich unverzüglich informieren, wenn auf Ihrem Konto etwas Ungewöhnliches geschieht – legen Sie eine Obergrenze für Überweisungen fest und lassen Sie Mitteilungen verschicken, wenn diese Grenze überstiegen wird oder eine Auslandsüberweisung stattfindet. Weil die Cyber-Kriminellen aber ebenfalls nicht blöd sind, sollten Sie veranlassen, dass Sie in jedem Fall eine Mitteilung mitbekommen, sobald diese Grundeinstellungen verändert werden.

1.4.11 Mahnbescheide wegen nicht bezahlter Ware

Das kann der Fall sein, wenn in Ihrem Namen eingekauft wurde. Sind Sie Opfer eines Identitätsdiebstahls geworden, ist davon auszugehen, dass massenweise Zeug in diversen Shops eingekauft wurde und Kreditkarte oder Konto nicht gedeckt sind.

Was zu tun ist: Überlegen Sie, wie Ihre Identität respektive der Zugang zu Online-Shops in die falschen Hände gelangen konnte. Ist es mutmaßlich über einen der bereits dargestellten Wege geschehen, befolgen Sie die dort aufgeführten Empfehlungen. In jedem Fall bitte wieder alle Benutzernamen und Passwörter ändern – auch die bei Diensten, die nicht direkt betroffen sind. Erstellen Sie Anzeige und überwachen Sie Ihre Konten.

Wahrscheinlich dauert es Monate, bis Sie alle Betrügereien entdecken, die in Ihrem Namen begangen worden sind. Die meisten von ihnen sollten sich klären lassen – gehen Sie aber davon aus, dass Sie auf gewissen Kosten sitzen bleiben werden. Früher konnte so etwas die eigene Kreditwürdigkeit auf Jahrzehnte demolieren. Heutzutage haben auch die Händler mehr Erfahrungen mit Cyber-Kriminalität und gehen besser damit um. Dennoch sollten Sie auf der Hut sein und jedem Hinweis, die sie seitens der Ermittlungs- und Strafverfolgungsbehörden, der Zahlungsdienstleister, Banken und der Kreditauskunft bekommen, nachgehen.

1.4.12 Allgemeine Hinweise

Keine Security-Suite der Welt bewahrt Sie vor allen genannten Betrügereien – achten auf Anzeichen und Symptome, die andeuten, dass Ihr System kompromittiert wurde. Erhärtet sich ein Verdacht, ist es besser, einmal zu viel einen System-Reset zu fahren als einmal zu wenig. Das meiste Übel lässt sich verhindern, indem Sie Ihre Software immer auf dem neuesten Stand halten, keine Trojaner starten und nicht auf Fake-Mails eingehen.

Simon Hülsbömer

Der Beitrag ist im Original bei unserer US-Schwesterpublikation Infoworld (www.infoworld.com) erschienen.



Simon Hülsbömer verantwortet redaktionell leitend die Themenbereiche IT-Sicherheit, Web und Datenschutz. Außerdem betreut der studierte Media Producer den täglichen Früh-Newsletter und ab und an die iPad-Ausgaben der COMPUTERWOCHE. Aufgaben als Online-News-Aushelfer, in der Traffic- und Keyword-Analyse, dem Content Management sowie die inoffizielle Funktion „redaktioneller Fußballexperte“ runden sein Profil ab.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Wie verwaltet man Risiken in Projekten?**
(www.tecchannel.de/2047087)
- **PCs, Notebooks, Tablets oder Smartphones im Unternehmen richtig verwalten**
(www.tecchannel.de/2053738)
- **Empfehlungen für ein intelligenzbasiertes Risikomanagement**
(www.tecchannel.de/2046793)

1.5 Identitätsdiebstahl schwer gemacht

Gehen Kundendaten, technisches Know-how oder Firmenstrategien verloren, bekommt jedes Unternehmen Schmerzen. Wie lässt sich Datendiebstahl, gerade im Bereich Nutzerzugänge und Identitäten, verhindern? Und was ist im Schadensfall zu tun? Zunächst zu den möglichen Szenarien. Es gibt zwei mögliche Varianten des Identitätsdiebstahls – den ungezielten, der auf Masse abstellt, und den gezielten, der es auf bestimmte, meist privilegierte Nutzer abgesehen hat.

1.5.1 Massenidentitätsdiebstahl

Seien es nun Wettbewerber, die der Reputation eines Unternehmens schaden wollen, oder kriminelle Cyber-Gangster, die es ausschließlich auf den Weiterverkauf von Kundendaten abgesehen haben: Datenklau im großen Stil ist kein Einzelphänomen, wie diverse Vorfälle der Vergangenheit zeigen. Ob Sky, der französische Telefonriese Orange oder der Super-GAU bei Sony vor drei Jahren – kaum jemand scheint vor Massenidentitätsdiebstahl sicher. Und jedes Mal sind Tausende von Menschen betroffen.

1.5.2 Gezielter Identitätsdiebstahl

Stellen wir uns vor, es existieren zwei Konzerne, die weltweit den Markt bei Passagierflugzeugen dominieren. Da ist ein Zweikampf um größere Ausschreibungen geradezu programmiert. Denkbar sind Spionageattacken, um die Konkurrenz auszuspähen: Firma A schleust einen Mitarbeiter in Firma B ein – Firma B hingegen sucht sich direkt einen unzufriedenen Mitarbeiter von Firma A, der die „Arbeit“ noch günstiger erledigt. Nehmen wir an, dass sich besagte Mitarbeiter Zugang zu kritischen Unternehmensdaten wie Preislisten oder vergangene Angebote verschaffen. Und das ganz ohne das Telefon des Vorstands abzuhören. Denn im Idealfall arbeiten die Spione in der eigenständigen IT-Sicherheitsabteilung und besitzen entsprechende Zugangsberechtigungen. Sollte es sich „nur“ um die IT-Abteilung handeln, sind clevere Social-Engineering-Attacken, um sich Passwörter und Zugangsdaten zu erschleichen, aber ebenfalls nahezu problemlos möglich. Dieses konstruierte Beispiel ist durchaus realistisch, wie der Zweikampf der Flugzeugbauer Boeing und EADS zeigt, in dem es vor knapp zehn Jahren entsprechende Verdachtsmomente gab, in die sogar Regierungsvertreter verwickelt schienen.

1.5.3 Der Schaden

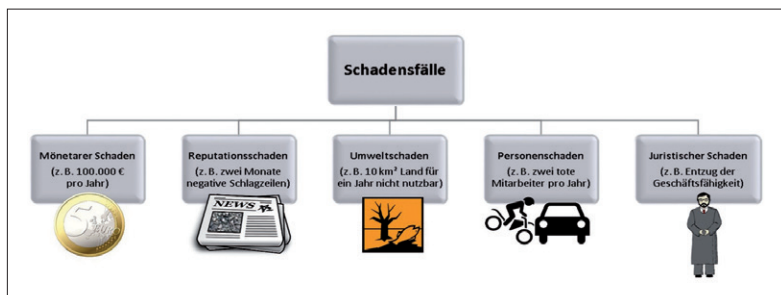
Kommt eine solche Meldung an die Öffentlichkeit, entstehen Schäden für ein Unternehmen. Ob nun Kunden- oder Angebotsdaten verfälscht werden (Integrität), Server ausfallen (Verfügbarkeit) oder Daten in falsche Hände gelangen (Vertrau-

lichkeit) – alle drei Grundwerte der Informationssicherheit wären gefährdet. Der monetäre und der Reputationsschaden stehen in der Regel im Vordergrund. Außerdem kann bei großen Konzernen das Image durchaus eine bedeutende Rolle spielen. Gerade wenn diese an der Börse notiert sind, ist es für den Shareholder Value nicht gerade förderlich, wenn sich Identitätsdiebstahl oder Spionageversuche aufgrund von möglichen Wettbewerbsvorteilen aufdecken lassen.

So geht es: Beispiele für die verletzten Grundwerte in der Informationssicherheit in Fall eines Identitätsdiebstahls. (Quelle: Stanislav Wittmann)



Nicht nur Unternehmen, sondern auch Privatanwender können von Sicherheitslücken im Access Management betroffen sein. So gab es kürzlich gleich zwei millonenfache Identitätsdiebstähle, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtet (www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Mailtest_21012014.html).



Im Detail: Für jedes Unternehmen sind fünf grundsätzliche Arten von Schäden denkbar, im Kontext Datendiebstahl zumeist drei (monetärer Schaden, Reputationsschaden, juristischer Schaden). Besonders der Reputationsschaden kann schnell zum Verhängnis werden. Je größer der mediale Auftritt, desto gravierender können die Imageeinbußen für das Unternehmen sein. (Quelle: Stanislav Wittmann)

1.5.4 Vorgehen bei einem Datenleck

Wer als Unternehmen oder Verein von einem möglichen Angriff und einem Datenleck betroffen ist, muss allein schon nach dem Willen des Bundesdatenschutzgesetzes (BDSG) unverzüglich handeln. Schließlich heißt es unter § 3 (7) über die sogenannte „verantwortliche Stelle“: „Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.“ Sollte ein drittes, externes Unternehmen die Daten beispielsweise im Rahmen einer Website verarbeiten, gilt dieses ebenfalls als verantwortliche Stelle.

Wichtig ist, die vom Identitätsdiebstahl Betroffenen zu informieren – idealerweise persönlich, was bei Massendiebstählen jedoch kaum machbar ist. Deshalb schreibt § 42 a des BDSG bei „unverhältnismäßigem Aufwand“ die Benachrichtigung in der Öffentlichkeit vor. Das bedeutet beispielsweise eine Meldung über eine halbe Seite in mindestens zwei bundesweit erscheinenden Tageszeitungen oder einen Fernsehbeitrag oder Meldungen auf anderen Medienkanälen.



Alle sind betroffen: Ein Datenleck – ob im Unternehmen oder im Verein oder in einer Organisation – trifft meist verschiedene Interessengruppen. (Quelle: Stanislav Wittmann)

„Anstatt sich um den eigenen Imageschaden zu sorgen, spricht das Aufzeigen einer Datenpanne für eine aktiv gelebte Sicherheitskultur“, unterstreicht Datenschützer Michael Werner. Es helfe außerdem, drohende Bußgelder (§ 43 BDSG – Bußgelder) und mögliche Haftstrafen (§ 44 BDSG – Strafvorschriften) zu vermeiden. Überhaupt ist es eine sinnvolle Vorsichtsmaßnahme für Unternehmen, für solche Szenarien bereits im Vorfeld Notfallpläne zu erstellen. Nicht nur, um mögliche Schäden der Betroffenen zu reduzieren, sondern auch, um das eigene Image aufrechtzuerhalten. Denn je schneller die Warnmeldungen an die Betroffenen rausgehen, desto eher können alle Parteien reagieren und als Konsequenz versuchen, vorhandene Schäden zu mindern.

1.5.5 Täterprofile

Hacker, Social Engineers oder eingeschleuste Mitarbeiter: Um Daten zu entwenden, bedarf es immer Menschen mit einer gewissen kriminellen Energie und bestimmten technischen Fertigkeiten. Zumeist sind es Insider, die für Sicherheitsvorfälle verantwortlich zeichnen – so zumindest das Ergebnis der 2012er-Studie von Corporate Trust (www.corporate-trust.de/studie/studie-2012.html). Demnach führt die Spur in mehr als der Hälfte aller Spionageattacken zu Innentätern. „Mitarbeiter, die sich ausgenutzt fühlen, sind nicht loyal. Der Schaden, der Unternehmen dadurch entsteht, geht in die Milliarden“, erklärt Professor Wolfgang Berger, Leiter des Business REFRAMING Instituts Karlsruhe (www.business-reframing.de).



Den Tätern auf der Spur: Die Studie „Industriespionage 2012“ von Corporate Trust macht deutlich, dass Innentäter die häufigste Ursache sind. (Quelle: Corporate Trust)

Nur jede achte Fall von Spionage ist laut Corporate Trust auf Hacker von außen zurückzuführen. Dazu kommen Attacken von Wettbewerbern und auch von Nachrichtendiensten. So berichtet der Whistleblower Edward Snowden in einem Videobeitrag (www.youtube.com/watch?v=-6QmwLpse3E#t=1237), dass Nachrichtendienste teils sogar wissentlich nicht die „idealen Sicherheitslösungen für Unternehmen empfehlen“, um deren potenzielle Schwachstellen bei Bedarf auszunutzen zu können. „Bei der Reduzierung des Sicherheitsniveaus in der Kommunikation setzen Nachrichtendienste nicht nur die Welt, sondern auch Amerikaner Risiken aus“, so Snowden.

1.5.6 Fazit

Ein ganzheitliches Sicherheitskonzept wie die ISO 27001 ist bestimmt ein passender Schlüssel zum Schutz vor Identitätsdiebstahl und Datenmissbrauch. Unternehmen sollten sich trotzdem Gedanken über das Betriebsklima und eine eventuell hohe Personalfuktuation machen. Auf den ersten Blick sparen sie Geld, wenn sie kurzfristig beispielsweise Werkstudenten oder Praktikanten für kleinere (Sicherheits-)Projekte beauftragen. Möglicherweise machen diese auch einen guten Job. Jedoch gibt es auch eine Kehrseite der Medaille: Mit jedem Mitarbeiter, der das Unternehmen verlässt, geht ein Stück Know-how verloren, und das Risiko von Schäden durch die beschriebenen Angriffe steigt. Zudem freut sich das eigene Personal nicht gerade über eine hohen Fluktuation. Mitarbeiter spüren, wenn Unternehmen höhere Umsätze einer zufriedenen Belschaft vorziehen.

Um das Betriebsklima zu wahren, sollen Unternehmen alle Mitarbeiter wertschätzen, aktiv wahrnehmen und auf ihre Bedürfnisse eingehen. Erfahrungsgemäß gehen die Besten zuerst – und mit ihnen das wertvollste Wissen. Daher ist neben einem ganzheitlichen und individuell abgestimmten Sicherheitskonzept das Betriebsklima entscheidend. Berger macht deutlich: „Die härteste Realität in jedem Unternehmen ist nicht die ‚Hardware‘, sondern eine sehr spezielle Software: das, was die Mitarbeiter über ihr eigenes Unternehmen denken.“ Genau diese Gedanken entscheiden letztlich über ihre Handlungen. Dagegen können manchmal selbst die besten Schutzmaßnahmen nichts ausrichten. Nicht einmal die der NSA. So konnte es ein einziger Mann mit dem vielleicht mächtigsten Nachrichtendienst unseres Planeten aufnehmen.

Stanislav Wittmann



Stanislav Wittmann ist selbständiger Sicherheitsberater und freier Autor. Seine Schwerpunkte liegen im vorbeugenden und planerischen Brandschutz sowie in der Informationssicherheit. Hierzu zählen vor allem Risiko- und Notfallmanagement, Spionage-Prävention und die Schulung von Mitarbeitern gegen Know-How-Verlust (Security Awareness).

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Die Sicherheit liegt im Prozess**
(www.tecchannel.de/2056964)
- **IT-Risiko-Management ist eine juristische Pflicht**
(www.tecchannel.de/2048166)
- **Was bringt softwaregestütztes Identity & Access Management?**
(www.tecchannel.de/2053455)
- **So vernichten Sie Daten und Datenträger richtig**
(www.tecchannel.de/2048681)

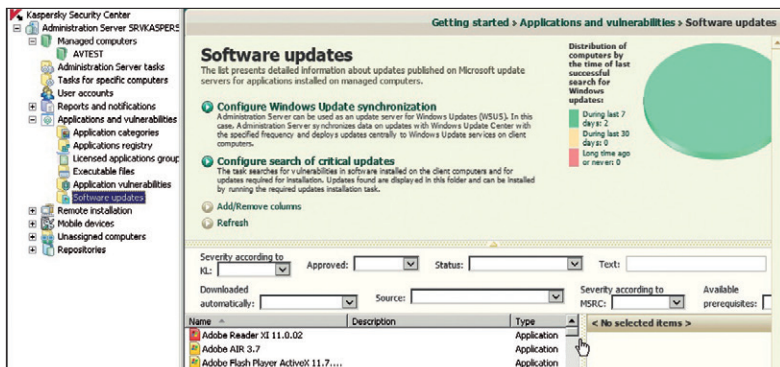
1.6 Vier Patch-Management-Lösungen im Test

Ein geregeltes Patch-Management sorgt nicht nur für gut arbeitende Software, indem es sie auf dem neuesten Stand hält. Vielmehr wird die Sicherheit auf Clients und Servern erhöht, da Patches Schwachstellen in der eingesetzten Software schließen. Die Lösungen sollen dabei vorhandene Betriebssysteme und Softwareinstallationen automatisch mit den Datenbanken des jeweiligen Anbieters abgleichen und die Updates auslösen. In der Praxis kommt es aber darauf an, wie schnell Updates eingespielt werden, ob alle laufenden Applikationen erkannt und die Updates fehlerfrei ausgeführt werden. Denn jeder hängende Client oder Server ist unter dem Strich mehr Belastung als Hilfe.

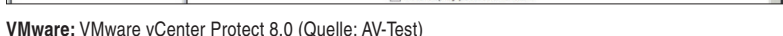
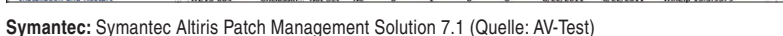
1.6.1 Das Testfeld

Den Test der Patch-Management-Lösungen hat die Firma Kaspersky Lab bei dem unabhängigen Magdeburger Antivirentestlabor AV-Test in Auftrag gegeben. Dabei wurde nur der Testumfang von Kaspersky Lab vorgegeben, die finalen Testmethoden hingegen hat AV-Test selbst festgelegt und den Test auch im eigenen Labor durchgeführt. Die Ergebnisse der Produkte von Kaspersky Lab, Lumension, VMware und Symantec wurden ohne Einflussnahme von Kaspersky Lab veröffentlicht. Getestet wurden folgende Produkte:

- Kaspersky Security Center 10.1
- Lumension Endpoint Management and Security Suite 7.3
- Symantec Altiris Patch Management Solution 7.1
- VMware vCenter Protect 8.0



Kaspersky: Kaspersky Security Center 10.1 (Quelle: AV-Test)



1.6.2 Die bewerteten Funktionen

Die Tester haben sich die elf wichtigsten Funktionen der Softwarelösungen herausgegriffen und miteinander verglichen:

1. Die Zahl der unterstützten Applikationen
2. Die Erkennung der installierten Programme
3. Die Reaktionsrate zum Einspielen neuer Patches
4. Den Sprach-Support der installierten Anwendungen
5. Die Qualität und den Ablauf der Patch-Installation
6. Das Verhalten bei Installationsproblemen
7. Das Deaktivieren unerwünschter Add-ons
8. Die Kontrolle der Auto-Update-Konfiguration von Software
9. Den Einsatz des Microsoft-Update-Supports (WSUS)
10. Die Steuerung des Server- oder Client-Neustarts
11. Den Umgang mit Nutzerlizenzen bei Updates

1.6.3 Die Hürden im Test

Schwachstellen im Betriebssystem lassen sich bei Microsoft-Systemen mithilfe der Microsoft-Datenbank WSUS relativ schnell schließen, sofern die Patch-Lösung darüber Bescheid weiß und den Service nutzt. Bei anderen Betriebssystemen wie Mac-OS X, Red-Hat- oder SUSE-Linux sind die Datenbanken der Lösungsanbieter gefragt. Weiterhin ist die Menge der von Firmen eingesetzten Applikationen fast unbegrenzt. Die Patch-Management-Lösungen mussten im Test mehr als 290 Programme und Betriebssysteme erkennen und unterstützen. Diese Summe ergab sich aus den Angaben aller unterstützten Applikationen der vier Lösungen.

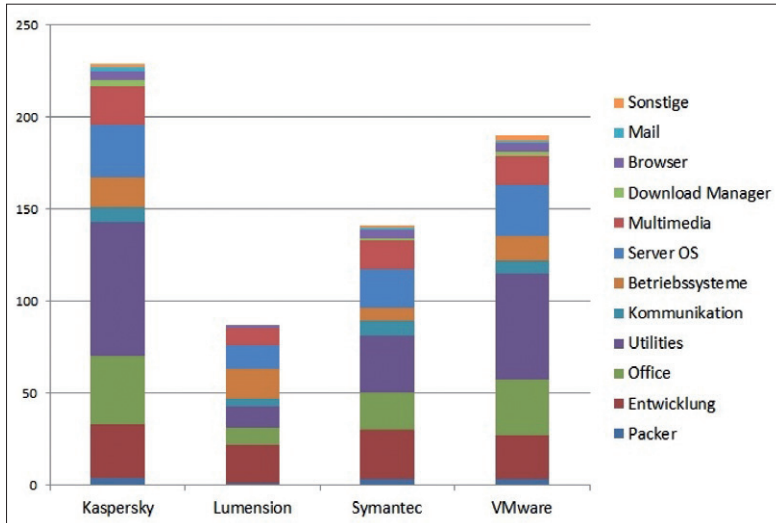
An dieser Stelle zeigte die Lösung von Kaspersky mit über 78 Prozent den besten Wert. Die Lösung von VMware folgte mit 65 Prozent, Symantec mit 48 und Lumension mit knapp 27 Prozent. Nur Kaspersky und Lumension erkannten alle Betriebssysteme zu 100 Prozent.

1.6.4 Wer erkennt die Software?

Im Weiteren wurde geprüft, ob die Lösungen die 60 populärsten Applikationen erkennen und updaten. Mit vertreten: Browser wie Firefox, Chrome, Safari oder Opera, Mailclients wie Thunderbird oder Packer wie Winrar und 7-Zip.

Das Ergebnis: Die Lösungen von VMware und Symantec kennen zwar die meisten Programme, lesen aber mehrfach die Versionsnummer falsch oder gar nicht aus. Kaspersky kennt zwar weniger Applikationen als VMware und Symantec, aktuali-

siert sie aber dafür korrekt. Lumension arbeitet sauber, kennt jedoch im Vergleich zu den anderen Lösungen nur etwa die Hälfte der Programme. Populäre Tools wie Chrome, Opera, Safari, Thunderbird oder Winrar kennt die Lösung gar nicht.



Patch-Management-Testergebnisse: Anzahl der unterstützten Applikationen im Patch-Management: Mit knapp 230 Applikationen ist das Programm-Portfolio der Kaspersky-Lab-Lösung am größten. Lumension kennt nicht einmal 90 Programme. (Quelle: AV-Test)

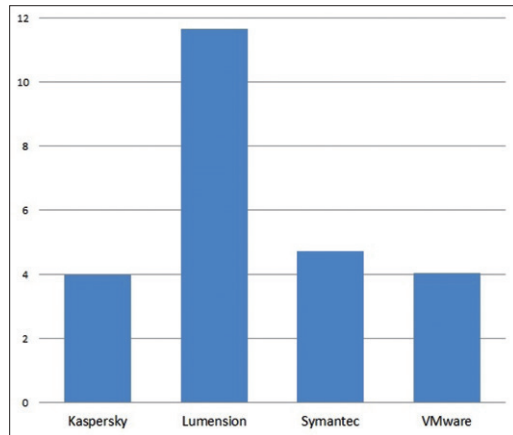
1.6.5 Falsche Sprache wird passend gemacht

Ist eine Applikation nicht in der Systemsprache installiert, dann verweigern einige Lösungen die volle Unterstützung. Vor allem Lumension kennt lediglich zwei zusätzliche Sprachen. Von 14 getesteten Sprachen kennen Symantec und Kaspersky Lab zwölf, VMware sogar 13 Sprachen. VMware und Symantec leisten sich allerdings Ausrutscher: Sie bringen zwar sechs beziehungsweise sieben Programme auf den neuesten Stand, ändern dabei aber die zuvor eingestellte Sprache.

1.6.6 Wie schnell wird gepatcht?

Sobald eine Applikation eine Schwachstelle meldet, wird damit auch zeitnah ein Patch veröffentlicht. Im Test reagierten die Lösungen von VMware und Kaspersky Lab im Schnitt nach vier Tagen, Symantec nach fünf. Lumension benötigte dagegen fast zwölf Tage.

Patch-Management-Test-ergebnisse: Durchschnittlich gemessene Dauer für Updates in Tagen: Während die Lösungen von Kaspersky Lab und VMware vier Tage für das Update benötigen, braucht Symantec fünf und Lumension fast 12. (Quelle: AV-Test)



1.6.7 Was passiert, wenn das Update schief läuft?

Der wichtigste Punkt ist das Patchen selbst. Denn jede Update-Installation, die scheitert, mit Fehlern endet oder im schlimmsten Fall in einer Endlosschleife landet, muss der Administrator von Hand erledigen.

Im Test mussten die Lösungen aus dem Test-Pool an Applikationen nur diejenigen updaten, die sie auch kennen. Diese Qualität wurde festgehalten. VMware und Symantec unterstützten jeweils 63 Programme, patchten sie indes nur zu 97 beziehungsweise 87 Prozent. Bei Symantec streikten nach dem Update acht Programme, bei VMware eines. Die Patch-Lösung von Kaspersky Lab unterstützt nur 51 Programme, patcht diese jedoch alle fehlerfrei. Lumension erreichte mit fast 97 Prozent Verlässlichkeit zwar einen hohen Wert, das aber mit nur 27 Applikationen.

1.6.8 Stolpersteine bei Updates

Wenn ein Update auf den Clients keinen Aufschub duldet, kollidieren einige Lösungen gerne mit bestimmten Systemsituationen wie laufenden Installationen, offenen Browsern, fehlender Internetverbindung oder dem Umstand, dass die zu patchende Applikation gerade läuft. Im Test wurde dies nachgestellt.

Bei den von den Patch-Management-Paketen unterstützten Applikationen konnten nur Kaspersky Lab und Lumension punkten. Letztere Lösung hatte nur drei Mal ein Problem, weil die zu patchende Software in dem Augenblick am Arbeiten war. VMware und Symantec hatten in allen Störszenarien ihre Probleme. Besonders offene Browser und zu patchende Software, die gerade lief, machten den Lösungen zu schaffen.

1.6.9 Sicherheitslücken durch Add-ons

Während eines Updates versuchen einige Applikationen, Toolbars oder Optimierungs-Tools mit zu installieren. Auf diese Weise werden neue Sicherheitslücken geschaffen. Daher muss die Add-on-Installation verhindert werden. Im Test schlüpfen sowohl Symantec als auch VMware einzelne Add-ons ins Update. Nur Lumension und Kaspersky Lab blieben fehlerfrei.

1.6.10 Auto-Updates können querschießen

Viele Applikationen wissen über ihre permanente Anfälligkeit für Sicherheitslücken Bescheid – ganz vorne rangiert da etwa der Adobe Reader. Daher bringt er auch ein Auto-Update mit. Die Patch-Management-Lösung sollte die Auto-Update-Funktion der Applikationen deaktivieren können. Nur Lumension, Kaspersky Lab und VMware bringen dies von Haus aus als Option mit. Die Lösungen von Lumension und VMware unterstützen allerdings nur wenige Applikationen direkt. Zumindest VMware bietet daher auch zusätzlich die Lösung via Scriptsteuerung an. Nutzer von Symantec müssen den ganzen Ablauf der Auto-Updates per vorhandener Script-Steuerung verhindern.

1.6.11 Nutzerlizenzen sollten einsehbar sein

Bei jeder Installation von Software sollte der Administrator zumindest die Möglichkeit haben, die Nutzungsbedingungen zu lesen und bei Bedarf abzulehnen. Nur die Lösungen von Lumension und Kaspersky Lab bieten einem Admin diese Möglichkeit. Symantec und VMware verzichten darauf.

1.6.12 Integration des Update-Support von Microsoft

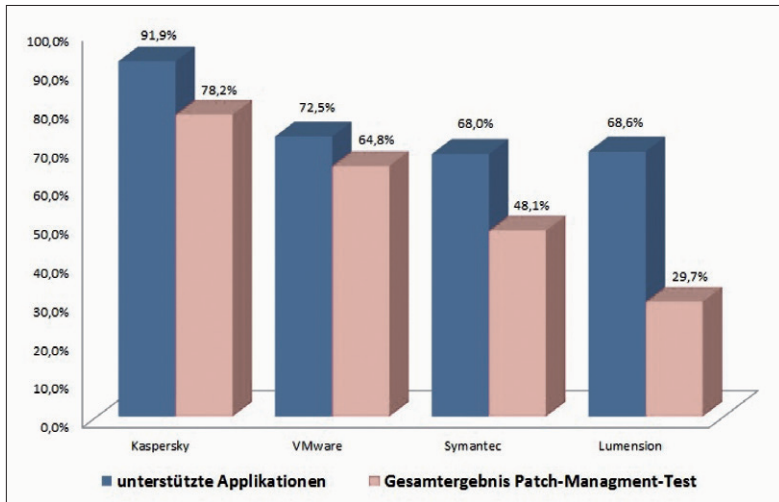
Microsoft bietet für Updates den Windows Software Update Service, kurz WSUS, an. Während Kaspersky Lab diesen Service in seine Lösung eingebunden hat und steuert, verzichten alle anderen Lösungen auf eine Anbindung.

1.6.13 Gute Steuerung der Neustarts

Im Test wurde auch das Verhalten nach den Updates registriert. Musste ein Neustart des Systems eingeleitet werden, so wurden die Nutzer des Client- oder Server-Systems gut informiert und die Systeme verlässlich neu gestartet. Es ließen sich sogar Neustarts verschieben oder zeitlich neu planen. In diesem Punkt waren alle Lösungen gleich verlässlich und umgänglich.

1.6.14 Fazit: Patch-Management sichert Systeme und entlastet Admins

Auch wenn die Zahlen der einzelnen Testabschnitte es nicht direkt erkennen lassen: Jede der getesteten Patch-Management-Lösungen kann für mehr Sicherheit bei Clients oder Servern sorgen. Zudem werden sie ständig überarbeitet und verbessert.



Patch-Management-Testergebnisse: Im Gesamtergebnis kann die Lösung von Kaspersky Lab einen Vorsprung nach Prozenten für sich verbuchen. Sehr positiv ist auch der Umfang der unterstützten Applikationen. (Quelle: AV-Test)

Unter dem Strich arbeitet von den getesteten Probanden die Lösung Kaspersky Security Center im Vergleich zu den Paketen Lumension Endpoint Management and Security Suite, Symantec Altiris Patch Management Solution und VMware vCenter Protect am verlässlichsten. Die hohe Zahl an unterstützten Applikationen und vor allem das meist fehlerfreie automatische Update können den Administrator massiv entlasten und die Sicherheit hochhalten.

Markus Selinger

Markus Selinger ist IT-Fachjournalist in München.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Was bringt softwaregestütztes Identity & Access Management?**
(www.tecchannel.de/2053455)

1.7 Cloud- und Social-Media-Daten richtig verschlüsseln

Vertrauliche Daten sollten verschlüsselt werden – das gilt auch bei Facebook, auf dem Smartphone und in der Cloud. Verschlüsselungs-Tools helfen dabei.

Enthalten E-Mails oder E-Mail-Anhänge personenbezogene Daten, sehen die rechtlichen Vorgaben für den Datenschutz – bei entsprechendem Schutzbedarf – eine Verschlüsselung nach dem Stand der Technik vor. Gleiches gilt für Daten, die in eine Cloud übertragen werden sollen. Ohne Verschlüsselung würden Datenschutzgesetze und andere Compliance-Vorgaben gebrochen.

Genau das aber geschieht in der Praxis – selbst in technikaffinen Branchen: Nur 53 Prozent der IT-Unternehmen verschlüsseln ihre E-Mails an externe Empfänger, 47 Prozent nutzen eine Verschlüsselung für Daten, bevor diese in eine Cloud ausgelagert werden, so eine BITKOM-Umfrage. Dabei wäre zum Beispiel bei E-Mails der Bedarf an Verschlüsselung weitaus höher: Nur ein Viertel der befragten Unternehmen verschickt keine vertraulichen Dokumente per E-Mail.

Verschlüsselung stellt also für viele Unternehmen offensichtlich eine große Herausforderung dar. Erschwerend kommt hinzu, dass die pauschale Forderung nach Verschlüsselung zu einfach ist. Die praktische Umsetzung nämlich hängt stark davon ab, wo die Daten gespeichert werden und mit welchem Verfahren sie übermittelt oder verarbeitet werden sollen.

1.7.1 Vielfältige Verschlüsselungsmöglichkeiten

Die Forderung nach Verschlüsselung bezieht sich auf E-Mails und Cloud-Daten genauso wie auf vertrauliche Chats und Internettelefonate, auf Datenspeicher in (mobilen) Endgeräten, auf Speichermedien, Netzwerke und Online-Dienste. Fast überall befinden sich vertrauliche Daten, die verschlüsselt sein wollen.

Doch nicht nur die Speicherorte und Übermittlungsverfahren sind vielfältig, auch die Verschlüsselungslösungen, die es inzwischen auf dem Markt gibt. Im Folgenden sollen verschiedene Verschlüsselungs-Tools näher betrachtet werden, die dabei helfen können, die generelle Forderung nach Verschlüsselung vertraulicher Daten konkret umzusetzen.

1.7.2 Verschlüsselung für Speichermedien

CDs, USB-Sticks und externe Festplatten werden bevorzugt für den Datentransport eingesetzt. Gehen solche Speichermedien unterwegs verloren, können große Datenmengen in Gefahr sein. Diebe oder unehrliche Finder könnten mehrere Gigabyte an vertraulichen Informationen einsehen und missbrauchen, wenn die Daten unverschlüsselt vorliegen.

Der flexible Umgang mit Speichermedien und die häufige Nutzung von USB-Sticks oder externen Festplatten bringen es mit sich, dass die erforderliche Verschlüsselung oftmals ausgelassen wird. Sie gilt als umständlich und zeitaufwendig. Ideal sind deshalb Tools, die eine Verschlüsselung erzwingen oder aber zumindest sehr einfach machen.

DataLocker EncryptDisc von Origin Storage (www.originstorage.com/datalocker-encryptdisc.asp) ist ein optisches Speichermedium mit integrierter Verschlüsselung: Jede EncryptDisc enthält bereits eine Brenn- und Verschlüsselungssoftware und kann wie ein herkömmlicher CD- oder DVD-Rohling für die Speicherung von Daten verwendet werden. Eine 256-Bit-AES-Verschlüsselung mit Passwortabfrage hält Unbefugte vom Datenzugriff ab. Systemvoraussetzung sind Windows XP, Vista oder 7; Windows 8 soll in Kürze ebenfalls unterstützt werden.

Hilfreich: Bei DataLocker EncryptDisc handelt es sich um optische Speichermedien, die die Verschlüsselungslösung bereits in sich tragen. (Quelle: Origin Storage Ltd)



Für die Verschlüsselung von USB-Sticks und Festplatten bietet sich beispielsweise Protectorion ToGo Pro an (<http://de.protectorion.com/usb-stick-verschluesseln/>). Die Verschlüsselungslösung wird auf dem zu schützenden USB-Speichermedium installiert und erzeugt einen speziellen Ordner, den der Nutzer mit einem persönlichen Passwort belegt. Alle Daten, die anschließend in diesem Ordner abgelegt werden, werden automatisch verschlüsselt.

Hilfreich sind auch Verschlüsselungswerkzeuge, die sich für mehrere Anwendungsfälle eignen, wie zum Beispiel Sophos SafeGuard Encryption (www.sophos.com/de-de/products/safeguard-encryption.aspx). Mit einer solchen Lösung können Daten auf dem PC, auf externen Festplatten und vor der Übertragung in die Cloud verschlüsselt werden. Die Lösung unterstützt zum Beispiel eine zentrale Verwaltung der Verschlüsselung, Single-Sign-on-Verfahren und die Wiederherstellung vergessener Schlüssel.

1.7.3 Verschlüsselung für mobile Endgeräte

Genauso wie mobile Speichermedien laufen auch mobile Endgeräte Gefahr, verloren zu gehen oder gestohlen zu werden. Trotzdem werden Smartphones und Tablets munter für die Speicherung vertraulicher Daten verwendet, wie eine Kaspersky-Umfrage ergab.

Für die Verschlüsselung mobiler Endgeräte stehen die Bordmittel der mobilen Betriebssysteme wie Apple iOS oder Android OS zur Verfügung. Apple iOS sorgt für eine automatische Verschlüsselung, bei Android OS gibt es eine optionale Datenverschlüsselung, die der Nutzer erst aktivieren muss. Verschiedene mobile Anti-Malware-Lösungen wie Kaspersky Security for Mobile sehen eine zusätzliche Verschlüsselungsfunktion für Daten auf mobilen Endgeräten vor.

Smartphones brauchen allerdings noch weitere Formen der Verschlüsselung, um auch den Versand von SMS oder die vertraulichen Telefonate vor Lauschangriffen zu schützen. etaPhone (www.ethon.com) ist eine Sprachverschlüsselungs-Applikation für Android-Smartphones oder iPhones. PhoneCrypt (www.securstar.de/phonecrypt.html) verschlüsselt ebenfalls mobile Telefonate. Die SecuSUITE for BlackBerry 10 (www.secsmart.com/secsuite/) bietet eine mobile Transportverschlüsselung (E-Mail, Sprache, SMS, Secure Browsing) und eine mobile Ablageverschlüsselung (Daten, Kontakte, Notizen).



Geheime Kommunikation: Bei mobilen Endgeräten sollten nicht nur die gespeicherten Daten, sondern auch die vertraulichen Telefonate verschlüsselt werden, zum Beispiel mit PhoneCrypt. (Quelle: SecurStar)

1.7.4 Verschlüsselung für E-Mail

Die E-Mail-Verschlüsselung setzt im Prinzip nur einen kostenlosen Standard-Mail-Client wie Mozilla Thunderbird (www.thunderbird-mail.de) und digitale Zertifikate für Absender und Empfänger voraus, wobei die Zertifikate relativ einfach in das E-Mail-Programm importiert werden können. Doch in der Praxis stellt das Management der – öffentlichen und privaten – Schlüssel die Unternehmen vor

große Schwierigkeiten. Deshalb sind Lösungen sinnvoll, die entweder gezielt das Schlüsselmanagement übernehmen und vereinfachen, wie dies die Secardeo cert-Box anbietet (www.secardeo.de/produkte/certbox.html). Oder die E-Mail-Verschlüsselung unterstützt alternative Verfahren: Z1 SecureMail Gateway (www.zertificon.com/produkte/secure-email-gateway/) hilft nicht nur bei der PKI (Public Key Infrastructure), sondern unterstützt auch den Versand vertraulicher Nachrichten mittels passwortgeschützter PDF-Dateien. Eine Lösung wie der E-Mail Verschlüsselungsservice von antispaceurope (www.antispaceurope.com/de/) erlaubt das Outsourcing der E-Mail-Verschlüsselung.



Verschlüsselungskünstler: Appliances mit dem Z1-SecureMail-Gateway unterstützen die Verschlüsselung von E-Mail auf mehreren Wegen und erleichtern so die Anbindung von Partnern, die keine Public Key Infrastructure (PKI) betreiben. (Quelle: Zertificon Solutions GmbH)

1.7.5 Verschlüsselung für Netzwerke

Gerade bei Netzwerkzugriffen mobiler und externer Mitarbeiter sollte die Verschlüsselung nicht fehlen. Hier spielen VPN-Lösungen (Virtual Private Networks) eine entscheidende Rolle. Da die anzubindenden Nutzer meist eine sehr heterogene IT-Landschaft mit unterschiedlichen mobilen Geräten und Betriebssystemen nutzen, sind VPN-Lösungen mit breiter Systemunterstützung empfehlenswert.

Der NCP Secure Entry Client (www.ncp-e.com/de/produkte/ipsec-vpn-client-suite.html) für Verbindungen zu verschiedenen VPN-Gateways ist zum Beispiel für Windows 8/7, Windows Vista, Windows XP, Android OS (ab 4.0), Mac OS X und Windows Mobile verfügbar. Praktisch sind auch VPN-Sticks wie SINA Business (www.secunet.com/de/). Sie helfen beim schnellen Aufbau einer verschlüsselten Verbindung zum Unternehmensnetzwerk.

1.7.6 Verschlüsselung für Clouds

Werden Clouds als Storage genutzt, sollten sowohl die Übertragung als auch die Speicherung der Daten verschlüsselt erfolgen, da Unternehmen Cloud-Storage-Lösungen zunehmend für vertrauliche Inhalte nutzen. Dabei sollte die Verschlüs-

selung vom Betreiber der Cloud unabhängig sein. Verschlüsselungs-Tools wie IndependenceKey (www.intellicomp.de), Boxcryptor (www.boxcryptor.com/de) oder Cloudfogger (www.cloudfogger.com) erlauben zum Beispiel die Verschlüsselung der Daten bei Nutzung von Dropbox, Skydrive oder Google Drive. Wuala (www.wuala.com) bietet sich als Cloud-Speicher mit integrierten Sicherheitsfunktionen an, wozu auch eine Datenverschlüsselung vor Übertragung in die Cloud gehört.



Universal-Tool: Der IndependenceKey verschlüsselt Daten für Mail, Skype, Dropbox oder andere Cloud-Speicher. (Quelle: Intellicomp GmbH)

1.7.7 Verschlüsselung für Social Media

Auch wenn eine Verschlüsselung bei sozialen Medien wie Facebook auf den ersten Blick ungewöhnlich erscheint, kann auch hier der Bedarf an verschlüsselter Kommunikation bestehen. Marktanalysen gehen davon aus, dass die elektronische Kommunikation zunehmend über soziale Netzwerke stattfinden wird.

Sollen vertrauliche Nachrichten zum Beispiel auf Facebook vor Unbefugten geschützt werden, hilft eine Lösung wie Scrambls Enterprise (www.scrambls.com). Über spezielle Browser-Erweiterungen können Nutzer, die das entsprechende Passwort kennen, die verschlüsselten Statusnachrichten auf Facebook & Co. lesen. Andere Nutzer können nicht Einsicht nehmen.

1.7.8 Wichtig für alle Verschlüsselungslösungen

Was für jeden Anwendungsbereich beachtet werden sollte: Verschlüsselungs-Tools schützen nur dann zuverlässig, wenn sie die Datenübertragung vom Sender bis zum Empfänger vollständig verschlüsseln. Datenschützer fordern deshalb für eine sichere elektronische Kommunikation eine Ende-zu-Ende-Verschlüsselung.

Bei der sicheren Datenspeicherung und bei der geschützten Datenübertragung sollte zudem immer eine Verschlüsselung nach dem Stand der Technik genutzt werden, wie im Bundesdatenschutzgesetz (BDSG) gefordert. Was als Stand der Technik hinsichtlich Schlüssellängen und Verfahren betrachtet werden kann, zeigt insbesondere ein Blick in die Technische Richtlinie „BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (www.bsi.bund.de/DE/Publikationen/

TechnischeRichtlinien/tr02102/index_htm.html) des Bundesamtes für Sicherheit in der Informationstechnik. So wichtig komfortable Verschlüsselungs-Tools für die Umsetzung der gesetzlichen Forderungen auch sind: Es hilft wenig, wenn die Verschlüsselung zwar ohne Widerwillen genutzt wird, aber dafür zu schwach ist.

1.7.9 Beispiele für Verschlüsselungs-Tools

Verschlüsselungs-Tools		
Verschlüsselungsbereich	Zu verschlüsselnde Daten	Beispiel-Tools
Speichermedien	Gespeicherte Daten	DataLocker EncryptDisc, Protectorion ToGo Pro, Sophos SafeGuard Encryption
Mobile Endgeräte	Gespeicherte Daten, Telefonate, SMS, E-Mails	Kaspersky Mobile Security, aetaPhone, PhoneCrypt, SecuSUITE for BlackBerry 10
E-Mail	E-Mails, E-Mail-Anhänge	E-Mail-Clients mit S/MIMESecardeo certBox, Z1 SecureMail Gateway E-Mail, Verschlüsselungsservice von antispameurope
Netzwerke	Übertragene Daten, Datenzugriff	VPN-Clients wie NCP Secure Entry, ClientVPN-Sticks wie SINA Business
Cloud	Übertragene Daten, Datenzugriff (vom Cloud-Betreiber unabhängige Verschlüsselung!)	Boxcryptor, Cloudfogger, IndendenceKey, Wuala
Social Media	Vertrauliche Statusinformationen und Nachrichten	Scrambls Enterprise

Oliver Schonschek



Oliver Schonschek ist freier IT-Fachjournalist und IT-Analyst in Bad Ems.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Biometrie-Tools aus der Cloud**
(www.tecchannel.de/2054132)

1.8 Tools zur Anonymisierung von Daten

Die größte Hürde bei der praktischen Umsetzung von Big-Data-Projekten ist die Sicherheit der Daten, so das Ergebnis einer aktuellen Umfrage von PricewaterhouseCoopers (PwC) unter Entscheidern aus Industrieunternehmen (www.pwc.de/de/pressemitteilung/en/2014/die-meisten-industrieunternehmen-wollen-big-data-nutzen.jhtml). Demnach sehen die Befragten die Datensicherheit (50 Prozent der Teilnehmer), die Datenqualität (44 Prozent) und den Datenschutz (42 Prozent) als größte Schwierigkeiten.

Auch den Verbrauchern ist der Schutz der Daten in Big-Data-Projekten wichtig, wie die Studie „Big Data und Datenschutz“ (www.telekom.com/medienloesungen-fuer-unternehmen/205852) des Handelsblatt Research Institute im Auftrag der Deutschen Telekom gezeigt hat: 62 Prozent der Befragten wünschen sich mehr Datenschutz.

Datensicherheit und Datenschutz geraten allerdings durch die große Menge und Vielfalt der schützenden Daten zu einer anspruchsvollen Aufgabe. Will man die Absicherung der Daten vereinfachen, empfiehlt sich eine Verringerung des Schutzbedarfs. Praktisch bedeutet das bei personenbezogenen Daten, die Zuordnung zu einer natürlichen Person zu erschweren, die Daten also zu anonymisieren. Ohne Personenbezug entfallen die strengen Vorgaben aus dem Datenschutz.

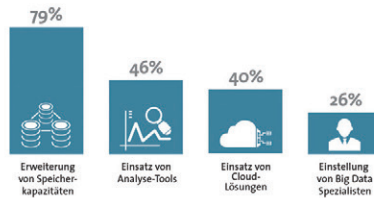
Von Big Data zu Datability

Datability beschreibt die Fähigkeit, große Datenmengen in hoher Geschwindigkeit auszuwerten sowie mit Daten und Analyseergebnissen verantwortungsvoll umzugehen.

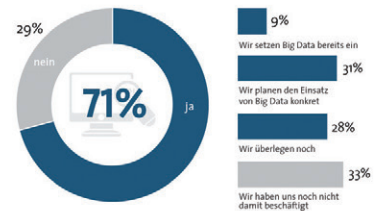
Veränderung des Datenvolumens in Unternehmen im Jahr 2013¹



Wie Unternehmen auf das steigende Datenvolumen reagieren^{1,2}



Ist Big Data für Ihr Unternehmen relevant?



55% der Unternehmen analysieren personenbezogene Daten.³

Die Sicht der Bürger: Sorge und Pragmatismus¹

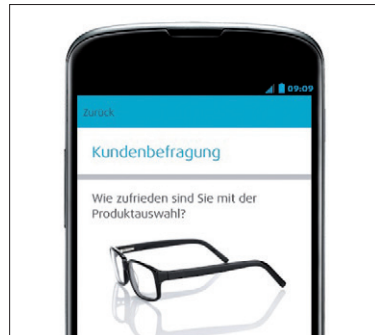


Ergebnisse der Studie: Als Hindernisse für die Nutzung von Big Data sehen viele Unternehmen die Anforderungen an die technische Sicherheit (61 Prozent) und an den Datenschutz (48 Prozent), so eine BITKOM-Umfrage. Um den Datenschutz in Big-Data-Projekten zu vereinfachen, empfiehlt sich die Anonymisierung personenbezogener Daten oder bereits eine Datensparsamkeit bei der Erhebung. (Quelle: BITKOM)

1.8.1 Anonymisierung erleichtert Datensicherheit

Nicht ohne Grund werden Datensparsamkeit und Datenvermeidung und damit die Reduzierung personenbezogener Daten auf ein notwendiges Minimum als Königsweg im Datenschutz bezeichnet („Datenvermeidung“). Das Bundesdatenschutzgesetz sagt aus, dass personenbezogene Daten zu anonymisieren oder zu pseudonymisieren sind, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zum angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Im Verborgenen arbeiten: Der beste Weg zu anonymen oder pseudonymen Daten ist, überhaupt keine Daten mit konkretem Personenbezug zu erheben (Datenvermeidung). Der Dienst WeWant verspricht unter anderem die Möglichkeit der anonymen Teilnahme an Umfragen via Smartphone-App. (Quelle: WeWant GmbH)



Unter Anonymisierung versteht das Gesetz dabei „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können“.

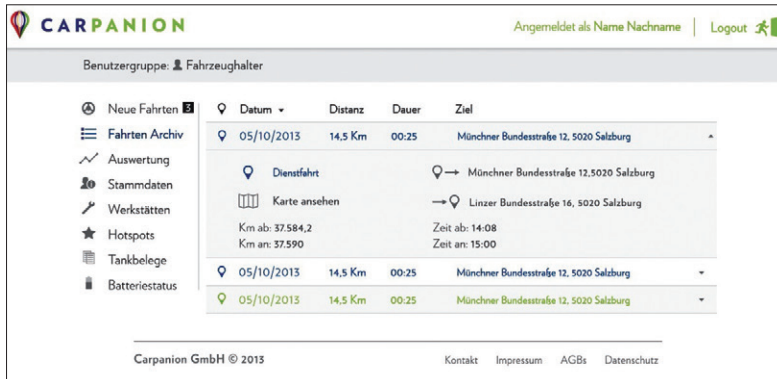
Pseudonymisierung hingegen ist „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“.

1.8.2 Nicht immer, aber öfter anonymisieren

Datenschützer ermuntern grundsätzlich zu Anonymisierung, Datenvermeidung und Datensparsamkeit, um die Verarbeitung personenbezogener Daten auf ein Mindestmaß zu reduzieren. Trotzdem wird von keinem Unternehmen verlangt, jeden Personenbezug aus den Datenbeständen zu tilgen.

Vielmehr entfällt die Notwendigkeit zur Anonymisierung oder Pseudonymisierung immer dann, wenn der Erhebungs- und Verwendungszweck einen eindeutigen Personenbezug notwendig macht oder der Aufwand für Anonymisierung/Pseudonymisierung im Vergleich zum Schutzzweck viel zu hoch wäre.

Zwei Beispiele: Bei Systemprotokollen darf aus Compliance-Gründen nicht einfach jeder Personenbezug entfernt werden – sonst kann im konkreten Verdachtsfall der schuldige Nutzer nicht ausgemacht werden. Kundendaten müssen ebenfalls nicht anonymisiert werden, wenn sie für die Vertragsabwicklung benötigt werden oder einer gesetzlichen Aufbewahrungspflicht unterliegen.



Ein weiteres Beispiel der Datenvermeidung: Das elektronische Fahrtenbuch von Carpanion nutzt die AMV-Technologie, bei der die Datenübermittlung anonym über verschlüsselte Datenverbindungen erfolgen soll. (Quelle: Carpanion)

Entscheidend ist die sogenannte Zweckbindung für die personenbezogenen Daten oder bei Systemprotokollen die sogenannte besondere Zweckbindung: Personenbezogene Daten, die für die Datenschutzkontrolle, die Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden. Werden personenbezogene Daten nur für ihren Erhebungszweck verarbeitet, müssen sie nicht anonymisiert werden.

1.8.3 Anonymes Big Data ist möglich

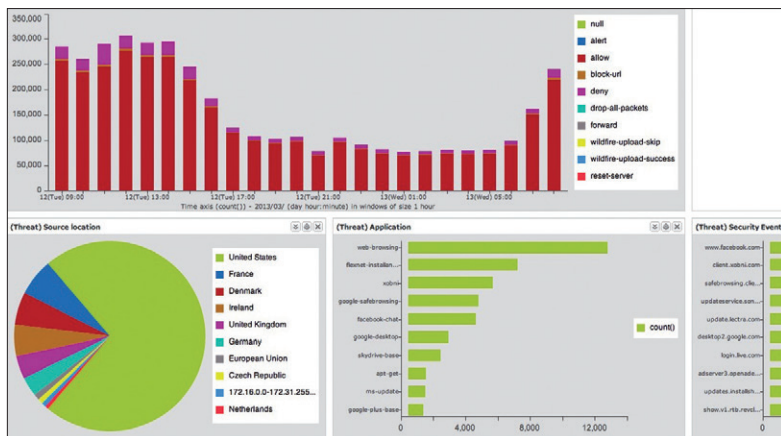
Wenn Unternehmen den gesetzlichen Vorgaben und den Verbraucherwünsche nachkommen und in ihren umfangreichen Datenbeständen eine gezielte Anonymisierung/Pseudonymisierung vornehmen wollen, scheint die nächste Herausforderung im Raum zu stehen: Man braucht ein leistungsfähiges, zuverlässiges Verfahren. Die personenbezogenen Daten müssen in den „Datenbergen“ aufgespürt, klassifiziert und nach bestimmten Kriterien anonymisiert werden, ohne dabei Daten zu übersehen oder fälschlicherweise den erforderlichen Personenbezug zu entfernen. Dafür gibt es je nach Aufgabenstellung spezielle Werkzeuge, die nun beispielhaft betrachtet werden sollen.



Anonymität sollte Nutzern wo immer möglich angeboten werden: Die Lancom-Hotspot-Lösung für Hotels unterstützt verschiedene Anmeldemöglichkeiten, neben Benutzernamen und Passwort, Zugangs-Voucher oder zusätzlichen Passwörter per SMS auch die anonyme WLAN-Nutzung nach Bestätigung der AGB. (Quelle: Lancom Systems)

1.8.4 Datenmaskierung

Die IRI FieldShield-Software (www.iri.com/products/fieldshield) oder die Informatica-Data-Masking-Produkte (www.informatica.com/de/products/data-masking) können dazu genutzt werden, um Datenbankinhalte oder unstrukturierte Daten nach personenbezogenen Daten zu durchsuchen. Fundstellen lassen sich nach definierten Regeln maskieren.



Anonym bleiben: Daten unerkant zu belassen, aber trotzdem auswerten zu können, ist die hohe Kunst. (Quelle: LogPoint, Andreas Kümmerling)

Das bedeutet, dass die personenbezogenen Daten durch Daten ersetzt werden, die keinen echten Personenbezug mehr aufweisen. Das können frei definierbare Zeichenketten oder bestimmte Ersetzungswörter sein. Alternativ können Daten so verkürzt werden, dass sie ihre Aussagekraft über bestimmte Personen verlieren.

Neben der statischen Datenmaskierung (Static Data Masking, SDM), die den Personenbezug von gespeicherten Daten entfernen kann, gibt es die dynamische Datenmaskierung (Dynamic Data Masking, DDM), die Daten nahezu in Echtzeit so abwandelt, dass erst gar keine personenbezogenen Daten gespeichert werden. Dabei machen leistungsfähige Lösungen zur Datenmaskierung vor großen Datenmengen nicht halt: Innovative Routines International (IRI) verspricht den Anwendern „Big Data Protection“, wozu eine Maskierung von personenbezogenen Daten innerhalb großer Datenmengen gehört.

1.8.5 Webanalysen: IP-Adresse verkürzen

Wie die Verkürzung personenbezogener Daten bei der Anonymisierung hilft, zeigt das Beispiel der Webanalyse mit Google Analytics: Nach Bestimmungen des Telemediengesetzes (TMG) dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist nach Ansicht der Datenschützer kein Pseudonym im Sinne des Telemediengesetzes. Nachdem die Aufsichtsbehörden für den Datenschutz in Deutschland mit Google längere Zeit über die Datenschutzanforderungen an eine Webanalyse diskutiert hatten, stellte Google eine Lösung vor, mit der auch die Datenschützer einverstanden waren.

Die Lösung besteht unter anderem darin, Google mit der Kürzung der IP-Adressen zu beauftragen – durch entsprechende Einstellungen im Programmcode von Google Analytics. Dazu ist auf jeder Internetseite mit Google-Analytics-Einbindung der Trackingcode um die Funktion „_anonymizeIp()“ zu ergänzen (<https://support.google.com/analytics/answer/2763052>). Die Kürzung der IP-Adressen dient der Anonymisierung der Nutzungsdaten.

1.8.6 Datenbanken: anonyme Datenfelder

Speziell zur Anonymisierung von Datenbanken gibt es Werkzeuge wie Anonimatron (<http://anonimatron.sourceforge.net>), eine Open-Source-Lösung auf Java-Basis, die unter anderem echte E-Mail-Adressen in zu anonymisierenden Datenbankbeständen durch erfundene Mail-Adressen ersetzt. Ein anderes Werkzeug ist DICOM Anonymizer&Masker (www.dicomtool.com/anonymizer.htm), das die Anonymisierung von Dateinamen, Verzeichnisnamen und Datenelementen aus Datenbanken anbietet.

Es sollte also kein Problem darstellen, Lösungen zur nachträglichen Anonymisierung oder Pseudonymisierung von Datenbanken aufzutreiben. Noch besserer ist es allerdings, personenbezogene Daten wenn möglich gleich ganz zu vermeiden. Im Bereich der Marktforschung ist das beispielsweise zumeist möglich, weil nicht der einzelne Nutzer, sondern Nutzergruppen zu untersuchen sind.

1.8.7 Marktforschung: anonyme Umfragen

Die Marktforschungslösung von Qualtrics (<http://qualtrics.com/research-suite/>) enthält eine Option, mit der sich personenbezogene Daten bei Umfragen vermeiden lassen. Unter den Umfrage-Optionen gibt es die Auswahl „Do not record any personal information and remove panel association“.

Bei dieser Auswahl werden personenbezogene Daten wie die IP-Adresse des Umfrageteilnehmers entfernt, bevor die Antworten gespeichert werden. Personenbezogene Angaben, die der Teilnehmer innerhalb seiner Antworten selbst gibt, bleiben indes bestehen. Auf Wunsch lassen sich die Antworten der Teilnehmer ebenfalls so überarbeiten, dass personenbezogene Daten vor einer Speicherung entfernt werden. Diese Überarbeitung ist nicht rückgängig zu machen. Unternehmen, die eine Umfrage mit dem Werkzeug starten wollen, sollten sich also überlegen, welche personenbezogenen Angaben wirklich benötigt werden und welche nicht. Die Optionen von Qualtrics lassen sich entsprechend anpassen.

1.8.8 Business Analytics: der anonyme Kunde

Abschließend stellt sich die Frage, ob denn Big-Data-Projekte für die Marktforschung und andere Datenerhebungen nicht ihre Aussagekraft verlieren, wenn man den Vorgaben der Datenschützer nachkommt. Diese Sorge dürfte bei vielen Unternehmen vorherrschen, die die Möglichkeiten zur Anonymisierung und die Vorgaben dazu kennen, aber nicht umsetzen.

Eine Lösung wie Aircloak zeigt aber, dass sich Nutzerdaten anonymisieren lassen, ohne auf eine hilfreiche Business-Analyse verzichten zu müssen. Kunden können anonym bleiben und trotzdem hinsichtlich ihrer Wünsche und Vorlieben untersucht werden. Zu diesem Zweck nutzt Aircloak Sandboxing für die Nutzerdaten, ein gehärtetes Betriebssystem, sowie Verschlüsselung und die Anonymisierung der Nutzerdaten, um die Identifizierung von Einzelnutzern zu verhindern.

Innovative Werkzeuge und Lösungen sind also verfügbar, um selbst große Datenmengen datenschutzgerecht zu verarbeiten. Big Data, Datenschutz und Business Intelligence sind kein Widerspruch, sondern gehören eng zusammen. Anonymisierung und Pseudonymisierung bauen die Brücke dorthin.

Oliver Schonschek



Oliver Schonschek ist freier IT-Fachjournalist und IT-Analyst in Bad Ems.

1.9 Das bieten Security-Assessment-Tools

Wesentliche Probleme bei der Entwicklung von IT-Sicherheitsrichtlinien sind die Aktualität und die Vollständigkeit. Um aktuelle Policies für alle relevanten Bereiche der IT-Sicherheit erstellen zu können, müssen Unternehmen ihre tatsächlichen, aktuellen Risiken kennen und bewerten. Für diese wichtige Arbeit aber fehlen oft Zeit und Budget, wie beispielsweise die Kaspersky-Studie „Global Corporate IT Security Risks“ herausfand (http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf).

Unterstützung finden Unternehmen durch zumeist kostenlose Security-Assessment-Tools – das sind in aller Regel Online-Dienste, die auf unterschiedlichen Wegen bei der Ermittlung von Schwachstellen und Risiken in der IT helfen.

Die Tools unterscheiden sich allerdings stark im Leistungsumfang und in der konkreten Hilfestellung. Im Folgenden werden deshalb mehrere Beispiele für Security-Assessment-Werkzeuge untersucht und Empfehlungen gegeben, was bei der Auswahl und Verwendung generell zu beachten ist.

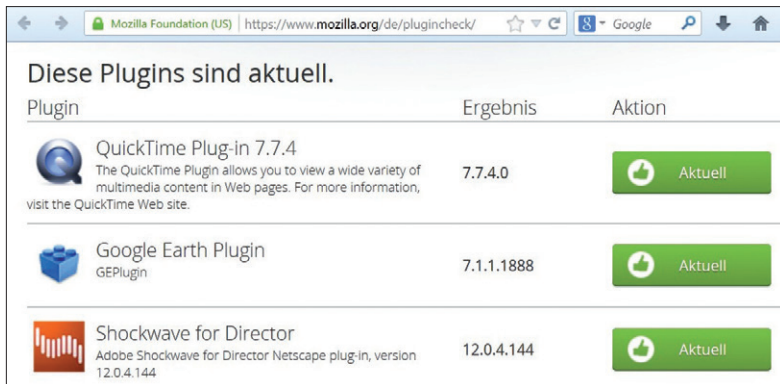
1.9.1 Mit dem Browser fängt es an

Wesentliche Bedrohungen für die IT-Sicherheit kommen aus dem Internet. Ein klassischer Angriffsweg besteht darin, Schwachstellen von Browsern und Browser-Erweiterungen auszunutzen. Es verwundert nicht, dass gerade für die Prüfung der Browser-Sicherheit zahlreiche Assessment-Tools existieren.



Multifunktional: Zu den Security-Assessment-Tools gehören auch Browser-Tests, die Nutzer im Internet ausführen können, um Schwachstellen im Browser oder in Browser-Erweiterungen aufzuspüren. Dadurch werden Risiken im Bereich Browser-Sicherheit und der Bedarf an entsprechenden Browser-Richtlinien sichtbar. (Quelle: Deutsches Sicherheitsnetz e.V.)

Beispiele sind der Browsercheck des Deutschen Sicherheitsnetz e.V. (www.desine.de/web/guest/browsercheck), der Qualys BrowserCheck (<https://browsercheck.qualys.com>), Rapid7 BrowserScan (<http://browserscan.rapid7.com>) und der Browser- und Plugincheck des Anti-Botnet Beratungszentrums (www.botfrei.de/browsercheck/). Diese und vergleichbare Browser-Tests richten sich an den einzelnen Internetnutzer und bieten Hinweise zur Aktualisierung von Browser und Plug-Ins.



Plugin	Ergebnis	Aktion
 QuickTime Plug-in 7.7.4 The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the QuickTime Web site.	7.7.4.0	 Aktuell
 Google Earth Plugin GEPlugin	7.1.1.1888	 Aktuell
 Shockwave for Director Adobe Shockwave for Director Netscape plug-in, version 12.0.4.144	12.0.4.144	 Aktuell

Unkompliziert: Schon ein einfacher Plug-In-Check im Firefox liefert Hinweise zum Sicherheitsstatus.

Aussagen zu möglichen Risiken auf Unternehmensebene sind möglich, wenn ein einheitlicher Browser und eine einheitliche Plug-In-Ausstattung vorgeschrieben sind. In diese Richtlinie sollte dann auch die regelmäßige oder automatische Aktualisierung des Browsers und der Erweiterungen aufgenommen werden.

Zudem bietet beispielsweise Qualys eine Business-Version für Browser-Tests an (www.qualys.com/forms/browsercheck-business-edition/), die zentral gesteuert und ausgewertet werden kann. Administratoren erhalten so mittels Dashboard einen Überblick über die bestehende Browser- und Plug-In-Sicherheit.

1.9.2 Websites im Blick

Online-Risiken zu begegnen bedeutet auch, die eigene Website in den Blick zu nehmen. Ob diese verseucht und für Besucher zur Gefahr werden kann, zeigt zum Beispiel der Website-Test der Initiative-S (www.initiative-s.de/de/index.html). Wer ganze Webapplikationen einem Sicherheitstest unterziehen möchte, kann das unter anderem mit dem Veracode Web Application Testing Tool tun (www.veracode.com/security/web-application-security-testing).

Administratoren können die eigene Website auf typische Schwachstellen (siehe beispielsweise OWASP Top Ten Project, www.owasp.org/index.php/Category/OWASP_Top_Ten_Project) untersuchen und testen, ob diese durch entspre-

chende Attacken gefährdet wäre. Ein Beispiel-Tool für Webadministratoren ist Ratproxy (<https://code.google.com/p/ratproxy/wiki/RatproxyDoc>). Solche Werkzeuge sollten aber nur Anwender mit genügend Erfahrung und ausschließlich für die eigene Website einsetzen.

1.9.3 Systemanalyse auf Knopfdruck

Neue IT-Risiken können zum Beispiel dann auftreten, wenn eine Software installiert wurde, die auch potenziell neue Angriffsflächen bietet. Ebenso entstehen Sicherheitslücken durch fehlende Patches und falsche Sicherheitskonfigurationen. Security-Assessment-Tools wie Windows Attack Surface (www.microsoft.com/en-us/download/details.aspx?id=24487) untersuchen den Einfluss einer Installation auf das Betriebssystem, indem das Windows-System vor und nach der Installation verglichen wird. Der Microsoft Baseline Security Analyzer (<http://technet.microsoft.com/en-us/security/cc184924.aspx>) unterstützt Administratoren dabei, Windows-Systeme nach fehlerhaften Sicherheitseinstellungen und fehlenden Sicherheits-Updates zu durchsuchen.

1.9.4 Der Fehler steckt im Quellcode

Sicherheitslücken beginnen in aller Regel damit, dass bei der Softwareentwicklung eine Sicherheitsfunktion vergessen oder ein Programmfehler begangen wurde. Ein Security Assessment auf Basis des Programm-Codes bietet zum Beispiel HP Fortify on Demand, wobei der Nutzer die Tests startet und die Resultate der auswertenden Sicherheitsexperten innerhalb einer definierten Zeitspanne erhält. Veracode bietet eine Reihe von Code-Assessments – darunter die Veracode Static Analysis (www.veracode.com/products/static).

Solche Assessments richten sich an Entwickler und interne Tester und zeigen, an welchen Stellen der Quellcode noch verwundbar ist. Sie können eine wichtige Ergänzung der internen Qualitätssicherung darstellen und den Bedarf an neuen oder geänderten Entwicklungsrichtlinien aufzeigen.

1.9.5 Den Nutzer nicht vergessen

Ein wesentliches Sicherheitsrisiko stellen Nutzer dar, die die Sicherheitsrichtlinien nicht kennen oder nicht umsetzen – ob unwissentlich oder vorsätzlich. Zumindest gegen Ersteres können Tools helfen. Ein entsprechendes Angebot kommt zum Beispiel von SANS: CyberTalent Assessments (www.sans.org/cybertalent) – Wissenstests, die für Beschäftigte wie für Bewerber und Dienstleister gleichermaßen geeignet sind. Auch das Microsoft Security Assessment Tool (<http://technet.microsoft.com/de-de/security/cc185712.aspx>) bietet einen Fragenbereich, bei dem die Mitarbeiter, ihre Awareness und die für sie geplanten Schulungen im Fokus stehen.

1.9.6 Befragung statt Angriff

Security-Assessment-Tools unterscheiden sich nicht nur in der Zielgruppe, sondern auch darin, wie sie den Sicherheitsstatus im Unternehmen ermitteln, ob sie einen Fragenkatalog dazu anbieten, die Antworten auswerten und ob sie sogar einen Angriff simulieren.

Eine Befragung im Bereich IT-Sicherheit bieten zum Beispiel das Oracle Enterprise Data Security Assessment (www.oracle.com/us/media/survey/index-191234.html), das IT Security Assessment Tool der Aberdeen Group (<http://securityassessment.aberdeen.com>), der DsiN-Sicherheitscheck (www.sicher-im-netz.de/unternehmen/DsiN-Sicherheitscheck.aspx) und das Microsoft Security Assessment Tool (www.microsoft.com/en-us/download/details.aspx?id=12273) mit Fragen aus den Themenbereichen Infrastruktursicherheit, Anwendungssicherheit, Betriebssicherheit und Mitarbeitersicherheit. Im Anschluss an die Beantwortung liefern die Tools eine Auswertung mit technisch-organisatorischen Handlungsempfehlungen im Bereich IT-Sicherheit.

Current Use of Enabling Technologies				
Category	Assessment Questions	Your Response	Best-in-Class	Laggards
Process	Patch / Configuration Management	Yes	90%	70%
	Intrusion Detection / Intrusion Prevention	No	95%	54%
	Network Access Control	Yes	77%	57%
	Penetration testing	No	85%	51%
	Approved Scanning Vendors (ASV)	No	72%	37%
Knowledge / Business Intelligence	Application vulnerability scanners	No	65%	40%
	Application firewall / gateway	No	81%	67%
	Secure application development tools	Yes	67%	37%
Technology / Automation	Secure data transmission for "data in motion"	No	90%	59%
	Data encryption for "data at rest"	No	71%	49%
	Data discovery / classification	No	68%	27%
	Data content monitoring / filtering	Yes	59%	27%
Performance Management	Log management	No	86%	43%
	Security information / event management	No	86%	54%
	Qualified Security Assessors (QSA)	No	83%	30%

Based on your responses, your company's comparison with the top performers ("Best-in-Class") and lagging performers ("Laggards") in terms of current Enabling Technologies is summarized in the following chart:

Mittelstandssoftware: Die Aberdeen Group hat ein Security Assessment im Angebot, das sich speziell an KMU richtet. Die Auswertung vergleicht die Antworten des Teilnehmers mit denen anderer Teilnehmer und erlaubt so ein Benchmarking für bestimmte Bereiche der IT-Sicherheit. (Quelle: Aberdeen Group)

Ebenfalls eine Befragung zur IT-Sicherheit mit anschließender Auswertung bietet RiskRater (www.rapid7.com/resources/free-tools.jsp). Teilnehmende Unterneh-

men erhalten ein Benchmarking darüber, wie das eigene Unternehmen seine IT-Sicherheit im Vergleich zu anderen Teilnehmern im Griff hat.

Trend Micro bietet verschiedene Assessment-Tools, die Befragungen und Auswertungen für die Bereiche Internetsicherheit, Cloud-Sicherheit und mobile Sicherheit vornehmen. Fragen und Auswertungen speziell im Bereich Mobile Security bietet auch das Tool Secure Mobility Hot Zone von Mobile Work Exchange. Von HP gibt es eine Befragung als Assessment-Tool zum Thema Sicheres Drucken.

Vielseitig: Trend Micro bietet kostenlose Online-Assessments zu Cyber, Cloud und Mobile Security. Nutzer erhalten im Anschluss einen ausführlichen Risikobericht. (Quelle: Trend Micro)



1.9.7 Fazit

Die zahlreichen Security-Assessment-Tools, die es auf dem IT-Sicherheitsmarkt bereits gibt, bieten wertvolle Hilfestellung bei der Suche nach Risiken, für die es entsprechende IT-Sicherheitsrichtlinien geben sollte.

Allerdings sollten Unternehmen nicht vorschnell scheinbar nützliche Online-Dienste verwenden, um ihre IT nach Schwachstellen zu durchsuchen. Es sollte immer zuerst überprüft werden, wer der Anbieter ist, was mit den eingegebenen oder ermittelten Daten geschieht (Nutzungsbedingung, Datenschutzerklärung) und ob von dem (angeblichen) Sicherheits-Tool nicht selbst eine Bedrohung ausgeht. Statt eines hilfreichen System-Scans könnte der Online-Test schließlich auch Schadsoftware installieren oder nach vertraulichen Informationen suchen wollen.

Es ist ratsam, vor der Verwendung von Security-Assessment-Tools eine spezielle IT-Sicherheitsrichtlinie zum Umgang mit diesen Werkzeugen einzusetzen. Dazu gehören die erwähnte Prüfung von Impressum, Nutzungsbedingungen und Datenschutzerklärung sowie eine Kontrolle, ob sich hinter dem Online-Dienst eine schadhafte Website verbirgt (beispielsweise durch Verwendung eines Link-Scanners). Auf keinen Fall sollten die eigenen Sicherheitslösungen deaktiviert werden, um angeblich den Sicherheitstest zu ermöglichen. Dann würde die Suche nach Risiken selbst zum Risiko.

Oliver Schonschek

1.10 Was mit den Online-Daten Verstorbener geschieht

Schluss. Aus. Ende. Am Ende eines Menschenlebens steht der Tod. Das Nichts. Das Paradies. Oder was auch immer man glauben mag. Am Ende eines Internetlebens hingegen steht ein großes Fragezeichen. Was ist mit den zahllosen digitalen Identitäten, den Social-Network-Profilen, den E-Mail-Postfächern, den unzähligen elektronischen Unterlagen, digitalen Familienfotos, persönlichen MP3- und Filmsammlungen, die auf Festplatten, DVDs, USB-Sticks und im Web schlummern, wenn ihr Besitzer nicht mehr da ist?

Hand aufs Herz – wer hat sich schon einmal mit dem eigenen Tod beschäftigt? Na klar, wenn jemand stirbt, der einem nahesteht, kommen wohl jedem die Gedanken zumindest kurz in den Kopf. Doch welcher „Digital Native“, also nach 1980 Geborene, hat sein Testament heute bereits gemacht und dabei seine digitalen Daten mit berücksichtigt? Ist es doch gerade diese Altersgruppe, die zu großen Teilen online lebt, mehr digitale Freundschaften als persönliche pflegt, wichtige Verträge und Dokumente nur noch digital verwaltet, lieber via Sofortnachricht, SMS und E-Mail korrespondiert. Umso wichtiger, einmal kurz in sich zu gehen und den digitalen Nachlass zu regeln – oder zumindest zu wissen, inwiefern er überhaupt geregelt werden kann. Denn der Tod kommt – früher oder später – in jedem Fall irgendwann. Und es ist nicht anmaßend zu behaupten, dass das Internet und damit unsere digitalen Hinterlassenschaften uns alle überleben werden.

1.10.1 Neue Dienstleistungen

„Den meisten Menschen ist nicht bewusst, was sich heute bereits in ihrem digitalen Nachlass befindet“, berichtet Birgit Janetzky. Die Theologin hat vor drei Jahren Semno (www.semno.de) gegründet, einen Dienstleister, der den digitalen Nachlass Verstorbener im Auftrag der Erben regelt.

semno
für Ihr digitales Erbe

■ Startseite

Das digitale Erbe

Semno-Leistungen

Beauftragung

Das Unternehmen

Daten sind unsterblich

Wer viel Zeit am PC und im Internet verbringt, hinterlässt Spuren, die ihn überleben. Texte, Bilder, persönliche Daten im Computer und vor allem im Internet sind für die Erben nicht ohne weiteres zugänglich. Beim Anblick des geerbten Computers kommen Zweifel auf: Was musste noch erledigt und zu Ende geführt werden?

Digitalisiert über den Tod hinaus

Früher fanden die Erben wichtige Unterlagen und Fotos in Aktenordnern oder im Schreibtisch der verstorbenen Person. Heute befinden sich solche

Deutschlandweiter Service

- zum Antrag
- zur Preisliste 2013 (.pdf)

Zusätzlicher regionaler Service in Freiburg i.Br.

Semno: Gibt Hinterbliebenen die Möglichkeit, den digitalen Nachlass Verstorbener prüfen zu lassen.

Das Unternehmen analysiert deren Computer, um den Hinterbliebenen einen ersten Eindruck zu geben, welche Arten von digitalen Informationen überhaupt vorliegen. Daraus wird ein Gutachten erstellt, auf dessen Basis die Angehörigen über das weitere Vorgehen entscheiden können. Auf Wunsch kümmert sich Semno dann auch um die Kündigung von Verträgen, E-Mail-Konten oder Social-Network-Profilen.



Theologin: Birgit Janetzky bietet neben der rein technischen Dienstleistung auch Trauerbegleitung an. (Quelle: Birgit Janetzky / Semno)

Ihr theologischer Hintergrund und jahrelange Berufserfahrung in der Bestattungsbranche erlauben es Janetzky, Angehörige auch in psychologischer Hinsicht betreuen zu können, wenn ein nahestehender Mensch verstorben ist. „Wir erbringen nicht nur eine rein technische Dienstleistung“, erklärt sie. Groß ist die Nachfrage trotz dieser ratsamen Kombination dennoch nicht – viel häufiger ist Janetzky als Vortragsrednerin unterwegs und referiert zum Thema „digitaler Nachlass“. „Der einem Menschen nahe Tod ist ein großes Tabuthema, ganz im Gegensatz zum öffentlichen Tod in den Medien“, bringt sie es auf den Punkt.

1.10.2 Rechtliche Unsicherheit

Diese Tabuisierung sorgt auch dafür, dass das Thema „digitales Erbe“ selbst bei vielen Nachlassverwaltern, Notaren und Juristen bisher kaum auf der Tagesordnung auftaucht und es keine allgemeinverbindliche Rechtsprechung hierzu gibt.

Thomas Schulte (www.dr-schulte.de), Rechtsanwalt und Gründungspartner seiner Berliner Kanzlei, erklärt: „Der materielle digitale Nachlass, zum Beispiel die Festplatte des Computers oder das Handy, geht nach § 1922 BGB an die Erben über, sofern im Testament nichts anderes geregelt wurde. Diese können dann entscheiden, was mit den dort gespeicherten Daten geschehen soll.“ Das müsse nicht unbedingt im Sinne des Erblassers sein – schließlich werde auch beispielsweise das Urheberpersönlichkeitsrecht vererbt („Cosima-Wagner-Urteil“, BGHZ 249-262).

Führte der Verstorbene also zum Beispiel ein Tagebuch, entscheiden die Erben, was mit diesen Aufzeichnungen geschieht – das gilt entsprechend auch für digital

vorliegende Texte oder Videologs. Schulte empfiehlt, testamentarisch zumindest mitzuverfügen, was mit lokal gespeicherten digitalen Daten geschehen soll.

Schwieriger zu klären sei die Frage nach dem Verbleib immaterieller Daten – also Daten, die nicht lokal, sondern im Web gespeichert sind. Hier entscheide „jeder Betreiber einer Online-Plattform zurzeit selbst, ob er die Daten den Erben preisgibt oder nicht“. Das sei insofern von Nachteil, als damit die geltenden Regelungen von Plattform zu Plattform verschieden seien und beispielsweise auch nicht kontrolliert werden könne, ob Daten Verstorbener beispielsweise für Online-Banking weiterbenutzt würden.

Rechtsanwalt: Thomas Schulte hat sich intensiv mit den rechtlichen Fragen des digitalen Nachlasses beschäftigt. (Schulte und Partner Rechtsanwälte)



„Wenn ein Betreiber wie Facebook in seinen Allgemeinen Geschäftsbedingungen stehen hat, dass er über sämtliche gespeicherten Informationen nach Belieben verfügen darf, gilt das auch für die Daten von verstorbenen Nutzern.“ Er könne sogar festlegen, dass den Erben der Zugriff auf das Nutzerkonto oder Profil verweigert werde. Soll heißen: Stirbt der Nutzer, bevor er testamentarisch etwas anderes verfügt hat, sind die Angehörigen auf den guten Willen eines Konzerns angewiesen. Bei deutschen Anbietern beispielsweise beißen sie in jedem Fall auf Granit, denn hierzulande gelten entsprechende Datenschutzgesetze. Angela Rittig, Pressesprecherin beim Business-Netzwerk Xing (www.xing.com/de), erklärt: „Angehörigen kann der Zugriff auf den Account nicht ermöglicht werden, denn wir geben keine personenbezogenen Daten an Dritte weiter.“

1.10.3 Streitthema E-Mail

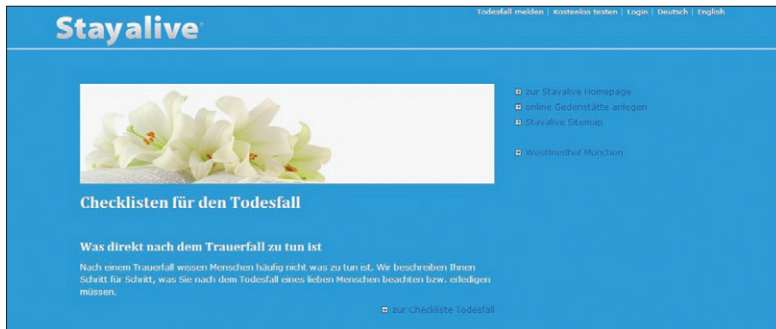
Anders sieht es bei US-Anbietern wie Facebook aus. Zwar sei die Wirksamkeit derartiger AGB-Klauseln rechtlich noch ungeklärt, weil es noch keinen Präzedenzfall gegeben habe, erläutert Schulte. Wer Rechtsstreitigkeiten vermeiden möchte, sollte aber vorbauen und testamentarisch festhalten, ob Erben derartige Dienste einsehen dürfen oder nicht.“ Es könne auch ratsam sein, die Zugangsdaten einem engen Vertrauten mitzuteilen, der dann von sich auf entsprechende Services zugrei-

fen könne, um Probleme gar nicht erst aufkommen zu lassen, empfiehlt der Rechtsanwalt. Strittig unter Juristen ist zudem der Umgang mit den E-Mail-Postfächern von Verstorbenen. Es sei rechtlich nicht geklärt, ob Hinterbliebene entsprechende Konten einsehen dürften. Selbst wenn sie offizielle Belege für den Tod eines Menschen vorlegten, könne ein Mail-Provider trotzdem noch selbst entscheiden, ob er den Erben die Zugangsdaten weiterleitet oder nicht, so Schulte. Vorsicht sei in jedem Fall geboten: „Wird das Konto einfach gelöscht, könnten wichtige Daten des Verstorbenen, die das Erbe betreffen, wie zum Beispiel Versicherungsverträge, verloren gehen.“

Der Rechtsanwalt weist abschließend darauf hin, dass bei der Vielzahl digitaler Persönlichkeiten den Angehörigen oftmals gar nicht bekannt sein könne, wo ein Verstorbener überall Spuren hinterlassen hat. Umso wichtiger seien testamentarische Regelungen zu Lebzeiten. Ideal sei es natürlich, eine gesetzliche Regelung zum Thema „immaterieller digitaler Nachlass“ zu erreichen – da sich das Internet aber nicht in nationalen Grenzen bewege, sei das quasi aussichtslos.

1.10.4 Sie beißen nicht

Nun könnte man fast befürchten, Online-Anbieter seien pietätslos und unheimlich umständlich, was die Abschaltung von Nutzerprofilen und die Herausgabe respektive Löschung persönlicher Daten von verstorbenen Nutzern angeht. Zum Glück ist das aber nicht die Regel.



Virtuelles Weiterleben: Online-Friedhöfe wie StayAlive wollen Verstorbenen auch ein digitales Andenken bewahren.

Rittig erklärt das Vorgehen bei Xing: „Üblicherweise werden wir bei Todesfällen sehr zeitnah durch die Netzwerkkontakte informiert. Selbstverständlich können sich auch die Hinterbliebenen per Mail oder telefonisch an unseren Kundenservice wenden. Auf Basis dessen schalten wir die Profile inaktiv, also für andere Mitglieder unsichtbar. Endgültig gelöscht werden sie erst nach etwa drei Monaten. So

vermeiden wir, dass bei Verwechslungen oder Namensgleichheit versehentlich Profile anderer Mitglieder gelöscht werden. Gleichzeitig entsprechen wir damit dem Wunsch vieler Angehöriger, dass ein Profil unmittelbar nicht mehr vorhanden sein soll.“ Facebook bietet zudem die Möglichkeit, Nutzerprofile in öffentliche Gedenkseiten umzugestalten. Webmail-Provider wie United Internet funktionieren Postfächer auf Wunsch der Angehörigen auch schon mal zu elektronischen Kondolenzbüchern um (siehe auch Interview mit Thomas Plünnecke am Ende dieses Artikels).



Über den Tod hinaus: Über GrabSicht.de können Angehörige die Gräber Verstorbener online pflegen.

Und danach? Eine digitale Existenz endet schließlich nie, trotz aller Verfügungen, Bemühungen und Services. Keine Sorge: Als letzte Ruhestätte bieten sich virtuelle Friedhöfe wie StayAlive (www.stayalive.com/de) an. Selbst echte Gräber lassen sich von daheim aus online pflegen – laut Anbieter GrabSicht (www.grabsicht.de) „so einfach, schnell und sicher wie Pizza bestellen“. Das ist nur konsequent: Wo das Leben immer digitaler wird, gilt für das Sterben das Gleiche.

1.10.5 Was die Anbieter sagen

Thomas Plünnecke, Pressesprecher bei United Internet (www.united-internet.de) für die E-Mail-Dienste GMX und Web.de, beantwortet im Interview mit unserer Schwesterpublikation „Computerwoche“ einige Fragen zum Umgang mit einem Nutzerkonto, wenn dessen Besitzer nicht mehr lebt.

CW: Wie verfährt United Internet mit Postfächern von Verstorbenen?

Plünnecke: Um den Datenschutz zu beachten und böswilligen Telefonstreichen entgegenzuwirken, benötigen wir grundsätzlich immer einen eindeutigen Nach-

weis, bevor wir Anfragen von Hinterbliebenen beantworten oder deren Wünschen nachkommen können. Will der Erbe den Vertrag lediglich kündigen, ohne Zugriff auf das Postfach zu erhalten, ist die Sterbeurkunde erforderlich. Um Zugang zum Postfach des Verstorbenen zu erlangen, muss uns der Erbberechtigte den Erbschein vorlegen und sich ausweisen.

Der Erbe muss den Zugriff auf das Postfach des verstorbenen Nutzers zudem mit einem handschriftlich unterschriebenen Schriftstück beantragen. Gibt es mehrere Erbberechtigte, ist die Zustimmung der Mehrheit der erbberechtigten Personen erforderlich. Dies erfolgt in der Regel über eine Vollmacht.



Thomas Plünnecke: Pressesprecher bei United Internet für die Dienste Web.de und GMX. (Quelle: United Internet)

CW: Inwiefern ist das Verfahren bei FreeMail-Nutzern anders als bei zahlenden GMX-ProMail/Web.de-Club-Nutzern?

Plünnecke: Im Unterschied zu kostenpflichtigen Tarifen, bei denen sich die Erbberechtigten meist nach einer der nächsten Abbuchungen direkt mit unserem Kundenservice in Verbindung setzen, um das weitere Vorgehen zu regeln, bleiben FreeMail-Konten oft verborgen. Wenn sich die Angehörigen nicht bei uns melden, bleibt der Account deshalb zunächst unverändert bestehen. Ist ein Postfach sechs Monate inaktiv – also kein Login erfolgt, kein Abruf über POP3 oder IMAP –, wird der Nutzer per E-Mail informiert. Soweit eine alternative E-Mail-Adresse vom Nutzer hinterlegt wurde, wird die entsprechende Info auch an diese Adresse gesendet. Passiert daraufhin nichts, wird das Konto auf inaktiv gestellt. Die Adresse lässt sich jetzt noch ein halbes Jahr lang reaktivieren. Nach Ablauf dieser Zeit ist die E-Mail-Adresse wieder frei verfügbar.

CW: Was geschieht mit den entsprechenden Nutzerdaten in Ihrer Datenbank?

Plünnecke: Wenn die Angehörigen dies wünschen und alle erforderlichen Dokumente (etwa den Erbschein) vorliegen, werden die Nutzerdaten nach Löschung des Accounts auch physikalisch von unseren Servern entfernt. Selbstverständlich haben die Erbberechtigten auch die Möglichkeit, das E-Mail-Postfach weiterzuführen.

CW: Wie oft kommt es vor, dass Nutzer zwar verstorben sind, ihre Postfächer aber noch eine ganze Weile erreichbar sind, weil Angehörige keine Ahnung haben, dass ein Account existiert?

Plünnecke: Eine solche Statistik führen wir nicht. Da Internetanbieter wie GMX oder WEB.DE natürlich nur durch die Hinterbliebenen vom Tod eines Nutzers erfahren können, die Hinterbliebenen selbst aber insbesondere bei FreeMail-Accounts häufig nicht über den digitalen Nachlass informiert sind, ist das durchaus möglich.

CW: Gibt es eine Möglichkeit zur Vorausverfügung, was mit Nutzerdaten/Postfächern/anderen gespeicherten Daten post mortem geschieht?

Plünnecke: Unser Kundenservice ist die erste Anlaufstelle für alle Fragen. Sollte es juristischen Klärungsbedarf geben, unterstützen die Mitarbeiter der Rechtsabteilung praxisbezogen. Da sich die vorhandenen Prozesse und Strukturen bewährt haben, sind spezielle Services wie eine Art Testamentfunktion derzeit nicht geplant. Wenn sich herausstellen sollte, dass die Mehrheit unserer Nutzer dies wünscht, werden wir selbstverständlich entsprechende Optionen prüfen. Aktuell ist das Interesse jedoch eher gering. So erreichen uns zum digitalen Nachlass insgesamt nur einige wenige hundert Anfragen pro Jahr. Zum Vergleich: GMX und WEB.DE haben mehr als 30 Millionen Mail-Accounts.

CW: Gab es Fälle, in denen Postfächer zunächst auf ausdrücklichen Wunsch als Art „Kondolenzbuch“ erreichbar blieben?

Plünnecke: Ja, das kommt vor. Mir ist beispielsweise der Fall einer Witwe bekannt, die das E-Mail-Postfach ihres verstorbenen Mannes als Kondolenzadresse nutzen und über dessen einstigen Account unter anderem auch Bekannten das traurige Ereignis mitteilen wollte.

CW: Was empfehlen Sie Ihren Kunden, was den Verbleib ihrer Daten post mortem angeht? Was empfehlen Sie Angehörigen?

Plünnecke: Es ist auf jeden Fall ratsam, den digitalen Nachlass frühzeitig zu klären. Sind die entsprechenden Vertragsverhältnisse den Angehörigen bekannt, können sie nach dem Tod in der Regel ohne „buchhalterischen Anstoß“ beendet beziehungsweise weiterverwaltet werden. Auch in einem Testament lässt sich selbstverständlich genau festhalten, wer später einmal Zugang zu welchen Internetdiensten haben soll – und wer vielleicht gerade nicht.

Simon Hülsbömer



Simon Hülsbömer verantwortet redaktionell leitend die Themenbereiche IT-Sicherheit, Web und Datenschutz. Außerdem betreut der studierte Media Producer den täglichen Früh-Newsletter und ab und an die iPad-Ausgaben der COMPUTERWOCHE. Aufgaben als Online-News-Aushelfer, in der Traffic- und Keyword-Analyse, dem Content Management sowie die inoffizielle Funktion „redaktioneller Fußballexperte“ runden sein Profil ab.

2 Sicherheit im Unternehmen

Ziel aller präventiven IT-Sicherheitsprozesse ist das Vorbeugen von Server- und Client-Ausfällen, Datenverlust und Sabotage. Neben geeigneten technischen Voraussetzungen gilt es, Sicherheits-Policies einzuführen und das Sicherheitsbewusstsein bei Anwendern und Vorgesetzten zu schärfen. Nur ein kooperatives Zusammenwirken aller Beteiligten führt zu einer deutlichen Verbesserung der IT-Sicherheitslage in Unternehmen jeder Größe.

2.1 Intranator Business Server – Groupware- und Security-Lösung für kleine Unternehmen

Intranator Business Server der Tübinger Intra2net AG (www.intra2net.com/de/produkte/intranator.php) ist als Groupware-Server konzipiert und bietet abgesehen von Security-Services keine weiteren Funktionen, auch keinen File-Server und keine Active Directory Services. Das Produkt adressiert primär kleine Unternehmen bis 50 Benutzer.

Ebenso ist Intranator Business Server kein Community-Projekt, sondern wird vollständig von Intranet2net entwickelt und vertrieben. Es gibt eine 30-Tage-Testversion von Intranator Business Server sowie des Intranator Groupware Clients für die Outlook-Anbindung zum Herunterladen. Die Preise für die Software sowie drei optional angebotene Hardwareversionen der Appliance finden sich in der Preisliste (www.intra2net.com/de/download/intra2net_preisliste.pdf). Intranator Business Server wird nicht im Subskriptionsmodell vertrieben.

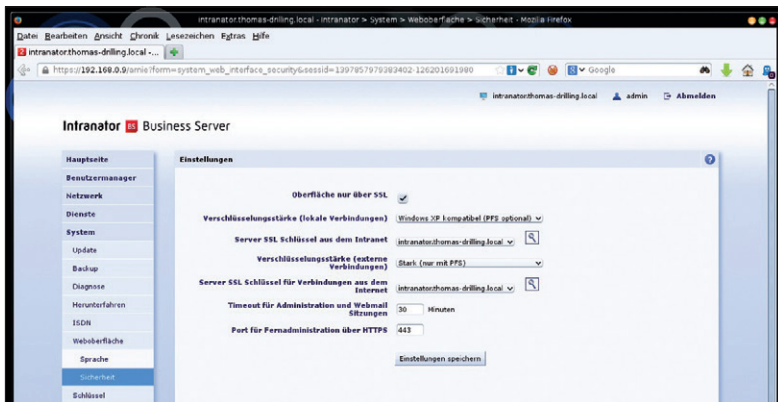
In der Staffelfung für 10 bis 24 Nutzer kostet die Lizenz einschließlich zwölf Monate Updates, Antivirus und Spamfilter 48 Euro pro Nutzer und Jahr; zwölf weitere Monate Updates kosten 40 Euro pro Nutzer und Jahr. Damit fallen für die Lösung beispielsweise für zehn Nutzer einschließlich drei Jahren Updates 1.280 Euro an. Ergänzend zum Endkunden-Support durch Vertriebspartner bietet Intra2net auch direkt Endkundenunterstützung per E-Mail. Wer nur die Software erwerben möchte, findet online die unterstützte Hardware. Weitere Details liefern die Datenblätter (www.intra2net.com/de/download/datenblaetter.php) und Handbücher.

2.1.1 Funktionen von Intranator Business Server

Intranator Business Server basiert vollständig auf Open-Source-Komponenten. Fundament ist die eigene 32Bit-RPM-Distribution mit PAE-Kernel. Intra2net baut sämtliche RPM-Pakete selbst auf Basis von Quellpaketen aus dem Red-Hat-

Umfeld (Fedora, CentOS), verwendet einen individuell angepassten Kernel und pflegt ein eigenes Paketdepot. Regulär veröffentlicht Intra2net alle sechs Wochen ein Update, sicherheitskritische Updates sind innerhalb von 48 Stunden verfügbar.

Da die Software als Appliance konzipiert ist, hat der Systemverwalter während der Installation mit Ausnahme der Netzwerkeinstellungen und der Wahl des root-Passworts keinen Einfluss auf die Konfiguration; eine vorhandene Festplatte wird vollständig für Intranator Business Server veranschlagt. Die weitere Konfiguration findet über das ansprechende Web-Interface statt, das per Default via SSL unter der angegebenen IP-Adresse erreichbar ist. Nach dem Einstellen der Art der Internetverbindung über ein Profil im Menü *Netzwerk / Provider / Profile* (z.B. „über einen Router im lokalen Netzwerk“) ist Intranator Business Server einsatzbereit.



Intranator Business Server: SSL ist nicht per Default eingerichtet, sondern lässt sich auch im Detail konfigurieren. So ist die Verschlüsselungsstärke unter anderem per Default auf PFS gesetzt.

Das Web-Interface bietet auf der Hauptseite Statusinformationen zum laufenden Betrieb und erlaubt das direkte Auswählen von Profilen für Internetzugang oder VPN. Das Web-Interface offeriert darüber hinaus die Möglichkeit zum Anlegen und Verwalten von Benutzern, zur vollständigen Kontrolle der Netzwerkeinstellungen (Internet, Intranet, Firewall, DNS, Netzwerkkarten) und zum Einrichten des Fernzugriffs sowie für das Verwalten der von Intranator Business Server zur Verfügung gestellten Dienste.

Deren Anzahl ist mit Mail, Spam, Antivirus, Proxy, Fax, DynDNS, VPN, Monitoring und Zeitserver relativ übersichtlich. Im Menü *System* kann der Administrator zudem Backups einleiten, von Intra2net bereitgestellte Updates einspielen, Diagnosefunktionen ausführen, seine Zertifikate verwalten, RAID- und USV-Systeme konfigurieren oder einen Fernzugang für Mitarbeiter von Intra2net freischalten. Außerdem können Nutzer über das Menü „Groupware“ auf das Web-Interface des auf dem Horde-Framework basierenden Groupware-Systems zugreifen.

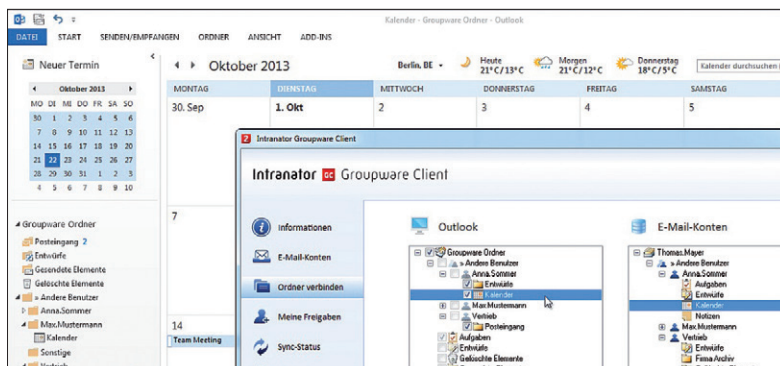
2.1.2 Der Groupware Server im Detail

Im Detail kommt die Horde-Groupware-Suite als Webmailer, Kalender, Kontakt-Datenbank, Task-Manager und Notiz-Verwalter auf Basis des Kolab-XML-Format und einem Cyrus-IMAP-Server als Speicher-Back-End zum Einsatz.

Das Horde-Framework zählt zu den funktionsreichsten Webmailern, auch wenn Bedienung sowie Look&Feel trotz Drag&Drop-Support nicht an die modernen HTML5/ExtJS-Clienten von Zafra oder Open-Xchange heranreicht. Optional steht ein von Intra2net selbst entwickelter MAPI-Connector für den Einsatz von MS Outlook als Client zur Verfügung, der das optisch nicht ganz zeitgemäße Web-Interface wettmacht. Dieser (inzwischen steht Version 2.2.2 parat) unterstützt alle Outlook-Versionen von 2003 bis 2013 (auch ein Mischbetrieb ist problemlos möglich), läuft sehr stabil und weist gegenüber einem echten Gespann mit Exchange/Outlook kaum Defizite auf. So fehlt etwa eine Journalfunktion. Der Connector ist wie gewohnt als EXE-Datei auf dem Windows-Client-Arbeitsplatz zu installieren und stellt den MAPI-Provider auf der Client-Seite zur Verfügung. Beim Intranator Business Server ist beim Anlegen eines entsprechenden Outlook-Profiles darauf zu achten, dass der Admin als Servertyp nicht „Zusätzliche Servertypen“, sondern „IMAP“ wählt, weil das Horde-Framework über das Kolab-XML-Format sämtliche Funktionen in einem IMAP-Server als Speicher-Back-End abbildet.

2.1.3 Outlook- und Smartphone-Unterstützung

Ansonsten steht der Funktionsumfang dem eines Exchange-Server kaum nach, im Gegenteil: Nutzer können mit Intranator Groupware Client individuelle Ordnerstrukturen aus beliebigen Serverordnern kombinieren. Das klappt sowohl mit persönlichen Ordnern als auch mit Freigaben. Nutzer können Ordner außerdem lokal speichern und nach Bedarf synchronisieren.



Der Groupware-Client: Nutzer können Ordner verbinden.

Die Synchronisation lässt sich jederzeit unterbrechen und wird automatisch an der richtigen Stelle fortgesetzt, wobei die jeweils neuesten Objekte zuerst synchronisiert werden, sodass externe Nutzer mit den aktuellen Daten arbeiten können, während ältere Daten noch im Hintergrund übertragen werden. Ferner können Nutzer innerhalb eines E-Mail-Profiles mehrere Konten von unterschiedlichen Servern über separate Datendateien verwalten. Zusätzlich werden Outlook-Kontaktgruppen automatisch synchronisiert.

Seit Version 6.1 beherrscht Intranator Business Server auch die Datensynchronisation via ActiveSync für iOS, Android und Windows Phone. Die Push-Technologie basiert auf einer Open-Source-Implementierung von ActiveSync 14.1 und sorgt für eine automatische Synchronisation von E-Mails, Kalendern und Kontakten.

2.1.4 Fazit, Pro und Contra

Unternehmen, die in erster Linie einen Ersatz für MS Exchange suchen, sollten durchaus einen Blick auf Intranator Business Server werfen. Der bietet kleinen Unternehmen eine funktionierende Groupware mit Outlook- und ActiveSync-Anbindung, basiert auf einem stabilen Kernel, versorgt Anwender zeitnah mit Patches und lässt sich als Appliance out-of-the-box einsetzen.

2.1.5 Pro und Contra Intranator Business Server

Vorteile

- als Appliance (sehr einfache Installation), auf Wunsch auch mit zertifizierter Hardware, verfügbar
- viele Sicherheitsfunktionen einschließlich Antivirus, Antispam und VPN
- integrierte Groupware mit Outlook-Anbindung und ActiveSync-Support

Nachteile

- Funktionsumfang auf Groupware und UTM beschränkt, kein Active Directory, keine Datei-Services
- nicht ganz zeitgemäßes Web-Interface
- keine Community-Version verfügbar

Thomas Drilling

Thomas Drilling ist freier Autor und befasst sich schwerpunktmäßig mit dem Themen Linux und Open-Source-Software.

2.2 SSL – beliebt, aber gefährlich

Durch die „Heartbleed“-Sicherheitslücke ist das SSL/TLS-Netzwerkprotokoll ein wenig in Verruf geraten – nicht zum ersten Mal. Wahr ist aber auch: Unternehmen haben für die Absicherung ihres Datenverkehrs keine wirkliche Alternative.

20 Jahre ist es her, dass Browser-Pionier Netscape die erste Version des SSL-Protokolls veröffentlicht hat – heute offiziell als TLS (Transport Layer Security) bekannt. In den frühen Tagen des Internets entwickelt, sollte SSL das Kommunikationsprotokoll TCP/IP um Funktionen für Sicherheit und Authentifizierung erweitern, weil dieses für solche Aufgaben nicht vorgesehen war. So sollte zumindest das Auslesen abgegriffener Inhalte verhindern werden, wenn Hacker es geschafft hatten, sich in die Verbindung zwischen zwei Rechnern einzuklinken.

Heute ist SSL der Standard schlechthin für sichere Kommunikation im Internethandel, beim E-Banking und für die Nutzung von Web- respektive Cloud-basierten Business-Plattformen. Auf ihrer Reise durch das Netz soll das Verschlüsselungsprotokoll sensible Daten vor Diebstahl und Manipulation schützen. Etwa ein Viertel des Datenverkehrs in Unternehmen läuft über das SSL-Protokoll, in der Finanz- oder Gesundheitsbranche sogar die Hälfte aller Daten.

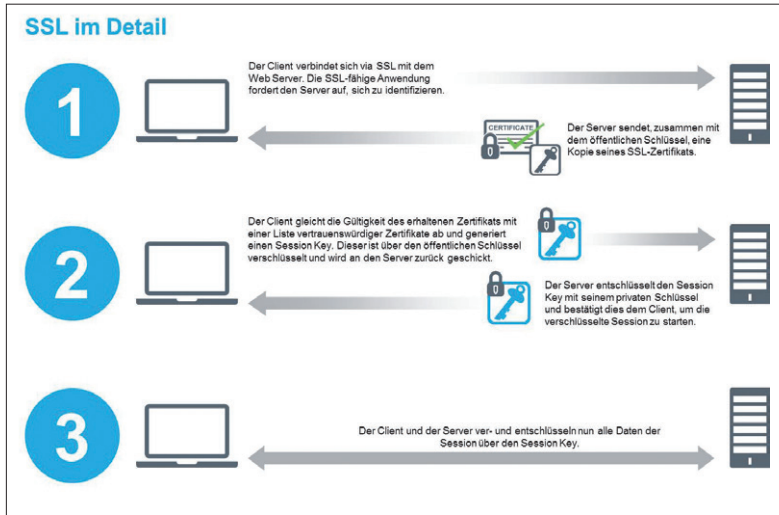
Weil die Nutzer heute zunehmend für Sicherheitsaspekte sensibilisiert sind und die Einbettung von Verschlüsselungstechniken auch für Hersteller und Integratoren einfacher wird, liegen beliebte (Web-)Anwendungen heute zunehmend in verschlüsselter Version vor. Marktauguren gehen davon aus, dass der SSL-Verkehr im Internet künftig um bis zu 20 Prozent pro Jahr zulegt.

2.2.1 Funktionsweise des Protokolls

SSL gewährleistet einen sicheren und vertraulichen Datenaustausch, indem es Funktionen für Authentifizierung, Verschlüsselung und Datenintegrität bereitstellt. Der Client kann sich sicher sein, dass der aufgerufene Server auch wirklich derjenige ist, der er vorgibt zu sein (Authentifizierung). Vertrauliche Daten wie beispielsweise Kreditkartennummern oder Passwörter werden verschlüsselt übertragen und können, selbst wenn es gelingt, sie abzufangen, nicht ausgelesen oder manipuliert werden (Datenintegrität). Die Basis bilden Zertifikate, anhand derer sich SSL-fähige Browser und Server gegenseitig identifizieren können. Sie werden von professionellen Dienstleistern ausgegeben und erfüllen gleichsam die Funktion eines fälschungssicheren Personalausweises. Schließlich prüfen die Zertifikatanbieter vor der Ausgabe von Prüfsiegeln die Identität der anfragenden Organisation, um die Sicherheit auch tatsächlich zu gewährleisten.

Eine SSL-Transaktion wird vom Client initiiert und ist am Protokollnamen „https“ in der Adressleiste des Browsers erkennbar. Sie besteht aus zwei Phasen: dem SSL-Handshake, bei dem die Schlüssel ausgetauscht werden, wodurch die Authentifizierung erfolgt, und dem eigentlichen Datentransport. Beim Handshake ver-

schlüsselt der Urheber die gefragten Inhalte mit dem öffentlichen Schlüssel des Servers. Entschlüsselt und damit verifiziert werden diese durch den privaten Schlüssel des Empfängers.



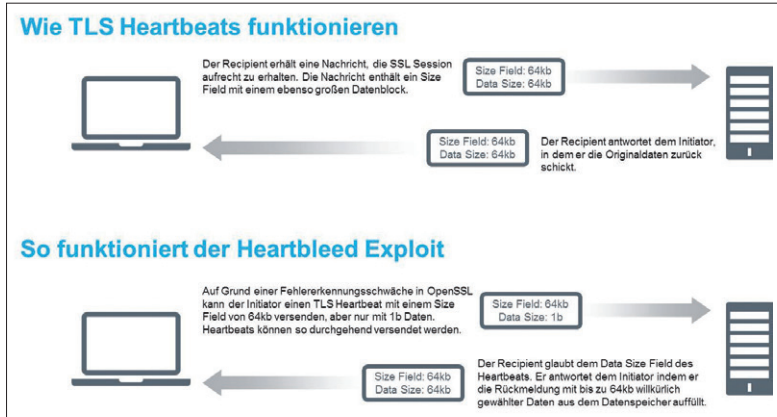
Technikdetails: Das SSL- respektive TLS-Protokoll arbeitet nach einem dreistufigen Prozess.
(Quelle: Blue Coat)

Die beiden Kommunikationspartner einigen sich im nächsten Schritt auf einen sogenannten Session Key, der während dieser Sitzung zur Verschlüsselung der ausgetauschten Daten benutzt wird. Selbst wenn Kriminelle diese Daten abfangen, können sie nichts damit anfangen, da die 128- beziehungsweise 256-Bit-Verschlüsselung so lang und komplex ist, dass sie selbst mit fortschrittlichen Methoden nur mit sehr hohem Aufwand und viel Zeit geknackt werden kann.

2.2.2 Heartbleed zeigt: SSL ist verletzlich

„Heartbleed“, die schwerwiegendste Sicherheitslücke seit Langem, zeigt jedoch, dass auch das SSL/TLS-Protokoll nicht unantastbar ist. Angreifer finden trotz aller Vorkehrungen immer Wege und Möglichkeiten, unbemerkt Inhalte aus dem Arbeitsspeicher auszulesen und damit auf sensible Daten zuzugreifen. Auch im Apple-Betriebssystem iOS konnten Hacker eine Lücke in der SSL-verschlüsselten Kommunikation ausnutzen („GoToFail“). So untergraben sie die gesamte Sicherheit eines Systems, wenn die Lücke nicht sofort durch ein Patch geschlossen wird. Nichtsdestotrotz ist SSL heutzutage die sicherste Methode für IP-Kommunikation.

Heartbleed und GoToFail müssen jedoch als wichtige Hinweise darauf verstanden werden, dass SSL-verschlüsselter Datenverkehr keine hundertprozentige Immunität gegen Angriffe gewährt.



Kleiner Workshop: Wir erklären, wie und warum „Heartbleed“ funktionieren konnte. (Quelle: Blue Coat)

Ein weiterer entscheidender Malus steckt gerade in der Stärke von SSL. Der Umstand nämlich, dass nur Absender und Empfänger die Inhalte lesen können, führt dazu, dass die derart abgesicherten Datenpakete auch die Sicherheitssperren, die das Unternehmensnetzwerk schützen sollen, unkontrolliert passieren können. Viele Sicherheitslösungen wie Firewalls und Intrusion-Detection/Prevention-Systeme können die verschlüsselten Daten nicht lesen und schleusen sie ungeprüft durch. Unter dem Deckmantel SSL können Kriminelle Schadsoftware in Unternehmenssysteme einschleusen, und vertrauliche Daten können unentdeckt versendet werden. Laut einer Schätzung Gartners (www.gartner.com/doc/2635018/security-leaders-address-threats-rising) werden bis 2017 mehr als die Hälfte aller Angriffe auf Unternehmen über einen solchen verschlüsselten Weg geführt werden. Zurzeit liegt diese Quote bei gerade einmal fünf Prozent.

2.2.3 Abhilfe schaffen

Festzustellen, ob sich in einer SSL-verschlüsselten Datei Schadsoftware verbirgt, kann das aktuelle Security-Policy-Enforcement vieler Unternehmen nicht leisten. Dazu bedarf es einer modernen „Advanced Threat Protection“ (ATP). Eine solche SSL-Visibility-Lösung leitet dazu die entschlüsselten Daten zur Überprüfung an Sicherheitslösungen wie Malware-Prevention-Systeme beziehungsweise Next-Generation-Firewall-, Intrusion-Detection- oder Data-Loss-Prevention-Systeme weiter. Diese blockieren dann unerwünschten und schadhaften Datenverkehr.

Sind die Inhalte hingegen in Ordnung, werden sie an die SSL-Appliance zurückgeleitet und dort erneut verschlüsselt und an den Empfänger übertragen.

Bleibt die Frage, wie es um die Vertraulichkeit und Integrität der betroffenen Daten bestellt ist, wenn sie zwar per SSL übertragen, auf dem Transportweg durch die ATP aber trotzdem ausgelesen werden können. Es wird gerade dann „kribbelig“, wenn es um Gehälter, Pensionen oder gesundheitliche Themen geht.

Ein eindeutige Antwort gibt es nicht: Sicherheit ist nicht mehr nur ein technologisches Problem, das mit Technologie gelöst werden kann. Vielmehr sind es menschliche Überlegungen, die zu einer strategischen Antwort führen müssen. Bevor Unternehmen in Technologie oder Personal investieren, sollten sie ihre Rechts- und Personalabteilungen sowie ihre Mitarbeiter ins Boot holen, um zu verstehen, was auf dem Spiel steht und was man für die Sicherheit im Unternehmen tun kann. Nur dann kann eine Strategie für verschlüsselten Datenverkehr definiert werden. Danach sollten Unternehmen technologische Lösungen finden, die es ermöglichen, ihre eigene Sicherheitsstrategie zu nutzen und gleichzeitig ihre Leistungsfähigkeit beizubehalten.

Robert Arandjelovic



Robert Arandjelovic ist Director Product Marketing EMEA bei Blue Coat.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Sicherheitsrisiken in virtualisierten Umgebungen minimieren**
(www.tecchannel.de/2045345)
- **Security- und Risikomanagement in 15 Schritten**
(www.tecchannel.de/2046308)
- **Empfehlungen für ein intelligenzbasiertes Risikomanagement**
(www.tecchannel.de/2046793)
- **Cloud- und Social-Media-Daten richtig verschlüsseln**
(www.tecchannel.de/2049929)
- **Was bringt softwaregestütztes Identity & Access Management?**
(www.tecchannel.de/2053455)
- **Das Smartphone als sichere Zutrittskontrolle nutzen**
(www.tecchannel.de/2045218)
- **50 Tipps & Tricks: Facebook sicher nutzen**
(www.tecchannel.de/2055378)

2.3 Sichere E-Mail – bessere und vertrauenswürdige Kommunikation

Die Apologeten der neuen „sozialen Medien“ wie Facebook und Twitter verkünden zwar immer wieder, das Ende der E-Mail sei gekommen. Aber ebenso wenig, wie wir in absehbarer Zukunft das „papierlose Büro“ erleben werden, werden E-Mails als gängiges Mittel zur Kommunikation über das Netz verschwinden. So kommen dann E-Mails jeden Tag an fast jedem Arbeitsplatz wie selbstverständlich zum Einsatz – so selbstverständlich, dass sich viele Anwender bisher kaum Gedanken über die Sicherheit dieses Kommunikationskanals gemacht haben.

Das gewaltige mediale Echo, das die Snowdon-Enthüllungen hervorgerufen haben, hat nicht zuletzt auch viele Nutzer dazu gebracht, sich etwas eingehender mit den Sicherheitsaspekten bei Versand, Empfang und Einsatz von E-Mails zu befassen. Wir haben in unserer FAQ-Aufstellung einige wichtige Fragen, Antworten und Lösungen rund um das Thema „E-Mail sicher nutzen“ zusammengestellt.

2.3.1 Wie sicher ist der Inhalt einer E-Mail?

Es wurde schon oft geschrieben und gesagt, aber viele Anwender scheinen es immer wieder zu vergessen: Der Inhalt einer E-Mail ist grundsätzlich nicht gesichert. Alles, was ein Nutzer in einer E-Mail-Nachricht schreibt, geht im Klartext über die Verbindung. Deshalb wird eine solche Nachricht auch immer wieder gerne mit einer Postkarte verglichen: Auch die kann jeder lesen, der sie zufällig (oder absichtlich) in die Hand bekommt. Um Daten mitzulesen, die offen über eine Netzwerkverbindung gesendet werden, bedarf es zudem keiner großartigen „Hacker-Kenntnisse“: Werkzeuge zur Netzwerküberwachung – sogenannte Sniffer – wie etwa das bekannte Wireshark (www.wireshark.org) oder auch Microsofts Network Monitor (<http://blogs.technet.com/b/netmon/p/downloads.aspx>) erlauben das einfache Mitlesen der Nachrichten im Klartext.

Praxis-Tipp: Überlegen Sie immer gut, was Sie in einer Mail schreiben, und überlegen Sie, ob Sie diese Informationen auch einer Postkarte anvertrauen würden. Kreditkarten- und Bankkontodaten sowie ähnlich sensible Daten haben in einer normalen Mail nichts verloren!

2.3.2 Reicht eine AV-Lösung auf dem System zum Schutz der E-Mail?

Es ist wohl selbstverständlich, dass heute kein System mehr ohne eine entsprechende Antivirenlösung betrieben werden sollte. Doch braucht sich ein Anwender keine Gedanken mehr um die Gefahren machen, die aus den E-Mail-Nachrichten drohen, wenn sein System mit einer solchen Sicherheitslösung geschützt ist? Ein

großer Teil der Schadprogramme gelangt heute mittels einer E-Mail auf die Systeme und damit häufig auch in die Netzwerke.

Antivirenprogramme tragen dieser Entwicklung Rechnung und können häufig bereits auf dieser Ebene eingreifen. Aber gerade wenn eine der ansonsten sehr guten freien AV-Lösungen zum Einsatz kommt, kann es sein, dass diese nicht dezipiert die Nachrichten und – noch viel wichtiger – die diversen Anhänge durchsucht. Einige Anbieter stellten diese Möglichkeiten erst mit den kommerziellen Versionen ihrer Antivirenlösungen zur Verfügung. Deshalb ist eine Antivirensoftware auch in Hinblick auf die Sicherheit der E-Mail nur ein Baustein in der Abwehr von Angriffen auf die Computersysteme.

Auch die Gefahren, die beispielsweise durch den Einsatz von HTML-Nachrichten entstehen – wir gehen darauf in diesem Bericht noch detaillierter ein –, können durch diese Programme nicht erkannt und bewältigt werden.

2.3.3 Wie kann ich E-Mail-Nachrichten sicherer versenden?

Die einfache Antwort auf diese Frage lautet: Verschlüsseln Sie Ihre Nachrichten! Warum aber verschlüsseln dann nicht mehr Anwender ihre Nachrichten standardmäßig? Wer zudem einmal versucht hat, einem Geschäftspartner oder gar einer Bank oder Behörde eine verschlüsselte Nachricht zu übermitteln, wird ebenfalls festgestellt haben, dass die Verbreitung dieser Sicherheitsmaßnahme eher gering ist. Das liegt unter anderem daran, dass die Anbieter von Mail-Programmen keine entsprechende Standardlösung in ihren Produkten integrieren (oder auch nur so etwas etablieren) und viele Lösungen auf dem Markt leider recht unpraktisch in der Anwendung sind.

Lösungen zum Verschlüsseln der E-Mails: Das BSI (Bundesamt für Sicherheit in der Informationstechnik) unterstützt aktiv die Lösung GPG4win (GNU Privacy for Windows). Sie steht für Windows-Systeme zum kostenlosen Download bereit (www.gpg4win.org/download-de.html). Die Software kann nicht nur die E-Mail-Nachrichten, sondern auch Dateien und Ordner auf dem PC verschlüsseln. Die Integrität der Daten lässt sich dabei ebenfalls mittels der Software durch den Einsatz digitaler Signaturen sichern. Als Standards werden dabei OpenPGP (www.openpgp.org) und S/MIME (X.509) unterstützt. Neben dem eigentlichen Verschlüsselungsprogramm GNUPG beinhaltet das Paket eine Software mit Namen „Kleopatra“, die als Zertifikatsmanager arbeitet. Die Software ist so angelegt, dass sie sich leicht unter Windows installieren lässt. Sie arbeitet mit Windows XP (das aber aus Sicherheitsgründen gerade in diesem Zusammenhang NICHT mehr zum Einsatz kommen sollte), Vista, Windows 7 und Windows 8/8.1 zusammen und unterstützt dabei sowohl 32- als auch 64-Bit-Systeme.

Wer Microsoft Outlook in der Version 2003 oder 2007 verwendet, findet nach der Installation einen neuen Menüpunkt in seinem Programm, der ihm das Verschlüsseln und Signieren seiner Nachrichten erlaubt. Das Programm führt schon bei der

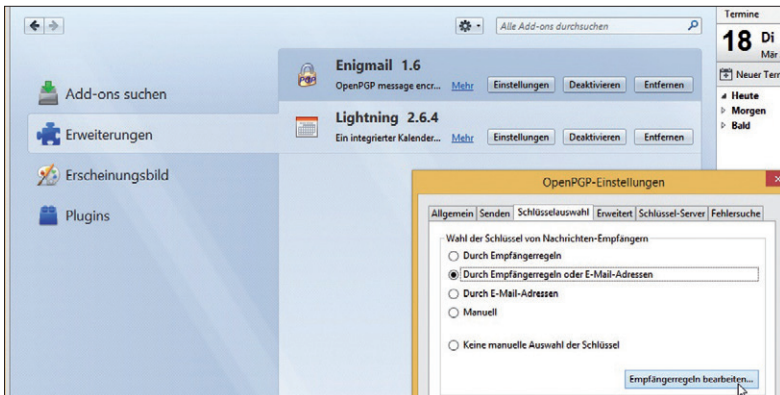
Installation durch das Anlegen eines entsprechenden Schlüsselpaares. Auch für die Outlook-Versionen 2010 oder 2013 steht jetzt ein GpgOL-Plug-in bereit, das aber nach wie vor vom Anwender ein wenig zusätzliche „Handarbeit“ erfordert, will er seine Nachrichten verschlüsseln. Wichtiger Hinweis: In allen Fällen unterstützt die Software nur die 32-Bit-Versionen von Outlook.



Verschlüsselung bringt Sicherheit: Mit der Software GPG4win steht eine Lösung zur Verfügung, die unter anderem OpenPGP auch für Windows-Systeme bereitstellt.

2.3.4 Security auch für Thunderbird

Für Anwender von Mozillas Thunderbird bietet sich die Erweiterung EnigMail (<http://enigmail.mozdev.org/>) an, die ebenfalls auf OpenPGP aufsetzt und eine entsprechende Integration in das Mail-Programm bietet: Sie ist im Gegensatz zu GPG4win nicht von der Version des Mail-Programms abhängig und arbeitete in unseren Tests problemlos auch mit der Version 13 von Thunderbird zusammen.



Auch für Thunderbird existieren entsprechende Lösungen zur Verschlüsselung: Mithilfe der Erweiterung „Enigmail“ steht der Einsatz von OpenPGP direkt im Mail-Programm zur Verfügung.

Praxis-Tipp: Wer diese beiden Anwendungen testet, wird feststellen, dass es zunächst einmal eine gewisse Lernkurve zu bewältigen gilt. Das größere Problem dürfte es aber sein, sein Gegenüber vom Einsatz einer solchen Lösung zu überzeugen – hier gilt es noch Pionierarbeit zu leisten. Unser Vorschlag deshalb: Setzen Sie eine der gängigen freien Verschlüsselungslösungen wie Truecrypt (www.truecrypt.org) ein, erzeugen damit einen sicheren Container, schreiben Ihren Text in dem Textverarbeitungsprogramm ihrer Wahl und legen ihn in diesen Container.

Dieser wird an den Empfänger als E-Mail-Attachment geschickt, das benötigte Passwort zum Entschlüsseln wird dabei natürlich auf einem anderen Weg (beispielsweise per Telefon oder persönlich) übermittelt.

Wichtig: Die meisten Verschlüsselungsprogramme bieten auch die Möglichkeit, selbst-entpackende, ausführbare Dateien zu erstellen. Auch wenn dieses Vorgehen zunächst wie eine gute Idee erscheint, sollten Sie diese Methode nicht verwenden: Diese Programme erzeugen zumeist Dateien mit der Endung *.exe, und solche Anhänge werden aus Sicherheitsgründen von einem Großteil der Mail-Server und -Gateways blockiert und nicht angenommen.

2.3.5 Warum sollte man keine HTML-Nachrichten verwenden?

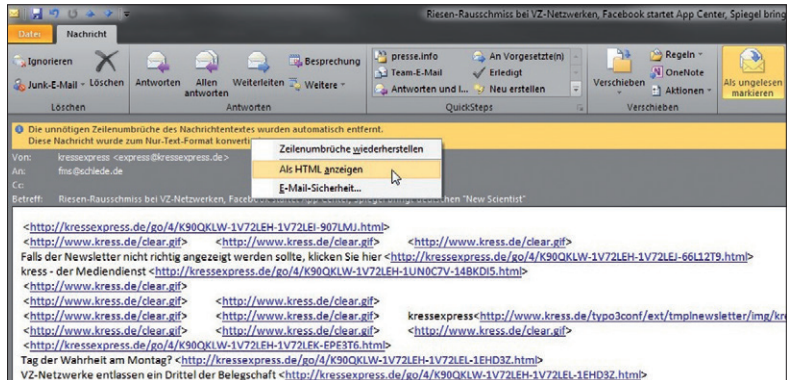
Reine Textnachrichten sind langweilig – jedenfalls scheinen das sowohl die Entwickler der meisten E-Mail-Programme als auch die Absender eines Großteils der Nachrichten zu meinen: Nachrichten im HTML-Format sind zumeist Standard. Vom Standpunkt der Sicherheit aus betrachtet stellt der Einsatz dieses Formats allerdings ein erhebliches Risiko da. Durch die Möglichkeit, in HTML auch entsprechende Skripte einzubetten, können so ungewollt potenziell gefährliche Programme auf den Rechner gelangen. Auch wenn die Nachrichten dann keine „bunten“ Überschriften und eingebetteten Bildern bieten – das reine Textformat ist der sicherere Weg.

2.3.6 Welche Sicherheitseinstellungen sind bei Outlook sinnvoll?

In Zusammenhang mit der vorherigen Frage ist es zunächst einmal sehr sinnvoll, das Mail-Programm so zu konfigurieren, dass es automatisch alle Nachrichten nur noch im Textformat anzeigt. Dies gelingt in neueren Outlook-Versionen über das sogenannte Vertrauensstellungscenter (bis Outlook 2007) oder Sicherheitscenter (ab Outlook 2010).

Erreicht werden können diese Einstellungen über den Weg: Datei/Optionen/Sicherheitscenter/Einstellungen für das Sicherheitscenter/E-Mail-Sicherheit. Dort kann ein Anwender festlegen, dass Standardnachrichten (und auch signierte

Nachrichten) nur im Textformat angezeigt werden. Zeigt sich beim Lesen einer derart konvertierten E-Mail, dass sie im Textformat nur schwer oder überhaupt nicht lesbar ist, lassen sich die ursprünglichen Formatierungen wiederherstellen. Dies geschieht per Mausklick auf „als HTML anzeigen“. Bitte nur anwenden, wenn die Nachricht aus einer verlässlichen Quelle stammt!



Mit einem Klick rückgängig: Ist die Nachricht im Nur-Text-Format nur noch schlecht oder überhaupt nicht mehr zu lesen und kann man sich sicher sein, dass sie von einem vertrauenswürdigen Absender stammt, so kann sie mittels eines Klicks wieder im HTML-Format angezeigt werden.

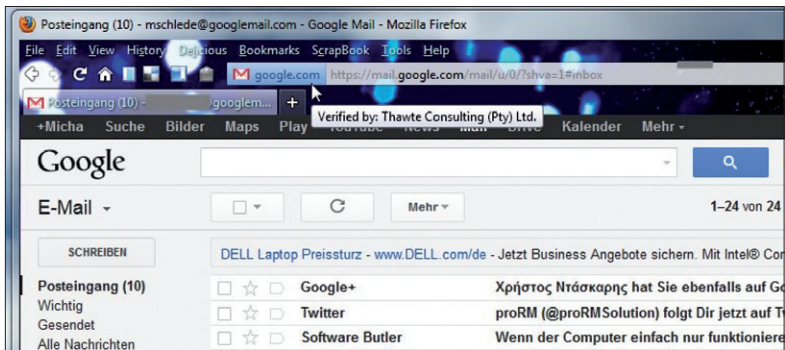
Wer nicht ganz auf HTML-Nachrichten verzichten will, dabei aber die Sicherheit verbessern möchte, kann im Sicherheits- oder Vertrauensstellungszentrum auch den Eintrag „Automatischer Download“ auswählen. Hier sind verschiedene Konfigurationen möglich, wie das Ausschalten des automatischen Bilder-Downloads in HTML-Nachrichten. Höchste Sicherheit bietet nur das Sperren aller angebotenen Optionen – seien Sie sich jedoch darüber im Klaren, dass die Nachrichten dann nicht mehr unbedingt „leserfreundlich“ aussehen.

2.3.7 Ist vom Einsatz einer Web-Mail-Lösung grundsätzlich abzuraten?

Grundsätzlich können Web-Mail-Lösungen heute ebenso gut eingesetzt werden wie „althergebrachte“ E-Mail-Lösungen auf dem Rechner. Allerdings gilt beim Einsatz von Web-Mail-Anwendungen das Gleiche wie für Cloud-Dienste ganz allgemein. Wer eine Web-Mail-Lösung verwendet, muss immer ein besonderes Augenmerk auf die Client-Server-Verbindung haben (sei es auf Notebook, Tablet oder Smartphone) und die folgenden Grundsätze beachten:

- Zugriff auf Web-Mail-Konten nur und ausschließlich über SSL-Verbindungen – nie eine offene Verbindung zulassen.

- Sicherstellen, dass die Webseite auch schon bei der Anmeldung verschlüsselt ist – mache Seiten schalten die SSL-Verbindung erst NACH dem Verbindungsaufbau ein, wodurch der Name und das Passwort des Anwenders unverschlüsselt übertragen werden.
- Kommt das Mail-Konto für geschäftliche Zwecke zum Einsatz, sollte sichergestellt sein, dass der Provider die Daten in Deutschland oder mindestens in der EU hostet.
- Wer mit seinem mobilen Client auf eine Web-Mail-Lösung oder auch auf den regulären Mail-Server zugreift, sollte dazu NIEMALS einen öffentlichen nicht verschlüsselten WLAN-Hotspot verwenden.



Ein wichtige Grundregel beim Einsatz von Web-Mail-Anwendungen: Der Übertragungsweg muss immer verschlüsselt sein – wie hier bei Google-Mail mittels einer SSL-Verbindung.

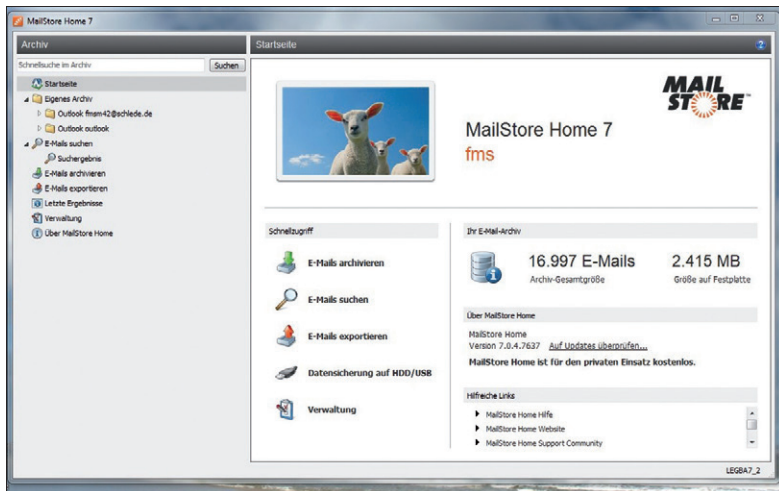
Ein Web-Mail-Konto eignet sich gut als „Zweit-Postfach“: Wer sein eigenes „echtes“ Mail-Postfach konsequent nur für die wichtige Kommunikation mit vertrauenswürdigen Absendern/Empfänger verwendet, kann ein solches (zumeist kostenloses) Zweitkonto gut dazu verwenden, beispielsweise interessante Beiträge von Firmenseiten herunterzuladen, die zumeist die Eingabe einer E-Mail-Adresse verlangen. Auch die Teilnahme an Gewinnspielen und ähnlichen Aktivitäten wird so sicherer: Werden im Rahmen dieser Kontakte Spam-Nachrichten ausgelöst (was leider immer noch der Fall ist), landen diese nur auf dem Zweitkonto und verstopfen nicht die wirklich wichtige Adresse.

2.3.8 Last but not least: sichern, sichern, sichern...

Einen Ratschlag sollte jeder Anwender immer beherzigen: Sichern Sie ihre Mail regelmäßig und häufig. Heute werden sehr viele Nachrichten und Informationen über diesen Kanal verschickt, die für den Geschäftsbetrieb wichtig sind. Geht die komplette gesammelte Mail verloren, weil beispielsweise die Festplatte im Rechner

defekt ist, kann es im günstigsten Fall möglich sein, die Nachrichten mithilfe des Providers wiederherzustellen.

Wer eine gehostete E-Mail-Lösung verwendet, kann sich in der Regel darauf verlassen, dass der Provider grundsätzlich entsprechende Sicherungsmaßnahmen einsetzt und so die Nachrichten wiederherstellbar sind. Kommen aber in kleinen und mittleren Betrieben oder in SOHO-Umgebungen (Small Office / Home Office) beispielsweise nur individuelle Systeme mit Outlook zum Einsatz, ist der Anwender gefordert, seine Nachrichten selbst zu sichern.



Eine gute Sicherungsstrategie gehört dazu: Wer sich nicht mit dem umständlichen Kopieren einzelner PST-Dateien herumärgern will und zudem auch seine Web-Mail-Konten mitsichern möchte, kann dazu eine freie Lösung wie MailStore Home einsetzen.

Die einfachste Möglichkeit der Sicherung besteht beim Einsatz von Microsoft Outlook darin, die zentrale Datenbank des Mail-Programms regelmäßig in einer Sicherungskopie abzulegen. Bei dieser PST-Datei (Personal Store) handelt es sich um ein proprietäres Dateiformat von Microsoft. Es enthält nicht nur die Nachrichten, sondern auch die Kontakte, Notizen und Kalenderdaten, die der Anwender in Outlook gespeichert hat.

Während diese Datei bei früheren Outlook-Versionen in den Ordnern des Benutzerprofils zu finden war, wird sie heute standardmäßig unter dem Pfad C:\Benutzer\ (Benutzername)\eigene Dokumente\Outlook-Dateien abgelegt und kann von dort einfach kopiert werden. Thunderbird verwendet mehrere Dateien, die bei Windows 7 unter dem Pfad C:\Benutzer\ (Benutzername)\AppData\Roaming\Thunderbird\Profiles zu finden sind. Auch diese Dateien können von dort kopiert und gesichert werden.



Ist viel mehr als nur eine Sicherung und trägt zur Sicherheit bei: Dadurch, dass die für den privaten Gebrauch freie Lösung MailStore Home auch einen Index anlegt, werden die Nachrichten archiviert und lassen sich schnell wiederfinden.

Praxistipp: Sichern ist eine lästige Aufgabe, die man sich so einfach wie möglich gestalten sollte. Deshalb ist es sinnvoll, auf eine der vielen Free- und Shareware-Lösungen zurückzugreifen, die diese Aufgabe deutlich erleichtern können. So hat sich bei uns unter anderem die Lösung MailStore Home (www.mailstore.com/de/) bewährt, die für den privaten Bereich kostenlos ist und sowohl mit den verschiedenen Outlook-Versionen als auch mit Thunderbird und Web-Mail-Lösungen zusammenarbeitet. Wer nur mit Mozilla-Tools arbeitet, sollte einen Blick auf MozBackup (www.mozbackup.de) werfen, eine Open-Source-Lösung, die dann auch noch die Daten des Firefox-Browsers mitsichert.

Auf jeden Fall darf eine regelmäßige Sicherung der E-Mail-Daten nicht vernachlässigt werden und sollte fester Bestandteil eines jeden Sicherheitskonzepts rund um die elektronischen Nachrichten sein.

Thomas Bär, Frank-Michael Schlede



Thomas Bär, der seit Ende der neunziger Jahre in der IT tätig ist, bringt weit reichende Erfahrungen bei der Einführung und Umsetzung von IT-Prozessen im Gesundheitswesen mit. Dieses in der Praxis gewonnene Wissen hat er seit Anfang 2000 in zahlreichen Publikationen als Fachjournalist in einer großen Zahl von Artikeln umgesetzt. Er lebt und arbeitet in Irsee im Allgäu.



Frank-Michael Schlede arbeitet seit den achtziger Jahren in der IT und ist seit 1990 als Trainer und Fachjournalist tätig. Nach unterschiedlichen Tätigkeiten als Redakteur und Chefredakteur in verschiedenen Verlagen arbeitet er seit Ende 2009 als freier IT-Journalist für verschiedene Online- und Print-Publikationen. Er lebt und arbeitet in Pfaffenhofen an der Ilm.

2.4 Single-Sign-On statt Login-Marathon

Bereits für ihre privaten Anwendungen müssen sich Nutzer zahlreiche verschiedene Nutzernamen und Passwörter merken. Kommen dann neben dem Login für das Firmennetzwerk weitere Accounts im Unternehmen hinzu, neigen die Mitarbeiter dazu, entweder immer dasselbe Passwort oder möglichst einfache Passwörter zu verwenden, die sie sich leicht merken können – die aber auch leicht zu knacken sind. Die Anzahl der Passwörter pro Mitarbeiter steigt auch deshalb, weil vor allem Fachabteilungen verstärkt dazu übergehen, Cloud-basierte Lösungen selbst einzuführen – oft ohne Wissen der IT-Leiter. Da viele dieser Anwendungen direkt im Browser laufen, muss auch keine zusätzliche Software auf den Clientcomputern installiert werden. Einfach einloggen und los geht's. Doch genau damit entstehen neue Probleme.

Eine Single-Sign-On-Lösung auf Basis der Security Assertion Markup Language (SAML) versetzt Unternehmen in die Lage, diese Sicherheitsrisiken auszuräumen, indem sie ihre Mitarbeiter von der Last dieser zahlreichen Passwörter befreien. Das XML-basierte Kommunikationsprotokoll für eine sichere Authentifizierung und Autorisierung ermöglicht es, Mitarbeitern schneller, einfacher und sicherer Zugang zu Cloud-Diensten zu verschaffen. Statt eines ganzen Bündels an Nutzername-Passwort-Kombinationen müssen sich Mitarbeiter nur noch ein einziges Passwort für die Anmeldung am SAML-Identity Provider des Unternehmens merken. Der Identity Provider übernimmt anschließend die weitere Authentifizierung des Nutzers gegenüber den verwendeten Cloud-Diensten.

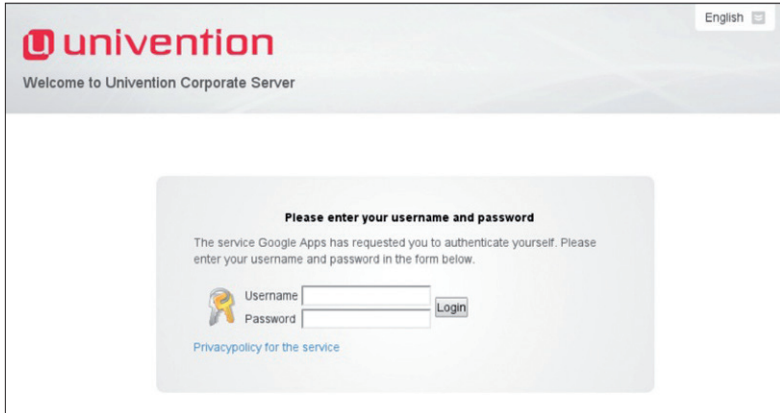
2.4.1 Identity Provider – das zentrale Steuerelement

Der Identity Provider ist das Kernelement eines solchen SAML-Single-Sign-On-Systems. Er wird im Unternehmensnetzwerk eingerichtet, verfügt über ein Nutzerverzeichnis und kennt die Authentifizierungsmechanismen der Webdienste. Im Identity Provider lassen sich für die unternehmensinternen Nutzer Konten anlegen, in denen der Administrator nutzerspezifisch festlegen kann, welchem Mitarbeiter welche Webanwendungen wann zugänglich gemacht werden.

Bei einer SAML-Integration, beispielsweise bei der Enterprise-Linux-Distribution Univention Corporate Server (UCS), lässt sich der Zugriff auf Cloud-Dienste direkt mit der Active-Directory-Benutzerverwaltung administrieren – entweder auf Microsoft Server über den Active Directory Connector oder auf UCS in den integrierten, auf Samba basierenden Active-Directory-Diensten. Administratoren entsteht damit kein zusätzlicher Mehraufwand, da der SAML-Identity-Provider die jeweiligen Berechtigungen eines Nutzers direkt aus Active Directory ausliest.

Nach dem Login am Identity Provider kann der Mitarbeiter dann an seinem Client sämtliche für ihn freigegebene Webdienste ohne weitere Login-Vorgänge nutzen. Er ruft einfach in seinem Browser die Anwendung auf und es öffnet sich direkt die Arbeitsoberfläche. Der Identity Provider hat in der Zwischenzeit die

Berechtigung des Nutzers anhand der hinterlegten Kontoeinstellungen geprüft, einen sicheren SAML-Token generiert, diesen an den Webdienst geschickt und den Nutzer damit authentifiziert.



univention

Welcome to Univention Corporate Server

English

Please enter your username and password

The service Google Apps has requested you to authenticate yourself. Please enter your username and password in the form below.

Username

Password

Login

[Privacy policy for the service](#)

Einmalig: Nach dem ersten Login stehen alle weiteren abgesicherten Dienste und Services sofort ohne weitere Authentifizierung zur Verfügung.

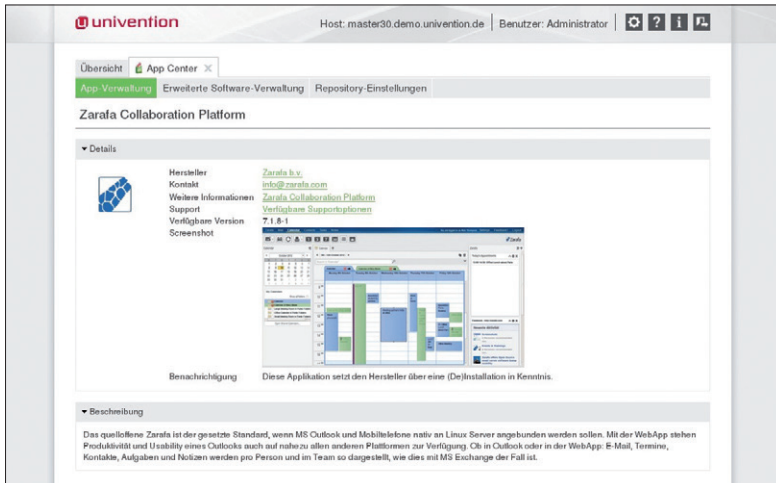
Damit der Service Provider den Token auch akzeptiert, tauschen bei der Einrichtung des Webdienstes der Identity Provider und der Dienste-Anbieter Zertifikate aus, durch die sich beide Seiten fortan als vertrauenswürdig ausweisen. Statt der üblichen Login-Daten werden bei einer Anmeldung eines Nutzers beim Service Provider anschließend nur noch Informationen übertragen, mit denen kein Dritter Zugang zu der Anwendung erlangen kann.

Für den Anwender im Unternehmen hat SAML damit den Vorteil, dass er sich nicht mehr für jeden Dienst seine individuellen Login-Daten merken und diese bei der Anmeldung eingeben muss, sondern unmittelbar Zugriff auf die Arbeitsfläche sowie sämtliche anderen Inhalte hat, für die er berechtigt ist. Ruft er eine andere Anwendung auf, ist diese ebenso sofort verfügbar – vorausgesetzt, der Nutzer ist im Identity Provider auch dafür freigeschaltet.

2.4.2 One-Klick-Access mit SAML

Unternehmen profitieren von der gesteigerten Sicherheit und der höheren Produktivität ihrer Mitarbeiter, die unterschiedliche Webdienste mit SAML noch einfacher nutzen können. Denn statt frustrierender, sich ständig wiederholender Login-Vorgänge können sie durch den One-Klick-Access direkt mit der Arbeit starten. Mit SAML bleiben die Benutzerpasswörter außerdem in der eigenen IT und liegen nicht mehr beim Dienstanbieter. Eine geringere Zahl an Passwörtern

bedeutet für Unternehmen auch, dass weniger Passwörter vergessen, verloren oder gestohlen werden. Der Zeitaufwand für die umständliche Wiederbeschaffung oder Neuerteilung dieser Login-Daten entfällt – ganz zu schweigen von den Schäden, die durch Missbrauch eines gestohlenen Passworts entstehen können.



Sicher und effizient: SAML ist für Unternehmen eine unkomplizierte und kostengünstige Methode, um ihre Mitarbeiter von der Belastung durch zahlreiche verschiedene Passwörter für unterschiedliche Cloud-Dienste zu befreien und die IT-Sicherheit zu steigern.

Als offener Standard wird SAML von ziemlich jedem Webdienst unterstützt. Bei einer guten Integration des SAML-Identity Providers wird die gewohnte Benutzerverwaltung nur um einen zusätzlichen Reiter erweitert und erlaubt damit die Administration der Nutzerfreigaben in der bekannten Nutzerverwaltung. Bei einer Kombination mit Active Directory entfällt eine doppelte Verwaltung von Passwörtern vollständig.

Mit SAML vermeiden Unternehmen außerdem, dass sie für zusätzliche lokal installierte Client-Anwendungen für cloudbasierte Dienste ihre Firewall weiter perforieren müssen, da die Webanwendungen sich über den Browser und damit über die herkömmliche Internetverbindung nutzen lassen. Der geringe Aufwand für die Einrichtung und der große Sicherheits- und Komfortgewinn machen SAML im Grunde zu einem Muss für jedes Unternehmensnetzwerk.

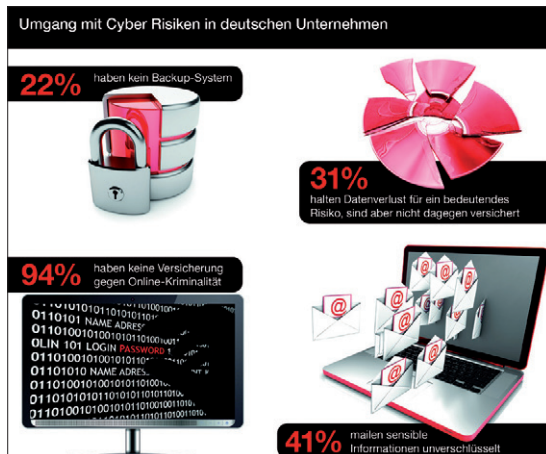
Alice Horstmann

Alice Horstmann ist Head of Marketing Communications bei der Univention GmbH.

2.5 Cyber-Kriminalität: Wann zahlt die Versicherung?

Ob Hacker-Angriff oder Datenverlust – Cyber-Risiken werden für Unternehmen zunehmend zum Problem. Die aufsehenerregenden Fälle der zurückliegenden Monate bei Vodafone, Adobe und Sky sind nur die Spitze des Eisbergs. Gerade kleine und mittlere Unternehmen haben häufig Probleme im Umgang mit Cyber-Risiken. Aus einem einfachen Vorfall wird schnell eine handfeste Krise. Und deren Auswirkungen sind oft nur schwer zu handhaben: Es lauern rechtliche Fallstricke, die Kunden sind beunruhigt, das Firmenimage leidet. Die öffentliche Aufmerksamkeit gegenüber Cyber-Risiken ist hoch und der potenzielle Schaden so bedrohlich wie diffus. Dennoch sind viele Unternehmen nur mangelhaft vorbereitet: So ergab die Hiscox-eDNA-Studie (www.hiscoxdnareport.com), eine repräsentative Umfrage auch unter deutschen Mittelständlern, dass 22 Prozent der befragten Unternehmen über kein Backup-System verfügen, 41 Prozent sensible Daten unverschlüsselt mailen und mit 94 Prozent die meisten Unternehmen nicht gegen Online-Kriminalität versichert sind.

Leichtsinnig: Die Ergebnisse der Hiscox-eDNA-Studie zeigen, dass deutsche Mittelständler immer noch unzureichend gegen IT-Risiken gewappnet sind. (Quelle: Hiscox)



Neben dem oftmals trügerischen Vertrauen in die Leistungsfähigkeit und Sicherheit der eigenen IT-Systeme besteht ein weiteres Problem: Cyber-Angriffe sind nicht zwangsläufig IT-basiert. Ebenso häufig nutzen Angreifer Schwächen in der Organisation oder bedienen sich der Hilfsbereitschaft von unbedarften Mitarbeitern, die dann unfreiwillig dafür sorgen, dass IT-Schutzmaßnahmen nicht mehr greifen („Social Engineering“). Doch selbst die Antizipation aller Risiken und die größtmögliche Anstrengung zu deren Minimierung können keinen absoluten Schutz garantieren.

2.5.1 Das Krisenmanagement entscheidet

Wenn sich scheinbar hypothetische Risiken doch in konkrete Krisen verwandeln, kann dies vor allem mittelständische Unternehmen schnell in Existenznöte bringen. Neben den juristischen Konsequenzen beim Verlust personenbezogener Daten (wie die Informationspflicht nach §42a BDSG) sind es vor allem die Herausforderungen des Krisenmanagements, die Mittelständler überfordern. Zur Bewältigung werden neben vertrauenswürdigen Experten für IT-Forensik vor allem Krisenmanager und Kommunikationsexperten benötigt, die entsprechende Erfahrung mit Cyber-Angriffen mitbringen. Denn Cyber-Krisen unterscheiden sich in zwei entscheidenden Punkten von anderen kriminellen Angriffen auf Unternehmen: Sie erzeugen fast immer und explosionsartig Öffentlichkeit – und sie erfordern die Übersetzung komplexer technischer Sachverhalte in eine Sprache, die Kunden und Geschäftspartner verstehen.

Hierbei spielt es keine Rolle, wodurch genau die Krise ausgelöst wurde – ob durch selbst verschuldete Nachlässigkeit oder einen komplexen Cyber-Angriff. In einer Situation, in der sich viele Menschen Sorgen um den Schutz ihrer Daten machen, ist die Schuldfrage für die Öffentlichkeit unerheblich. Deshalb ist eine gute Krisenkommunikation entscheidend dafür, dass das Vertrauen von Verbrauchern, Kunden und Partnern nicht verloren geht. Die eigene Kommunikationsabteilung eines Unternehmens kann viele IT-Krisen jedoch nicht alleine handhaben und benötigt oftmals Unterstützung von außen.

2.5.2 Wo die Versicherung ins Spiel kommt

Findet das gesamte Krisenmanagement rasch und professionell statt, lassen sich viele Vorfälle unterhalb der öffentlichen Wahrnehmungsschwelle managen. Um aber zumindest den monetären Schaden im erträglichen Rahmen zu halten, bieten seit einigen Jahren auch verschiedene Versicherungsgesellschaften eigene Policen zur finanziellen Absicherung gegen Cyber-Schäden und IT-Sicherheitsrisiken an. Jedes Unternehmen muss im eigenen Fall entscheiden, wo eine Versicherung sinnvoll ist – grundsätzlich gibt es verschiedene Arten von Policen.

Typische Risiken für IT-Systeme, gegen die sich Versicherungen abschließen lassen, lassen sich in sechs Bereiche aufteilen: **Malware, Hacking, Missbrauch durch Insider, Soziale Angriffe (Social Engineering), Physische Angriffe und Verlust von Speichermedien** sowie **Fehlfunktionen**.

2.5.3 Beispiel: Cyber Risk Management by Hiscox

Der Spezialversicherer Hiscox beispielsweise listet ausgeschlossene Risiken ebenso wie die Deckungsinhalte der Versicherung explizit auf – hier ein kurzer Überblick über die entsprechenden Bedingungen:

Prüfung vor Versicherungsbeginn: Zunächst füllt der Kunde einen Fragebogen aus. Dort werden vor allem die Art und Menge der gespeicherten Daten, die Art der elektronischen Zahlungsabwicklung und die Datensicherheit abgefragt. In Einzelfällen beauftragt der Versicherer einen externen Dienstleister mit der Prüfung und Einschätzung der Datensicherheit.

Wann zahlt die Versicherung?: Die Versicherung greift, wenn entweder Datenschutzrechte von Dritten verletzt wurden, etwa durch Datenverlust oder durch einen Angriff von außen, oder wenn das eigene System von Hackern attackiert worden ist. Bei Schadensersatzansprüchen von Dritten werden diese ebenfalls vom Versicherer geprüft: Sollten diese berechtigt sein, entschädigt die Versicherung; unberechtigte Ansprüche wehrt sie im Namen des Kunden ab. Zur weiteren Schadensbegrenzung unterstützen von der Versicherung bestellte externe Dienstleister, in diesem Fall HiSolutions, das Unternehmen bei der Wiederherstellung von Daten und beim Krisenmanagement.

Beispielrechnung eines typischen Cyber-Schadenfalles

Ein Unternehmen mittlerer Größe ist im Bereich des Onlinevertriebs Opfer von Datenklau geworden. Über mehrere Monate konnten sich Hacker rechtswidrigen Zugang zu dem eigentlich streng gesicherten onlinebasierten Abrechnungssystem für Bezahlkarten verschaffen, dem Payment Processing Tool. Während dieser Zeit konnten die Hacker rund zwei Millionen Kundendaten kopieren und unrechtmäßig nutzen. Das Schadensausmaß ist sowohl finanziell als auch für die Reputation immens. Als Spezialversicherer deckte Hiscox die bislang entstandenen Kosten wie folgt:

Kosten für:

Diverse forensische Arbeiten	150.000 €
Rechtsberatung und Rechtsbeistand	525.000 €
Gesetzliche Informationspflichten	2.170.000 €
Media- und PR-Arbeiten	253.000 €
Geltend gemachten Vermögensschaden der Payment Card Industry	2.000.000 €
Gesamtkosten	5.098.000 €

Unkalkulierbares Risiko: Die Kosten für einen klassischen Cyber-Schaden gehen schnell in die Millionen. (Quelle: Hiscox)

Welche Risiken sind ausgenommen?: Ausgeschlossen sind in der Regel Schäden durch Programmierfehler, Verschleiß oder Schäden durch unterbrochene Stromversorgung. Auch vorsätzlich herbeigeführte Versicherungsfälle sind nicht geschützt. Hiscox schließt jedoch nur den Vorsatz leitender Angestellter aus: Insider-Attacken durch Mitarbeiter sind also abgesichert.

Wer wird nicht versichert?: Unternehmen bestimmter Branchen werden in der Regel nicht versichert. Dazu zählen Anbieter von Bezahlssystemen, Social-Network-Plattformen oder Anbieter pornografischer Inhalte.

2.5.4 Im Ernstfall

Hat sich ein Unternehmen gegen Cyberrisiken versichert, ergibt sich im Ernstfall das im Folgenden dargestellte Szenario.

Ausgangslage: Ein kleiner IT-Dienstleister dient einer Hacker-Gruppe als Einfallstor in die Datenbank eines mittelständischen Unternehmens. Wie schon beim Angriff auf die Washington Post via Outbrain überwinden die Angreifer das schwach gesicherte System des Dienstleisters und verschaffen sich Kontrolle über die offene Schnittstelle zum Unternehmen. Den Tätern gelingt es, eine große Anzahl sensibler Kundendaten abzuschöpfen.

Das weitere Vorgehen:

- Der Versicherer wird über den Schaden informiert. Über eine eingerichtete Notfall-Hotline fordert das Unternehmen zusätzlich ein Expertenteam für die Unterstützung bei der Krisenbewältigung an. Der Versicherer verständigt seine Kooperationspartner für IT-Sicherheit.
- Der beauftragte IT-Sicherheitsdienstleister beginnt unverzüglich mit der Schadensbegrenzung und Sicherstellung von Beweisen. Es wird ein IT-forensisches Gutachten angefertigt.
- Experten für Krisenmanagement und -kommunikation unterstützen das betroffene Unternehmen bei der Krisenbewältigung und Öffentlichkeitsarbeit, um die hohe mediale Aufmerksamkeit zu bewältigen und einem drohenden Imageschaden entgegenzuwirken.
- Spezialisierte Anwälte beraten das Unternehmen bezüglich der Umsetzung der gesetzlichen Informationspflicht und stützen sich dabei auf die Ergebnisse der IT-Forensiker.

Alle bisherigen Aufwendungen sowie die Kosten für die Information der Dateninhaber und Ansprüche Dritter trägt der Versicherer.

2.5.5 Und danach?

Auf Wunsch der Geschäftsleitung vermittelt der Versicherer einen professionellen Dienstleister zur nachhaltigen Optimierung des IT-Sicherheitssystems. Der Versicherer subventioniert das Anliegen des Kunden und beauftragt eine externe Firma, eine umfassende Sicherheitsprüfung vorzunehmen.

Robin Kroha, Stefan Sievers

Robin Kroha leitet den Bereich Corporate Security Management bei der auf Sicherheits- und Krisenmanagement spezialisierten Unternehmensberatung HiSolutions AG mit Sitz in Berlin.

Stefan Sievers ist Underwriting Manager Specialty Lines bei der britischen Versicherungsgesellschaft Hiscox.

2.6 IT-Ausfällen vorbeugen

Brand, Stromausfall, Serverversagen, beschädigte Netzwerkkomponenten oder eine Krankheitswelle beim IT-Personal: alles realistische Szenarien, die Unternehmen in eine Krise führen können. Mit einer gründlichen IT-Notfallplanung lässt sich das verhindern.

Schon wenige Stunden Ausfall der Informations- und Kommunikationstechnik können je nach Branche und Unternehmen gravierende oder gar existenzbedrohende Schäden für den Geschäftsbetrieb mit sich bringen. Die IT-Notfallplanung beschäftigt sich – als Teilbereich des Business Continuity Management – konkret mit dem Prozessmanagement im Falle einer Störung oder eines Komplettausfalles der IT. Sie unterstützt Unternehmen bei der Prävention von Krisen oder Notfällen aus Störereignissen und sorgt im Ernstfall für eine strukturierte und schnelle Wiederherstellung der Systeme nach festgelegten Prioritäten, um betriebswirtschaftliche Schäden abzuwenden. 2010 waren bei dem weltweit größten Online-Versandhändler Amazon aufgrund eines Hardwarefehlers mehrere europäische Websites zeitweise ausgefallen, wodurch mitten in der Weihnachtszeit signifikante Umsatzeinbußen entstanden. Das ist nur ein Beispiel von vielen – früher oder später machen die meisten Unternehmen unliebsame Erfahrungen mit Datenverlusten, Störungen von Kern- oder Subsystemen und ähnlichen IT-Notfall-Szenarien – ob direkt oder indirekt. Denn die komplexen Strukturen der globalen Kollaborationsnetzwerke, Lieferketten und ineinandergreifenden Produktionsprozesse (Stichwort „Just-in-Time“) machen Unternehmen in hohem Maße abhängig von einem kontinuierlichen und störungsfreien Geschäftsbetrieb zwischen allen Prozessbeteiligten. Die Betriebsbereitschaft der IT zu sichern und ein Konzept für Disaster Recovery zu etablieren ist heute wichtiger denn je. Dazu gehört es auch, Risiken frühzeitig zu identifizieren, ungeplante Ausfallzeiten durch Vorkehrungsmaßnahmen zu minimieren, die Mitarbeiter auf den Ernstfall vorzubereiten und ein zuverlässiges Informations- und Notfallmanagement einzurichten.

2.6.1 Verantwortlichkeiten nicht klar geregelt

„Im Schnitt hat jedes zweite Unternehmen in Deutschland für Störfälle in der IT keine adäquate Notfallplanung parat, um negative Auswirkungen auf den laufenden Geschäftsbetrieb zu vermeiden oder zu minimieren“, berichtet Jochen Möller, Geschäftsführer der Hamburger mIT solutions GmbH, aus seinem Beratungsallday. Ein Grund sei, dass die Verantwortlichkeiten zwischen IT, Geschäftsführung oder Produktion nicht immer klar genug geregelt seien, um eine IT-Notfallplanung initiieren zu können. „Leider wird dieses Thema daher häufig erst dann mit dem notwendigen Engagement vorangetrieben, wenn das Kind schon in den Brunnen gefallen ist“, so Möller. Im Ernstfall fehle es dann am methodischen Know-how, sodass oftmals keine strukturierte Herangehensweise mehr möglich seien – mit unproduktiven Mehrarbeitszeiten und Umsatzeinbußen als Folge.

2.6.2 Workflow-gestützte Dokumentation

Um auf einen IT-Notfall angemessen zu reagieren, benötigen Unternehmen eine strukturierte IT-Notfallkonzeption, die verschiedene Eventualitäten bereits im Vorfeld beleuchtet. Tritt in der IT-Umgebung eine Notfallsituation ein, beschreibt sie die Vorgehensweise, wie in einer angemessenen Zeit zum einen der Notfallbetrieb und zum anderen die vollständige Verfügbarkeit der IT und der Daten sichergestellt werden können. Eine Orientierung gibt der IT-Service-Continuity-Management (ITSCM)-Standard nach ITIL 2011, der als vierstufiger Leitfaden zur Behebung von „Major Incidents“ und zur Realisierung einer gezielten Wiederherstellungsplanung von IT-Services verfasst wurde.



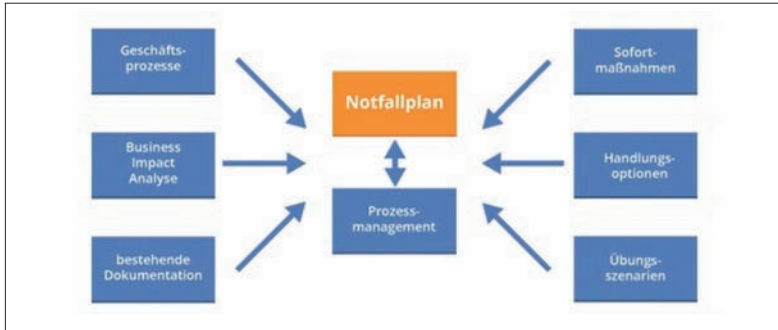
Kritik: Jochen Möller vermisst klare Zuständigkeiten, vor allem im Bereich Methodik. (Quelle: mIT Solutions GmbH)

Um Unternehmen bei der zuverlässigen IT-Notfallplanung zu unterstützen und die ITSCM-Maßnahmen unter Berücksichtigung individueller Strukturen erfolgreich umzusetzen, hat sich heute auf Basis dieses Leitfadens ein ganzheitliches Best-Practice-Modell etabliert. Dieses umfasst sowohl die Identifikation relevanter IT-Services und die Konzeptionierung der Notfallprozessplanung als auch die Einrichtung eines Notfall-Desks und die Informationsbereitstellung für den Wirtschaftsprüfer. Am Ende bekommt das Unternehmen eine vollständige, software- und Workflow-gestützte Dokumentation mit allen relevanten Informationen an die Hand, sodass die notwendigen Schritte zur Wiederherstellung der IT wie eine Checkliste abzuarbeiten sind.

2.6.3 Entwicklung des Notfallplans

Ein Notfall entsteht zumeist durch eine Verkettung einzelner Störungen, die jeweils für sich genommen nicht kritisch gewesen wären. Die Notfallplanung erfüllt daher nicht nur den Zweck, eine systematische Wiederherstellung des Betriebes und der Daten zu gewährleisten, sondern dient auch dazu, Risiken präventiv zu managen und zu verhindern, dass Notfälle überhaupt entstehen können. Am Anfang des Planungsprozesses steht daher eine Risikobetrachtung (Business-Impact). Deren Basis ist es, mögliche Risiken zu identifizieren, zu analysieren, zu bewerten und zu dokumentieren. Daraus lassen sich sowohl die kritischen Ausfall-

zeiten, quasi die „Überlebensdauer“ des Unternehmens im Hinblick auf bestehende Verträge und SLAs, als auch Schwachstellen auf Prozessebene, IT-Risiken und geeignete Gegenmaßnahmen ermitteln.



Vorlage für die Praxis: Ein mögliches Entwicklungsschema eines IT-Notfallplans.
(Quelle: mit Solutions GmbH)

In dieser Analysephase wird ebenfalls definiert, welche Systeme für die Leistungserbringung des Unternehmens als kritisch einzustufen sind, wie diese zusammenspielen und welche Bedingungen gegeben sein müssen, um bestimmte Workflows anzustoßen. Auf dieser Grundlage wird schließlich festgelegt, wann eine Störung zu einem Notfall beziehungsweise wann ein Notfall zu einer Krise wird sowie welche Kommunikationswege und Abläufe zur Wiederherstellung zu initiieren sind. Im Anschluss wird genau geplant, wie Notfallprozesse und Wiederanläufe auszu-sehen haben, um die Störung zu beheben.

Anhand einer „Notfall-Checkliste“ kann der verantwortliche Mitarbeiter die Einhaltung sämtlicher Prozessschritte von A bis Z überwachen.

2.6.4 Der Faktor Mensch

Störfälle treten im Unternehmensalltag immer wieder auf. Wichtig ist, dass aus den Störfällen keine Krisen entstehen. Beim Umgang mit kritischen Situationen sind daher auch psychologische Komponenten auf Mitarbeiterebene und der „Faktor Mensch“ zu beachten. Der arbeitsorganisatorischen Vorbereitung und dem Üben von Notfallszenarien kommt daher eine große Bedeutung zu. Es geht darum, alle Beteiligten mit den jeweiligen Aufgaben im Krisenfall vertraut zu machen und das Zusammenspiel aller Akteure und Prozesse zu trainieren. Mithilfe von Reviews können Schwachstellen identifiziert und die Testkonzepte beziehungsweise Ablaufpläne in einem iterativen Prozess stetig verbessert werden.

2.6.5 Krisen-, Prozess- und IT-Service-Management integriert abwickeln

In einer Notfallsituation müssen alle Rädchen ineinandergreifen und alle Beteiligten schnell reagieren. Wer übernimmt welche Aufgaben? Wer ist zu benachrichtigen, und wer hat welche Entscheidungsbefugnisse? Welche Dokumentationen sind vorhanden, und wo sind diese hinterlegt? Welche Systeme müssen zuerst wiederhergestellt werden? Welche Fristen sind unbedingt einzuhalten? Wie erreiche ich verantwortliche Systemspezialisten? Welche Vertreterregelungen gibt es?

„Die Mitarbeiter müssen diese anfallenden Fragen nicht nur ad hoc beantworten können, sondern sie müssen durch diesen Prozess effektiv geleitet werden, da Menschen in Extremsituationen anders ‚funktionieren‘“, unterstreicht Möller. Unternehmen könnten bisweilen dafür auch auf ITSM-Software zurückgreifen, die häufig bereits in ihrer IT-Infrastruktur vorhanden seien.

Sandra Effenberger

Sandra Effenberger ist Projektleiterin bei der mIT solutions GmbH.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **IT-Risiko-Management ist eine juristische Pflicht**
(www.tecchannel.de/2048166)
- **Wie verwaltet man Risiken in Projekten?**
(www.tecchannel.de/2047087)
- **Empfehlungen für ein intelligenzbasiertes Risikomanagement**
(www.tecchannel.de/2046793)
- **Sicherheitsrisiken in virtualisierten Umgebungen minimieren**
(www.tecchannel.de/2045345)
- **In vier Schritten zu mehr Informationssicherheit**
(www.tecchannel.de/2040725)
- **So sichern Sie mobile Systeme richtig ab**
(www.tecchannel.de/2056373)
- **Tipps & Tricks zur Absicherung der Unternehmens-IT**
(www.tecchannel.de/2047480)
- **Security-Lösungen für kleine und mittelständische Firmen**
(www.tecchannel.de/2045654)
- **So vermeiden Sie Informationsrisiken im Unternehmen**
(www.tecchannel.de/2040929)

2.7 Neue Trends im Identitäts- und Access-Management

Wohin geht die Reise in den Bereichen Identitätsverwaltung und Authentifizierung? Anhand aktueller Entwicklungen im IT-Markt und laufender Forschungsprojekte lassen sich einige Prognosen anstellen.

Obwohl Identitäts- und Access-Management (IAM) kein neues Thema ist, hat es in der jüngeren Vergangenheit als Querschnittsfunktion stark an Bedeutung gewonnen. Seine wichtigsten Treiber sind drei tief greifende Megatrends: Globalisierung, Digitales Leben und neue Konsummuster. Die Globalisierung führt zu einer deutlichen Ausweitung von unternehmens- und länderübergreifenden Geschäftsprozessen, für die eindeutige Identifikationen respektive gut abgesicherte Zugriffe auf IT-Ressourcen nötig sind. Das Digitale Leben, also die Entwicklung, die zwischenmenschliche Kommunikation zunehmend ins Internet zu verlagern, sorgt dafür, dass Menschen aus Gründen der Wiedererkennbarkeit ihre reale oder wahlweise auch pseudonymisierte Identität in die virtuelle Welt mitnehmen. Neue Konsummuster – wie das Shareconomy-Modell „Teilen statt Haben“ – machen es notwendig, Besitz bedarfsgerecht zur Verfügung zu stellen. Das gelingt aber nur, wenn der Zugriff hierauf schnell und einfach bereitgestellt werden kann – und das ist ohne ein funktionierendes IAM-System kaum denkbar.



Wichtig: Im Rahmen der wachsenden Zahl digitaler Identitäten steigt die Bedeutung des IAM immens. (Quelle: BioID AG)

2.7.1 Aktuelle Entwicklungen

Neben den langfristigen Trends spielen speziell auf die IT-Nutzung bezogene Entwicklungen eine wichtige Rolle. Aktuell ist zu beobachten, dass immer mehr lokale Daten in die Cloud verlagert werden, während eine wachsende Zahl unterschied-

lichster Endgeräte (zum Beispiel PC, Notebook, Smartphone, Tablets oder Fernseher) auf diese zugreifen. Trends wie „Bring Your Own Device“ zeigen schon jetzt, dass es in naher Zukunft selbstverständlich sein wird, auf alle privaten und geschäftlichen Daten von allen Endgeräten und allen Orten der Welt aus zuzugreifen. Das betrifft Programme und Anwendungen genauso wie Kontakte, E-Mails, Musikdateien, Tabellen, Fotos, Notizen, Grafiken, Urkunden und Bankdaten. Diese Entwicklung stellt immer größere Anforderungen an das Management von Identitäten und Zugriffsrechten, denen mit neuen Technologien und innovativeren Nutzungskonzepten begegnet werden muss.

2.7.2 Die Authentifizierung wird vielfältiger

Identitätsnachweise in der digitalen Welt lassen sich in drei Gruppen unterteilen:

1. Den Nachweis von Wissen, beispielsweise eines beiden Seiten bekannten Geheimnisses wie in der Kombination Username/Passwort
2. Den Nachweis eines Besitzes, also beispielsweise einer Smartcard mit Schlüssel
3. den Nachweis eines bestimmten physischen, also eines biometrischen Merkmals wie eines Fingerabdrucks

Der Trend geht zur Kombination von mindestens zwei dieser Nachweisarten – zur Zwei-Faktor-Authentifizierung. Diese erfolgt immer häufiger kontextsensitiv – beispielsweise nach Ort, Zeit oder Gerät. Der Authentifizierungsweg gestaltet sich zudem immer nutzerfreundlicher – etwa via optimierte Smartcards, mobileTAN oder photoTAN. Bei den beiden letztgenannten Verfahren werden die Zugriffs-codes auf die eine oder andere Weise auf das Smartphone des Anwenders geschickt.

2.7.3 Mobile Endgeräte

Das zeigt, dass mobile Endgeräte als Identitätstoken stark an Bedeutung gewinnen. Ein gutes Beispiel, diesen Trend zu belegen, ist die wachsende Zahl der Möglichkeiten, das Smartphone als persönliche Geldbörse samt aller Ausweisdokumente zu verwenden. Das geschieht einerseits mithilfe softwarebasierter Token, die auf das Endgerät geladen werden, um einen eindeutigen Identitätsnachweis erbringen zu können.

Andererseits werden seit einigen Jahren bereits hohe Erwartungen in den Funkstandard NFC (Near Field Communication) gesteckt, der sowohl eine Zwei-Faktor-Authentifizierung im Bereich Identitätsnachweis (Kombination aus Smartcard und Mobiltelefon) als auch im Bereich sicherer Zahlungsprozesse ermöglichen könnte. Die Zahl „gelebter“ NFC-Anwendungsfälle ist aber noch überschaubar – so wird die Technologie beispielsweise bereits in einigen Skipässen eingesetzt. Im Kreditkarten- und Nahverkehrsbereich befindet sich vieles noch in der Pilotphase.

Anlaufschwierigkeiten: Hochge-
lobt, aber noch immer nicht auf
breiter Front gelebte Praxis: der
Funkstandard NFC. (Quelle: vege;
Huseyin Bas, Fotolia; HID Global;
NXP; NFCWorld; Deutscher Spar-
kassen- und Giroverband)



2.7.4 Biometrie

Die bereits erwähnten biometrischen Faktoren als Identifikationsmerkmal gewinnen ebenfalls an Bedeutung. Eindeutige körperliche Charakteristika werden einmalig abgescannt, in ebenso eindeutige Prüfsummen umgewandelt, in Datenbanken hinterlegt und zur Wiedererkennung ihrer Besitzer verwendet. Zu den bekanntesten Verfahren für Personen zählen Fingerabdruck-, Iris- und Gesichtserkennung. Weitere Möglichkeiten sind Venenmuster-, Gang-, Tippmuster- oder Unterschriftenerkennung. Ebenso ist die biometrische Identifizierung von Objekten möglich – etwa anhand ihrer Form, Farbe, Oberfläche, Material oder Gewicht.

Komplexe Anforderungen: Im Rahmen des EU-Projekts „Turbine“ (Trusted Revocable Biometric Identities) soll erforscht werden, wie sich biometrische Identitäten pseudonymisieren und auch nachträglich widerrufen lassen.

In der Entwicklung befinden sich inzwischen auch Verfahren, die die Pseudonymisierung und Widerrufbarkeit von biometrischen Identitäten erlauben, wie beispielsweise das EU-Projekt „Turbine“ (Trusted Revocable Biometric Identities, www.turbine-project.eu). Am Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik (IPK, www.ipk.fraunhofer.de) wird darüber hinaus im Rahmen des SMI-Projekts (Secure Mobile Identity) erforscht, wie sich verschiedene Identitätsnachweise über mobile Endgeräte miteinander kombinieren lassen.

2.7.5 Neue Token und Smartcards

Der Bereich der physischen Zugangs-Token ist einer der IAM-Klassiker, bringt aber dennoch immer wieder Innovations sprünge hervor. War es in den vergangenen Jahren die Einführung kontaktloser, NFC-fähiger Token und Karten, so werden es in den kommenden Jahren insbesondere integrierte Karten und Token sein, die Eingabe- und teils auch Ausgabefelder direkt integrieren.



Gut zu wissen: Neben dem elektronischen Reisepass und der Gesundheitskarte sind auch auf dem neuen Personalausweis (nPA) Identitätsdaten in digitaler Form hinterlegt. (Quelle: BMI)

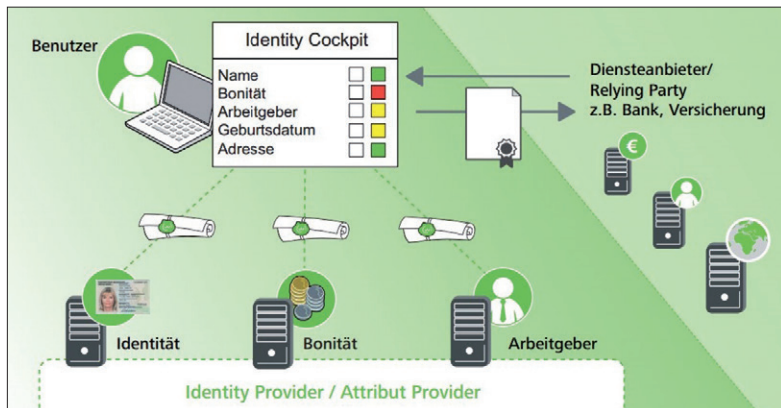
Beispiele für Eingabefelder sind Nummernblöcke, Unterschriftsfelder oder Biometrieleser. Als Ausgabefelder lassen sich OLED-Displays und ePaper nennen. Die Fraunhofer-Institute für Zuverlässigkeit und Mikrointegration (IZM, www.izm.fraunhofer.de) sowie für Angewandte Polymerforschung (IAP, www.iap.fraunhofer.de) arbeiten im Rahmen des „Secudis“-Projekts (Secure Digital Identity Solutions, www.bundesdruckerei.de/de/229-innovative-hochsicherheitsloesungen) beispielsweise daran, Sensor- und Displaytechnologie mit neuen Antennen und Chips zusammenzuführen. Ziel soll sein, digitale Ausweisdokumente zukunftstauglich zu machen und bereits die nächste Stufe nach nPA (neuer Personalausweis) und elektronischem Reisepass zu erforschen.

2.7.6 Single-Sign-On und Federation

Durch die wachsende Bedeutung von digitalen Services haben Anwender heutzutage eine zunehmende Anzahl an unterschiedlichen digitalen Identitäten und Zugangstoken, die sie verwalten müssen. Damit sie sich nicht x-fach authentifizieren müssen, wurde vor Jahren das Single-Sign-On-Konzept entwickelt. Mittels einmaliger Authentifizierung ist so der Zugriff auf alle Dienste und Systeme möglich, für die ein Anwender die Berechtigung besitzt. Dieser Ansatz der föderierten Identität versteht sich als eine „zusammengefasste“ Identität, die sich über mehrere Systeme erstreckt. Es wird eine Föderation verschiedener Dienstanbieter etabliert, um dem Nutzer einen vereinfachten Zugang zu gewährleisten. Identitätsinformationen werden in verschiedenen Systemen vorgehalten und genutzt. Dies ermöglicht eine vernetzte Nutzerverwaltung, bei der die eigentlichen Identitätsinformationen jedoch stets auf dem jeweiligen System verbleiben. Einheitliche Datenstandards stellen die bedarfsbezogene Nutzung und Austauschbarkeit sicher.

2.7.7 Nutzerzentrierung

Je häufiger sich Anwender Social-Engineering-Angriffen, Phishing oder Man-in-the-Middle-Attacken ausgesetzt sehen, desto vorsichtiger werden sie in der Entscheidung, wem sie noch ihre Daten anvertrauen können, um eine Identität nachzuweisen. Die Vertrauenswürdigkeit digitaler Identitäten leidet zusehendes.



Visionen: Das Projekt „myID.privat“ stellt den deutschen Bürger in den Mittelpunkt. Forscher versuchen zu ergründen, wie sich digitale Identitätsnachweise in Zukunft – getrennt nach Einsatzzweck – besser einsetzen und auch schützen lassen. (Quelle: myID.privat – Fraunhofer FOKUS)

Wenn es darum geht, einen Authentifizierungsprozess transparent zu gestalten oder ihn gar nutzerseitig beeinflussen zu können, rückt der Einzelne immer stär-

ker in den Hintergrund. Internetanbieter fordern Identitäten ein, weisen sich dem Nutzer gegenüber jedoch selbst äußerst selten eindeutig aus. Die Bereitschaft, neue Technologien im Web zu nutzen, sinkt. Um dieser Entwicklung entgegenzuwirken, wurden Ansätze entwickelt, die den Nutzer wieder in den Mittelpunkt des Geschehen zurückbringen sollen: die nutzerzentrierte Identität. Nutzerzentriertes Identitätsmanagement sieht den einzelnen Anwender als wichtigste Instanz im Identifizierungsprozess und versucht insbesondere seine persönlichen Daten und Attribute und damit seine Privatsphäre zu schützen. Ein vertrauenswürdiger Identitäts-Provider, der bestimmte Attribute des Nutzers kennt, erstellt einen passgenauen Nachweis, ein sogenanntes Sicherheits-Token, das genau (und nur) die Daten enthält, die der Nutzer einem bestimmten Anbieter senden möchte. Ein Beispiel für einen solchen Identitäts-Provider ist das Projekt „myID.privat“ des Fraunhofer-Instituts für Offene Kommunikations-Systeme (FOKUS, www.fokus.fraunhofer.de/de/fokus/).

2.7.8 Fazit

Identitäts- und Access-Management gewinnt mit der zunehmenden Digitalisierung stark an Bedeutung. Die Anwender stehen zahlreichen neuen Technologien und Trends gegenüber, ohne genau zu verstehen, wie diese funktionieren. Neben der technischen Sicherheit steht daher auch das Vertrauen in die jeweils angewandte Technologie im Vordergrund. Einfachheit und Verständlichkeit sollten daher oberstes Ziel jeder IAM-Anwendung sein – heute genauso wie in Zukunft.

Jens Fromm, Jan Ziesing



Jan Ziesing leitet das Fraunhofer-Innovationscluster „Next Generation ID“ am Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS) in Berlin.



Jens Fromm leitet das Kompetenzzentrum „Öffentliche IT“ am Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS) in Berlin.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Was bringt softwaregestütztes Identity & Access Management?**
(www.tecchannel.de/2053455)
- **Worauf es bei Single-Sign-On-Lösungen ankommt**
(www.tecchannel.de/2040883)
- **Das Smartphone als sichere Zutrittskontrolle nutzen**
(www.tecchannel.de/2045218)

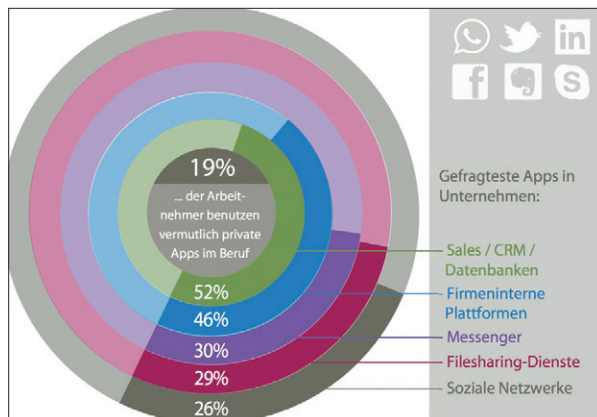
3 Mobile Security

Die wachsende Popularität mobiler Clients macht diese Geräte für Angriffe auf IT-Systeme interessant. Die Abwehr von Manipulation, Identitätsdiebstahl, Datenklau, Spionage und Sabotage ist daher ein vordringliches Ziel im Rahmen der Mobile Security. Es gilt, die mobilen Clients unter minimalen Auswirkungen auf die Geräteleistung vor gegenwärtigen Sicherheitsbedrohungen zu schützen.

3.1 Mobile Daten effizient schützen

IT-Abteilungen, Compliance-Fachleute und Chief Security Officers von Unternehmen müssen sich in immer stärkerem Maße damit auseinandersetzen, wie sich Smartphones, Tablets und Ultrabooks in Geschäftsabläufe integrieren lassen. Und dies, ohne dass Sicherheitsprobleme entstehen oder Geschäftsdaten in falsche Hände geraten. Laut einer Studie von IDC Deutschland zum Thema „Enterprise Mobility“ arbeiten 57 Prozent der Beschäftigten in Deutschland zumindest teilweise mit Mobilgeräten. Mehr als die Hälfte der befragten Unternehmen (54 Prozent) hat daher bereits eine Mobility-Strategie implementiert. Weitere 25 Prozent wollen das innerhalb der nächsten zwei Jahre zu tun.

Mobile Flexibilität: Laut einer Untersuchung von Citrix nutzen rund 19 Prozent der Arbeitnehmer private Apps auf Mobilsystemen, die sie auch für berufliche Zwecke einsetzen. Dies kann Sicherheitsrisiken mit sich bringen. (Quelle: Citrix)



Zu denken gibt, dass 16 Prozent der befragten IT- und Fachbereichsleiter einräumten, ihnen sei in den vergangenen Jahren mindestens einmal ein Mobilgerät mit Firmendaten an Bord abhandengekommen. Um die Risiken durch gestohlene oder unzureichend abgesicherte Mobilsysteme zu minimieren, sehen 52 Prozent der Entscheider ein Mobile Device Management (MDM) und eine Mobile-Security-Strategie als unverzichtbar an.

3.1.1 Fehlerhafte Mobile-Security-Strategien

In der Praxis werden bei der Umsetzung einer Mobile-Security-Strategie laut einer Untersuchung der Beratungsgesellschaft Deloitte (www.deloitte.com/de/) allerdings häufig Fehler gemacht. Folgende Vorgehensweisen seitens der IT-Abteilung seien besonders oft zu beobachten:

3.1.2 Die Nein-Sager

Die IT-Verantwortlichen sagen schlichtweg „Nein“: Der Einsatz von Smartphones, Notebooks und Tablet-Rechnern wird weitgehend unterbunden. Dies gilt insbesondere für private Geräte, die Beschäftigte im Unternehmen einsetzen wollen. Als Gründe führen IT-Fachleute Sicherheitsrisiken und mögliche Verstöße gegen Compliance-Regeln an. Es liegt auf der Hand, dass eine solche rigide Haltung kaum durchzuhalten ist – zum einen deshalb, weil dadurch die Produktivität der Mitarbeiter leidet, zum anderen, weil moderne Geschäftsprozesse kürzere Reaktionszeiten erfordern. Diese können nur dann erreicht werden, wenn Mitarbeiter auch auf einer Dienstreise oder vom Home-Office aus ihre Aufgabe erledigen können. Hinzu kommt, dass die IT-Abteilung spätestens dann klein begeben muss, wenn Führungskräfte darauf bestehen, dass sie selbst und ihre Abteilungen mit Mobilsystemen ausgestattet werden.

3.1.3 Einfach mal ein MDM-System kaufen

Die IT-Abteilung beschafft das erstbeste Mobile-Device-Management (MDM)-System und wähnt sich damit auf der sicheren Seite: Dies ist schon deshalb fahrlässig, weil es derzeit mehr als 100 unterschiedliche MDM-Lösungen auf dem Markt gibt. Sie unterscheiden sich erheblich in Bezug auf den Funktionsumfang, die Bereitstellungsmodelle (Cloud, Installation im Firmenrechenzentrum) und die Einbindung in die vorhandene IT-Management-Landschaft. IT-Fachleute sollten daher zunächst prüfen, welche mobilen Endgeräte im Unternehmen verwendet werden, welche Sicherheitsforderungen im Bereich „Mobility“ bestehen und welche Anforderungen die Anwender an Mobilsysteme und darauf abgestimmte Arbeitsabläufe haben, bevor sie ein MDM-System anschaffen.

3.1.4 Alle dicht

Die IT-Abteilung macht „die Schotten dicht“: Dies bedeutet, dass alle potenziell gefährlichen Funktionen des Mobilsystems deaktiviert werden. Dies kann beispielsweise die Installation oder Nutzung bestimmter Anwendungen betreffen, etwa Whatsapp oder Facebook, aber auch den Zugriff auf bestimmte Web-Services wie Musikdienste. Die Folge: Anwender suchen nach Wegen, solche Restriktionen

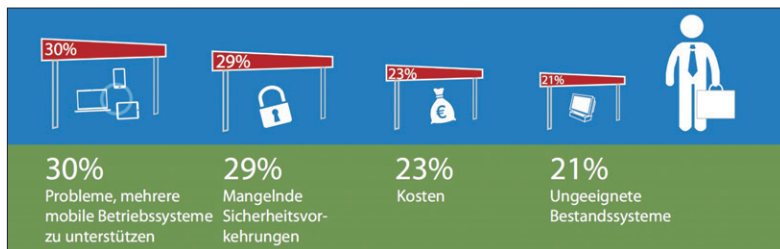
zu unterlaufen. Sie greifen verbotenerweise zu nicht „kastrierten“ privaten Systemen, oder sie weigern sich, an einem „Bring Your Own Device“-Programm des Unternehmens teilzunehmen. Ein weiteres Problemfeld: Cloud-basierte Storage- und File-Sharing-Dienste werden ohne Wissen der IT-Abteilung verwendet, wenn diese keine Alternativen bereitstellt.

3.1.5 Private Endgeräte

Der Einsatz privater Endgeräte wird unzureichend geregelt: Umgekehrt sind manche Unternehmen allzu liberal, wenn es um BYOD geht. Wenn überhaupt, werden nur wenige Grundregeln eingeführt, etwa dass Systeme mit einem bestimmten Betriebssystem nicht verwendet werden dürfen, weil dieses überholt ist. Das kann dazu führen, dass im Unternehmen viele unterschiedliche Systemplattformen unterstützt werden müssen. Dies wiederum erhöht den Support-Aufwand und führt zu Sicherheitsrisiken.

3.1.6 Problemfall IT-Abteilung

Die IT-Abteilung ist paralysiert: Angesichts der Komplexität, die mit dem Management und der Absicherung mobiler Geräte verbunden ist, sind laut Deloitte manche IT-Abteilungen überfordert. Sie wissen nicht, welche Maßnahmen sie treffen sollen, und „ducken“ sich gewissermaßen weg. Diese Strategie ist naturgemäß mit hohen Risiken verbunden und in hohem Maße kontraproduktiv.

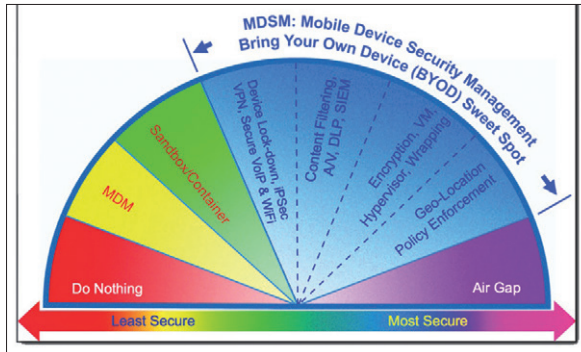


Hürden in Sachen Mobility: Einer Umfrage von Citrix unter IT-Fachleuten zufolge sind potenzielle Sicherheitsrisiken ein Grund dafür, dass Mobility-Strategien in Unternehmen nur zögerlich oder gar nicht umgesetzt werden. (Quelle: Citrix)

3.1.7 Restriktives Vorgehen

Restriktive Strategien sind in der Praxis in speziellen Branchen anzutreffen: „In unserem Unternehmen ist es schlichtweg untersagt, private Mobilgeräte zu verwenden“, sagt beispielsweise eine leitende Mitarbeiterin der IT-Abteilung eines ita-

lienisch-deutschen Bankhauses in München. „Als Mobiltelefone kommen immer noch BlackBerrys zum Einsatz, zudem Notebooks, die zentral von der IT-Abteilung bereitgestellt und verwaltet werden.“



Umfassender Schutz: Die amerikanische Sicherheitsfirma Mobile Active Defense hat Mobile-Security-Technologien anhand ihrer Schutzwirkung klassifiziert. Ein Mobile Device Management (MDM) allein ist demnach unzureichend. (Quelle: Mobile Active Defense)

Wer gegen diese Regelungen verstößt, riskiert der IT-Fachfrau zufolge eine Abmahnung oder gar die Kündigung. Die Folge: Mitarbeiter nutzen für offizielle Tätigkeiten ihre BlackBerrys, setzen aber sehr wohl daneben eigene Smartphones ein. Allerdings, so die IT-Spezialistin, würden diese privaten Systeme nicht – oder zumindest nicht mit Wissen der IT-Abteilung – in das Firmennetz der Bank integriert. Wie schnell sich eine solche homogene Mobility-Welt in ein buntes Miteinander diverser Plattformen verwandeln kann, belegt ein zweites Beispiel: der Fahrzeughersteller MAN. Auch dort war vor der Übernahme des Unternehmens durch den VW-Konzern nach Angaben eines IT-Spezialisten, der nicht namentlich genannt werden will, BlackBerry das Maß aller Dinge. Mitarbeiter waren mit entsprechenden Endgeräten ausgestattet. Als zentrales Kommunikationssystem diente der BlackBerry Enterprise Server.

„Jetzt müssen wir auf Wunsch von VW-Managern, die Führungsaufgaben bei MAN übernehmen, auch iPhones und iPads unterstützen“, sagt der IT-Fachmann. „Für uns bedeutete es einen erheblichen Aufwand, diese neuen Systeme in die IT-Infrastruktur zu integrieren und auf die entsprechenden Prozesse abzustimmen.“ Ein weiterer Effekt dieses Politikwechsels: Nun haben Mitarbeiter den Wunsch geäußert, dass auch Android-Smartphones und -Tablets unterstützt werden.

3.1.8 Technische Lösungen: von Containern bis hin zu Spaces

IT-Fachleute, die Daten und Anwendungen auf Mobilsystemen schützen möchten, haben die Wahl zwischen mehreren Techniken. Hoch im Kurs stehen bei etlichen Herstellern von Sicherheitslösungen sogenannte Container: „Nach unserer

Auffassung bieten Container ein hohes Schutzniveau und erlauben es zudem, private und geschäftliche Daten auf einem Mobilgerät zu trennen“, sagt Rüdiger Trost, Senior Sales Engineer beim finnischen IT-Security-Spezialisten F-Secure. Dies wiederum würde die Einführung von BYOD-Programmen (Bring Your Own Device) in Unternehmen erleichtern. Ein Container ist ein verschlüsselter, durch ein Passwort geschützter Bereich auf einem Mobilgerät, der mithilfe einer speziellen Software eingerichtet wird. Er agiert unabhängig von der „normalen“ Arbeitsumgebung des Smartphones oder Tablet-Rechners. In solchen Containern werden Geschäftsdaten und Anwendungen abgelegt, etwa E-Mail, Geschäftskontakte, Kalender und Browser, außerdem unternehmensspezifische Applikationen.

Vorteile der Containertechnik sind das hohe Sicherheitsniveau und die Möglichkeit, den Einsatz privater Endgeräte für geschäftliche Zwecke zu erlauben, ohne dass es zu einer Vermengung privater und beruflicher Daten und Anwendungen kommt. Die IT-Abteilung hat zudem die Kontrolle über die Container, kann also deren Inhalt ändern oder diese „Behälter“ komplett löschen.

Zu den Nachteilen zählt, dass viele Containertechnologien herstellerspezifisch sind. Dies bedeutet, dass sich der Anwender an einen Anbieter bindet. Hinzu kommt, dass einige Lösungen ein Rekompilieren der ursprünglichen Anwendung mithilfe von Software Development Kits (SDKs) erfordern. Das schränkt die Zahl der unterstützten Applikationen ein. Anbieter derartiger Containerlösungen sind unter anderem Citrix und Good Technology.

3.1.9 App Wrapping: Anwendungen werden eingepackt

Ohne SDKs kommen „App Wrapper“ aus. Der Anbieter, beispielsweise MobileIron oder VMware AirWatch, modifiziert in diesem Fall den ausführbaren Code einer Anwendung. Hinzugefügt werden beispielsweise Sicherheitsregeln. Diese legen fest, wo welche Daten gespeichert werden und über welche Verbindungen diese transportiert werden dürfen. Dieser Ansatz weist ähnliche Vorteile auf wie das „Containerisieren“ von Apps und Daten, insbesondere die Trennung zwischen privaten und geschäftlichen Bereichen auf einem Mobilgerät.

Schutzschild: Bei App Wrapping werden in eine mobile Anwendung beispielsweise unternehmenseigene Sicherheitsregeln „injiziert“. Dies kann mithilfe von Software Development Kits erfolgen, allerdings auch ohne massive Änderungen am Programmcode der Applikation. (Quelle: Good Technology)



Zu den potenziellen Problemen zählt, dass manche Hersteller von Anwendungen es untersagen, deren Code zu modifizieren. Zudem ist das Patchen solcher ummantelter Anwendungen komplexer als bei Originalapplikationen. Vor allem bei Standardapplikationen, die beispielsweise über die App-Stores von Google, Apple, Microsoft oder auch RIM/BlackBerry bezogen werden, sind Techniken wie Wrapping mit einem höheren Aufwand verbunden und lassen sich wegen des mangelnden Zugriffs auf den Programmcode oft gar nicht umsetzen.

Mittlerweile werben etliche Anbieter wie etwa Good Technology oder Apperian mit einem „App Wrapping ohne Coding“. So ersetzt beispielsweise die Good Dynamics Secure Mobility Platform Standardsystemaufrufe durch „Secure Calls“ von Sicherheitsbibliotheken von Good. Auch IT-Fachleute ohne profunde Programmierkenntnisse können so laut Good mobile Anwendungen „einpacken“.

Mit dem Good Dynamics SDK dagegen lassen sich Container erzeugen, indem der Programmcode der Anwendungen geändert wird. Dieses Verfahren eignet sich vorzugsweise für Apps, die ein Unternehmen selbst entwickelt hat. Der erhöhte Aufwand zahlt sich laut Good durch einen größeren Funktionsumfang aus: Apps können so konzipiert werden, dass sie untereinander auf sichere Weise Daten austauschen, oder applikationsspezifische Policies können über dieselbe zentrale Managementkonsole gesteuert werden, über die die Verwaltung von Standardsicherheitsregeln erfolgt.

3.1.10 Virtualisierung: Desktops und Anwendungen im Rechenzentrum

Gerade in jüngster Zeit haben Ansätze wie virtualisierte Desktops im Mobilbereich an Boden gewonnen. Ein Grund dafür ist, dass die erforderlichen Mobilfunkverbindungen oder Anbindungen über ein öffentliches Wireless LAN mittlerweile erschwinglich sind. Das gilt insbesondere für den Zugriff auf Desktop-Umgebungen über 3G- und 4G-Netze.

Unternehmen wie Citrix und VMware bieten solche virtualisierten Desktop-Umgebungen an (Virtual Desktop Infrastructures, VDIs). Anwendungen und Daten werden im Firmen-Data-Center oder in einem Cloud-Rechenzentrum vorgehalten. Der Nutzer greift darauf über VPN-Verbindungen (Virtual Private Network) vom Mobilgerät aus zu. Weder Anwendungen noch Daten werden auf dem Endgerät gespeichert – ein Vorteil in puncto Sicherheit.

Dem stehen Nachteile wie die Abhängigkeit von einer Datenverbindung und die eingeschränkte Zahl von Anwendungen gegenüber. Denn Original-Apps auf dem Endgerät, mit denen ein User vertraut ist, lassen sich bei diesem Ansatz nicht einsetzen. Zudem müssen die Anwendungen im Rechenzentrum auf die eingesetzten Mobilgeräte hin zugeschnitten werden, etwa die Displays (Größe, Auflösung) und die verwendeten Browser. Das verursacht einen höheren Aufwand.

3.1.11 Virtualisierung als App oder im Betriebssystem

Die Virtualisierungstechniken im mobilen Bereich lassen sich grundsätzlich in zwei Kategorien einteilen:

Typ-1-Hypervisors: Sie setzen direkt auf der Hardware des Mobilgeräts auf („Bare Metal“). Betriebssystem und Apps werden in Form von Virtual Machines auf dem Hypervisor ausgeführt. Dadurch ist es möglich, zwei komplett getrennte Systeme (Virtual Machines) aufzusetzen – eines für den privaten Gebrauch und eines für berufliche Zwecke. Als Ergänzung kann eine Verschlüsselung der Daten erfolgen, sowohl auf dem Endgerät auf der VM-Ebene als auch beim Transport. Der Nachteil: Dieses Verfahren ist aufwendig und erfordert eine dauerhafte Unterstützung durch den Hersteller des Mobilgeräts.

Typ-2-Hypervisors: Sie werden wie eine App auf dem Endgerät ausgeführt und erzeugen dort gewissermaßen ein zweites, virtualisiertes Smartphone oder Tablet. Auch in diesem Fall lassen sich private und berufliche Bereiche auf dem Endgerät trennen. Allerdings wirken sich Typ-2-Hypervisors negativ auf die Batterielaufzeit und Performance des Endgeräts aus. Zudem muss die Virtualisierungsfunktion Zugriff auf zentrale Funktionen des Betriebssystems haben.

3.1.12 Spezielle Ansätze: Samsung KNOX und Mobile Spaces

Einen eigenen Weg geht Samsung mit Knox. Diese Virtualisierungslösung setzt auf Security Enhanced Android (SE Android) auf und klinkt sich sowohl in die Hardware als auch in die Software eines Samsung-Galaxy-Systems ein. Ein Vorteil: Knox bietet eine AES-Verschlüsselung mittels AES (Advanced Encryption Standard) mit 256-Bit-Schlüsseln auf der Hardwareebene. Der User kann das Endgerät wie gewohnt einsetzen. Der Start der virtualisierten Arbeitsumgebung erfolgt über einen Button auf der Benutzeroberfläche. Zudem ist die Anbindung an MDM-Lösungen von Anbietern wie MobileIron möglich.

Ein Nachteil: SE Android wurde vom US-Geheimdienst NSA entwickelt. Auch wenn dieser nach eigenen Angaben keine Hintertüren in das Betriebssystem eingebaut hat, bleiben nach den Enthüllungen von Edward Snowden über die Ausspähaktionen der NSA Zweifel. Auf dem Mobile World Congress 2014 im Februar in Barcelona stellte Samsung Version 2.0 von Knox vor. Eine gravierende Änderung: Samsung hat selbst entwickelte MDM-Funktionen in Knox integriert.

Eine virtualisierte Runtime-Umgebung auf dem Mobilgerät richtet auch Mobile Spaces von der gleichnamigen amerikanischen Firma ein. Eine Besonderheit der Lösung ist, dass der Hersteller sie mit Mobile-Application-Management-Funktionen ausgestattet hat. So steht eine Agent-App zur Verfügung, die als App-Starter dient. Sie stellt dem User eine Liste mit Anwendungen zur Verfügung, die von der

IT-Abteilung freigegeben wurde. Der Nutzer wählt eine dieser Applikationen aus, die anschließend von Mobile Spaces gestartet wird. Das heißt, es erfolgt kein direkter Aufruf von Apps durch den Nutzer. Diese Aufgabe übernimmt Mobile Spaces.

3.1.13 Ein Trend: Mobile Application Management

Zu den Entwicklungen, die den Bereich Mobile Security in den kommenden Monaten prägen werden, zählt die Integration von Funktionen für das Mobile Application Management (MAM) in Mobilbetriebssysteme. Dies ist unter anderem bei Samsung KNOX und iOS 7 der Fall. Auch VMware beschreitet mit Horizon Mobile diesen Weg. Der Vorteil: Apps, die für die entsprechenden Betriebssysteme und Hardwareplattformen freigegeben wurden, lassen sich ohne Hilfe von Tools verwalten, die Drittanbieter bereitstellen. Der Nachteil: Die Zahl der unterstützten Endgeräte und Betriebssystemversionen ist stark eingeschränkt.

MAM-Lösungen solcher Drittanbieter unterstützen dagegen eine breitere Palette von Endgeräten, etwa Android-Systeme unterschiedlicher Hersteller. Dafür muss die IT-Abteilung inkaufnehmen, dass sich mit solchen Werkzeugen nur eine begrenzte Zahl von Apps verwalten lässt. Doch gleich, ob integraler Bestandteil eines Betriebssystems oder externe Applikation – eine zentrale Verwaltung von mobilen Anwendungen wird im Zusammenhang mit Mobile Security immer wichtiger.

3.1.14 Eine weitere Entwicklung: über MIM zu Mobile Risk Management

Bei den Anwendern und den Anbietern von Lösungen für das „mobile Unternehmen“ gewinnt zudem ein weiterer Aspekt an Bedeutung: die Absicherung und das Management der Daten selbst sowie der Verbindungen, über die diese Informationen transportiert werden. Das bestätigt auch F-Secure-Fachmann Rüdiger Trost: „Mobile Security hat viele Facetten, vom Virenschutz und von einer Firewall auf einem mobilen Endgerät über den Schutz von Geschäftsinformationen mittels Verschlüsselung und Virtualisierung bis hin zu VPNs und speziellen Cloud-Sharing-Lösungen.“ Mithilfe gesicherter Cloud-Speicher können Geschäftskunden Daten auf sichere Weise mit Kollegen und Partnerfirmen teilen und gemeinsam bearbeiten. „Allerdings sollte ein Unternehmen im Vorfeld festlegen, welche Daten in solchen Online-Speicherplätzen gespeichert werden dürfen. Dies setzt eine Klassifizierung der Unternehmensdaten und wirkungsvolle Policies voraus“, so Trost weiter, Stichwort Mobile Information Management (MIM).

Derzeit beschränken sich Lösungen für das Mobile Information Management in der Regel auf Produkte, die die Freigabe und das Synchronisieren von Dateien regeln, beispielsweise Citrix ShareFile oder AppSense DataNow. Ein „echtes“ MIM sollte jedoch den Zugriff und den Transfer aller Arten von Informationen von und

zu mobilen Systemen erfassen, etwa auch den Inhalt von E-Mails, nicht nur deren Attachments. Hier spielen andere IT-Disziplinen mit hinein wie etwa Data Loss Prevention und Information Lifecycle Management.

Oliver Schonschek, Research Fellow bei der Marktforschungs- und Beratungsfirma Experton Group, geht noch einen Schritt weiter: Angesichts der Risiken, die mit dem Einsatz von Mobile Enterprise Solutions verbunden sind, hält er ein Mobile Risk Management (MRM) für erforderlich. Dieser Ansatz stellt nicht allein die Sicherheit von Geräten, Anwendungen oder Daten in den Mittelpunkt, sondern erfasst alle Risiken, die mit dem Einsatz von mobilen Systemen und Anwendungen für ein Unternehmen verbunden sind. MRM schließt eine Risikobewertung und Priorisierung von Maßnahmen mit ein. Somit sei ein Mobile Risk Management gewissermaßen der Überbau von MDM, MAM und MIM.

Bernd Reder

Bernd Reder ist freier Journalist mit den Schwerpunkten Netzwerke, IT und Telekommunikation in München.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Die Buchstabensuppe rund um Mobile Management**
(www.tecchannel.de/2056058)
- **Das müssen Unternehmen bei der Einführung einer MDM-Lösung beachten**
(www.tecchannel.de/2047917)
- **Cloud- und Social-Media-Daten richtig verschlüsseln**
(www.tecchannel.de/2049929)
- **Das Smartphone als sichere Zutrittskontrolle nutzen**
(www.tecchannel.de/2045218)
- **So vernichten Sie Daten und Datenträger richtig**
(www.tecchannel.de/2048681)
- **50 Tipps & Tricks: Facebook sicher nutzen**
(www.tecchannel.de/2055378)
- **Mobile first – aber bitte ohne Risiko**
(www.tecchannel.de/2056967)
- **So sichern Sie mobile Systeme richtig ab**
(www.tecchannel.de/2056373)
- **In sechs Schritten zu mehr Cloud-Security**
(www.tecchannel.de/2045411)
- **Private Cloud und Public Cloud sicher verbinden**
(www.tecchannel.de/2040713)

3.2 Schutz vor Spionage und Datenmissbrauch

Unternehmen stellen ihre Mitarbeiter zunehmend mit Smartphones oder Tablets aus. Die neuen Kommunikationswerkzeuge sind allerdings nur halb so effektiv und attraktiv, wenn aus Sicherheitsgründen die Nutzung von Apps untersagt wird. Vom technikfernen Ansatz „Mitarbeiter werden vertraglich verpflichtet, Sicherheitsregeln bei der Nutzung ihrer Smartphones einzuhalten“ bis hin zur technisch aufwendigeren „Trennung des geschäftlichen und privaten Bereichs“ gibt es ein breites Spektrum an Möglichkeiten in unterschiedlich restriktiven Ausprägungen.

Unternehmen bewegen hierbei Fragen zum Arbeitsrecht, zur Einhaltung und Erweiterung von Gesetzen und Richtlinien, zur Corporate-Governance-Kompatibilität, zur Haftung oder zur Verwaltung und Synchronisation der Geräte und Daten. Die erste Herausforderung für CIOs und IT-Security-Verantwortliche entsteht durch die große Vielfalt an Endgeräten für die gängigen Betriebssysteme Android, iOS, Windows Phone und BlackBerry. Sie kann durch moderne Mobile-Device-Management-Systeme wie AirWatch, MobileIron, SAP Afaria oder 7P mittlerweile komfortabel bewältigt werden. Im Bereich der genutzten Software, der Apps, herrscht allerdings in den meisten Unternehmen ein undurchschaubarer Wildwuchs. Das Mobile Application Management wird deshalb zum zentralen Bestandteil einer ganzheitlichen Enterprise-Mobility-Strategie. Standardisierte Regeln und Kontrollen sind unumgänglich.

3.2.1 Gefahren durch Apps auf Tablets und Smartphones im Unternehmen

Laut aktuellen Zahlen verschiedener unabhängiger Testlabore steigt die Zahl der Sicherheitslücken und Schadsignaturen in Smartphone- und Tablet-Apps rasant. „mediaTest digital“ und das Fraunhofer-Institut haben kürzlich unabhängig voneinander Statistiken veröffentlicht, aus denen hervorgeht, dass jede zweite App über alle mobilen Betriebssysteme hinweg sicherheitskritisches Verhalten und Schadprofile aufweist.

Apps fehlt häufig die Transparenz im Umgang mit personenbezogenen Daten und erhobenem Nutzungsverhalten. Zudem wird Datensammeln und Spionieren die Arbeit durch mangelnde Sensibilisierung der App-Nutzer sowie fehlende Schutzmechanismen begünstigt. Für Unternehmen bedeutet die massenhafte und teils ungeschützte Übertragung sensibler Daten ein enormes Risiko, da unternehmensinterne Informationen in die falschen Hände gelangen. Aktuelle Enthüllungen rund um die NSA und andere Geheimdienste unterstreichen, in welchem Umfang personen- oder unternehmensbezogene Daten erhoben und ausgewertet werden. Die typischen Schadprofile und Sicherheitslücken in öffentlich zugänglichen Apps sind breit gefächert. Sie beginnen bei der ungefragten Einräumung von Berechni-

gungen und Zugriffen auf sensible Informationen wie Kontaktdaten, E-Mails, Passwörter, Kreditkartendaten, Kalendereinträge oder Standortdaten. Hinzu kommen Sicherheitslecks wie der unverschlüsselte und ungefragte Versand von Daten.

In vielen Fällen werden die Daten an Werbenetzwerke und Tracking-Anbieter geleitet – ohne Zustimmung der Nutzer und somit auch ohne Wissen des Arbeitgebers. Hinzu kommen bekannte Schadsignaturen wie Malware und Viren, die insbesondere bei Android-Geräten weit verbreitet und schwer kontrollierbar sind.

3.2.2 Beispiele für Bedrohungen

Im Folgenden sind einige beispielhafte Bedrohungen aufgelistet, die Unternehmen beim Einsatz von Smartphones und Apps bedenken sollten:

Datenspionage durch die Cloud

Neben der massenhaften Erhebung und Speicherung von Kommunikationsdaten durch die NSA und andere Geheimdienste sind insbesondere Cloud-Dienste anfällig für Spionageattacken. Die bekannten Cloud-Anbieter haben ihren Sitz in den USA und unterliegen somit dem Patriot Act. Sie müssen die Daten ihrer Nutzer auf Anfrage der Regierungsbehörden jederzeit herausgeben, auch ohne den konkreten Verdacht einer Straftat. Dass diese Möglichkeiten in der Vergangenheit verstärkt missbraucht wurden, ist hinreichend bekannt. Cloud-Dienste sollten nur verwendet werden, wenn der Anbieter in Deutschland oder mindestens in Europa sitzt und die abgelegten Daten hochverschlüsselt sind, sodass selbst der Betreiber keine Möglichkeit der Einsichtnahme hat.

Systematische Angriffe auf E-Mail-Accounts

Im Januar 2013 berichtete die „New York Times“, dass über den Zeitraum von vier Monaten ihre E-Mail-Accounts systematisch ausspioniert wurden. Seit Februar 2014 wird Rewe mit Daten erpresst, die ein Hacker aus dem E-Mail-Account eines Vorstandmitglieds gestohlen hat. Ob dies über einen stationären Zugriff oder den Zugang über sein Smartphone geschehen ist, ist bisher nicht bekannt. Es macht jedoch deutlich, wie wichtig eine vernünftige Absicherung der Smartphones und E-Mail-Apps ist.

Übermittlung der Standortdaten (GPS)

Die unverschlüsselte Übermittlung von Geodaten ist eine der häufigsten unbemerkten Sicherheitslücken in Smartphone-Apps. Für Unternehmen ergeben sich daraus das Risiko der Überwachung von Mitarbeitern und somit der Verlust vertraulicher und schützenswerter Informationen.

Hinzu kommt, dass durch die Erhebung von Standortdaten nicht nur der aktuelle Aufenthaltsort ermittelt, sondern auch der künftige vorhergesagt werden kann, was kürzlich britischen Studenten eindrucksvoll geglückt ist. Sie konnten auf Basis

von Telefonnummern, GPS-Verläufen, Anrufen, versendeten SMS, Adressbüchern sowie Bluetooth- und WLAN-Verbindungen bei 200 freiwilligen Smartphone-Nutzern mit einer Genauigkeit von bis zu drei Metern vorhersagen, wo sich der Nutzer künftig befinden wird.

Internationale Spionage

Immer häufiger finden Sicherheitsexperten chinesische Schadsoftware auf Geräten mittelständischer Unternehmen. In diesem Fall steht das Ziel der Industriespionage im Vordergrund, was sich nicht zuletzt in der Überschwemmung des Marktes mit Plagiaten manifestiert. Vertrauliche Konstruktionszeichnungen und Fotos aus Forschungsabteilungen stehen hoch im Kurs.

Diese Bedrohung ist eines von vielen Beispielen, bei denen die Gefahr aus dem stationären PC-Bereich auf die mobile Infrastruktur übergeht. Einige Unternehmen schützen sich bereits vor diesen Gefahren, indem sie die Smartphone-Kameras deaktivieren. Da jedoch sensible Daten wie Fotos und Zeichnungen nicht nur per Kamera, sondern auch über E-Mails, Cloud-Dienste oder Messenger-Apps auf die Geräte gelangen, sollte die Softwareseite ebenso gewissenhaft überprüft werden.

3.2.3 MAM: für eine sichere mobile Infrastruktur

Die oben genannten Beispiele zeigen das breite Spektrum an Bedrohungen für die mobile IT-Infrastruktur und für sensible Unternehmensdaten. Das Mobile Application Management (MAM) gibt Unternehmen als Teil der Enterprise Mobility Strategie die Werkzeuge an die Hand, die nötig sind, um dem Datenkontrollverlust entgegenzuwirken.

Mobile Application Management beinhaltet Software- und Servicelösungen, die die Nutzung von Apps auf betrieblich genutzten Smartphones und Tablets nach Unternehmensrichtlinien gewährleisten und absichern. Berücksichtigt werden dabei sowohl eigens entwickelte, interne Apps als auch Apps aus öffentlich zugänglichen App Stores wie iTunes von Apple oder Google Play für Android.

Eine skalierbare Sicherheitsprüfung von Apps wird von einigen unabhängigen Testinstituten angeboten. Es sollte darauf geachtet werden, deutsche Anbieter zu wählen, da diese einen entsprechend hohen Anspruch an Datenschutz- und Datensicherheitsmerkmale der Apps stellen und bei ihren Prüfungen die Vorgaben aus dem Bundesdatenschutzgesetz berücksichtigen. Darüber hinaus ist es sinnvoll, einen Anbieter zu wählen, der weitestgehend auf das Prüfen von Apps spezialisiert ist. Durch die große Dynamik des App-Marktes und die hohe Update-Frequenz haben nur wenige Anbieter bisher die Möglichkeit und die technologischen Voraussetzungen, standardisiert, skalierbar und trotzdem tief greifend und zuverlässig zu prüfen. Im Anschluss an das Testing bieten vereinzelte Institute schon die Möglichkeit, die Testergebnisse in Form von White- und Blacklisting-Katalogen zu bündeln und sie über die App Stores der Mobile-Device-Management (MDM)-

Systeme automatisiert auf die Geräte der Mitarbeiter auszurollen. Dieses integrierte Vorgehen bildet das Herzstück des Mobile Application Managements und schützt Unternehmen zunehmend vor aufwendigen Recherchen, händischen App-Freigaben und kostspieligen Datenverlusten. Das MAM arbeitet eng verzahnt mit dem Mobile Device Management und schafft im Zusammenspiel eine integrierte und standardisierte Umgebung.

3.2.4 Weitere Disziplinen des Enterprise Mobility Managements

Um eine sichere und nachhaltige Enterprise-Mobility-Strategie zu verfolgen, sollte neben den beiden beschriebenen Bereichen (Mobile Application Management und Mobile Device Management) auch die dritte Disziplin, das Mobile Information Management (MIM), berücksichtigt werden.

Beim Mobile Information Management stehen Cloud-basierte Services im Hinblick auf den geräteübergreifenden Austausch, die Speicherung, die Synchronisation und die Kontrolle von Daten, Medien und Dokumenten im Mittelpunkt. Eine der wichtigsten Funktionen des MIM ist die sichere Kontrolle der Daten. Sie ermöglicht das Vorhalten verschlüsselter Daten und gewährt ausschließlich vertrauenswürdigen Anwendungen Zugriff darauf.

Die drei Kerndisziplinen des Enterprise Mobility Managements werden durch das Enterprise Mobility Consulting (EMC) vervollständigt. Das EMC beantwortet alle Fragen, mit denen sich Unternehmen bei der Einführung von Enterprise-Mobility-Konzepten konfrontiert sehen. Beim EMC wird ein Fünf-Stufen-Prozess durchlaufen, an dessen Ende eine individuelle Enterprise-Mobility-Strategie steht.

Die drei wichtigsten Praxistipps für eine ganzheitliche MAM-Strategie im Unternehmen sind:

- Absichern der im Unternehmen verwendeten Apps
- Absichern der eigenen Apps durch Audits und Zertifikate
- Einführen von Sicherheitsrichtlinien (für App-Entwicklung und Nutzung von Apps im Unternehmen)

Weitere Informationen zum Enterprise Mobility Management finden Sie auch im Artikel „*So sichern Sie die mobile Infrastruktur ab*“ (www.tecchannel.de/2059338).

Sebastian Wolters



Sebastian Wolters ist Co-Founder und Geschäftsführer der mediaTest digital GmbH.

3.3 So sichern Sie mobile Systeme richtig ab

Regelwerke (Policies) sind ein Mittel, Mobilsysteme, Anwendungen und Unternehmensdaten abzusichern. Doch welche Punkte sollte eine Policy enthalten? Nach Angaben der IT-Security-Firma Sophos lassen sich unter anderem folgende Einzelregelungen in eine Policy integrieren:

Betriebssysteme

Festgelegt wird, dass Mobilsysteme beispielsweise unter aktuellen Betriebssystemen laufen müssen, etwa unter iOS ab Version 6.x oder Android 4.x. Dies minimiert die Gefahren, die von Geräten mit veralteter Systemsoftware ausgehen, weil für sie eventuell keine Sicherheits-Updates mehr verfügbar sind.

Passwortverwaltung

Alle vom User gespeicherten Passwörter müssen in einem besonders geschützten und verschlüsselten Passworttresor auf dem System abgelegt werden.

Passwortstärke

Der Zugriff auf das System wird mithilfe eines starken Passworts abgesichert, das den firmenweiten Regelungen für das Passwortmanagement entsprechen muss. Das heißt beispielsweise, dass nur Passcodes mit mindestens acht Ziffern, Buchstaben und Sonderzeichen verwendet werden dürfen, dass mindestens eine Ziffer und ein Sonderzeichen vorhanden sind und dass das Passwort nach einem bestimmten Zeitraum gegen ein neues getauscht werden muss.

Zugriff auf das Firmennetzwerk

Nur Endgeräte, die von der IT-Abteilung verwaltet werden, dürfen direkt mit dem Corporate Network verbunden werden. Zudem werden für einzelne User-Gruppen Zugriffsrechte definiert. Sie beziehen sich auf beispielsweise auf Anwendungen, Daten oder Netzwerklaufwerke.

Regeln für User

Ob solche Regeln eingehalten werden, kann die IT-Abteilung kontrollieren, wenn ein Mobile Device Management (MDM) implementiert ist. Gleiches gilt für weitere Vorgaben, die einzuhalten sind. Diese betreffen beispielsweise folgende Punkte:

Verbot des „Rootens“

Der User darf sein System weder „rooten“ (Android) noch „jailbreaken“ (iOS), also Nutzungsbeschränkungen seitens des Systemanbieters (Apple) entfernen oder sich zum „Super-User“ aufschwingen. Jailbreaking beziehungsweise Rooten erleichtert es Angreifern, die Kontrolle über ein Endgerät zu übernehmen und sich in ein Firmennetzwerk vorzuarbeiten.



Bitte nicht: Rooten und Jailbreaken ist für Geräte im Business-Einsatz tabu.

Softwareinstallation

Es dürfen keine Programme aus dubiosen Quellen installiert werden, auch nicht auf privaten Geräten, die geschäftlich genutzt werden. Notfalls kann die IT-Abteilung eine „White List“ oder eine „Black Liste“ mit erlaubten beziehungsweise verbotenen Apps erstellen.

Meldung sicherheitsrelevanter Vorfälle

Bei Verlust eines Endgeräts muss der User dies umgehend der IT-Abteilung melden, damit sie das System remote löschen oder sperren kann.

Verschlüsselung

Falls die firmeninternen Sicherheitsrichtlinien das vorsehen, müssen System und Massenspeicher wie SD-Karten verschlüsselt werden.

Management und firmeneigene Software

Der Nutzer muss dulden, dass das Unternehmen firmenspezifische Software auf dem System installiert und es in das Systemmanagement einbindet. Dies schließt die Anbindung an Verzeichnisdienste wie Microsoft Active Directory oder LDAP mit ein. Über solche Dienste kann die IT-Abteilung rollenspezifische Zugriffsrechte vergeben.

Trennung privat – geschäftlich

Speziell bei privaten Systemen, die ein Nutzer auch im Unternehmen einsetzt, sollten beide Sphären getrennt sein. Das heißt beispielsweise, dass der Nutzer keine Geschäfts-E-Mails über private E-Mail-Accounts verschickt. Außerdem kann festgelegt werden, dass keine Synchronisation von privaten Daten wie Musikdateien mit Workstations im Unternehmen erfolgt.

Bernd Reder

3.4 iOS und Android – was taugt die eingebaute Sicherheit?

Smartphones sind kleine Computer und verbinden die Funktionen von Telefon, Media-Player, Handspielkonsole, Informationsdatenbank und Navi in einem einzigen Gerät. Kein Wunder also, dass Smartphones allen soeben genannten Gerätetypen langsam, aber sicher den Rang ablaufen. Aufgrund des umfassenden Angebots und des deutlich günstigeren Preises erfreuen sich Android-basierte Smartphones der stärksten Verbreitung, gefolgt vom Quasi-Erfinder des modernen Telefons, der Firma Apple. Windows-basierte Geräte sind zwar auf dem Vormarsch, spielen aber weiterhin in Europa nur eine kleinere Nebenrolle.

Allen Anbietern ist ein gemeinsames Konzept bei der Bereitstellung der Software für ihre Plattformen gemein. Es gibt je einen zentralen Anlaufpunkt, um die vom Benutzer ausgewählten Programme, die Apps (Abkürzung für Application – auf Deutsch Anwendung), auf das Mobilgerät verteilen. Dieser konzeptionelle Unterschied zu den Desktop-Betriebssystemen oder Frühformen der Mobile Devices auf Palm- oder Windows CE/Mobile-Basis wirft eine entscheidende Frage auf: Wie schützen uns die Anbieter vor schlecht programmierten Apps, die für mich ein Sicherheitsrisiko darstellen können?



Gute Frage: Wozu braucht eine Taschenlampen-App den Zugriff auf Push-Mitteilungen?

Grundsätzlich unterscheidet sich das Risiko zwar nicht vom herkömmlichen Desktop-Rechner, da dort Programme sogar aus beliebigen Quellen stammen können. Da aber Google, Apple und Microsoft über ihre Stores nun als alleiniger Händler für ihre Plattformen auftreten, erhöht sich automatisch der Anspruch an den Anbieter, denn eine Alternative steht nicht zur Verfügung: Der Hersteller produziert das Gerät, liefert die Infrastruktur und verkauft letztendlich als Zwischenhändler die gesamte Software – bei so viel gefühltem Monopol auf einem Haufen sollte das grundsätzliche Sicherheitskonzept stimmen.

3.4.1 Wirtschaftliche Schäden und Datenschutzrisiko

So praktisch die kleinen Mini-Programme auch sind, sie haben nicht nur Gutes. Insbesondere bei kostenlosen Apps muss sich der Anwender darüber im Klaren sein, dass das Programm oder die Dienstleistung zwar gratis ist, der Benutzer zahlt aber dafür mit seinen Daten. Das gibt Dr. Julian Schütte von der Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit AISEC (www.aisec.fraunhofer.de) in Garching bei München zu bedenken (www.fraunhofer.de/de/presse/presseinformationen/2013/November/sicherer-app-store-android.html).

Bei diesen Daten handelt es sich um den aktuellen Aufenthaltsort, E-Mail-Daten oder Adressinformationen. Diese Daten münden in personen- oder ortsbezogene Werbung. Das sei ja gar nicht so schlimm, könnte man meinen. Stimmt, wenn es nur um Privatinformationen geht. Übermitteln die Apps jedoch Informationen aus geschäftlichen E-Mails mit unternehmenskritischen Inhalten, Geopositionen von Mitarbeitern oder vertrauliche Kontaktdaten, so könnte ein wirtschaftlicher Schaden drohen, so Schütte weiter.

Malware-Angriffe: Bereits vor drei Jahren sah Symantec eine deutliche Gefahr für Android-basierte Geräte gegenüber Datenverlust und Malware-Angriffen. Daran hat sich grundlegend nichts geändert.

Resisting attack types		
Resistance to:	Apple iOS	Google Android
Web-based attacks		
Malware attacks		
Social Engineering attacks		
Resource Abuse/Service attacks		
Data Loss (Malicious and Unintentional)		
Data Integrity attacks		

Kostenlose Apps stellen in puncto Datensicherheit grundsätzlich ein Risiko dar, da die Verarbeitung gefundener Daten das eigentliche Geschäftsmodell des Anbieters darstellt. Auf welche Informationen eine App Zugriff haben möchte, gibt sie bei der Installation bekannt. Ohne Frage benötigt eine „Taschenlampen-App“ wohl kaum den Zugriff auf das Adressbuch. Wem der Datenzugriff zu weit geht, der wählt eine andere App mit ähnlichem Leistungsumfang. Da es für jeden erdenklichen Einsatz mehrere Apps gibt, besteht stets die Hoffnung, auf eine solche Alternative zu stoßen. Namhafte Anbieter reduzieren lieber den Leistungsumfang ihrer Lite-Editionen und hoffen so, den Interessenten zum Erwerb der kostenpflichtigen Vollversion zu erwärmen. Die Weiterverarbeitung von persönlichen Daten zu Werbezwecken gilt bereits als verpönt.

3.4.2 Apples Sicherheitskonzept beginnt mit dem Booten

Apple verfolgt einen eher „geschlossenen Ansatz“ und versucht, möglichst nichts und niemanden an die direkten Betriebssystemressourcen heranzulassen. Einen klassischen Explorer oder Finder, der sich für den Zugriff auf das Dateisystem eignet, wie bei Android, gibt es überhaupt nicht. Da Apps ausschließlich Ressourcen nutzen können, die das Betriebssystem bereitstellt, ist es von entscheidender Bedeutung, dass sich das OS stets in einem sicheren Status befindet.

Bereits beim Systemstart eines Apple-Geräts, der sogenannten Initialisierungsphase der Hardware, wird das Einschleusen von Schadprogrammen durch das Zusammenspiel von Betriebssystem und Hardware verhindert. Durch kryptografisch signierte Komponenten, darunter der Kernel und der Bootloader, verhindert Apple, dass das iOS heimlich modifiziert wird. Kommt es zu Abweichungen, unterbricht das Gerät den Startvorgang und verlangt nach einem Firmware-Upgrade, zumeist über die Apple-eigene Verwaltungssoftware iTunes. Die sogenannte „System Software Personalization“ von Apple verhindert das Rücksetzen auf eine ältere, möglicherweise durch Sicherheitslücken anfällig gewordene iOS-Version. Bedingt durch die Tatsache, dass Apple jedem Gerät eine eindeutige Kennung mit auf den Weg gibt – die ECID –, und stets eine Verknüpfung mit einem iTunes-Account verlangt wird, ist es für den Anbieter recht einfach, eine Historie von Betriebssystemversion und Nutzer vorzuhalten. Diese Maßnahmen und andere, beispielsweise die permanente aktive Geräteverschlüsselung, die fehlende Möglichkeit, den Speicher durch externe Medien zu erweitern, sorgen letztendlich dafür, dass das Betriebssystem nur in einem gesicherten Status starten kann.



Lesenswert: Empfehlenswerte Lektüre des BSI – das Überblickspapier Apple iOS.

Auch wenn es treue Apple-Kunden nicht so gern hören: Es gab auch bei iOS Schwachstellen, die zu verschiedenen Sicherheitsproblemen führten. Nicht nur einmal ließ sich der Passcode durch einen einfachen Trick umgehen. Allein zwischen den Versionen 5 und 6 von iOS musste Apple laut Informationen eines Über-

blickpapiers des BSI 197 Sicherheitslücken schließen (www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Ueberblickspapier_Apple_iOS_30072013.html). Nur wenn das Betriebssystem sicher ist, können fragwürdige Apps diese Lücken nicht für ihre Zwecke missbrauchen. Apple erinnert den Benutzer bei jedem Blick auf die Systemeinstellungen daran, dass Updates eingespielt werden müssen. Ebenfalls warnt das BSI bei Geräten mit dem iOS-Betriebssystem vor indirekter Ausspähung des Benutzers durch Dienste oder Apps. Ein Beispiel wären die sogenannten Geolocation-Dienste, bei denen der Standort des Benutzers erfasst und mit einem Dienst verknüpft wird. Mit solchen Diensten lassen sich unter Umständen Zugangsbeschränkungen umgehen oder persönliche Informationen abgreifen. Oder der Beschleunigungssensor, dessen Daten missbraucht werden könnten, um Eingaben über den Touchscreen auszuspähen.

3.4.3 iOS ständig am Senden in Richtung Apple

Wenig bekannt sein dürfte der permanente Datenabfluss eines iOS-Geräts in Richtung Apple. iPhones & Co. senden seit iOS-Version 6 im Hintergrund laufend Protokoll-Log-Dateien und Fehlerberichte an den Hersteller. Nur falls der Benutzer bei der Installation des Updates dieser Übermittlung nicht explizit widerspricht, ist dies Standardverhalten. Da diese Daten durchaus auch vertrauliche oder persönliche Informationen enthalten können, handelt es sich, mit Blick auf den Datenschutz, um eine äußerst fragwürdige Funktionalität. Zudem können legitim installierte Apps, so das BSI, diese Daten, auch ohne Wissen des Anwenders, an Dritte weitergeben. Sicherheitsrelevante Software ist für iOS kaum verbreitet, da Apple durch das Design des Betriebssystems und der Technik des Sandboxings (keine Applikation darf auf die Daten und Ressourcen einer anderen App zugreifen) davon ausgeht, dass ein kritischer Sicherheitsstatus nicht erreicht werden kann. Regelmäßige Updates des Betriebssystems seien ausreichend. Sofern es also nicht das iOS selbst ist, das unerwünscht auf App-Daten zugreift, gibt es keine Notwendigkeit für Virenschutz & Co. Ganz anders sieht es aus, wenn der Benutzer das Gerät durch einen „Jailbreak“ öffnet, um auf die Ressourcen selbst direkt zugreifen zu können. Diese Geräte sind eine Gefahr für den Benutzer und insbesondere für alle darauf gespeicherten Unternehmensdaten.

3.4.4 Android orientiert sich am klassischen PC

Viele der Sicherheitsfunktionen, die Apple dem iOS mit auf den Weg gegeben hat, sind auch in der traditionellen PC-Branche nicht unbekannt. Sie heißen nur anders, und entgegen der Vermutung, dass es ein Vorteil wäre, dass alles aus einer Hand stammt, funktioniert es bei Linux oder Windows auch ohne monopolistische Anbieter. Android hat eine deutliche Anlehnung an Linux und ist – entsprechend dieser Konzeption – viel offener. Neben dem Linux-Grundgerüst nutzen Android-Apps Java und dessen virtuelle Maschinen für den Betrieb.

Wie iOS, so setzt auch Android auf eine starke Isolation von Apps und auf die Regelung, dass diese nur auf dedizierte Systemressourcen zugreifen können. Diese Isolierung schützt nicht nur die Apps untereinander, sondern auch das Betriebssystem vor ungewollten Änderungen. Sofern es einer App nicht gelingt, den sogenannten „Administrator-Level-Mode“ zu erreichen, was faktisch nur durch das bewusste „Rooten“ passieren kann, können Apps das Android-OS nicht anpassen. Zwar dürfen Apps nicht auf den Speicherbereich anderer Apps zugreifen, sie können jedoch sehr wohl – über das Betriebssystem – herausfinden, welche anderen Apps in welcher Version auf dem Gerät installiert sind.

Security feature implementation		
Security Pillar	Apple iOS	Google Android
Access Control		
Application Provenance		
Encryption		
Isolation		
Permission-based Access Control		

iOS und Android – Integrierte Sicherheitsfunktionen: Die Funktion der App-Isolation sieht Symantec bei Android besser als bei iOS.

Zudem sind die meisten Apps unter Android in der Lage, alle unverschlüsselten Daten einer SD-Karte auszulesen, jedoch ohne Schreibzugriff. Sollten sich auf der SD-Karte allerdings persönliche Informationen befinden, beispielsweise Fotos oder Dokumente, so könnte eine App diese für eigene Zwecke nutzen und beispielsweise über das Internet verschicken. Trotz der Isolierung ist es unter Android für eine App durchaus möglich, andere Apps zu starten. Letztendlich benötigt der Anwender, wie bei einem typischen PC, eine Sicherheitssoftware, die feststellt, dass die installierten Apps und die aktiven Prozesse keine Gefahr für das System darstellen.

3.4.5 Dem Entwickler auf die Finger schauen

Im direkten Vergleich zu Android-Anbieter Google setzt Apple auf eine sehr restriktive Politik, was die Erweiterbarkeit hinsichtlich der Software und vor allem der Hardware angeht. Softwareentwickler, die ihre Apps über den App Store anbieten, müssen ihre Software zunächst durch Apple in Tests prüfen lassen, ehe sie im Store verfügbar sind. Dieses Konzept, auch wenn es denkbare Lücken gibt, führte bisher dazu, dass es, im Gegensatz zu Android, wenig Schadsoftware gibt und kaum erfolgreiche Attacken auf iOS-Geräte dokumentiert sind.

Während es für iOS über den Enterprise Store schon seit längerer Zeit eine recht ausgefeilte Lösung gibt, mithilfe einer Lösung für das Mobile Device Management (MDM) dafür zu sorgen, dass nur zulässige Apps auf iPad, iPhone & Co. gelangen, waren derlei Einschränkungsmöglichkeiten für Android-Systeme in dieser Form lange Zeit nicht umsetzbar. Ende 2013 veröffentlichten Wissenschaftler am AISEC einen App-Store-Filter für Android. Dieser sortiert problematische Android-Apps automatisch aus und bietet den Mitarbeitern nur mobile Anwendungen an, die konform der unternehmenseigenen Vorgaben zur IT-Sicherheit sind.

3.4.6 Fazit: keine hundertprozentige Sicherheit

Wie dieser kleine Ausflug in die Sicherheitskonzepte von iOS und Android zeigt, gibt es keine hundertprozentige Sicherheit. Handelt es sich bei dem Gerät um ein rein privates Device, so bleibt die klassische Sicherheitsempfehlung, nur so wenig Apps wie nötig auf dem Gerät zu installieren. Für Unternehmen ist – nicht nur aus diesem Grund – die Verwendung einer Mobile-Device-Management-Software angeraten. Entsprechende Lösungen sind in der Lage, Apps im Sinne einer Whitelist oder über einen eigenen Enterprise Store zur Verfügung zu stellen oder in extrasi-cheren Containern abzuschirmen. Natürlich sind auch Mitarbeiter notwendig, die sich mit den Plattformen explizit auskennen. Am allerwichtigsten ist es jedoch, Mitarbeiter, Freunde oder Verwandte für das Thema Sicherheit zu sensibilisieren.

Thomas Bär, Frank-Michael Schlede



Thomas Bär, der seit Ende der neunziger Jahre in der IT tätig ist, bringt weit reichende Erfahrungen bei der Einführung und Umsetzung von IT-Prozessen im Gesundheitswesen mit. Dieses in der Praxis gewonnene Wissen hat er seit Anfang 2000 in zahlreichen Publikationen als Fachjournalist in einer großen Zahl von Artikeln umgesetzt. Er lebt und arbeitet in Irsee im Allgäu.



Frank-Michael Schlede arbeitet seit den achtziger Jahren in der IT und ist seit 1990 als Trainer und Fachjournalist tätig. Nach unterschiedlichen Tätigkeiten als Redakteur und Chefredakteur in verschiedenen Verlagen arbeitet er seit Ende 2009 als freier IT-Journalist für verschiedene Online- und Print-Publikationen. Er lebt und arbeitet in Pfaffenhofen an der Ilm.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Produktivitäts-Apps im Security-Check**
(www.tecchannel.de/2061865)
- **Apps für iOS, Android, Mac OS und Windows: So unsicher sind Messenger**
(www.tecchannel.de/2059507)
- **F-Secure Freedom für Android und iOS 7 im Test**
(www.tecchannel.de/2056050)

3.5 Samsung KNOX 2.0 – Sicherheit für Android

Sichere Android-Plattform, geschützte Apps und Daten sowie eine umfassende Gerätekontrolle – all das will Samsung mit seiner KNOX-Technologie erschlagen. KNOX soll Smartphones und Tablets der Galaxy-Serie für den Business-Einsatz fit machen. So will Samsung künftig nicht nur Endgeräte im Consumer-Bereich verkaufen, sondern auch im Business-Bereich Fuß fassen. Da Unternehmen immer mehr auf den Bring-Your-Own-Device (BYOD)-Ansatz setzen, also Anwendern erlauben, ihre privaten Geräte mit dem Firmennetzwerk zu verbinden, muss sich Samsung etwas einfallen lassen, um Android-Geräte salonfähig zu machen.

Android ist im Vergleich zu den anderen verbreiteten Smartphone-Systemen im Firmenbereich deutlich unsicherer, was nicht zuletzt an der starken Fragmentierung der Versionen und an der offenen Struktur des Betriebssystems liegt.

Was ist KNOX überhaupt?

Die grundsätzliche Sicherheitsfunktion von Samsung KNOX (www.samsungknox.com/de) basiert auf dem NSA-System Security Enhanced Android (SE Android) und einem besonders gesicherten Bootloader in Verbindung mit speziell abgesicherter Hardware. KNOX unterstützt auch Secure Boot. Das heißt, bereits beim Starten des Gerätes lässt sich sicherstellen, dass keine Schadsoftware geladen wird, obwohl KNOX noch gar nicht gestartet ist.

Samsung verwendet hierbei auch die Integrity Measurement Architecture TIMA. Das TIMA-Modul überwacht den Kernel des Betriebssystems auch ohne KNOX-Aktivierung. Das Modul soll sicherstellen, dass keine Sicherheitsprobleme vorliegen. Auf Wunsch schaltet das Modul das Gerät ab, wenn der Kernel kompromittiert ist. Security Enhancements for Android (<http://selinuxproject.org/page/SEAndroid>) lassen sich auch mit KNOX nutzen. Sie sorgen dafür, dass wichtige Daten und Apps in isolierten Bereichen gespeichert werden. Das verhindert die Auswirkungen eines Angriffs auf das Gerät. KNOX ist eine Erweiterung von Samsung für Enterprise (SAFE, www.samsung.com/global/business/mobile/solution/security/safe-samsung-for-enterprise), damit mehr Unternehmen auch dienstlich den Einsatz von Android-Geräten erlauben. Bestandteil der neuen Funktion ist zum Beispiel die Möglichkeit, automatisch die Kamera im Smartphone zu deaktivieren, sobald der Anwender das Firmengelände betritt. Außerdem soll KNOX verhindern, dass Viren auf den Endgeräten in das Firmennetzwerk eindringen oder wichtige Firmendaten auf den Endgeräten zerstören oder auslesen.

3.5.1 KNOX nur auf bestimmten Galaxy-Geräten

Sinn des Systems soll es sein, auf Endgeräten mehrere getrennte Bereiche parallel zu installieren. Das funktioniert natürlich nur mit spezieller Hardware, zum Bei-

spiel dem Galaxy Note 4 und dem neuen Galaxy Note 10.1. Dank der beiden Systeme auf den Geräten kann ein Anwender Profile anlegen. So besteht die Möglichkeit, ein privates System und ein abgesichertes berufliches Profil auf ein und demselben Gerät zu verwenden. Samsung will in Zukunft weitere Geräte KNOX-kompatibel machen. Welche Android-Versionen und Samsung-Geräte künftig mit KNOX zusammenarbeiten, ist aktuell noch nicht klar. Es ist aber zu erwarten, dass vor allem die Galaxy- und die Note-Geräte kompatibel gemacht werden.

Samsung führt auf der eigenen KNOX-Website (www.samsungknox.com/de/knox-supported-devices) alle unterstützten Geräte auf. Da KNOX den beruflichen vom geschäftlichen Teil trennt, schützt es Anwender allerdings nicht davor, sich unsichere Apps oder Viren auf dem Gerät zu installieren. Hier kann die Anwendung nicht eingreifen. Das heißt, Unternehmen, die KNOX einsetzen wollen, müssen parallel für Sicherheit auf dem privaten Teil des Smartphones sorgen.

3.5.2 Ablauf bei der Anbindung von KNOX

Die Anbindung eines KNOX-kompatiblen Gerätes an das Firmennetzwerk geht wie folgt vonstatten: Das Gerät des Anwenders wird in die MDM-Software (Mobile Device Management) des Unternehmens integriert, und KNOX wird installiert. Nach der Anbindung und der Installation von KNOX findet der Anwender auf dem Homescreen seines Gerätes ein neues Icon für KNOX.



Abgeschottet: Die Technologie trennt private Apps und Daten von den Unternehmensanwendungen. (Quelle: Samsung)

Klickt der Anwender dieses Icon an, öffnet sich die sichere Umgebung von KNOX, inklusive eines eigenen App-Stores (www.samsungknox.com/de/apps). Die Technik ist ähnlich wie bei BlackBerry Balance. Andere Einstellungen auf dem Endgerät ändern sich nicht, der Anwender kann, wie zuvor auch, problemlos weiterhin parallel mit seinem Gerät arbeiten. KNOX wird nicht als paralleles Betriebssystem ge-

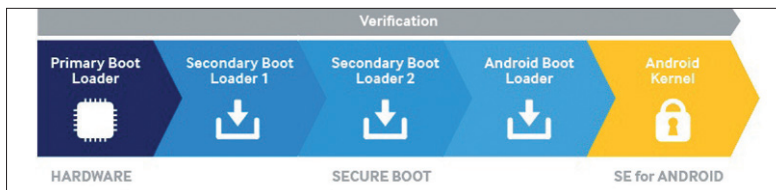
nutzt. Anwender müssen für den Einsatz von KNOX also nicht ihr System neu starten, vielmehr stellt die KNOX-Umgebung ein „Unterbetriebssystem“ dar, das im laufenden Betrieb gestartet und auch wieder beendet werden kann. Die Firmendaten bleiben ausschließlich im entsprechend abgesicherten Bereich gespeichert. Die KNOX-Umgebung, gestartet durch ein neues Icon auf dem Homescreen, verfügt dann wiederum über einen eigenen Homescreen mit eigenem Launcher, eigenen Apps und eigenen Widgets.

3.5.3 Privates und Geschäftliches auf einem Smartphone

Durch die strikte Trennung der beiden Systeme können Anwender ihr Smartphone privat und beruflich nutzen. Bestandteil von Security Enhanced Edition von Android ist auch eine Verschlüsselung. Da das System eigentlich von der NSA entwickelt wurde, bleibt natürlich ein Beigeschmack, was die Abhörsicherheit betrifft. Indes handelt es sich bei SE Android um eine Open-Source-Linux-Lösung. Das heißt, Hintertürchen für die amerikanischen Geheimdienste wären mittlerweile entdeckt worden. Im Fokus der NSA steht im Bereich Android im Übrigen vor allem die Absicherung von Android vor gegnerischen Spionageangriffen, weniger die eigenen Abhörmöglichkeiten. Nach ersten Tests soll keine Backdoor enthalten sein. Verlassen sollte man sich allerdings darauf nicht, denn die NSA ist nicht gerade bekannt dafür, sichere Anwendungen für externe Nutzer zu programmieren. SE-Android ist allerdings auch Bestandteil von AOSP (Android Open Source Project). Das heißt, Sicherheitslücken oder Hintertüren werden normalerweise durch Entwickler erkannt und beseitigt, sollten welche vorhanden sein.

3.5.4 KNOX und das Rooten

Viele Android-Anwender, vor allem Profis, rooten ihr Gerät. Dadurch erhalten sie mehr Zugriff auf die Funktionen von Android und dessen Dateisystem. Das ist auch beim Einsatz von KNOX möglich. Allerdings lässt sich zum einen nur der private, nicht der von KNOX abgesicherte Teil rooten. Zum anderen erkennt der KNOX-Teil den Root-Vorgang und protokolliert ihn auch.

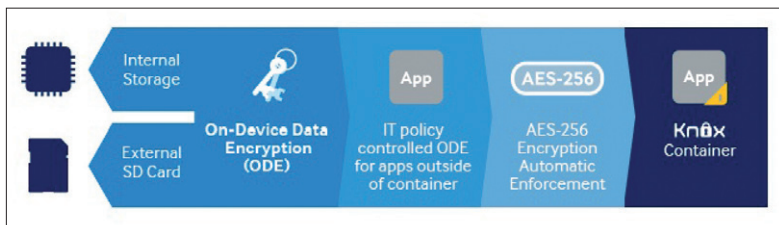


Secure Boot: Die Authentizität des Android-Kernels wird beim Booten überprüft. Das heißt, bereits beim Starten des Gerätes lässt sich sicherstellen, dass keine Schadsoftware geladen wird, obwohl KNOX noch gar nicht gestartet ist. (Quelle: Samsung)

Die Hardware von KNOX-kompatiblen Geräten erkennt einen Root-Vorgang in den meisten Fällen an einer durchgebrannten E-Fuse. Das heißt, bei Hardwareproblemen mit einem gerooteten Endgerät kann Samsung die Garantie für solche Geräte ausschließen. Die Administratoren im Unternehmen erkennen außerdem solche Vorgänge und können gerootete Geräte von der Firmenumgebung ausschließen. Standardmäßig blockiert KNOX den Zugriff auf den verschlüsselten Teil der Daten, sobald das Gerät einen Root-Zugriff erkennt. Auch hier wird der Root-Vorgang an der durchgebrannten E-Fuse erkannt. Anwender sollten sich also vor der Anbindung an KNOX mit den Administratoren des Unternehmens absprechen.

3.5.5 Private und berufliche Daten nutzen

KNOX beeinträchtigt Smartphones oder auch Tablets ansonsten nicht. Die Anwender können ihr Gerät uneingeschränkt privat und beruflich nutzen. Auch Apps aus Google Play lassen sich weiterhin problemlos installieren. Allerdings stehen diese Apps nicht in der KNOX-Umgebung zur Verfügung. Der einzige Unterschied ist die Tatsache, dass ein zweites System auf dem Gerät verfügbar ist, das Anwender aus ihrer Standardumgebung heraus starten können. Über ein Icon auf dem Homescreen lässt sich die sichere Umgebung schnell und unkompliziert starten. Die Daten der beiden Systeme sind voneinander getrennt. Das heißt, der berufliche und durch KNOX abgesicherte Teil hat keinen Zugriff auf die privaten Daten und umgekehrt. Die beiden Systeme sind komplett voneinander abgeschottet. Allerdings erscheinen die privaten Termine im KNOX-Kalender. Umgekehrt sind die geschäftlichen Termine aus dem KNOX-Container nicht im privaten Kalender zu sehen. Auch der Lesezugriff auf Kontaktdaten, die außerhalb des Containers liegen, ist möglich. Diese Vorgänge muss der Anwender aber erst erlauben.



Encryption: KNOX arbeitet mit einer 256-Bit-AES-Verschlüsselung. (Quelle: Samsung)

Die beruflichen Daten verbleiben in einem sogenannten KNOX-Container. Dieser soll laut Samsung auch vor Malware, Phishing und physischem Zugriff auf das Endgerät geschützt sein. Das heißt, auch beim Verlust oder Diebstahl des Gerätes sollen die durch KNOX geschützten Daten sicher sein. Die Daten in diesem Container sind durch eine zertifizierte Advanced Encryption Standard (AES) mit 256-Bit-Verschlüsselung (AES-256) gesichert. Die Prozesse im KNOX-Container können nicht

mit außenliegenden Apps oder Prozessen interagieren. Administratoren haben die Möglichkeit, den KNOX-Container und seine Daten vom Endgerät des Anwenders zu entfernen. Die privaten Daten des Anwenders sind davon nicht betroffen.

3.5.6 MDM und mehr mit KNOX

Samsung unterstützt mit KNOX viele Verwaltungslösungen (MDM, www.samsungknox.com/de/knox-mdm-feature-list). Das ist klar, da sich solche komplexen Umgebungen nur mit einer zentralen Lösung nutzen lassen. Mit KNOX können Unternehmen außerdem VPN-Szenarien darstellen, auf Verwaltungslösungen Dritter setzen und auf Basis von Exchange ActiveSync die gesicherte Android-Version auch an Exchange anbinden. Alle Daten in der KNOX-Umgebung sind AES-verschlüsselt. Die Umgebung erlaubt es Administratoren, die Einrichtung von VPNs für einzelne Apps in KNOX zu konfigurieren.



MDM: KNOX arbeitet mit vielen etablierten Lösungen zusammen. (Quelle: Samsung)

Auch hier bleiben die gesicherten Daten in der KNOX-Umgebung. Im Rahmen dieser zentralen Verwaltung können Administratoren remote auch Apps auf den Endgeräten installieren oder entfernen. Allerdings unterstützt die KNOX-Umgebung hier nicht die offiziellen Android-Apps aus Google Play, sondern nur die besonders abgesicherten und signierten KNOX-Apps von Samsung.

Auch die Absicherung von Daten und die Anpassung von Rechten sind möglich. KNOX kann nicht nur von Anwendern manuell aktiviert werden, sondern ist in der Lage, sich in bestimmten Szenarien auch automatisch zu aktivieren, zum Beispiel wenn ein Anwender ein Firmengebäude betritt. Wie bei solchen Anwendungen üblich, lassen sich mit KNOX auch Hardwarefunktionen, wie die Kamera oder Speicherkarten, deaktivieren. Darüber hinaus besteht

3.5.7 KNOX 2.0 mit zusätzlichen Features

Mit der neuen, im Februar 2014 vorgestellten Version KNOX 2.0 (www.samsungmobilepress.com/2014/02/25/Samsung-KNOX-Keeps-Evolving-to-Meet-Changing-Enterprise-Needs-1) integriert Samsung auch Funktionen, die mit dem neuen Galaxy S5 ausgeliefert werden. Ein wichtiges Feature ist die Zwei-Faktor-Authentifizierung. Wird sie aktiviert, muss sich der Benutzer mit seinem Fingerabdruck und zusätzlich mit einem Kennwort anmelden. Diese Funktion ist dem neuen Fingerabdrucksensor des Galaxy S5 zu verdanken.

Eine weitere neue Funktion ist die Analyse des Datenaufkommens das von privaten und geschäftlichen Apps verursacht wird. Außerdem bindet Samsung die Lösung stärker an die Cloud. Das soll für die Anwender, aber auch für Administratoren mehr Flexibilität bringen. Mit den Mobile Device Management Services lassen sich mobile Geräte und der KNOX Marketplace verwalten, im KNOX-Marketplace spezielle Enterprise-Apps positionieren. KNOX 2.0 setzt Android 4.4 voraus. Anwender, die auf das neue Samsung Galaxy 5 setzen, bekommen KNOX 2 bereits vorinstalliert auf dem Smartphone. Mit dem Smartphone lässt sich auch die neue Key-Store-Funktion nutzen. Diese erlaubt die Erstellung eines Schlüssels in einer gesicherten Umgebung. Außerdem werden dadurch der Kernel von Android und wichtige Systembereiche überwacht. Das soll Android sicherer für Unternehmen machen. Da Samsung mit Good Technology zusammenarbeitet, können Anwender die meisten Google-Pay-Apps auch in einem sicheren Container betreiben. Möglich wird das durch eine sogenannte „Good Secure Domain“. In dieser lässt sich eine spezielle Sicherheitsumgebung erstellen, die auch von KNOX 2.0 gesichert wird. Es ist geplant, dass Knox noch weitere Sicherheitsumgebungen unterstützt, zum Beispiel von Fixmos SafeZone oder MobileIron AppConnect.

3.5.8 Fazit

Dass Android für Unternehmen nicht gerade die sicherste Umgebung ist, stellt kein Geheimnis dar. Samsung will indes, als Marktführer bei Android-Geräten, auch im Business-Bereich punkten, doch dafür müssen Sicherheit und Verwaltbarkeit her. KNOX stellt einen durchaus interessanten Ansatz dar, vor allem angesichts der Tatsache, dass Android derzeit mit Abstand das am weitesten verbreitete Smartphone-System ist. Unternehmen, die den BYOD-Ansatz verfolgen, kommen daher um die Anbindung von Android-Geräten kaum herum. Hier kann KNOX durchaus sinnvoll sein. Allerdings ist die Umgebung auch stark eingeschränkt und erfordert einiges an Sicherheitswissen von den Anwendern. KNOX blendet nämlich immer Informationen ein, wenn das System der Ansicht ist, eine App würde Zugriff auf das System nehmen. Das kann den Anwender schnell überfordern. Doch einen Blick ist die Lösung auf jeden Fall wert.

Thomas Joos

3.6 Vorsicht: die raffinierten Geschäftsmodelle der Gratis-Apps

Wer heute ein Smartphone benutzt, wird sicher neben den bereits vorinstallierten Apps noch weitere Anwendungen auf seinem Gerät installieren – schließlich bringen häufig erst die Apps die nützlichen Fähigkeiten auf das Gerät, die der Nutzer erwartet und benötigt. Nichts leichter als das: Die Apps werden bereits millionenfach über die App-Stores der jeweiligen Anbieter, also Google Play für das Android-System und Apple AppStore für iOS-Geräte, angeboten. Ein erster Blick in diese „Läden“ scheint dann zunächst auch paradiesische Zustände zu bieten: Ein Großteil der Anwendungen steht zum kostenlosen Download bereit, wobei viele Anbieter sogar mit uneingeschränkten Features selbst bei diesen freien Versionen werben. Das ist jedoch nicht die ganze Wahrheit: Auch deren Anbieter wollen Geld verdienen. Wir blicken hinter die Kulissen der freien Apps und der damit verbundenen Geschäftsmodelle.

Es gibt nichts (wirklich) umsonst ...

Ein in den Vereinigten Staaten sehr verbreitetes Sprichwort lautet: „There's no such thing as a free lunch“ – was frei übersetzt für „Es gibt nichts umsonst“ steht.

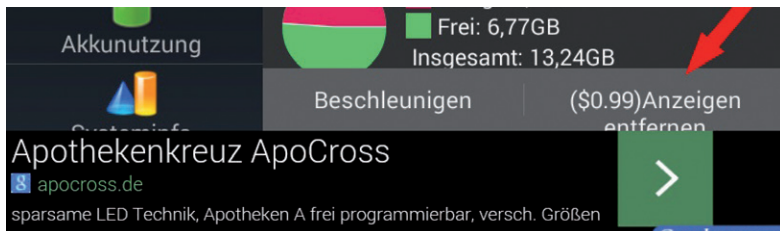


Denken hilft: Nicht nur die schlechte automatische Übersetzung, sondern vor allen Dingen das Geschäftsmodell, die „übrig gebliebenen“ SMS weiterzuverkaufen, ist mehr als dubios.

Das gilt natürlich auch für die im Google Play Store, im Apple App Store oder im Windows Store angebotenen Apps. Da viele Anwender aber nach wie vor der Meinung sind, im Internet gebe es sowieso alles gratis, setzt sich auch bei mobilen Geräten wie Smartphones und Tablets der Trend zur kostenlosen App fort.

Wie schon bei den Webseiten müssen sich die Nutzer aber darüber im Klaren sein, dass sie für die Apps dann wenigstens mit einem Klick auf Werbeanzeigen „bezahlen“. Und genauso, wie es die Nutzer bereits von ihrem Browser auf dem Desktop kennen, kommen gerade bei den Gratis-Apps die unterschiedlichsten Formen der Werbeanzeigen – teilweise recht aggressiv – auch auf diesen Geräten zum Einsatz:

- **Bannerwerbung:** Dabei werden die Werbebanner auf dem eng begrenzten Raum der mobilen Geräte so über die Information auf dem Bildschirm gelegt, dass der Nutzer sie häufig zwangsläufig anklicken muss. In diesen Fällen kommen zudem häufig Geolocations-Dienste (Standortdienste) zum Einsatz, auf die mittels einer Programmierschnittstelle (API) aus der App heraus zugegriffen wird, um den Anwendern gezielte Werbung in Abhängigkeit von ihrem Standort zu präsentieren.
- **Capture-Formulare oder Signup-Apps:** Diese Apps treiben diese Art des Geschäfts noch ein Stück weiter. Hier öffnen sich gleich nach dem Start oder manchmal auch, während die App bereits benutzt wird, Fenster. Sie füllen den ganzen Bildschirm aus und fordern den Nutzer auf, sich anzumelden oder bestimmte Daten einzugeben. Ein Nutzer, der die Gratis-App nutzen will, kommt nicht umhin, mit seinen Daten „zu bezahlen“.
- **Push-Benachrichtigungen:** Bei dieser Form der Werbung, die häufig in kostenlosen Spiele-Apps zum Einsatz kommt, werden Werbenachrichten direkt und aktiv vom Remote-Server auf das Mobilgerät geschickt. Der Nutzer kann das nur schlecht verhindern, da viele dieser freien Apps nicht zu verwenden sind, wenn keine Online-Verbindung besteht.
- **App-Walls:** Ähnlich aufdringlich wie die Push-Nachrichten wird beispielsweise während eines Spieles eine Liste weiterer populärer Apps mit dem Ziel eingeblendet, den Nutzer zu einem Kauf über das jeweilige Advertising-Netzwerk zu verleiten.
- **Automatisches Anlegen von Icons auf dem Home-Bildschirm:** Die Gratis-App legt dabei während der Installation ein Icon auf dem Home-Bildschirm des Geräts an. Klickt der Nutzer darauf, wird er wiederum auf ein Ad-Netzwerk geführt.



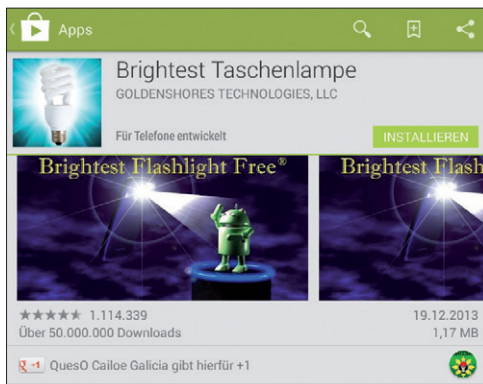
Freikaufen von Werbung: Nur 99 Cent und die Anzeigen erscheinen nicht mehr auf dem Bildschirm – Viele Gratis-Apps wie hier der „Android Assistant“ stopfen eine ohnehin überladenen Oberfläche noch mit Anzeigen voll – von denen sich der Nutzer dann durch Zahlung einer Gebühr befreien kann.

Dabei bauen die Entwickler der Gratis-App den Code, der diese Werbung auf den Bildschirm der Mobilgeräte bringt, mittels eines SDK (Software Development Kit) fest in die Anwendung ein. Der Source-Code mancher Gratis-Apps beinhaltet sogar zwei oder mehr dieser Advertising-SDKs.

Für den Anwender bleibt die Frage, wie gefährlich der Einsatz von Gratis-Apps dadurch letztendlich ist. Wir haben die Frage an Kaspersky Labs weitergegeben, und dessen Senior Virus Analyst Christian Funk schätzt die Gefährdung durch die kostenlosen Apps folgendermaßen ein: „Gratis-Apps verlangen immer häufiger Zugriff auf allerlei Bereiche des Smartphones, die für die eigentliche Funktion nicht benötigt würden. Hier muss man sich aus der Sicht des Anwenders fragen, welche Daten tatsächlich übertragen werden, ob der Transfer verschlüsselt erfolgt und, am wichtigsten: Wie und wo werden die Daten abgespeichert, damit sie kein leichtes Ziel für Cyber-Kriminelle sind?“

3.6.1 Auf welche persönlichen Daten greifen Apps zu?

Die Spezialisten der Firma Lookout, die ihren Fokus auf die Sicherheit von mobilen Geräten gelegt haben, begannen bereits im Jahr 2011 mit dem sogenannten App Genome Project (www.lookout.com/resources/reports/appgenome), mit dessen Hilfe sie die mobilen Apps und deren Aufbau übergreifend über verschiedene mobile Plattformen und Marktplätze für Apps untersuchen. Dabei wurden neben dem Android Play Store (damals noch Android Market) und dem Apple App Store auch jeweils zwei alternative App-Märkte für Android und iOS in die Untersuchung mit einbezogen.



Datensammler: Sorgte Ende 2013 für Probleme – Die kostenlose „Taschenlampe“-App von Goldenshore Technologies sammelte nicht nur Daten der Nutzer, sondern gab sie auch an Anzeigenkunden weiter.

Laut dieser Erhebung griffen bereits Ende 2011 mehr als ein Drittel der untersuchten Apps in den beiden großen App-Stores auf den jeweiligen Standort des Nutzers zu, mindestens zehn Prozent nutzten den direkten Zugriff auf die Kon-

takte. Es ist sicher nicht falsch, davon auszugehen, dass diese Art der Zugriffe im Lauf der vergangenen Jahre weiter zugenommen hat.

So zeigte eine kürzlich durchgeführte Untersuchung der Security-Spezialisten von TÜV Trust IT aus Österreich (www.it-tuv.com) ein noch erschreckenderes Bild: Bei einer Analyse von über 1000 mobilen Anwendungen fanden die Fachleute Folgendes heraus: Bei 45 Prozent der untersuchten Apps besteht die Möglichkeit, dass mit ihnen Daten gestohlen werden.

Bewertung im Store	★★★★★
Größe der App	11940000 Byte
Virus check	
SSL analysierbar	
Gesamtlampelwertung	
Erklärung des Ergebnisses	Twitter-Nutzername, Twitter-Passwort und Liste der letzten Mailempfänger werden verschlüsselt an Yelp-Server übertragen. – PLZ wird unverschlüsselt an ein Werbe-Netzwerk übertragen.

Auskunftsfreudig: Die „kostenlose“ App Yelp holt sich vom Nutzer Auskünfte ein, wie eine Analyse von „mediaTest“ ergab.

Das Hannoveraner Testinstitut „mediaTest digital“, das sich auf die Sicherheitsprüfung und Zertifizierung mobiler Applikationen spezialisiert hat, kommt zu ähnlichen Ergebnissen: Sowohl bei Auskunfts-Apps als auch bei Reise-Apps oder Messenger gibt es teilweise erhebliche Sicherheitsmängel; die Experten raten bei vielen Apps von der Nutzung im Unternehmen wie auch privat ab.

Immer wieder zeigt sich dabei auch, dass viele Gratis-Apps mithilfe der integrierten SDK ein Device-Tracking durchführten: Sie verfolgen anhand bestimmter Daten und Merkmale, die sie auf dem Gerät auslesen, das Smartphone oder Tablet und damit den Nutzer und seine Gewohnheiten. Zu diesen Daten, die dabei häufig ausgelesen werden, gehören unter anderem:

- die **IMEI** (International Mobile Equipment Identity) – eine 15-stellige, für jedes Mobilgerät eindeutige Identifikationsnummer. Sie ändert sich auch dann nicht, wenn beispielsweise die SIM-Karte eines Smartphones ausgetauscht wird.
- die **IMSI** (International Subscriber Identity) – sie dient zur Identifikation eines Geräts innerhalb eines mobilen GSM- und UTMS-Netzwerks. Auch sie besteht aus 15 Ziffern. Anhand dieser Nummer ist es beispielsweise auch möglich festzustellen, über welchen Provider sich das Gerät angemeldet hat.
- die **UDID** (Unique Device ID) – eine spezielle Gerätekenung der iOS-Geräte von Apple, die unter anderem auch als Kennung beim Einkauf im App-Store zum Einsatz kam. Seit Version iOS 6 untersagt Apple deren Verwendung in Apps. Beim aktuellen iOS7 kam zudem eine Funktion hinzu, die das Auslesen dieser Nummer und unter anderem auch der WLAN-MAC-Adresse unterbindet.

- die **Android ID** – eine eindeutige, 64 Bit lange Nummer, die das Gerät automatisch beim ersten Einschalten erstellt. Sie kann sich allerdings ändern, wenn das Gerät gerootet oder auf den Werkszustand zurückgesetzt wird.
- die **WLAN MAC-Adresse** – genauso wie bei den normalen Netzwerkadaptern handelt es sich auch hier um eine eindeutige Adresse, mit der die Netzwerkschnittstelle des Gerätes identifiziert werden kann.
- die üblichen Daten – Gerätetyp, Betriebssystemversion, Jail-Break/Rooting-Status, Geoposition und Telefonnummer.

3.6.2 Praxis-Tipp: Welche App darf was auf meinem Smartphone?

All diese Faktoren zeigen deutlich, dass immer ein gewisses Risiko für die Privatsphäre des Anwenders besteht, wenn eine App eine spezielle Fähigkeit hat beziehungsweise auf bestimmte Daten des Geräts zugreifen kann. Natürlich muss eine Gratis-App, die Zugriff auf bestimmte Daten und Bereiche des Smartphones oder Tablets bekommt, deshalb nicht gleich ein Spionage-Tool sein. Wer beispielsweise einen Dienst wie Google Maps sinnvoll einsetzen will, muss den Zugriff auf die Geoposition erlauben.

Apps, die eine bestimmte Fähigkeit einsetzen, sind sicher nicht unbedingt gleich Spyware. Alle mobilen Betriebssysteme zeigen dem Nutzer bei der Installation im Prinzip an, auf welche Daten die App zugreifen möchte. Wer das bei den bereits auf seinem Android-System installierten Apps kontrollieren möchte, kann sich dazu eine äußerst nützliche Gratis-App der finnischen Sicherheitsspezialisten von F-Secure herunterladen. F-Secure App Permissions (www.f-secure.com/de/web/home_de/app-permissions) zeigt sehr übersichtlich alle Berechtigungen, der auf einem Android-Gerät installierten Apps an.

So können Nutzer schnell sehen, welche Apps im Hintergrund dann doch Kosten verursachen oder welche Apps auf vertrauliche Daten zugreifen, ohne dass dies für ihre grundlegende Funktion notwendig wäre. Die App führt den Nutzer dann auch zu den entsprechenden Einstellungen des Android-Systems – leider ist es vielfach nicht möglich, einer App einzelne Berechtigungen zu entziehen. Im Zweifelsfall bleibt dem Nutzer als sinnvolle Alternative dann nur die Deinstallation der entsprechenden Gratis-App.

3.6.3 Grundlegende Tipps zur Verwendung von Gratis-Apps

Wie überall beim Einsatz von Software, die direkt aus dem Internet geladen und installiert wird, wie auch beim Besuch diverser Angebote und Webseiten im Netz sollten Nutzer die entsprechende Vorsicht walten lassen. Die Sicherheitsfirma Sophos hat dazu ein paar grundsätzliche Tipps bereitgestellt:

- **Wenn irgendetwas bereits verdächtig aussieht, dann ist es in der Regel auch schädlich:** Nutzer sollten auch auf ihren Mobilgeräten grundsätzlich nie auf Anzeigen klicken, die vollmundig versprechen, Schadsoftware auf diesem Gerät zu finden. Auch die Links in Anzeigen, die mit großen roten Alarmknöpfen und -meldungen auf dem Bildschirm auftauchen, sollten nie angeklickt werden – es ist für einen Anwender einfach unmöglich zu beurteilen, was dahintersteckt.
- **Nutzen Sie den „gesunden Menschenverstand“, gerade wenn es um Zugriffsberechtigungen geht:** Wenn eine App (ganz gleich ob Gratis- oder Bezahl-App) nach dem Zugriff auf die Kontakte oder gar die Geräteeinstellungen verlangt, sollte dabei auch erklärt werden, warum die App diesen Zugriff benötigt. Wenn Sie von der Erklärung nicht vollständig überzeugt sind, sollten Sie den Zugriff verweigern.
- **App-Stores von Drittanbietern können große Gefahren bergen:** Zwar sind auch die App-Stores von Apple und Google nicht perfekt, und gerade bei den Gratis-Apps gilt es auch hier, vorsichtig zu sein. Aber die Gefahren durch Apps, die mit Malware infiziert sind, oder solche, die als PUA (Potential Unwanted Application) bezeichnet werden, sind in den Stores von Drittanbietern weitaus höher. Genauso sollen Nutzer File-Sharing-Webseiten vermeiden, die vermeintliche freie Versionen von Bezahl-Apps zur Verfügung stellen. Viele solcher Anwendungen wurden verändert und mit Schadsoftware versehen.
- **Nutzerbewertungen können wertvolle Hinweise geben:** Wenn sich bei der Beschreibung einer App die negativen Beschreibungen und Warnungen häufen, so sollten Anwender dies als Warnhinweis nehmen und solche Apps meiden.
- **Daten schützen, mobiles Telefon/Tablet schützen:** Nutzer sollten wenn möglich ihre Daten auf ihren mobilen Geräten und auf Cloud-Speichern verschlüsseln.
- **Schutzsoftware auch auf mobilen Geräten:** Der Einsatz von Antivirenlösungen und anderer Schutzsoftware ist auf mobilen Systeme noch viel zu wenig verbreitet. Wobei es auf diesen Geräten weniger um den Schutz vor Viren geht als um die Zugriffe der Apps und schädliche Anwendungsprogramme, die beispielsweise auf die Daten der Nutzer zugreifen oder kostenpflichtige Dienste nutzen.

3.6.4 Eine besonders dreiste Geschäftsidee: Bazuc

Von Google wurde mit der App Bazuc eine Geschäftsidee für Gratis-Apps aus dem Play Store entfernt, die ein besonders gutes Beispiel für die häufig merkwürdigen Methoden solcher Anbieter ist: Den Anwendern wurde die Möglichkeit versprochen, durch die Installation dieses App „einfach Geld zu verdienen“, indem sie der

App erlauben, die nicht benötigten SMS-Nachrichten für die Zwecke des Anbieters einzusetzen. Dieser setzt auf die Tatsache, dass viele Nutzer eine Flatrate für SMS oder wenigstens eine so große Anzahl von kostenlosen SMS mit ihrem Mobilfunkvertrag besitzen, dass sie diese unmöglich alle verwenden können. Die Bazuc-App versendet dann auf diesem Weg beispielsweise Massen-SMS im Auftrag anderer Firmen. Da diese so mit der Kennung des jeweiligen Nutzers versendet werden, können so zumeist Spam-Filter und ähnliche Schutzmaßnahmen wirkungsvoll umgangen werden.

Die App wurde laut Aussagen der Spezialisten von Lookout aus dem Google Play Store zwischen 10.000- und 50.000-mal heruntergeladen, bevor sie schließlich entfernt wurde. Der Verlockung des „freien Geldes“ können dann wohl doch nur wenige Nutzer widerstehen. Der Anbieter stellt seine Geschäftsidee und damit auch noch die App weiterhin auf <http://earn.bazuc.net/de/> zum Download bereit. Spätestens der scheinbar durch ein Übersetzungsprogramm mehr schlecht als recht erstellte Text auf der Seite sollte aber jeden vernünftig denkenden Nutzer vom Download und Gebrauch dieser Gratis-App abhalten – auch wenn der Anbieter vollmundig verspricht, dass sie demnächst im Apple App Store erhältlich sei.

3.6.5 Zum Abschluss: kostenpflichtige App, die nichts tut

Sind die Nutzer also sicher, wenn sie auf Gratis-Apps verzichten? Das folgende Beispiel zeigt, dass dem leider nicht so ist: Eine Sicherheits-App im Google Play Store, die 3,99 Dollar kostet, 10.000 Downloads und eine Bewertung von 4,7 Sternen aufweist – das kann doch nur eine gute Lösung sein. Oder etwa nicht?

Der Fall der App „Virus Shield“, der ganz entscheidend durch das Team des Web-Blogs Android Police (www.androidpolice.com/about/) aufgeklärt wurde, demonstriert ein weiteres „Geschäftsmodell“, das hier zwar keine Gratis-App anbietet, aber ebenfalls die Nutzer betrügt. In der Beschreibung der App „Virus Shield“ wurde behauptet, dieses Programm könne verhindern, dass schädliche Apps auf dem Android-Gerät installiert werden. Leider war diese App Betrug in Reinform, den sie tat: absolut nichts! Die Experten des Blogs haben das Programm heruntergeladen, ausprobiert und vor allen Dingen auch dekompiert – das Ergebnis haben sie in ihrem Blog publiziert (www.androidpolice.com/2014/04/06/the-1-new-paid-app-in-the-play-store-costs-4-has-over-10000-downloads-a-4-7-star-rating-and-its-a-total-scam/). Wenigstens könnte man dem Anbieter „Deviant Solutions“ zugutehalten, dass er keine schädliche Software auf das Gerät bringt – aber Google hat diese App dann auch schnell aus dem Play Store verbannt.

Dieses Beispiel zeigt sehr schön, dass es nicht nur die Anwender von Gratis-Apps sind, die versuchen, die Nutzer mittels unlauterer Geschäftsmodelle zu schädigen: Auch kostenpflichtige Apps verwenden oft unlautere Geschäftsmodelle – und wenn sie einfach nur Snake Oil anbieten.

Thomas Bär, Frank-Michael Schleder

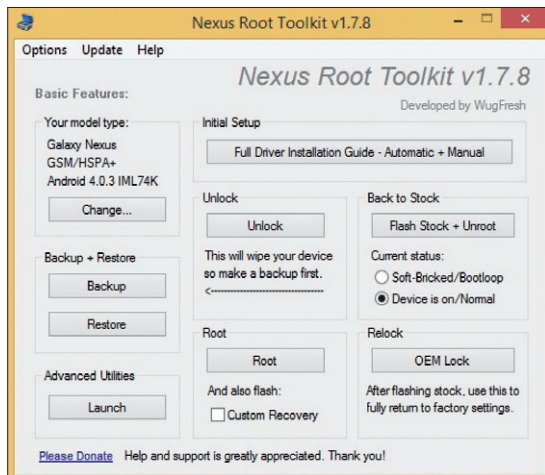
3.7 Android-Rooting: Vorzüge und Gefahren

Android-Anwender „rooten“ oder „jailbreaken“ oft ihr Android-Gerät. Anreize sind mehr Funktionalität, alternative Firmware und der Zugriff auf Apps von Quellen wie Cydia. Missbraucht wird dies häufig für die Verbreitung von Viren und Trojanern. Wir zeigen auf, was die Vorteile sind und worauf Sie achten sollten.

Android baut auf einem Linux-Kernel auf. In den Standardeinstellungen haben Anwender nur begrenzten Zugriff auf die Einstellungen und Möglichkeiten des Gerätes. Der Begriff „Root“ stammt aus dem Linux/Open-Source-Bereich und soll Anwender in die Lage versetzen, umfassende Rechte auf ihrem Gerät zu erhalten.

Ein Benutzer mit Root-Rechten ist auf dem Gerät nicht eingeschränkt, sondern hat umfassende Schreib- und Leserechte in allen Bereichen. Das wirkt sich bei Android in den verschiedenen Apps und Einstellungsmöglichkeiten auf. Daher gibt es für viele Endgeräte im Internet Anleitungen, wie sich Geräte rooten lassen.

Rooting: Tools wie das Nexus Root Toolkit helfen beim Rooten verschiedener Smartphones und Tablets, im Beispiel bei den Nexus-Geräten.



Gerootete Geräte können nicht nur auf externe App-Stores zugreifen, sondern auch mehr Einstellungen auf dem System vornehmen. Viele Apps, die Systemzugriff benötigen, funktionieren erst, wenn das entsprechende Gerät gerootet wurde. Das gilt häufig auch für Apps, die auf Systemdateien zugreifen wollen. Generell ist eine solche Vorgehensweise nur für solche Anwender sinnvoll, die sämtliche Funktionen nutzen, die das Rooting bietet. Nur um ein gerootetes Gerät zu besitzen, ist dies sicherlich überflüssig.

Für Profis sind die wichtigsten Vorteile beim Rooting zunächst flexiblere Möglichkeiten bei der Installation von Apps aus verschiedenen Quellen. Außerdem lassen sich mehr Systemeinstellungen auf dem Gerät ändern und zusätzliche Funktionen

integrieren. Beispiele dafür sind die Installation von Custom-ROMs wie CyanogenMod oder die Anpassung des Kernels für eine Beschleunigung der Geräte. Natürlich lässt sich auch die Oberfläche viel umfassender anpassen.

3.7.1 Gefahren und Probleme beim Rooting

Anwender kommen aber nicht nur in den Genuss der zahlreichen Vorteile, sondern gehen auch Risiken und Gefahren ein. Diese sind beim Rooting nicht zu unterschätzen: Wer Raubkopien installiert, macht sich strafbar – unabhängig davon, ob der entsprechende Anwender überhaupt weiß, ob eine bestimmte App legal ist oder illegal kopiert wurde. Zudem können fehlerhafte Einstellungen, die durch das Rooting erst möglich werden, Geräte irreparabel beschädigen.



UnLock Phone: Tools wie UnLock Phone können dabei helfen Android-Geräte zu rooten. Allerdings müssen Sie hier besonders aufpassen, da es in diesem Bereich ebenfalls viele Schädlinge gibt.

Eine weitere Gefahr sind viren- und trojanerverseuchte Apps aus den externen App-Stores oder anderen Quellen im Internet. Häufig bekommen Anwender nichts von diesen Trojanern mit. Die Schädlinge können Geräte nicht nur beschädigen, sondern auch enorme Kosten verursachen.

Für Firmenanwender sind gerootete Geräte besonders problematisch. Zunächst können viele Mobile-Device-Management (MDM)-Systeme von Unternehmen gerootete Geräte erkennen und aussperren. Im schlimmsten Fall haben Sie also nach einem Rooting-Vorgang keinen Zugriff mehr auf das Firmennetzwerk – diese Nachteile überwiegen die Vorteile des Rootings deutlich. Außerdem verbieten viele Unternehmen das Verbinden gerooteter Geräte mit dem Firmennetzwerk. Wer eine Verbindung dennoch durchführt und dabei erwischt wird oder, noch schlimmer, Schaden im Netzwerk verursacht, sollte sich warm anziehen. Viele MDM-Anwendungen können gezielt gerootete Geräte aussperren. In einem solchen Fall lohnt sich das Rooting sicherlich nicht.

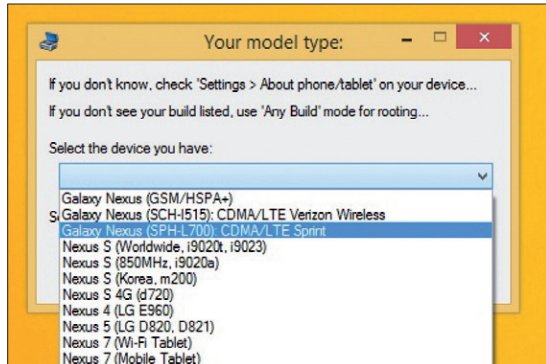
3.7.2 Kein Support bei Rooting-Problemen

Eine weitere Gefahr ist der Support, den der Hersteller für gerootete Geräte häufig nicht mehr gewährt. Viele Hersteller erkennen, dass ein Gerät gerootet wurde, auch wenn es nach einem Problem wieder zurückgesetzt wurde. Softwareaktuali-

sierungen oder neue Android-Versionen funktionieren häufig mit gerooteten Systemen nicht oder versetzen diese in einen inkonsistenten Zustand.

Wenn Sie Geräte gerootet haben, müssen Sie entweder den Rooting-Vorgang bei neuen Versionen wiederholen oder zumindest genau darauf achten, wie Sie Aktualisierungsvorgänge durchführen. In jedem Fall macht ein gerootetes Gerät die Aktualisierung von Android und Apps komplizierter beziehungsweise erfordert einiges an Kontrolle und Mehraufwand. Anfänger sind hier meistens überfordert.

Rooting: Hier lassen sich die verschiedenen Nexus-Geräte auswählen.



Bereits beim eigentlichen Rooting-Vorgang kann einiges schiefgehen. Funktionierte die Anpassung der Software nicht, startet das Android-Gerät häufig nicht mehr oder stürzt ab. Diese Fehler werden auch als Soft-Bricks bezeichnet. Schlimmer sind Hard-Bricks, bei denen die Hardware des Gerätes zerstört wird. Während Sie bei Soft-Bricks mit Softwareanpassungen noch gegensteuern können, sind Hard-Bricks für gerootete Smartphones in der Regel tödlich. Die meisten Hersteller bieten dann auch keine Gewährleistung mehr, was bei neuen und teuren Top-Geräten sehr ärgerlich ist.

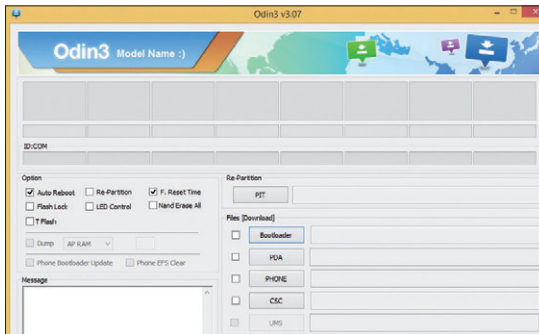
Sicherheitskritische Apps wie Home-Banking oder Verbindungen mit Firmennetzwerken sollten tunlichst nicht auf gerooteten Geräten verwendet werden. Vor allem ungetübte Anwender setzen sich damit einer hohen Gefahr aus – insbesondere wenn auch externe Apps aus unbekannten Quellen installiert wurden. Viren und Trojaner aus nicht seriösen Quellen gehören zu den größten Gefahren von gerooteten Smartphones bei Android.

3.7.3 Vorteile des Rootings

Viele Einstellungen in Android, zum Beispiel wenn es um VPNs oder eine effiziente Datensicherung geht, erfordern gerootete Geräte. Hier müssen Anwender und verantwortliche IT-Mitarbeiter einfach abwägen, ob Nutzen und Risiken in

einem ausgewogenen Verhältnis stehen. In den meisten Fällen lohnt sich das Rooting nur, wenn der entsprechende Anwender genau weiß, was auf dem Gerät durchgeführt wird. Außerdem sollten auch hier nur bekannte Apps installiert werden. Sogar Profi-Android-Anwender sollten unseriöse App-Stores meiden. Selbst bei Cydia (<https://play.google.com/store/apps/details?id=com.saurik.substrate>) besteht die Gefahr, sich Viren einzufangen. Der Einsatz eines Virenschanners auf gerooteten Geräten ist da nur ein kleines Hilfsmittel, da auch diese Apps nicht alle Angriffe erkennen können.

Ein großer Vorteil beim Rooting ist die Möglichkeit, die komplette Oberfläche des Systems zu ändern. Selbst die Android-Version lässt sich austauschen. Neben CyanogenMod gibt es weitere Custom ROMs, mit eigenen Schwächen und Stärken. Manche Entwickler legen vor allem Wert auf eine Beschleunigung der Geräte, andere auf mehr Akku-Laufzeit und wieder andere auf komplett neue Oberflächen.



Odin: Zum Rooten von Samsung-Smartphones über einen PC wird häufig das Tool Odin verwendet.

Vor einem Rooting-Vorgang steht daher erst einmal Recherchearbeit an. Nicht alle Geräte lassen sich gleich rooten, und nicht alle Versionen der Custom-ROMs arbeiten mit allen Android-Versionen auf allen Geräten zusammen. Anwender, die ihr Gerät rooten wollen, sollten genau durchlesen, ob das Rooten möglich ist und ob das Custom-ROM, das installiert werden soll, mit dem entsprechenden Endgerät kompatibel ist.

3.7.4 Custom-ROMs versus Rooting

Beim Rooting machen Sie im Grunde genommen nichts anderes, als sich erhöhte Rechte für Ihr Android-Gerät zu geben. Auf Basis dieser Rechte können Sie dann mehr Einstellungen ändern, Funktionen hinzufügen und Apps installieren, die offiziell nicht freigegeben sind. Custom-ROMs ersetzen das installierte Android durch eine neue Version. Das kann eine aktuellere Version sein, zum Beispiel für Geräte, die nicht mehr offiziell vom Hersteller unterstützt werden, oder eine Version mit angepasster Oberfläche. Um ein Custom-ROM zu installieren, brauchen

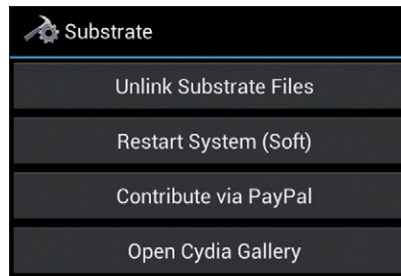
Sie Root-Rechte. Viele Custom-ROMs, wie das bekannte CyanogenMod (www.cyanogenmod.org), führen beide Vorgänge selbständig durch. Erst wird das Gerät gerootet, danach das Custom-ROM installiert.

3.7.5 Wann lohnt sich das Rooten am meisten?

Am meisten profitieren Anwender beim Rooting dann, wenn sie ein altes Gerät einsetzen, für das es keine neue Android-Version mehr gibt. Sollen hier neue Funktionen installiert werden, muss häufig ein Custom-ROM ran. Prominentestes Beispiel ist CyanogenMod (www.cyanogenmod.org). Es baut in der Regel auf der aktuellsten Android-Version auf und kann daher auch neue Funktionen schnell und einfach bereitstellen. Da bei alten Geräten die Risiken nicht ganz so hoch sind, dafür der Nutzen aber umso höher, kann sich das Rooten und das Installieren eines Custom-ROMs lohnen – allerdings auch hier nur dann, wenn ein praktischer Hintergrund vorliegt, also eine neue Android-Version installiert werden muss, aus welchem Grund auch immer.

Nur damit generell eine neue Android-Version installiert wird, zahlt sich das Rooting selten aus. Sollen jedoch aus einer neuen Version Funktionen genutzt werden, zum Beispiel die Benutzerverwaltung aus Android 4, oder Sicherheitslücken geschlossen werden, ist das Aktualisierung von Endgeräten durchaus sinnvoll. Da bei diesen Geräten häufig ohnehin die Garantie/Gewährleistung ausgelaufen ist und sie kaum noch einen echten Wert haben, lohnt sich eine Aktualisierung.

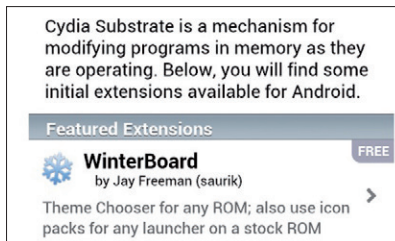
Cydia: Bei alternativen App Stores wie Cydia besteht die Gefahr, sich Viren einzufangen.



Das Installieren von Custom-ROMs und das damit verbundene Rooting können die Sicherheit von Android-Geräten aber auch erhöhen. Vor allem bei billigen und alten Geräten findet keine Aktualisierung der installierten Android-Version mehr statt. Dadurch werden auch keine Sicherheitslücken mehr geschlossen. Installieren Sie aber auf einem solchen alten Gerät die aktuelle CyanogenMod-Version, wird auch die neue Android-Version installiert, die natürlich wesentlich sicherer ist als veraltete Versionen. Wenn Geräte mit SIM-Locks versehen sind, sich also nur SIM-Karten einzelner Anbieter nutzen lassen, können Sie mit dem Rooting diesen Lock entfernen und auch andere SIM-Karten nutzen.

3.7.6 Stable, Nightly Build, AOSP und Stock

Wer sich mit dem Thema Rooting und Custom-ROMs auseinandersetzt, stößt häufig auf Begriffe, die wenig bekannt sind. Vor allem bei CyanogenMod spielen hier Nightly Builds und Stable Builds eine wichtige Rolle. Stable Builds sind getestete und freigegebene Versionen, die funktionieren sollten. Diese Version ist zwar häufig nicht mit den neuesten Features ausgestattet, dafür aber weitgehend frei von Fehlern. Nightly Builds enthalten alle aktuell verfügbaren Funktionen, sind aber noch nicht umfassend getestet. Hier können noch Fehler drinstecken, die sich in unstabilem Verhalten äußern oder das System womöglich komplett zum Absturz bringen. Nightly Builds sollten nur Anwender installieren, die genau wissen, was sie tun, und notfalls ein Gerät reparieren können, zumindest was die Software betrifft. Selbstverständlich ist auch hier die Installation nur dann sinnvoll, wenn eine Funktion aus diesem Build genutzt werden soll.



Cydia: Natürlich gibt es auch deutlich mehr Möglichkeiten und Einstellungen durch die Apps auch Stores wie Cydia.

Viele Custom-ROM-Anbieter bieten die Möglichkeit, zwischen AOSP und Stock zu wählen. AOSP (Android Open Source Project) ist der offizielle und frei zugängliche Source-Code von Android. Setzen Sie aber auf ein Custom-ROM mit Stock-Software, wurden Änderungen an diesem Code vorgenommen. Auch hier sollten Anwender gründlich überlegen, ob sich eine Aktualisierung lohnt.

Die Installation eines Custom-ROMs läuft häufig in mehreren Stufen ab. Sie müssen Ihr Gerät zuerst rooten. Danach übertragen Sie das ROM auf Ihr Endgerät und starten einen Wiederherstellungsvorgang. Durch ihn wird die neue Version installiert. Achten Sie aber darauf, dass dabei alle Daten auf dem Gerät gelöscht und alle Einstellungen angepasst werden. Die Installation eines Custom-ROMs entspricht im Grunde genommen einem Reset des Gerätes und einer anschließenden Neuinstallation von Android in angepasster Form.

3.7.7 Gerootete Geräte sichern

Ein Vorteil von gerooteten Geräten ist die Möglichkeit, mehr Daten zu sichern. Mit Apps wie Titanium Backup (<https://play.google.com/store/apps/details?id=com.keramidas.TitaniumBackup&hl=de>) können Sie nicht nur die Daten auf Ihrem

Android-Gerät sichern, sondern auch alle Einstellungen, Android selbst, die installierten Apps, Daten dieser Apps und auch hier die meisten Einstellungen. Der Vorteil dieser Sicherung liegt auf der Hand: Die Wiederherstellung eines solchen Gerätes umfasst ebenfalls alle diese Einstellungen. Titanium Backup kann zudem Apps zwischen SD-Karten und dem internen Speicher hin- und herschieben. Auch zeitgeplante Sicherungen werden unterstützt. Die Software lässt sich ausschließlich auf gerooteten Geräten nutzen. Wer häufig mit seinem Gerät experimentiert, sollte sich die App ansehen.

3.7.8 Fazit

Die Frage, ob sich das Rooten eines Gerätes lohnt, lässt sich nicht mit einem einfachen Ja oder Nein beantworten. Grundsätzlich gehen Anwender ein Risiko beim Rooting ein. Das Gerät funktioniert unter Umständen nach dem Vorgang nicht mehr, Viren werden durch unseriöse Apps eingeschleust, und fehlerhafte Einstellungen können das Gerät zerstören.

Allerdings bietet das Routing auch Vorteile: Es gibt mehr Einstellungen, alte Android-Versionen von nicht mehr unterstützten Geräten lassen sich aktualisieren, und man kann viele Apps nutzen, die ohne Rooting nicht funktionieren. Beispiele dafür sind Datensicherungs-Apps oder Apps für VPN-Verbindungen.

Allerdings sollte kein Gerät gerootet werden, nur damit es gerootet ist. Es sollte schon ein Sinn hinter dem Vorgang stehen, wie das Entfernen eines SIM-Lock, der Einsatz einer notwendigen App oder das Aufspielen einer neuen Android-Version, die sicherer und stabiler ist.

Ungeübte Anwender sollten besser auf das Rooten verzichten oder zumindest mit einem alten Gerät beginnen, das nicht mehr verwendet wird. Bei neuen Android-Geräten, die häufig auch noch teuer sind, macht das Rooting selten Sinn. Ausnahme ist auch hier die Verwendung einer Custom-Rom wie CyanogenMod.

Thomas Joos



Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt. Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Produktivitäts-Apps im Security-Check**
(www.tecchannel.de/2061865)
- **F-Secure Freedom für Android und iOS 7 im Test**
(www.tecchannel.de/2056050)

4 Security aus der Cloud

Cloud-Sicherheit zielt in zwei Richtungen: Einmal geht es um den Schutz der online genutzten Anwendungen mit den in der Cloud abgelegten Daten. Vor allem die Sicherheitsrichtlinien für die Nutzung von Cloud-Diensten sind oft noch unzureichend. Zum Anderen wächst die Zahl Cloud-gestützten Security-Lösungen, etwa wenn es um das Erkennen von Malware oder Online-Biometrie-Tools geht.

4.1 Ratgeber: mehr Sicherheit für Unternehmensdaten in der Cloud

Die Vorteile von Cloud-Dienstleistungen liegen auf der Hand: geringere Fix- und Anschaffungskosten, mehr Flexibilität und höhere Technologiestandards im Unternehmen. Doch die nötigen Sicherheitsrichtlinien für die Nutzung von Cloud-Diensten hinken hinterher.

Nur ein Drittel der kleinen und mittelständischen Unternehmen (KMU) in Deutschland nutzt derzeit Dienstleistungen aus der Cloud, wie TecChannel kürzlich mit seiner Studie „Cloud Computing im Mittelstand“ (www.tecchannel.de/2056851/) gezeigt hat. Der Grund: Angst der Unternehmer vor Sicherheitslücken und Datenverlust. Eine Angst, die unbegründet ist, wenn die Geschäftsführer und IT-Leiter bei der Auslagerung ihrer Daten und der Nutzung der Cloud einige Grundregeln beachten. Die KMU versprechen sich von der Cloud vor allem die schnellere Bereitstellung von IT-Services und deren verbesserte Skalierbarkeit, den ortsunabhängigen Zugriff auf IT-Ressourcen und automatische Updates. Auch dies hat die TecChannel-Studie gezeigt. Dennoch: So klar sie die Vorteile der Cloud sehen, so skeptisch sind die betreffenden Firmen bei der Frage, mit welchem Risiko diese Benefits verbunden sind. Die Sicherheitsbedenken aufgrund medialer Großereignisse wie der NSA-Affäre sind in Deutschland viel größer als in anderen Industrienationen – und bescheren dem deutschen Mittelstand damit international einen Wettbewerbsnachteil. Das ist paradox, wenn man bedenkt, dass der Datenschutz in Deutschland höchsten Ansprüchen genügt. Planen KMU die Verlagerung von Daten oder Anwendungen in die Cloud, ist aber auch die genaue Prüfung des Dienstleisters – etwa hinsichtlich bestehender Zertifizierungen – wichtige Grundlage für ein entsprechendes Sicherheitsniveau.

4.1.1 Die Cloud gibt es nicht als Standardlösung

Eine gute Lösung ist auf jeden Kunden individuell zugeschnitten. Public, Private oder Hybrid Cloud? In Verbindung mit Managed-Services oder gar komplettes Outsourcing? Der Provider sollte den Kunden beraten können, wo welche Daten

am besten aufgehoben sind. Das ist abhängig von der Größe des Unternehmens, der Branche, einer Bewertung und Klassifizierung der Unternehmensdaten und dem Umfang der Services, die benötigt werden. Standardisierte Elemente sind dabei günstig und erprobt, die Kunden sollten aber immer auch Wert auf Flexibilität legen. Der technische Support und die Kapazitäten müssen an den persönlichen Anforderungen gemessen – und abgerechnet – werden, nicht am durchschnittlichen Bedarf. Bei der Nutzung von externen Providern gibt es zudem verschiedene Sicherheitsaspekte:

Individuell: Bei der Auswahl von Cloud-Services muss man die eigenen Anforderungen in den Vordergrund stellen. (Quelle: Barracuda Networks)



Der Provider schützt seine Infrastruktur und Software vor Angriffen von außen und sollte eine sichere Verbindung zwischen Kunde und Rechenzentrum bereitstellen. Von den hohen Sicherheitsstandards eines externen Providers kann die IT-Abteilung nur profitieren. Dank neuester Sicherheitssoftware und regelmäßiger Wartung ist die umfassende Datensicherheit meist weitaus besser gewährleistet als im eigenen Rechenzentrum. Welche Personen auf welche Daten zugreifen dürfen, muss im Unternehmen geregelt sein. Auch hier kann und sollte ein professioneller Anbieter helfen, klare Regeln aufzustellen.

4.1.2 Security-Services: auf den individuellen Bedarf zugeschnitten

Grundlegend für eine sichere IT ist eine qualifizierte Analyse, welche speziellen Security-Mechanismen für bestimmte Daten und Anwendungen bereitgestellt

werden müssen. Dabei spielt eine Rolle, welche Daten wohin migriert werden sollen und ob sie nur für Interna oder auch für den Kundenkontakt genutzt werden sollen. Sollten Kundendaten bei einem externen Provider lagern, können KMU auf einer strikten Trennung bestehen: Ein guter Provider installiert pro Kunde eine eigene Umgebung – eine versehentliche Verwechslung oder Vermengung der Daten ist damit ausgeschlossen.

Die Unternehmen sollten darauf achten, dass besondere Sicherheitsvorkehrungen eingehalten werden, etwa wenn sie in der Cloud sensible Daten verwalten wollen. So ist zum Beispiel beim Dateiaustausch mittels Triple-Crypt-Verschlüsselungstechnologie die Garantie gegeben, dass der Schutz höchsten Sicherheitsstandards genügt. Eine weitere gute Option zur Absicherung sind Back-up-Systeme, die Kunden selbst steuern können – ohne dass Provider Zugriff darauf haben.

4.1.3 „Schatten-IT“ schadet der Sicherheit – und wird dank der Cloud überflüssig

Sicherheitslücken, die wegen der Unachtsamkeit der eigenen Mitarbeiter im System entstehen, stellen die IT-Abteilung von KMU vielfach vor größere Herausforderungen als gezielte Angriffe von außen. Das größte Problem ist die „Schatten-IT“: Viele Mitarbeiter meiden den Weg über die hausinterne IT, weil sie schnelle, unbürokratische Geschäftslösungen wie etwa Dienstleistungen zum Datentransfer oder zur Aktualisierung von Software benötigen.

Die finden sie vielfach auf Online-Portalen mit undurchsichtigen Sicherheitsvorkehrungen. Über einen Anbieter mit einer transparenten Datenschutzpolitik könnte Software-as-a-Service ohne hohe Anfangsinvestition bezogen werden. Dort sind die Anwendungen ständig auf dem aktuellsten Stand und durch den Provider zusätzlich geschützt. Das hilft der IT-Abteilung, Compliance und Sicherheitsvorschriften des Unternehmens einzuhalten. Unternehmen sollten ihre Mitarbeiter auch darüber hinaus sensibilisieren: Wenn diese mit privaten Geräten auf Firmendaten zugreifen, birgt das bei mangelndem Schutz der Devices große Sicherheitsrisiken. Ein sicheres Mobile Device Management ist also entscheidend für die Nutzung von externen Services und Cloud-Lösungen.

4.1.4 Unternehmen müssen Cloud-ready sein, bevor sie die Services nutzen

Um Cloud-Lösungen effizient und sicher nutzen zu können, sollten KMU den Datenumzug gewissenhaft planen. Ein guter Provider wird die Unternehmens-IT dafür auf Cloud-Readiness überprüfen. Dazu gehört die Analyse der unternehmerischen Anforderungen, der betrieblichen Abläufe sowie der vorhandenen Technologien mit Blick auf den Nutzen beim Einsatz von Cloud-Computing.

Wichtig ist, die bei einem Umstieg auf die Cloud-Lösung entstehenden Kosten mit denen zu vergleichen, die der Aus- und Umbau der bestehenden IT-Infrastruktur nach sich ziehen würde. Wenn die Cloud finanzielle Vorteile bringt, müssen KMU notwendige Änderungen in der IT-Umgebung und ihre spezifischen Cloud-Anforderungen identifizieren. Basis sind die vier zentralen Aspekte des Cloud-Computings: Unternehmensausrichtung, Organisation, Infrastruktur und Anwendungen. Schlussendlich sollte der Anbieter den richtigen Zeitpunkt für den Umstieg wählen. Entwicklungs- und Implementierungsverzögerungen bei der Cloud selbst sowie solche, die bei wichtigen Projekten durch die Implementierung der Cloud-Strategie entstehen könnten, sollen so vermieden werden.

4.1.5 Zertifizierungen als Hinweis auf die Verlässlichkeit des Providers

Zertifizierungen sind ein guter Hinweis auf die Verlässlichkeit und Qualität des Providers. Allerdings gibt es eine große Anzahl dieser Prüfsiegel, die auf den ersten Blick verwirrt. Wichtig ist, dass ein Provider Zertifizierungen erhalten hat, die sich sowohl an globalen als auch an lokalen Standards orientieren, dass er also für seine weltweite Verfügbarkeit sowie für die Einhaltung der lokalen Datenschutzbestimmungen gute Zeugnisse bekommt. Natürlich ist es auch wichtig, welche Institution das Siegel vergibt:

Die ISO-Standards definiert und überprüft das Bundesamt für Sicherheit in der Informationstechnik (BSI, www.bsi.bund.de), eine der vertrauenswürdigsten Quellen. Der Provider sollte dort über alle und vor allem die aktuellsten Zertifikate verfügen. Bei Bedenken in Bezug auf Datenschutz ist das EU-Safe-Harbor-Zertifikat eine gute Richtschnur: Damit ist gewährleistet, dass der Provider die Daten nach europäischem Recht schützt und nicht etwa nach amerikanischem. Wer genau hinschaut, sollte neben der Layer2-Verschlüsselung auch auf ein rollenbasiertes Sicherheitskonzept achten. Das reglementiert Zugriffe noch stärker. Beide Sicherheitsmechanismen werden zum Beispiel von einem Provider wie Dimension Data aufgrund ihrer netzwerkzentrischen Cloud-Architektur angewendet.

4.1.6 Herstellerzertifizierungen bedeuten einfache Implementierung

Ein weiteres Entscheidungskriterium bei der Wahl des passenden Providers sind etwaige Zertifizierungen durch Hersteller. Wenn Kunden Anwendungen zu einem Cloud-Provider „umziehen“ wollen, ist es wichtig zu wissen, wie leicht diese in die Umgebung eingebettet und wie reibungslos die gesamten Abläufe dort implementiert werden können. Namhafte Hersteller wie Microsoft oder SAP haben daher ihre eigenen Zertifizierungen. Der deutsche Softwarehersteller SAP (www.sap.com) überprüft vor der Zertifizierung beispielsweise die Infrastruktur der Rechen-

zentren eines Providers, dessen IT-Spezialisten, die physikalischen und logischen Vorkehrungen zum Schutz der Daten, die Prozesse sowie Portale eingehend. Alle Faktoren müssen den Ansprüchen von SAP im Bereich der Qualität, Verfügbarkeit und Sicherheit genügen. Wenn ein Provider diese Zertifizierung erhält, dann können die bereits genutzten Anwendungen dort einfach implementiert und die mit ihrer Nutzung verbundene Rechenleistung noch besser skaliert werden.

4.1.7 Die rechtlichen Grundlagen im Hinterkopf

Wenn Unternehmen die Daten vor fremdem Zugriff schützen wollen, müssen sie auch die rechtlichen Grundlagen parat haben. Der Datenschutz in Deutschland genügt dabei höchsten Ansprüchen. Man sollte sich aber auch darüber im Klaren sein, dass es „die deutsche Cloud“ im eigentlichen Sinne nicht geben kann, denn die Cloud macht nicht vor Ländergrenzen halt. Gerade bei den Globalisierungsvorhaben vieler Mittelständler ist die weltweite Verfügbarkeit von Cloud-Services eines Provider entscheidend dafür, den Ambitionen der Kunden Rechnung zu tragen. Das deutsche Bundesdatenschutzgesetz ist ein wichtiger Eckpfeiler, und auch die europäische Datenschutz-Richtlinie 95/46/EG ist bis zur Entwicklung eines neuen und umfassenden Gesetzes ein Hinweis auf eine gute Datenschutzpolitik. Wichtig ist, einen Partner auszuwählen, der mit seinen Cloud-Diensten und Rechenzentren im europäischen Rechtsraum auf sicherem Terrain verankert ist. Dieser Partner sollte die IT-Transformation der Kunden begleiten, die nicht nur Cloud-Lösungen, sondern auch Beratungsleistungen, Managed-Services oder gar Outsourcing beinhaltet, damit die IT bedarfsgerecht und auf die individuelle Kundensituation zugeschnitten bereitgestellt werden kann.

4.1.8 Kunden können entscheiden, wo ihre Daten liegen

Die Frage nach der sicheren Nutzung von Cloud-Technologien ist in erster Linie eine Frage der Beherrschbarkeit und der damit verbundenen Risiken. Je nach Einsatzszenario ergeben sich unterschiedliche Sicherheitsanforderungen. Bei der richtigen Beratung sind vorrangig die Anbieter in der Pflicht und dafür zuständig, Transparenz zu schaffen. Sie müssen dem Kunden jederzeit Auskunft erteilen können, in welchem Rechenzentrum seine Daten liegen und auf welcher Plattform sie gehostet werden. Verfügt ein Provider über mehrere Rechenzentren mit Standorten in mehreren Ländern, können die Kunden entscheiden, wo ihre Daten gelagert werden. Ausschließlich sie selbst legen fest, wer Zugriff auf die Daten hat und wie die Zugriffe auf die Cloud überwacht werden sollen. Der Provider selbst darf und kann nicht auf die Daten zugreifen, die Unternehmer in der Cloud lagern

Bernd Reder

Bernd Reder ist freier Journalist mit den Schwerpunkten Netzwerke, IT und Telekommunikation in München.

4.2 Kalkulierbares Risiko – Schatten-IT in Unternehmen

Schatten-IT in Firmen lässt sich schwer vermeiden, aber auch hier sind Sicherheitsstandards Pflicht. Um das Bewusstsein für Datensicherheit in allen Abteilungen eines Unternehmens zu schärfen, ist es wichtig, diesen Aspekt zu thematisieren, damit die Compliance nicht gefährdet wird.

Sobald der Begriff Cloud fällt, denken IT-Profis fast sofort an die damit verbundenen Sicherheitsrisiken. Diese sind gleichzeitig der Hauptgrund dafür, dass viele Unternehmen immer noch den Schritt in diese virtuelle Welt scheuen. Doch was tun, wenn einzelne Abteilungen in Eigenverantwortung und ohne das Wissen der IT Cloud-Dienste in Anspruch nehmen – quasi als Schatten-IT?

Dabei ist es häufig sehr einfach, diese Dienste und Ressourcen zu nutzen, meistens sogar – wenigstens zu Beginn – kostenlos oder zumindest sehr preisgünstig. Dennoch hat es durchaus seine Gründe, dass dies normalerweise über die IT läuft, denn nur so können auch wirklich die Integrität der Daten und die Einhaltung der Compliance-Richtlinien garantiert werden. Zusätzlich berücksichtigt die IT, im Gegensatz zu vielen „normalen“ Anwendern, solche Punkte wie Verschlüsselung und Zugriffsrechte bei Cloud-Diensten.

So muss zunächst einmal geklärt werden, ob Ihre Daten bereits verschlüsselt sind und ob sie überhaupt verschlüsselt werden sollten oder müssen. Denn nicht alle Daten müssen verschlüsselt werden. Dies ist insbesondere angesichts der mit der Verschlüsselung von Daten verbundenen Verarbeitungs- und Übertragungslast wichtig. So ist es zum Beispiel nicht notwendig, Musikdateien, Archivfotos oder andere allgemein verfügbare Dateien zu verschlüsseln.

Andere Daten hingegen müssen definitiv verschlüsselt werden. Bestimmte Compliance-Anforderungen, zum Beispiel HIPAA oder PCI, verlangen ausdrücklich eine Kontrolle des Datenzugriffs. Dabei lässt sich der unautorisierte Zugriff auf Daten, die sich unter der physischen Obhut eines Diensteanbieters befinden, nur verhindern, indem sie verschlüsselt werden.

4.2.1 Verschlüsselung ja – aber wo?

Sobald klar ist, dass Daten verschlüsselt werden sollen, müssen Sie entscheiden, wo die Verschlüsselung erfolgt. Denn viele Cloud-Dienste bieten bereits von Haus aus eine Verschlüsselung an, diese erfolgt jedoch nur innerhalb der Cloud. Außerhalb sind die Daten immer noch frei zugänglich.

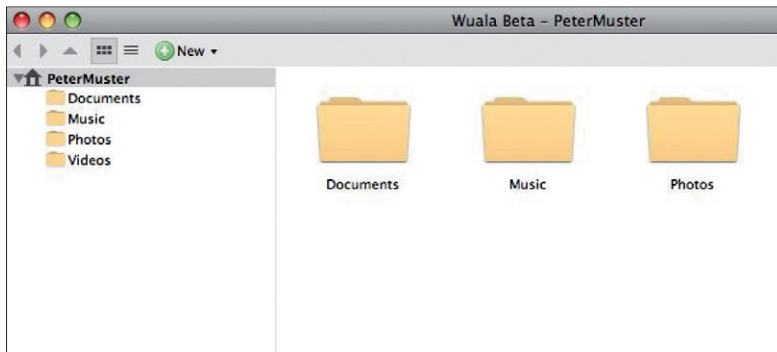
Dabei bestimmt der Ort der Datenverschlüsselung, wer Zugriff auf die Daten hat und wer nicht. Wenn also Ihr Anbieter die Verschlüsselung übernimmt, hat er auch die Möglichkeit, auf die Daten zuzugreifen. Bereits bei oberflächlicher Betrachtung ist dies wichtig, weil somit unbekannte Personen potenziellen Zugriff

auf die Daten haben. Dies birgt jedoch die Gefahr, dass Daten aus der Speicherumgebung des Cloud-Anbieters gestohlen werden können.

Sie sollten also den Schutz Ihrer Daten nie auf die leichte Schulter nehmen und immer damit rechnen, dass es zu Eindring-/Kompromittierungsversuchen kommen kann. Daher sollten die Daten noch bei Ihnen vor Ort verschlüsselt werden, bevor sie in die Cloud verschoben werden.

4.2.2 Verschlüsselung ja – aber womit?

Üblicherweise werden die Daten, die in die Cloud übertragen werden, mit einem symmetrischen Algorithmus verschlüsselt. Dabei gibt es zwei hauptsächlich verwendete Varianten. Die gebräuchlichere dieser beiden ist AES; sie kann mit einer von drei Schlüssellängen implementiert werden: 128 Bit, 192 Bit oder 256 Bit – je länger, desto besser. Die andere symmetrische Verschlüsselungstechnologie ist Blowfish. Blowfish ist ein nicht patentierter Algorithmus, der von Bruce Schneier entwickelt wurde, und hat eine Schlüssellänge von 32 bis 448 Bit. Auch hier gilt: „Mehr ist besser“ – beachten Sie, dass ein 448-Bit-Blowfish-Schlüssel beinahe doppelt so lang ist wie ein 256-Bit-AES-Schlüssel.

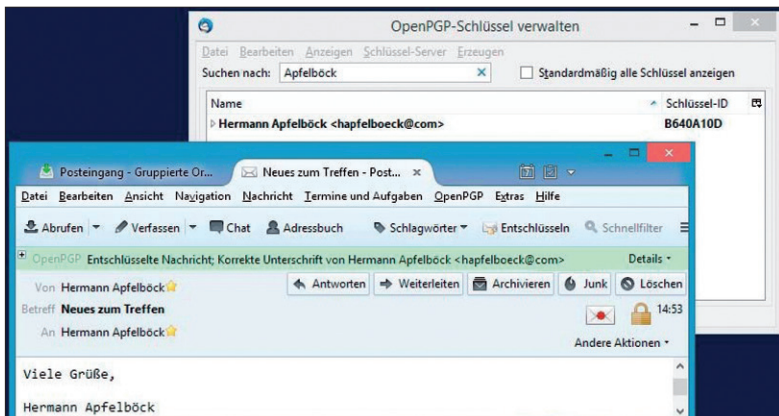


LaCie Wuala: Cloud-Speicherdienste wie Wuala bieten eine integrierte Verschlüsselung an. Alle Daten, die in bestimmte Nutzerverzeichnisse abgelegt werden, werden automatisch verschlüsselt, bevor sie in die Cloud übertragen werden. (Quelle: LaCie AG)

Falls doch eine asymmetrische Verschlüsselung zum Einsatz kommt, um die symmetrischen Schlüssel zu verschlüsseln, sollten Sie sich fragen, warum dies überhaupt notwendig ist. Wahrscheinlich liegt es daran, dass der symmetrische Schlüssel vom Anbieter gespeichert wird, der ihn braucht, um Ihre Daten zu entschlüsseln – was bedeutet, dass die Daten nicht an Ihrem Ende der Internetverbindung verschlüsselt und entschlüsselt werden, sondern auf der Seite des Anbieters, und das wiederum stellt, wie bereits erwähnt, ein Sicherheitsrisiko dar.

4.2.3 Die Schlüssel unter der Fußmatte sind auch virtuell keine gute Idee

Symmetrische Schlüssel müssen immer gut im Auge behalten werden. Daher sollten Sie stets mehrere Kopien des symmetrischen Schlüssels an verschiedenen Orten speichern, um den Zugriff bei Bedarf zu ermöglichen, aber auch aus Gründen der Notfallwiederherstellung und Geschäftskontinuität. Die Kontrolle des Zugriffs auf den Schlüssel ist ebenfalls wichtig. Eine kleine Auswahl besonders vertrauenswürdiger Personen sollte Zugang zum Schlüssel und zu dessen Verwendung haben. Hier lohnt sich der Einsatz asymmetrischer Schlüssel, um die Sicherheit zu garantieren. Dabei sollte jeder einzelne der vertrauenswürdigen Verwahrer des symmetrischen Schlüssels ein persönliches asymmetrisches Schlüsselpaar erstellen. Die öffentlichen Schlüssel sollten anschließend unter den Verwahrern geteilt werden. Wenn nun einer der Verwahrer den symmetrischen Schlüssel ändern muss, kann der Schlüssel mithilfe der asymmetrischen Verschlüsselung an die anderen Verwahrer weitergegeben werden. Der Verwahrer, der den Schlüssel ändert, erstellt dabei eine verschlüsselte Kopie des symmetrischen Schlüssels, wobei er die jeweiligen öffentlichen Schlüssel der Verwahrer verwendet.



Asymmetrische Mailverschlüsselung: Thunderbird, Enigmail und Gnu PG machen sichere Mails relativ komfortabel. Der öffentliche Schlüssel eines Partners kann manuell gesendet werden oder ist auf einem Key-Server zu finden.

Anschließend leitet er den verschlüsselten symmetrischen Schlüssel an die übrigen Verwahrer weiter. Jeder kann diesen symmetrischen Schlüssel dann mit seinem eigenen privaten Schlüssel speichern und darauf zugreifen. Wenn ein Verwahrer ersetzt wird oder nicht mehr als vertrauenswürdig gilt, wird einfach ein neuer symmetrischer Schlüssel erstellt und an die anderen Verwahrer weitergeben; der frühere symmetrische Schlüssel kann dann nicht mehr verwendet werden.

4.2.4 AGB – ich verstehe nur Bahnhof ...

Auch wenn Sie Ihre Daten in der Cloud selbst verschlüsselt haben, sollten Sie immer die Allgemeinen Geschäftsbedingungen Ihres Anbieters genau kennen. Denn falls er innerhalb des Vertrags ausdrücklich erklärt, dass er „allen Auskunftsanordnungen, Durchsuchungsbefehlen und Geheimdienstanfragen“ bezüglich Ihrer Daten nachkommen wird, ist es besonders wichtig, dass Ihre Daten verschlüsselt sind, und zwar auf eine Weise, die es dem Dienstanbieter nicht ermöglicht, die Daten nach eigenem Gutdünken zu entschlüsseln. Denn sollte es eine Auskunftsanordnung oder einen Durchsuchungsbefehl für Ihre Daten geben, können Sie sicherstellen, dass die Gerichtsbeschlüsse direkt Ihrem Unternehmen und nicht einem Dritten vorgelegt werden. In diesem Zusammenhang ist es auch wichtig, ob der Dienstanbieter die Speicherungsdienste, bei denen die Daten physisch aufbewahrt werden, tatsächlich besitzt. Denn wenn er selbst Kunde eines anderen Dienstanbieters ist, sind Sie unter Umständen indirekt Risiken ausgesetzt, die sich aus den Richtlinien des tatsächlichen Dienstanbieters ergeben.

Sie sehen also: Cloud ist kein Freibrief für Fahrlässigkeit. Dies müssen Sie sich immer wieder vor Augen halten – sonst übernimmt bald die Schatten-IT Ihren Job.

Lawrence Garvin



Lawrence Garvin ist ein Head Geek; und technischer Product Marketing Manager bei Solarwinds, ein Microsoft Certified IT Professional (MCITP) und ein neun Mal in Folge Empfänger der Microsoft MVP-Auszeichnung in Anerkennung für seine Beiträge zu der Microsoft TechNet WSUS Forum.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

- **Security-Lösungen für kleine und mittelständische Firmen**
(www.tecchannel.de/2058228)
- **So vermeiden Sie Informationsrisiken im Unternehmen**
(www.tecchannel.de/2040929)
- **Identitätsdiebstahl schwer gemacht**
(www.tecchannel.de/2058228)
- **IT-Sicherheit: 9 neue Security-Mythen**
(www.tecchannel.de/2056604)
- **Tipps & Tricks zur Absicherung der Unternehmens-IT**
(www.tecchannel.de/2047480)
- **So vermeiden Sie Informationsrisiken im Unternehmen**
(www.tecchannel.de/2040929)
- **Security-Konzepte für Smartphone, Tablet und Co.**
(www.tecchannel.de/2040698)

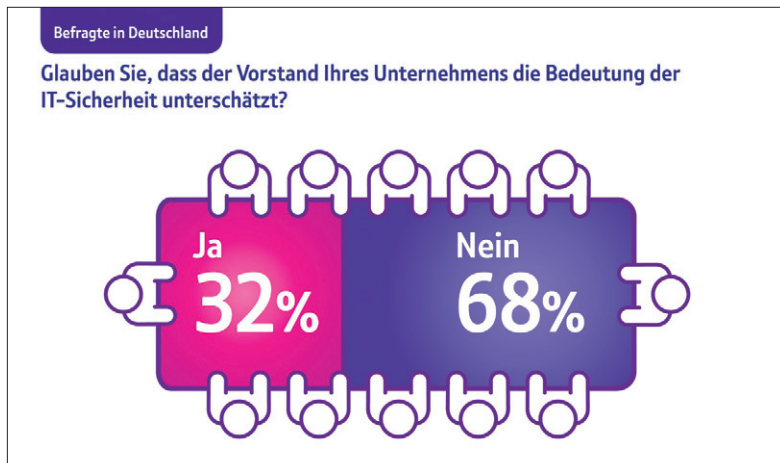
4.3 Ratgeber: Threat-Monitoring-Services aus der Cloud

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht davon aus, dass heute jedes international aufgestellte Unternehmen in Deutschland ein potenzielles Ziel für fortgeschrittene Cyber-Attacks („Advanced Persistent Threats“, kurz APTs) ist. Kleine und mittlere Unternehmen gehören genauso zu den Angriffszielen wie große Konzerne.

Die Möglichkeiten, sich gegen komplexe Angriffe zu schützen, sind im Mittelstand allerdings oftmals gering ausgeprägt. Umso wichtiger ist es, mögliche Angriffe frühzeitig erkennen und bereits vor dem eigenen Netzwerk abwehren zu können.

4.3.1 Frühwarnsysteme fehlen gerade im Mittelstand

Viele Unternehmen in Deutschland sind sich der neuen Cyber-Bedrohungen aber nicht bewusst, wie eine Studie von Vanson Bourne im Auftrag von BT (www.globalservices.bt.com/de/de/news/deutschen_unternehmen_fehlt_bewusstsein_fuer_cyber_bedrohungen) zeigt: Für nur 19 Prozent der deutschen Top-Manager genießt die IT-Sicherheit eine hohe Priorität. An Frühwarnsysteme, Threat-Monitoring- oder Threat-Intelligence-Lösungen gegen Cyber-Attacks denken viele deshalb noch nicht.



BT-Umfrage: 32 Prozent der in der BT Cyber-Security-Studie Befragten glauben, dass ihre Geschäftsleitung die Bedeutung von IT-Sicherheit unterschätzt. Ohne Bewusstsein für die neuartigen Cyber-Bedrohungen werden aber kaum präventive Maßnahmen wie z.B. Cyber-Frühwarnsysteme eingesetzt. (Quelle: BT Germany)

Threat-Monitoring- beziehungsweise Threat-Intelligence-Lösungen könnten dabei helfen, Cyber-Attacken früher zu erkennen, indem sicherheitsrelevante Daten aus verschiedenen, verteilten Quellen ausgewertet und für die Bedrohungsvorhersage genutzt werden, zum Beispiel Daten über erkannte Malware- und Spam-Attacken auf andere Unternehmen.

Eine Umfrage unter IT-Sicherheitsverantwortlichen durch das Ponemon-Institut (www.ponemon.org) ergab, dass 40 Prozent der Befragten in keiner ihrer Sicherheitslösungen Hinweise aus Threat-Intelligence-Lösungen als Frühwarnsystem importieren. 59 Prozent der Befragten sind nicht in der Lage, Threat-Intelligence-Analysen mit ihren existierenden Security-Produkten effektiv zu nutzen.

Es besteht somit ein hoher Bedarf an einfach zu integrierenden, leicht zu bedienenden Frühwarnsystemen, die die Sicherheitslösungen der Unternehmen mit konkreten Warnhinweisen versorgen. Hier kommen Threat-Monitoring-Lösungen aus der Cloud ins Spiel, die extern betrieben werden, vielfältige sicherheitsrelevante Informationsquellen nutzen und kein ausgeprägtes Fach-Know-how bei den Anwenderunternehmen voraussetzen.

4.3.2 Threat Monitoring gibt es aus der Cloud

Die Auswahl an Threat-Monitoring-Lösungen aus der Cloud ist inzwischen reichlich, darunter finden sich Arbor Networks Pravail Security Analytics, BT Assure Threat Monitoring-Service, Check Point ThreatCloud Managed Security Service, Cisco Cognitive Threat Analytics, Dell SecureWorks Advanced Endpoint Threat Detection, FireEye Managed Defense, RSA Web Threat Detection und Trustwave Threat Correlation Service. Anwenderunternehmen sollten allerdings nicht nur auf die monatlichen Nutzungsgebühren achten, wenn eine Entscheidung für einen Cloud-Service als Cyber-Frühwarnsystem ansteht. Damit der Service der Wahl auch tatsächlich die Cyber-Sicherheit erhöht, müssen die jeweiligen Anforderungen an Schnittstellen, Berichte und Alarmierung erfüllt sein. Zudem gibt es Unterschiede bei der Zahl und Art der „Bedrohungssensoren“.

4.3.3 Zahl und Art der Sensoren hinterfragen

Ein Threat-Monitoring-Service erkennt mögliche Cyber-Gefahren durch die zeitnahe Analyse möglichst vieler, relevanter Sicherheitsinformationen, die von Gefahrensensoren bereitgestellt werden. Diese Sensoren sind in der Regel IT-Systeme wie Server, Endgeräte und Netzwerkkomponenten, die der jeweilige Cloud-Service-Provider überwacht. Eine globale, zumindest aber breite Verteilung der Sensoren, viele verschiedene Typen überwachter Geräte und eine möglichst große Zahl an Sensoren spielen bei der Qualität der Bedrohungsanalysen ebenso eine Rolle wie ein schnelles, leistungsstarkes und intelligentes Analyseverfahren des Threat-Monitoring-Service.

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Critical Infrastr.	Mobile Computing	Social Networking	Cloud Computing	Trust Infrastr.	Big Data	Internet of Things
1. Drive-by Downloads	🔴	🔴	🔴	🔴		🔴	🔴	
2. Worms/Trojans	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
3. Code Injection	🔴	🔴	🔴	🟡	🔴	🔴	🔴	
4. Exploit Kits	🔴	🟡	🔴	🔴	🔴	🔴	🔴	
5. Botnets	🟡	🔴	🔴	🔴	🔴			
6. Physical Damage/Theft/Loss	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
7. Identity Theft/Fraud	🔴		🔴	🔴	🔴	🔴	🔴	🔴
8. Denial of Service	🔴	🔴			🔴			🔴
9. Phishing	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
10. Spam	🟡			🔴				🔴
11. Rogueware/Ransomware/Scareware	🔴							
12. Data Breaches	🔴		🔴		🔴	🔴	🔴	🔴
13. Information Leakage	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
14. Targeted Attacks	🔴	🔴				🟡	🔴	🔴
15. Watering Hole	🔴							

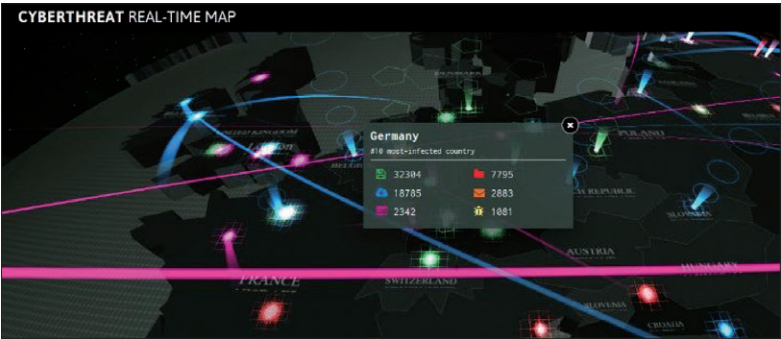
Legend: Trends: 🟢 Declining, 🟡 Stable, 🔴 Increasing

ENISA Threat Landscape 2013: Die Bedrohungen für IT-Systeme werden immer vielfältiger und komplexer. Gerade kleine und mittlere Unternehmen brauchen Unterstützung, um Angriffe möglichst frühzeitig erkennen und abwehren zu können. Eine wichtige Rolle können dabei Threat-Monitoring-Services aus der Cloud spielen. (Quelle: ENISA)

Anwenderunternehmen sollten deshalb nach der Zahl und Art der überwachten IT-Systeme fragen – nicht nur als Referenz, welche Verbreitung der Service bereits genießt, sondern als wichtigen Hinweis auf die Basis für die Bedrohungsanalysen und -vorhersagen. BT zum Beispiel nennt für BT Counterpane mehr als 1.000 Kunden in aller Welt und eine Überwachung von 300.000 Kundengeräten in neun international verteilten Secure Operations Centres (SOC).

4.3.4 Schnittstellen prüfen

Wie hilfreich ein Threat-Monitoring-Service sein kann, hängt einerseits davon ab, von welchen IT-Systemen sicherheitsrelevante Informationen bezogen und analysiert werden können. Andererseits kommt es darauf an, an welche Sicherheitslösungen die Warnungen und konkreten Alarmierung übergeben werden können.



Kaspersky Cybermap: Die Visualisierung von Cyber-Attacks in Echtzeit, wie dies zum Beispiel die Kaspersky-Cyberbedrohungsweltkarte bietet, zeigt die Bedrohungslage und hilft bei der Sensibilisierung. Zusätzlich besteht Bedarf an Bedrohungsdaten, die in IT-Sicherheitslösungen importiert werden können, um so die Abwehr möglichst automatisch optimieren zu können. (Quelle: Kaspersky)

Informationsdienste wie Cyberthreat Real Map (<http://cybermap.kaspersky.com/>) auf Basis des Kaspersky Security Network (KSN) zeigen eindrucksvoll die Gefahrenlage im Internet und liefern sehr wertvolle Informationen. Die Bedrohungsdaten lassen sich jedoch nicht ohne Weiteres automatisiert nutzen und in Sicherheitslösungen eines Anwenderunternehmens integrieren, sodass diese auf die Gefahrenlage automatisch besser reagieren könnten. Anders sieht dies bei Sicherheitstacho.eu aus. Hier gibt es eine definierte Schnittstelle und Anleitung zur Integration des Frühwarnsystems der Deutschen Telekom.

Nachstehende Tabelle gibt eine Übersicht zu den Schnittstellen, die die eingangs erwähnten Anbieter für ihre Threat-Monitoring-Services nennen.

Threat-Monitoring-Services	
Name des Service	Schnittstellen
Arbor Networks Pravail Security Analytics (Cloud-Version)	• ATLAS (Active Threat Level Analysis System) Intelligence Feed: Sicherheitsinformationen aus den Arbor-Network-Internetanalysen • weitere Threat Intelligence Feeds anderer Anbieter • Upload der Systemprotokolle des Anwenderunternehmens

BT Assure Threat Monitoring-Service (BT Counterpane)	• Betriebssysteme und Anwendungen wie Datenbank-anwendungen • Webserver und Host Intrusion Protection • Netzwerkgeräte wie Firewalls, Switches, Router • Network-Intrusion-Detection- und Intrusion-Protection-Systeme (IPS)
Check Point ThreatCloud Managed Security Service	• IPS, Anti-Bot, Antivirus • ThreatCloud Real-time Security Intelligence Feeds von Check Point
Cisco Cognitive Threat Analytics	• Cloud-Security-Netzwerke von Cisco und Sourcefire (Cisco-Unternehmen) • Sicherheitslösung Cisco Cloud-Web-Security • Cisco Advanced Malware Protection (AMP) als Netzwerk- und Endgeräteschutz
Dell SecureWorks Advanced Endpoint Threat Detection	• Windows Server, Notebooks, Desktops • Sicherheitsinformationen aus dem Dell SecureWorks Targeted Threat Hunting Service, der für über Hundert Auftraggeber ausgeführt wird
FireEye Managed Defense	• Sicherheitsinformationen der überwachten Geräte • FireEye-Cybercon-Berichte zum Beispiel über Advanced-Persistent-Threat (APT)-Kampagnen oder Zero-Day-Attacken
RSA Web Threat Detection	• RSA Web Session Intelligence zur Analyse des Verhaltens von Webseiten-Besuchern • RSA Profile Analyzer zum Vergleich des Webseiten-Besucherverhaltens mit früheren Verhaltensmustern
Trustwave Threat Correlation Service (TTCS)	• Datenbanken mit Botnet Domains, Malware Domains, Phishing Domains • Bedrohungsdaten von TTCS-Crowd-Source-Kunden, die die Trustwave SIEM Enterprise oder SIEM Operations Edition nutzen • Informationen über verseuchte Hosts und Malware-Quellen aus automatischen SpiderLabs-Untersuchungen • Sicherheitsinformationen von Trustwave-Security-Lösungen wie Secure Web Gateway

4.3.5 Reporting, Alarming und Dashboards müssen passen

Neben der Übertragung der Bedrohungsanalysen an interne oder ebenfalls als Service angebotene Sicherheitssysteme wie ein IPS (Intrusion Prevention System) bieten Threat-Monitoring-Services auch Berichtsfunktionen. Dies können E-Mails an den Administrator des Anwenderunternehmens sein mit dem regelmä-

ßigen Bericht in PDF-Form, aber auch SMS-Nachrichten über akute Bedrohungen. Je nach Service-Level werden zum Beispiel beim Check Point ThreatCloud Managed Security Service (www.checkpoint.com/services/threatcloud-security-services/managed-security-service.html) die Warnmeldungen direkt dem Nutzer automatisch zugestellt oder von Security-Analysten im Check Point Security Operation Center zuvor einer genauen Prüfung unterzogen. Je nach Kritikalität der Warnungen und je nach Service-Stufe sind zudem die garantierten Reaktionszeiten bei Sicherheitsvorfällen verschieden.

Zusätzlich bieten viele Threat-Monitoring-Services für den Nutzer ein Managementportal mit Dashboard an, das in einem bestimmten Rahmen individualisiert werden kann. Je nach internem Bedarf lassen sich so übersichtliche Management-Reports oder Nachweise über ergriffene Sicherheitsmaßnahmen entsprechend der jeweiligen Compliance-Vorgaben generieren.

4.3.6 Datenschutz nicht vergessen

Wenn Daten an Dritte übertragen werden, sollte auch an den Datenschutz gedacht werden: Wer einen Threat-Monitoring-Service nutzt, wird oftmals auch selbst sicherheitsrelevante Daten zurückspielen. Die sicherheitsrelevanten Informationen, die an den Threat-Monitoring-Service übertragen werden, könnten personenbezogene Nutzerdaten enthalten. Diese unterliegen einer besonderen Zweckbindung (§ 31 BDSG) und müssen vor Missbrauch geschützt werden.

Bevor die Systemprotokolle der überwachten Anwendungen und Geräte an den Threat-Monitoring-Service-Provider geschickt werden, sollte deshalb sichergestellt werden, dass die Daten anonymisiert oder pseudonymisiert sind. Andernfalls könnte die Steigerung der Cyber-Sicherheit durch einen Threat-Monitoring-Service ungewollt dazu führen, dass die Daten der Mitarbeiterinnen und Mitarbeiter des Unternehmens oder anderer Nutzer gefährdet oder zumindest unerlaubt an Dritte übermittelt werden. Gute Threat-Monitoring-Services nehmen den Datenschutz ernst, machen auf die notwendige Anonymisierung oder Pseudonymisierung der Systemprotokolle in der Schnittstellenbeschreibung aufmerksam und verfügen über eine entsprechende Datenschutzerklärung (Privacy Policy).

Oliver Schonschek



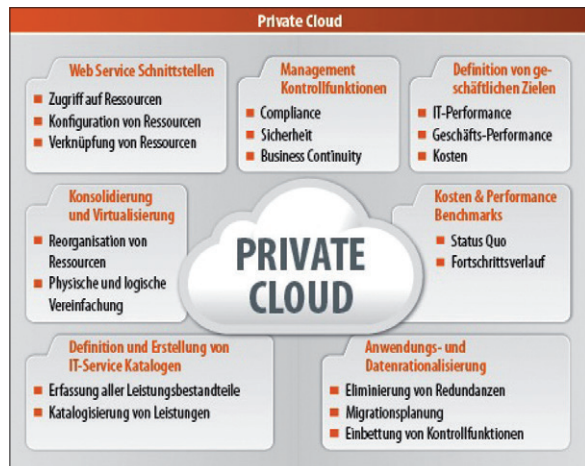
Oliver Schonschek ist freier IT-Fachjournalist und IT-Analyst in Bad Ems.

4.4 Sieben Tipps für Ihren sicheren Weg in die Cloud

Immer mehr Firmen lagern Teile ihrer IT-Infrastruktur aus und greifen auf die Rechnerwolke zurück. Unternehmen wollen optimierte und flexiblere Geschäftsabläufe in einer abgesicherten Umgebung. Cloud Computing wird zunehmend zu einem wichtigen Erfolgsfaktor für Fachbereiche. Wer Cloud Computing nutzt, darf nicht auf Wolke sieben schweben und sich von augenscheinlich attraktiven Angeboten täuschen lassen: Denn Sicherheit und Datenschutz müssen gewährleistet sein. Unzählige Cloud-Angebote erschweren es, das richtige Produkt zu finden. Unternehmensdaten sind der Goldschatz einer jeden Firma. Diesen gibt man nicht leichtfertig aus der Hand. Daher sollten bei der Auswahl des Cloud-Anbieters folgende Punkte kritisch betrachtet und abgefragt werden:

- Wer ist mein Servicepartner?
- Wo werden meine Daten gespeichert?
- Sind Qualität und Verfügbarkeit der Serviceerbringung geprüft und transparent?
- Kann der Anbieter Zertifizierungen vorweisen?
- Welche Authentifizierungsformen finden Verwendung?
- Werden die digitalen Identitäten tatsächlich geprüft, um sicher zu sein, mit wem man zusammenarbeitet?
- Was passiert mit meinen Daten? Ist nachvollziehbar, wer diese bearbeitet?

Definition einer unternehmensweiten Cloud-Strategie: Wer auf eine Cloud-Infrastruktur umsteigen möchte, sollte zunächst eine entsprechende Strategie definieren. (Quelle: Pironet)



4.4.1 Vertrauen in den Servicepartner

Vertrauen in einen x-beliebigen Cloud-Anbieter in einem x-beliebigen Land zu haben und nicht sicher zu sein, welche rechtlichen Grundlagen bei der Datenspeicherung Anwendung finden, ist schwierig. Das Wort „Briefkastenfirma“ erscheint unbewusst vor dem geistigen Auge. Daher sollte darauf geachtet werden, dass der Cloud-Anbieter in Europa, idealerweise in Deutschland, sitzt, Verträge in deutscher Sprache, nach deutschem Recht mit Gerichtsstandort in Deutschland anbietet und auch eine Vereinbarung über Auftragsdatenverarbeitung gemäß § 11 Bundesdatenschutzgesetz bei Bedarf zur Verfügung stellt. Erfolgt die Datenhaltung dann noch in Europa und bestehen vertraglich zugesicherte Service-Levels, ist ein Unternehmen sicher in der Cloud unterwegs.

4.4.2 Gewissheit, wo die Daten sind

Die wesentliche Fragestellung im Bereich der Datensicherheit ist: Wo speichert der Cloud-Anbieter die Cloud-Daten der Kunden? Laut einer aktuellen IDC-Studie zum Thema „Mobile Content Management in Deutschland“ legen mehr als 60 Prozent der deutschen Unternehmen Wert darauf, dass die Cloud-Datencenter in Deutschland oder zumindest in Europa stehen (www.fabasoft.de/idc-mobile). Und das ist wichtig und gut. Denn nur so werden die regionale Versorgungssicherheit und Unabhängigkeit Europas gewährleistet und die Sicherheit erhöht. Die geschäftlichen Daten und Dokumente bleiben in Deutschland oder in einem Land der europäischen Union und unterliegen den deutschen beziehungsweise europäischen Richtlinien für Datenschutz und Datensicherheit. Manche Cloud-Anbieter geben dem Kunden die Wahlfreiheit, wo der Speicherort der Daten liegen soll. Beachtung findet auch der Aspekt, dass die kaufmännische Sorgfaltspflicht eine sichere Cloud-Lokation im Sinne eines geeigneten Risikomanagements verlangt.

4.4.3 Ist die Servicequalität geprüft?

Eine Überprüfung aller Standards für Sicherheit und Zuverlässigkeit sollte regelmäßig erfolgen. Einen seriösen Anbieter erkennt man unter anderem daran, dass dieser die Service Levels, geplante Wartungsarbeiten und Monitoring-Berichte veröffentlicht. Ein weiteres Indiz für ein gutes Cloud-Service sind Zertifizierungen.

4.4.4 Zertifizierte Qualitätsstandards

Dabei weist ein Anbieter die Professionalität seines Rechenzentrumsbetriebs objektiv nach, beispielsweise durch Zertifizierungen wie ISO 27001, ISO 20000, ISAE 3402 Standard oder eine TÜV-Zertifizierung. Diese Zertifikate bestätigen die Informationssicherheit, die Qualität beim IT-Service-Management und dass es sich

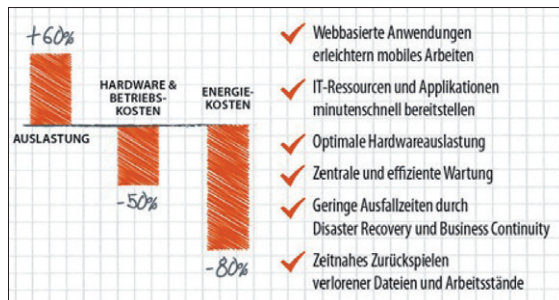
um einen sicheren, verlässlichen und qualitativ hochwertigen Cloud-Service handelt. Das Zertifikat des TÜV Rheinland ist das Prüfsiegel mit den derzeit international umfangreichsten Anforderungen: Beginnend mit einem „Cloud-Readiness-Check“ prüft der TÜV die Cloud auf ihre Tauglichkeit in puncto Sicherheit, Interoperabilität, Compliance und Datenschutz. Danach begutachtet er das Cloud-Design und die eigentliche Umsetzung genauso wie Themen der Architektur, Netzwerksicherheit oder Zugriffskontrollen. Nach erfolgreichem Abschluss dieser Prüfung erhält ein Anbieter das Zertifikat „Certified Cloud-Service“.

4.4.5 Exakt definierte Zugriffsrechte und -sicherheit

In Europa ist der Schutz der Daten in der Cloud ein zentrales Grundbedürfnis. Das betrifft besonders den geschützten Zugang zu Cloud-Daten (Login). Eine Zwei-Faktor-Authentifizierung (neben Login-Name und Passwort benötigt man eine per SMS zugestellte PIN, oder man nutzt für die Anmeldung eine „Digitale Identität“ wie die eID-Funktion des neuen Personalausweises) sorgt dabei für noch höhere Sicherheit bei der Anmeldung. Zusätzlich zur besonders sicheren Zwei-Faktor-Authentifizierung erlaubt die Verknüpfung des Cloud-Accounts mit dem bestehenden Active-Directory-Account eine sichere und einfach zu verwaltende Integration in die IT-Sicherheitsinfrastrukturen von Unternehmen.

Umfassende Konsolidierung und Standardisierung der bestehenden IT-Landschaft:

Grundvoraussetzung für eine flexible Verteilung und Nutzung von Ressourcen in der Cloud ist eine weitgehende Virtualisierung der IT-Systeme. (Quelle: Pironet)



4.4.6 Sichere Zusammenarbeit

In Zeiten von digitalen Identitäten muss im Business gewährleistet sein, dass man mit realen Personen zusammenarbeitet. Mit der Nutzung von digitalen Identitäten, wie der eID-Funktion des neuen Personalausweises, schaffen Unternehmen die Gewissheit, dass Geschäftspartner in der Cloud nicht mit gefälschten Identitäten zusammenarbeiten. Die derzeit höchste Sicherheit erreichen Unternehmen mit der Anmeldung über die digitale Identität. So haben sie in der Cloud immer die Gewissheit, dass sie mit staatlich verifizierten Identitäten zusammenarbeiten.

4.4.7 Gewissheit, was mit den Daten passiert

Grundsätzlich sollten Unternehmen abwägen, welche Daten sie in der Cloud lagern. Geht ein Unternehmen mit der Datenhaltung in der Cloud sensibel um und beachtet Empfehlungen zu Datenspeicherung, Collaboration und Zugriffsrechten, kann es die Effizienz deutlich steigern. Um B2B-Collaboration noch sicherer zu machen, muss ein Cloud-Anbieter Compliance-Anforderungen umsetzen. Idealerweise bietet er auch eine Versionierung von Dokumenten an, um Änderungen nachvollziehbar machen zu können. Dynamische Wasserzeichen sind ebenfalls ein nützliches Tool, wenn es darum geht, Daten zu schützen. Druckt oder legt ein autorisierter Nutzer eine Kopie Ihrer Inhalte auf der lokalen Festplatte ab, sind diese noch immer durch ein Wasserzeichen gekennzeichnet.

4.4.8 Fazit

Die Umsetzung dieser sieben Punkte ist ein sehr guter Ansatz für sicheres Cloud Computing. Dennoch sind Anbieter auf rechtliche Rahmenbedingungen angewiesen. Die Europäische Union arbeitet im Rahmen ihrer Cloud-Strategie mit Hochdruck daran, den Wirtschaftsstandort Europa für Cloud Computing noch attraktiver und sicherer zu machen.

Harald Pfoser



Harald Pfoser arbeitet seit über 15 Jahren bei Fabasoft und ist zertifizierter Scrum Product Owner sowie zertifizierter Senior Project Manager nach IPMAI. Er implementiert seit mehr als drei Jahren agile Projekte mittels der Scrum Projektmanagementmethode. Aktuell ist er Product Owner für die Fabasoft Cloud.

Lesen Sie passend zum Thema auch unsere folgenden Artikel:

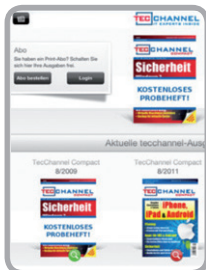
- **Cloud- und Social-Media-Daten richtig verschlüsseln**
(www.tecchannel.de/2049929)
- **In sechs Schritten zu mehr Cloud-Security**
(www.tecchannel.de/2045411)
- **Ratgeber: mehr Sicherheit für Unternehmensdaten in der Cloud**
(www.tecchannel.de/2061446)
- **Cloud Computing in der Praxis**
(www.tecchannel.de/2051057)
- **Cloud und Hadoop – Sicherheit ist nie absolut**
(www.tecchannel.de/2061555)
- **Hybrid Clouds im Unternehmen richtig managen**
(www.tecchannel.de/2056060)



Mobile Webseite

Für Smartphones bieten wir eine in Design und Funktion angepasste Webseite, die automatisch gestartet wird, wenn Sie mit Ihrem mobilen Gerät auf www.TecChannel.de surfen. Für das iPhone und für Android gibt es außerdem eigene Apps unter

www.tecchannel.de/iphone
www.tecchannel.de/android



iPad Kiosk-App

Machen Sie sich für ein neues Lesegefühl bereit: Ab sofort können Sie TecChannel-Compact auf Ihr Apple iPad laden, lesen und archivieren. Zum Start gibt es eine Ausgabe mit über 160 Seiten gratis zum Download. Die kostenlose TecChannel Kiosk-App informiert Sie außerdem direkt täglich mit den aktuellen Online-Beiträgen von TecChannel.de. Infos und Download unter

www.tecchannel.de/ipad



TecChannel-Newsletter

Das einspaltige Layout der neuen TecChannel-Newsletter haben wir so ausgelegt, dass die Informationen nicht nur auf dem PC oder Notebook perfekt dargestellt werden. Sie können die Newsletter nun auch direkt auf mobilen Geräten wie Smartphones und Tablet-PCs bequem lesen.

www.tecchannel.de/newsletter

Impressum

Verlag:

IDG Business Media GmbH
 Lyonel-Feinstein-Straße 26
 80807 München

Telefon: +49-89-360-86-0
 Telefax: +49-89-36086-118

E-Mail: info@idgbusiness.de

Vertretungsberechtigter:

York von Heimburg, Geschäftsführer

Registergericht:

Amtsgericht München, HRB 99187

Verantwortlicher für den

redaktionellen Teil:
 Wolfgang Herrmann, Chefredakteur
 (Anschrift siehe Verlag)

Verantwortlicher für den

Anzeigenteil:
 Sebastian Wörle,
 Gesamtanzeigenleiter
 (Anschrift siehe Verlag)

089/36086-113,
sworle@idgbusiness.de

**Umsatzsteuer-
 identifikationsnummer:**
 DE 811 257 800

ISSN: 2195-4747

Abonnement, Einzel- und Nachbestellung, Umtausch defekter Datenträger:

TecChannel Kundenservice, Postfach 81 05 80, 70522 Stuttgart, Tel: (+49) 07 11/72 52-276, Fax: -377, für Österreich 1/21 95 560, für Schweiz, 0 71/3 14 06-15, E-Mail: shop@TecChannel.de

TecChannel ist Mitglied der IDG Business Media GmbH und somit ein Teil der IDG-Verlagsgruppe. Darin erscheinen unter anderem auch folgende Zeitschriften:





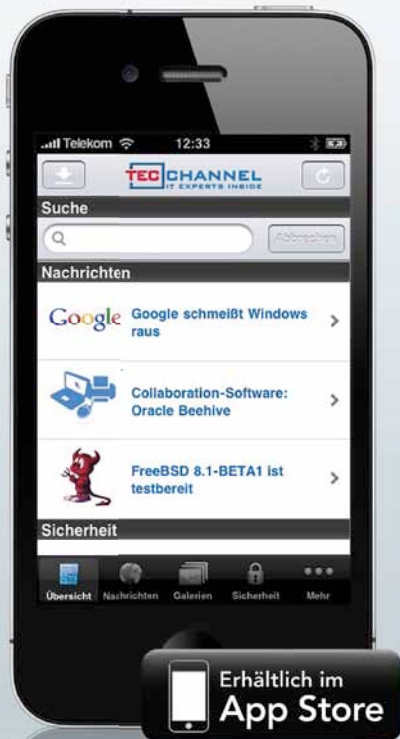
Die neue TecChannel App

Alles drin. Immer dabei. Jetzt fürs iPhone.

News, Infos,
Tipps & Tricks
für unterwegs!

- ▶ topaktuelle News
- ▶ Hintergründe
- ▶ Analysen
- ▶ Tests und Bilderstreifen

» **Gratis laden**



Voraussetzungen: Kompatibel
mit iPhone, iPod touch und iPad.
Erfordert iOS 3.0 oder neuer.

www.tecchannel.de/iphoneapp



Einfach QR-Code mit dem Codereader Ihres iPhones einscannen. Sie werden direkt in den App-Store verlinkt und können die App downloaden. Einen kostenlosen Reader erhalten Sie z.B. unter <http://get.beetagg.com/>. Es entstehen lediglich Kosten für die Verbindung ins (mobile) Internet.