



IT-Grundschutz

Informationsdienst

Praxis und Anwendungen

Grundschutz im Kranken- haus

Seite 7



Quelle: iStockphoto.com/fs2k5

NEWS

**19. EICAR-Konferenz
in Paris legt Fokus auf
ICT Security** Seite 2

**Certgate tritt dem
IT-Verband BITKOM bei** Seite 2

**Gefahr für mobile
Anwendungen nimmt zu** Seite 2

Workshops

**Windows 7 und die Sicherheit
Compliance im eHealth verbessern** Seite 3
Seite 9

Praxis und Anwendungen

**Kolumne: Die größte Schwachstelle im System
Klinikum Braunschweig sichert IT-Infrastruktur** Seite 6
Seite 7

Studien und Analysen

**Wirtschaftskriminalität nimmt zu
Interview: Freud und Leid mit dem GSTOOL** Seite 12
Seite 14

Rubriken

Editorial Seite 2

Veranstaltungen Seite 16

Impressum Seite 6



Liebe Leserin, lieber Leser,

der IT-Grundschutz nach den Vorgaben des BSI ist ein sehr universelles Werkzeug. Er schützt nicht nur alle Bereiche der IT vor Angriffen sondern findet seinen Platz auch in den verschiedensten Branchen. In der aktuellen Ausgabe beweist der IT-Grundschutz seine Praxistauglichkeit unter den harten Anforderungen des deutschen Gesundheitswesens. Das Klinikum Braunschweig hat den kompletten Zertifizierungsprozess durchlaufen und steht gerade vor der ersten Rezertifizierung. Auch wenn die IT-Abteilung mit manchen Aspekten des umfangreichen Prozesses haderte, blieb unter dem Strich ein klares Fazit: Der Sicherheitsfaktor nach der Zertifizierung durch das BSI ist deutlich höher als bei anderen Methoden. Ob man in seinem eigenen Unternehmen den Grundschutz nach BSI mit allen Konsequenzen umsetzen will, ist immer eine Einzelfallentscheidung. Autorin Judith Balfanz hält auch die Zertifizierung nach ISO 27001 für eine gute Lösung, wie sie in einem anderen Artikel, ebenfalls mit Schwerpunkt Gesundheitswesen, beschreibt. Aber ich bin davon überzeugt, dass die Beschäftigung mit IT-Grundschutz und den umfangreichen IT-Grundschutzkatalogen in jedem Fall positive Auswirkungen für die IT-Sicherheit in Ihrer Firma hat.

Herzlichst Ihr Elmar Török

19. EICAR-Konferenz in Paris legt Fokus auf ICT Security

Am 10. und 11. Mai 2010 veranstaltet der EICAR e.V. seine jährliche Konferenz am Institut für Informatik in Paris. Hauptthema wird die Zukunft der ICT Security sein. In diesem Zusammenhang veröffentlichte der EICAR auch sein jüngstes Positionspapier zum Thema Antivirus-Tests, welches die Testverfahren modernisieren soll. Traditionell beschäftigt sich die EICAR-Konferenz mit allen Aspekten von Schadcodes sowie der Entwicklung entsprechender Gegenmaßnahmen. „Als Botschafter der Anwender legen wir Wert auf eine neutrale und objektive Herangehensweise an das Thema AV-Testing. Deshalb ist für die EICAR nur eine wissenschaftlich fundierte Lösung sinnvoll“, so Rainer Fahs, Chairman der EICAR und Security Experte bei der NATO. Die diesjährige Konferenz wird tiefer ins Detail gehen und sich auch mit der Nutzerfreundlichkeit und den Herausforderungen beim unabhängigen Testen von Antivirus- und Antimalware-Produkten beschäftigen. Zudem sollen Reflexionen zu besorgniserregenden Trends und zur Weiterentwicklung im Bereich ICT-Security angeregt werden, besonders im Bereich der Anti-Malware-Welt.

certgate tritt dem IT-Verband BITKOM bei

Der Nürnberger IT-Security-Spezialist certgate ist dem Branchenverband BITKOM beigetreten. Die größte deutsche IT-Organisation bildet sich zunehmend auch als die deutsche Plattform für IT-Sicherheitsthemen heraus. Als Anbieter auf dem Gebiet der Sicherheitslösungen für mobile Kommunikation erwartet certgate Synergieeffekte und Netzwerkvorteile sowie Informationen aus erster Hand. „BITKOM ist das größte Wissens-

Netzwerk der ITK-Branche in Deutschland und hat sich in den letzten Jahren zunehmend auch als Vertreter der IT-Sicherheitsindustrie etabliert“, erklärt Dr. Paschalis Papagrigoriou, Geschäftsführer von certgate. Certgate werde sein Know-how in Foren und Arbeitskreisen für Telekommunikation und IT-Sicherheit einbringen und an Veranstaltungen, Jahrestagungen und Messen sowie IT-Gipfeltreffen teilnehmen.

Gefahr für mobile Anwendungen nimmt zu

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat den aktuellen Lagebericht zur IT-Sicherheit für das vierte Quartal 2009 veröffentlicht. „Cyberkriminelle nutzen neben Botnetzen, Spamversand und Phishing-E-Mails zunehmend Infiltration über Mobiltelefone und WLAN“, stellt Stefan Ritter, Leiter des Nationalen IT-Lagezentrums im BSI, fest. Generell bewertet das BSI die Gesamtlage der IT-Sicherheit in Deutschland im vierten Quartal mit erhöhtem Risiko. Die Risiken mobiler Internetnutzung beweist der Fall einer im November 2009 verbreiteten modifizierten Version des ersten iPhone-Wurms „Ikee“: Die mit der neueren „Ikex“- oder „Duh“-Version infizierten iPhones verbinden sich mit einem Command-&Control-Server, um von ihm Befehle zu erhalten, zum Beispiel für einen Pharming-Angriff auf die Webseite der niederländischen ING-Bank. Im vierten Quartal 2009 wurden außerdem verstärkt sicherheitsrelevante Ereignisse beobachtet, bei denen die Infrastruktur des Internet den Angreifern sowohl als Ziel wie auch als Verteilungsmedium diene. Die Attacken zeigen, dass auch das weltumspannende Kommunikationsnetz anfällig für Störungen ist – seien sie durch technische Probleme oder durch gezielte Sabotage-Akte verursacht.

Alles richtig im zweiten Anlauf?

Windows 7 und die Sicherheit

Matthias Fraunhofer, Consultant, Secaron AG

Nach der generell schlechten Akzeptanz von Windows Vista verspricht Microsoft Besserung durch Windows 7. Windows 7 stellt keine revolutionäre Neuerfindung, sondern eine evolutionäre Weiterentwicklung des Vorgängers dar, in der die Wünsche der Benutzer berücksichtigt wurden.

Die Kritik am Vorgänger von Windows 7 war oft berechtigt, vom Standpunkt der Client-Sicherheit konnte man Vista jedoch keinen Vorwurf machen. Den Erfolg der Strategie bezeugen auch die Statistiken, die Windows Vista ca. 60% weniger Malware-Befall bescheinigen als Windows XP, was nicht nur an der geringeren Verbreitung von Vista liegt. Die Symbiose aus Benutzbarkeit und Leistung soll nun den Erfolg des neuen Hoffnungsträgers Windows 7 aus dem Hause Microsoft sicherstellen. Eine

große Rolle werden dabei die Sicherheitsfunktionen spielen.

Das Hosentaschen-DLP

Ein Versehen oder auch gezielte Wirtschaftsspionage – der Effekt bleibt gleich. Der Verlust sensibler Unternehmensdaten kann zu hohen Imageschäden und wirtschaftlichen Einbußen führen. Schnell verloren und leicht entwendet sind vor allem mobile Datenträger. In Form von externen Festplatten und USB-Sticks

sind sie in jedem Unternehmen im Einsatz. Steigende Kapazitäten bei immer geringerer Größe und über Jahre eingeschliffene Arbeitsabläufe machen sie zu einem unkalkulierbaren Sicherheitsrisiko. Als Schutz bei Verlust oder Diebstahl hilft nur starke Verschlüsselung der gespeicherten Daten.

Zur Verschlüsselung von Partitionen konnte BitLocker bereits seit Vista eingesetzt werden. Allerdings bekamen die ausgereifteren Festplatten-Verschlüsselungslösungen

Weniger Sicherheitslücken mit Windows 7

Wertung	Rubrik	Ergebnis
!	Office-Sicherheitsupdates	1 Service Packs oder Updaterollups fehlen. Gegenstand der Überprüfung Ergebnisdetails Vorgehensweise zur Behebung
!	Windows-Sicherheitsupdates	1 Service Packs oder Updaterollups fehlen. Gegenstand der Überprüfung Ergebnisdetails Vorgehensweise zur Behebung
✓	SDK Components-Sicherheitsupdates	Es fehlt kein Sicherheitsupdate. Gegenstand der Überprüfung Ergebnisdetails
✓	SQL Server-Sicherheitsupdates	Es fehlt kein Sicherheitsupdate. Gegenstand der Überprüfung Ergebnisdetails
✓	Silverlight-Sicherheitsupdates	Es fehlt kein Sicherheitsupdate. Gegenstand der Überprüfung Ergebnisdetails
✓	Visual Studio-Sicherheitsupdates	Es fehlt kein Sicherheitsupdate. Gegenstand der Überprüfung Ergebnisdetails

Überprüfungsergebnisse für Windows

Verwaltungsfähigkeiten

Wertung	Rubrik	Ergebnis
!	Administratoren	Es wurden mehr als 2 Administratoren auf diesem Computer gefunden. Gegenstand der Überprüfung Ergebnisdetails Vorgehensweise zur Behebung
!	Kennwortablauf	Einige Benutzerkonten (2 von 4) haben nicht ablaufende Kennwörter. Gegenstand der Überprüfung Ergebnisdetails Vorgehensweise zur Behebung
!	Automatische	Automatische Updates werden auf diesem Computer über eine Gruppenrichtlinie verwaltet.

Diesen Bericht drucken In Zwischenablage kopieren Vorheriger Sicherheitsbericht Nächster Sicherheitsbericht OK

anderer Hersteller deutlich mehr Akzeptanz. Neu hinzugekommen ist mit Windows 7 Enterprise die mobile Variante BitLocker To Go, die zur Verschlüsselung von USB-Datenträgern eingesetzt werden kann. Um darauf gespeicherte Daten vor dem Zugriff Unberechtigter zu schützen, kann über zentrale Einstellungen eine Verschlüsselung der Geräte mittels Smartcard oder Passwort erzwungen werden. Ein BitLocker To Go Reader hilft bei der Nutzung des verschlüsselten USB-Datenträgers auf Clients ohne Windows 7. Der Zugriff erfolgt dann nur im Lesemodus.

Mit BitLocker To Go könnte das Unternehmen das folgende Szenario abbilden: Es werden grundsätzlich USB-Datenträger erlaubt, die jedoch vor der ersten Benutzung verschlüsselt werden müssen. Dabei spielt es keine Rolle, woher das Gerät stammt, da dies aus Sicherheitssicht irrelevant ist. Stimmt der Benutzer einer Verschlüsselung nicht zu, ist das Gerät nicht verwendbar. Sollte der Benutzer das Passwort vergessen, kann das Recovery von Daten über zentral im Active Directory abgelegte Schlüssel durchgeführt werden.

BitLocker To Go ist eine sinnvolle Ergänzung, bietet einen guten Funktionsumfang und ist in Windows 7 Enterprise bereits integriert. Zentral verwaltbar könnte es für viele Firmen ein interessantes Feature sein, das sich gut über das Active Directory steuern lässt.

Immer verbunden

Auch DirectAccess ist auf den mobilen Arbeitsplatz ausgerichtet. Während der Zugriff auf Firmenressourcen bisher über einen VPN-Tunnel lief, sorgt DirectAccess mittels Technologien wie IPv6 und IPSec für eine automatische Verbindung zum Unternehmensnetz. Dazu sind keine expliziten Benutzeraktionen nötig, DirectAccess funktioniert auch über beliebige Netzwerkver-



Matthias Fraunhofer ist Consultant bei der Secaron AG

bindungen. Der Client ist immer im Firmennetz eingeloggt und kann somit auch immer verwaltet oder mit Richtlinien versorgt werden. Wenn der Client die Einhaltung der vorgegebenen Richtlinien nicht nachweisen kann, wird ihm der Zugriff verwehrt – Network Access Protection macht es möglich.

Die Daten fließen bei DirectAccess getrennt ans Ziel. Internet und Intranet-Traffic wird nicht wahllos über einen Tunnel geleitet. Mit einer 2-Faktor-Authentisierung kombiniert, erhält man einen realen Zugewinn an Administrierbarkeit und eine durchgehend benutzerfreundliche Lösung. Allerdings ist der zusätzliche Aufwand für den Aufbau der Infrastruktur zu berücksichtigen, da klassische VPN-Verfahren in der Regel bereits umgesetzt und etabliert sind. Die bei DirectAccess angesprochene Zwei-Faktor-Authentisierung kann klassisch über Smartcard und PIN realisiert werden. Generell möglich wäre auch die Variante mit biometrischen Merkmalen wie dem Fingerabdruck zusammen mit einer PIN oder einem Passwort. In vielen der momentan erhältlichen Business Notebooks gehört ein Fingerabdruckleser bereits zur Standardausstattung.

Natürlich war die Verwendung von 2-Faktor-Authentisierung auch

in Windows XP bereits möglich, jedoch durch technische Eigenheiten kaum zuverlässig zu betreiben. Durch die Einführung des Credential Provider-Systems und des Windows Biometric Frameworks ist die Nutzung von Fingerabdrücken für die Authentifizierung erheblich einfacher geworden.

Dies ist insbesondere in Kombination mit User Account Control interessant, die im Vergleich zu Vista überarbeitet wurde. Obwohl Benutzer nach wie vor keine Administratorrechte haben sollten, ist dies in Ausnahmefällen unvermeidbar. Hier kann es aus Sicherheitssicht sinnvoll sein, als eingeschränkter Benutzer zu arbeiten und jegliche UAC-Prompts für notwendige administrative Rechte durch einen Fingerabdruck bestätigen zu lassen. Natürlich erfordert das auch die Zustimmung und Mitarbeit der Benutzer.

Die totale Kontrolle

Ein großes Problem für die Client-Sicherheit ist der Wildwuchs an Anwendungssoftware, die auf den Clients eingesetzt wird. Applikationen müssen aktuell gehalten werden, da sie den Großteil der Sicherheitslücken enthalten. Zusätzlich ist es oft sinnvoll, nur eine fest definierte Menge an Applikationen benutzbar zu machen, sei es aus Lizenz- oder aus Compliance-Gründen.

In Windows XP und Vista konnte man mit den relativ unflexiblen und unkomfortablen Software Restriction Policies regeln, welche Benutzer welche Software ausführen durften. Der Nachfolger dieser Technologie bei Windows 7 ist AppLocker. Mit AppLocker ist es möglich, den Effekt von Regeln vorher zu auditieren. Dies ist insbesondere dann nützlich, wenn man die Menge an Software im Feld nicht vollständig überblicken kann. AppLocker erlaubt es, flexible Regeln zu

gestalten, um beispielsweise allen Benutzern die Ausführung von signierter Software von Microsoft und des Adobe Readers ab einer bestimmten Version zu erlauben.

Wie man am Beispiel AppLocker sehen kann, ermöglicht oft erst ein gezieltes Auditing den Einsatz eines Sicherheitsfeatures. Um eine umfassende Client-Sicherheitsstrategie zu vervollständigen, müssen sicherheitskritische Vorfälle erkannt werden. Das Erkennen stellt die Basis für eine angemessene Reaktion auf einen Vorfall dar und ist die Grundlage für eine Bewertung.

Clientseitig wird auf Windows-Systemen über sogenannte Audit-Richtlinien definiert, welche Ereignisse von Interesse sind. Hier gab es auch schon in der Vergangenheit die Wahl zwischen verschiedenen Kategorien, die jedoch oft eine Unmenge an Hintergrundrauschen produzierten. Um dies zu verbessern, wurde

in Vista das feingranulare Auditing eingeführt. Es erlaubt das gezieltere Auditing, war aber nicht über die Gruppenrichtlinien verwaltbar sondern musste per Kommandozeile und Startup-Skripte eingerichtet werden. Microsoft hat das Konzept nun in Windows 7 weiterentwickelt. Jegliche Konfigurationen sind nun über die Gruppenrichtlinien durchführbar. Zusätzlich kann man das Auditing für den Zugriff kompletter Gruppen auf das Dateisystem aktivieren. Dies ist insbesondere dann hilfreich, wenn man die Zugriffe von zentralen Instanzen und sicherheitskritische Operationen wie Berechtigungsänderungen zu jeder Zeit nachvollziehen will.

Um die Erbsünden von Lan Manager und NTLM aus den Unternehmen zu bekommen, können auch diese Protokolle erstmals auditiert werden. Damit finden endlich nur noch die sicheren Protokolle NTLMv2 und Kerberos als allei-

nige Authentisierungsprotokolle Anwendung. Das Auditing in Windows 7 und dem zugehörigen Server ist eine große Fortentwicklung und eines der wirksamsten Mittel um ein umfassendes Sicherheitskonzept zu verfolgen.

Aufforderung zum Wechsel

Features sind nicht alles. Doch Windows 7 bringt eine konsequente Weiterentwicklung der guten Seiten des Vorgängers Vista. Nicht zuletzt ist Windows 7 durch eine sparsamere Auswahl von Softwaremodulen und Services schlanker und sicherer geworden. Schon aus diesen Gründen sollten Unternehmen den Wechsel anstreben. Und falls Vista übersprungen wurde, auch damit Benutzer und IT-Abteilung den Anschluss nicht versäumen.

EUROPEAN

IDENTITY CONFERENCE 2010

Thought Leadership & Best Practices in Identity Management and GRC

KUPPINGER COLE
www.kuppingercole.com

CLOUD 2010

thought leadership
+ best practices
in cloud computing

04 – 07 May 2010
MUNICH | GERMANY

MITTELSTANDSDIALOG
INFORMATIONSSICHERHEIT 2010

European Identity Conference (EIC) is the place to meet with enterprise technologists, thought leaders and experts to learn about, discuss and shape the market in most significant technology topics such as Identity Management, Governance, Risk Management and Compliance (GRC) and Cloud Computing. With its world class speakers, an unique mix of best practices presentations, panel discussions, thought leadership statements and analyst views, **EIC** has become an absolute must-attend event for enterprise IT leaders all over Europe. **CLOUD 2010** and **Mittelstandsdialog Informationssicherheit (MIS) 2010** are co-located with **EIC 2010**.

HOT TOPICS EIC 2010

- Market Maturity: Expansion & Replacement Best Practices
- Lean IT: Creating more value for less through IdM, GRC and Cloud Computing
- Compliance, Mitigating Risk: Strategy, Controls, Processes
- Authentication & Authorization
- Integrating Identity, Roles & Data Loss Prevention
- Regulation, Privacy, Information Security
- Cloud Computing & Trust: Extending Identity based information Security into the Cloud

Further Information and Registration:
www.id-conf.com

KUPPINGER COLE
arnheimer str. 46 | 40489 düsseldorf | germany
tel +49 (0)211 23 70 77-0

Further Information about KUPPINGER COLE:
www.kuppingercole.com

Lead Sponsor:



Platinum Sponsor:

betasystems



Microsoft

SIEMENS



Novell

CITRIX

VÖLCKER INFORMATIK AG



ORACLE



Kolumne: Aus dem Alltag eines IT-Sicherheitsbeauftragten

Der Mensch, die größte Schwachstelle im System

Sebastian Horzela, Geschäftsführer, CIPHON GmbH

Schon in seinem mittlerweile legendären Buch „Die Kunst der Täuschung“ hat Kevin Mitnick auf den Risikofaktor Mensch verwiesen, den aus seiner Sicht größten Risikofaktor im System der IT-Sicherheit.

Egal, ob es sich um einen großen Konzern oder ein mittelständisches Unternehmen handelt, technologisch fundierter Schutz ist ebenso wichtig wie die Einstellung jedes einzelnen Mitarbeiters. Denn die Mitarbeiter schaffen erst die Verbindung zwischen scheinbar belanglosen, „unschädlichen“ Handlungen und den Zugriffs- und Missbrauchsmöglichkeiten auf sensible Daten.

Zahlreiche, aktuelle Statistiken belegen: immer noch werden etwa die Hälfte aller sicherheitsrelevanten Vorfälle durch die eigenen Mitarbeiter verursacht. Und das vergleichsweise selten aus betrügerischer Absicht oder um einem Unternehmen willentlich zu schaden. Man beantwortet vielmehr höflich eine Frage, man schätzt den einen oder anderen Geschäftsvorgang als nicht sicherheitsrelevant ein, man ist einfach mal unachtsam, bevor man seinen Arbeitsplatz verlässt, hat einen fatalen Hang zu einer bestimmten Passwortstruktur oder ist in seinem „Sicherheitsverhalten“ schlicht nicht entsprechend geschult.

Um diese Sicherheitslücke zu schließen, haben sich im Lauf meiner praktischen Arbeit im Wesentlichen vier Bereiche herauskristallisiert. Als erstes versuchen wir den Mitarbeitern zu erklären, wie die technologischen Sicherheitsanforderungen

mit den menschlichen Schnittstellen verzahnt sind. Hieraus leitet sich der nächste Komplex ab: wo genau sind diese Schnittstellen lokalisiert und wie greifen sie ineinander? Wie verlaufen Organisations- und Meldesysteme üblicherweise in einem Unternehmen? Wissen alle Beteiligten, warum auch nebensächlich erscheinende Informationen hilfreich für einen Angriff auf sensible Datenbestände sein können?

Vollständige Sicherheit ist nur eine Illusion, wir bemühen uns eher kontinuierlich Risiken zu managen. Das gilt für alle Beteiligten im Unternehmen, von der Führungsriege bis zu jedem einzelnen Mitarbeiter. Daher kommen, drittens, Tools zur schnellen Selbsthilfe für die Administratoren zum Einsatz. IT-Sicherheit darf nicht zusätzlich belasten. Sie soll im Hintergrund für Ruhe in den Abläufen und einen insgesamt wesentlich stabileren Betrieb sorgen.

Aber alle Sicherheitsmaßnahmen reichen nicht aus, wenn das, was wir seit einigen Jahren als „Social Engineering“ bezeichnen, greift. Trotz, und teilweise sogar wegen aller technischen Sicherheitsmaßnahmen. Wir müssen mit Schulungen für Awareness gegenüber den Gefahren sorgen. Und das geht nur durch ständigen Dialog, ständiges Anpassen und ständiges Wiederholen.

Impressum

Informationsdienst IT-Grundschutz

5. Jahrgang – ISSN 1862-4375

Herausgeber

Nina Malchus

Redaktion

Elmar Török, Fachjournalist
(verantwort. für den redaktionellen Teil)
bits + bites, Auf dem Rain 2, 86150 Augsburg
Tel.: +49 821 4981635
E-Mail: redaktion@grundschutz.info

Verlag

SecuMedia Verlags-GmbH
Lise-Meitner-Str. 4, 55435 Gau-Algesheim
www.secu-media.de

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

Registereintragung: Handelsregister Mainz B 22282
Umsatzsteuer-Identifikationsnummer: DE 148266233

Abo-Service

Veronika Leuschner
Tel.: +49 6725 9304-25
Fax: +49 6725 5994
E-Mail: aboservice@secu-media.de
www.grundschutz.info

Anzeigenleitung

Birgit Eckert
(verantwort. für den Anzeigenteil)
Tel.: +49 6725 9304-20
E-Mail: anzeigenleitung@secu-media.de
Mediadaten unter: www.grundschutz.info

Bezugspreise/Bestellungen/Kündigung

Erscheinungsweise 10 Mal jährlich
(2 Doppelausgaben)

Jahresabopreis für die Printausgabe:
98,00 € inkl. MwSt. u. Vers.k. (Inland) /
116,10 € inkl. MwSt. u. Vers.k. (Ausland) /
187,00 SFR inkl. MwSt. u. Vers.k. (Schweiz).
Einzelheft: 9,50 € inkl. MwSt. u. Vers.k. (Inland) /
11,00 € inkl. MwSt. u. Vers.k. (Ausland) /
18,00 SFR inkl. MwSt. u. Vers.k. (Schweiz).

Eine Kündigung ist jederzeit zur nächsten noch nicht gelieferten Ausgabe möglich. Überzahlte Beträge werden rückerstattet.

Preis im Koppelabonnement mit den Zeitschriften <kes> oder WIK:
Jahresabopreis: 76,00 € inkl. (Inland) / 84,53 € (Ausland) inkl. MwSt. und Versandkosten 130,00 SFR. (Schweiz)

Vertriebskennzeichen: ZKZ 78871

Satz/Druckvorstufe

BLACKART Werbestudio Schnaas und Schweitzer,
Stromberger Str. 47, 55413 Weiler

Druck

Silber Druck oHG,
Am Waldstrauch 1, 34266 Niestetal

Urheber- und Verlagsrechte: Alle in diesem Informationsdienst veröffentlichten Beiträge sind urheberrechtlich geschützt. Jegliche Verwendung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und Einspeicherung in elektronische Systeme. Haftung/Gewährleistung Die in diesem Informationsdienst veröffentlichten Beiträge wurden nach bestem Wissen und Gewissen zusammengestellt. Eine Gewähr für die Richtigkeit und Vollständigkeit kann seitens der Herausgeber nicht übernommen werden. Die Herausgeber haften ebenfalls nicht für etwaige mittelbare und unmittelbare Folgeschäden und Ansprüche Dritter.

Titelbild: © iStockphoto



1.425 Betten und
mehr als 30 Kliniken:
Das Klinikum
Braunschweig

Grundschutz im Krankenhaus

Klinikum Braunschweig sichert IT-Infrastruktur

Elmar Török, bits+bites

Eine Zertifizierung nach IT-Grundschutz bestätigt dem Klinikum Braunschweig höchste Standards beim Betrieb der zentralen Komponenten der elektronischen Patientenakte. Damit ist das Klinikum das erste Krankenhaus Deutschlands, dass die hohe Hürde einer Sicherheitszertifizierung auf Basis des BSI IT-Grundschutz genommen hat. Dies schließt auch umfassende übergeordnete Maßnahmen im Informationssicherheitsmanagement ein.

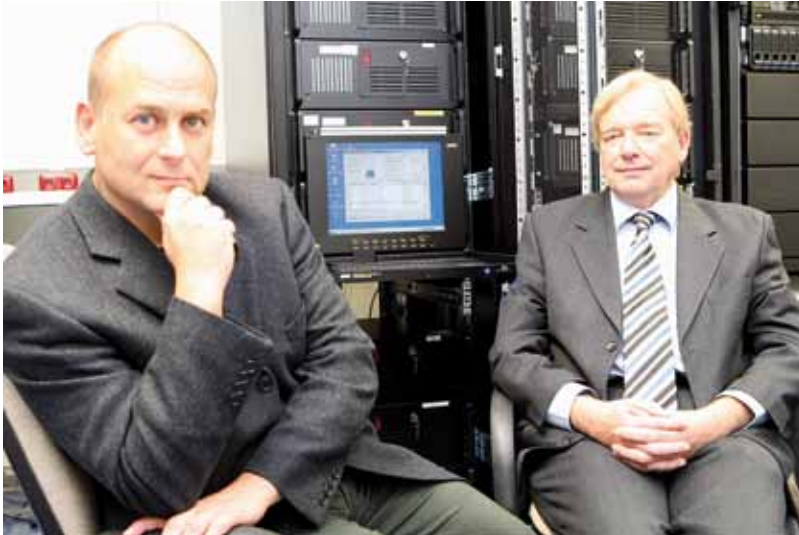
Sicherheit spielt in Kliniken seit jeher eine Hauptrolle, ob im direkten Kontakt mit den Patienten oder in der unterstützenden Infrastruktur. Im Klinikum Braunschweig, das schon früh mit der Einführung von EDV-Systemen begonnen hatte, ist das Thema Informationssicherheit schon seit langem von zentraler Bedeutung. Durch ein externes Security Audit wurde bereits 2002 ein Verbesserungsprozess in diesem Bereich eingeleitet. Mit der Einführung der elektronischen Patientenakte bot sich dem Klinikum Braunschweig die Gelegenheit, das

Informationssicherheitsmanagement deutlich auszubauen. Auch die Lieferanten konnten auf ihre Mitwirkung bei einer Sicherheitszertifizierung verpflichtet werden.

Vorbereitender Workshop durchgeführt

Das Klinikum entschied sich für die Zertifizierung nach ISO27001 auf Basis des IT-Grundschutz nach BSI, da es nicht nur organisatorische sondern auch konkrete technische Maßnahmen betrachtet.

Um die Administratoren in die „Denke“ und das Vorgehensmodell des BSI einzuweisen, veranstaltete die IT-Abteilung im Herbst 2007 einen vorbereitenden Workshop. Unter anderem erstellten die Mitarbeiter die ersten Arbeitspakete, definierten den zu zertifizierenden Systemverbund und begannen mit der Einarbeitung in das Zertifizierungswerkzeug GSTOOL des BSI. Nachdem die ersten Konzepte ausgearbeitet worden waren, beauftragte das Klinikum Braunschweig im März 2008 den eigentlichen Audit. Zur Unterstützung zog Dr. Seidel,



Im Team für IT-Sicherheit: Rüdiger Gruetz und Dr. Christoph Seidel

IT-Leiter und CIO, auch einen externen Coach heran, der Detailkenntnisse des Zertifizierungsvorgangs hatte und den IT-Mitarbeitern bei der Abstimmung der Maßnahmen half.

Zum Glück gab es bei der physikalischen Sicherheit nur wenig Grund zur Nacharbeit. Aufwendige Baumaßnahmen fielen flach, da das Klinikum im Rahmen einer SAP Hardware-Migration bereits 2002 das Rechenzentrum in einem alten Bunker auf dem Campus untergebracht hatte. „Der Bunker stand seit dem Ende des zweiten Weltkriegs ungenutzt, aber die Kosten für den Abriss waren einfach zu hoch,“ so Rüdiger Gruetz, Leiter des Rechenzentrums und stellvertretende IT-Leiter am Klinikum. Nach dem Umzug erfolgt im ehemaligen Serverraum nun die Datensicherung.

Als der Auditor im Juni 2008 seine Arbeit aufnahm, war das Krankenhaus bestens vorbereitet. Für fast alle Systeme war eine Testumgebung vorhanden, ein notwendiges Management-LAN konnte schnell eingeführt werden. Die Datensicherung erfolgte bereits zentralisiert durch geschulte Administratoren. Trotzdem gab und gibt es Nachholbedarf. So ist das System zur

Erstellung der digitalen Signatur noch im Pilotbetrieb, für einen produktiven Einsatz sind noch einige Anforderungen umzusetzen. Die BSI-Vorgaben an die Kernanwendung des Verbundes, das Archivsystem, haben Eingang in die Releaseplanung des Herstellers gefunden. Die offen gebliebenen Punkte zu einigen sicherheitsrelevanten Fragen führten zur Einführung eines Installationsfragebogens. Erst wenn dieser Fragebogen durch den Hersteller des Produkts ausgefüllt und abgezeichnet ist, wird mit der Implementierung begonnen.

Sicherheitsrichtlinien überarbeitet

Ebenfalls eine Folge des Zertifizierungsverfahrens war die Ausschreibung der Stelle für einen externen Sicherheitsbeauftragten. Diese Position gewinnt durch den externen Charakter mehr Gewicht im Unternehmen. Durch die externe Vergabe wird auch die notwendige Neutralität und Kompetenz für diese Aufgabe sicher gestellt. Im Vorfeld der Zertifizierung wurden die Sicherheitsrichtlinien grundlegend überarbeitet oder neu eingeführt. Das Klinikum hatte bis zum Vorliegen eigener Richtlinien den generischen

Richtlinien der Stadt Braunschweig zu folgen. Eigene Vorgaben bedeuten aber eine weitaus bessere und flexiblere Anpassung an die Anforderungen eines Klinikbetriebs. Der Auditor nahm sich im Juni viel Zeit für die Kontrolle der Maßnahmen. Von den 22 Tagen verbrachte der Prüfer etwa die Hälfte vor Ort. Dabei ging er durchaus bis ins Detail und begutachtete die Sicherungsmaßnahmen eines Raumes oder die Rechtevergabe auf Anwendungen und Verzeichnisse. „Der Prüfer war umgänglich aber unnachgiebig“, erzählt Rüdiger Gruetz.

Hier zahlte sich die Vorbereitung durch den externen Coach besonders aus. „Ich kann anderen Unternehmen nur empfehlen, sich auch der Hilfe durch einen externen Ratgeber zu bedienen,“ so Dr. Seidel. „Man muss dessen Ratschläge aber auch ernst nehmen. Der Coach kann auf kritische Punkte hinweisen, aber nicht die Abhilfe forcieren.“

Ein wichtiger Bestandteil des Audits war die Risikübernahme. Für eine ganze Reihe von Punkten musste die Verantwortung durch den Geschäftsführer getragen werden. Die Unterschrift unter dieses Dokument wurde zeitgleich mit dem Abgabetermin des Auditreports v1 am 30. Juni 2008 vorgenommen. Seidel: „Die Risikübernahme ist auch ein Vertrauensbeweis der Geschäftsführung gegenüber der IT-Abteilung. Es war sehr wichtig, dass unser Geschäftsführer wusste, was er mit dieser Unterschrift an Verantwortung übernimmt.“ Die Einbindung der Geschäftsführung war aber ohnehin von Anfang an einer der Kernpunkte des Projekts BSI-Zertifizierung. Während des Projekts mussten andere Aufgaben zurückgestellt oder mit geringerem Einsatz abgewickelt werden, das wäre ohne die volle Unterstützung des Managements nicht möglich gewesen. Das Team um den IT-Leiter berichtete auch kontinuierlich an die Betriebsleitung.

Abstimmung mit dem BSI

Nach der Abgabe des Auditreports wartete das Klinikum Braunschweig gespannt auf die Kommentare des BSI. Dort dauerte die Bearbeitung wegen Ressourcenengpässen bis Mitte Oktober. Dafür waren die Kommentare durchaus positiv. Einige Rückfragen gab es zu Begrifflichkeiten. Das BSI definiert Begriffe wie „Archivierung“ anders, als sie im Klinikum eingesetzt werden, daher musste das was gesagt und was gemeint wurde, aufeinander abgestimmt werden. Andere Kommentare bezogen sich auf reine Formalienfehler wie eine missglückte Copy&Paste Aktion in den Beschreibungstexten. Die wenigen Rückfragen mit echtem Diskussionspotenzial waren gering und konnten schnell geklärt werden.

Offiziell wurde die Auditierung am 21. November 2008 abgeschlossen, kurz darauf, am 4. Dezember erfolgte die offizielle Zertifikatsübergabe.

Doch der Lohn des Projekts bestand weniger in der Urkunde als vielmehr in handfesten Vorteilen, wie Dr. Seidel aufzählt: „Generell hat die Zertifizierung und deren Vorbereitung die Gesamtsicherheit enorm erhöht. Wir haben die Sicherheitsrichtlinien formuliert, uns intensiv mit den Prozessen auseinandergesetzt und das Sicherheitsbewusstsein im Management erhöht. Dazu kommen Detailverbesserungen wie der verpflichtende Installationsfragebogen und ein neues MAC-Monitoring. Darüber hinaus sind die bestehenden Richtlinien und Konzepte weiterverwendbar, zum Beispiel für eine Wirtschaftsprüfung.“

„Wir haben allerdings inzwischen die Erfahrung gemacht, dass viele Softwareanbieter die IT-Sicherheit eher nebenbei behandeln, mehr als Add-On denn als integralen Bestandteil,“ hebt Rüdiger Gruetz hervor. Wie es mit der Erfolgsgeschichte der Zertifizierung nach IT-Grundschutz weitergeht steht trotzdem noch nicht endgültig fest. Dem Nutzen steht der hohe Aufwand für die Wiederholungsprüfung gegenüber, um weiterhin das Siegel des BSI tragen zu dürfen. Trotzdem empfiehlt Rüdiger Gruetz die Maßnahme auch anderen Organisationen: „Der Sicherheitsfaktor nach der Zertifizierung durch das BSI ist deutlich höher als bei anderen Methoden.“

Workshops

Compliance im eHealth verbessern

Basis für die erfolgreiche ISO 27001 Zertifizierung

Judith Balfanz, Vice President Marketing, AuthentiDate International AG

Die zunehmende Digitalisierung geschäftlicher Abläufe führt zu zunehmend komplexen Prozessen. Dies ist, nicht zuletzt durch die elektronische Gesundheitskarte, auch im Gesundheitswesen zu beobachten. Um Compliance-Vorschriften zu genügen ist die Zertifizierung nach ISO 27001 eine gute Lösung.

Ein Dienstleister oder Hersteller im Gesundheitswesen muss sein Unternehmen nicht nur genauso sicher und regelkonform führen wie in einer anderen Branche sondern sogar noch genauer auf die internen und externen Prozesse achten. Viele der Prozesse sind höchst unternehmenskritisch, verlaufen diese unplanmäßig oder fallen gar aus, entsteht ein nur schwer oder gar nicht regulierbarer Schaden für die Organisation.

Gleichzeitig steigt aber die Menge der sensiblen, personenbezogenen Daten, die verarbeitet, weitergeleitet und langfristig vorgehalten werden müssen. Für Führungskräfte in Krankenhäusern, Rehabilitationszentren, bei Krankenkassen, Krankenversicherungen, Einkaufsgemeinschaften und auch der Zulieferindustrie wird daher sowohl die Prozess-, als auch Datensicherheit immer schwerer kontrollierbar.

Die Verantwortlichen müssen sicherstellen, dass die Informationssicherheit zu jedem Zeitpunkt gewährleistet ist, um eigene Haftungsrisiken zu minimieren. Hierbei gilt es für die Verantwortlichen nicht nur unbeabsichtigte Fehler zu vermeiden, sondern auch absichtlichen Manipulationen von Prozessen und Daten vorzubeugen. Schäden durch nicht funktionierende Informationstechnologie gehören hierzu genauso, wie die ungewollte Veröf-

fentlichung von sensiblen Patientendaten. In beiden Fällen entsteht der Organisation ein Schaden. In einem Fall dadurch, dass eine Leistung nicht erbracht werden kann, im anderen Fall durch Schadensersatzklagen oder Imageschaden.

Um ein höchstmögliches Maß an Informationssicherheit in allen Facetten sicherzustellen, hat sich in der Praxis der Einsatz von Informations-Sicherheits-Management-Systemen (ISMS) bewährt. Die Vorgehensweise für die Einrichtung eines ISMS ist mittlerweile in internationalen Standards festgeschrieben. Die Konformität mit diesen Standards ist zertifizierbar, so dass hierüber ein Nachweis gegenüber Dritten erbracht werden kann. Ein sehr weit verbreiteter Standard ist ISO/IEC 27001:2005; kurz ISO 27001.

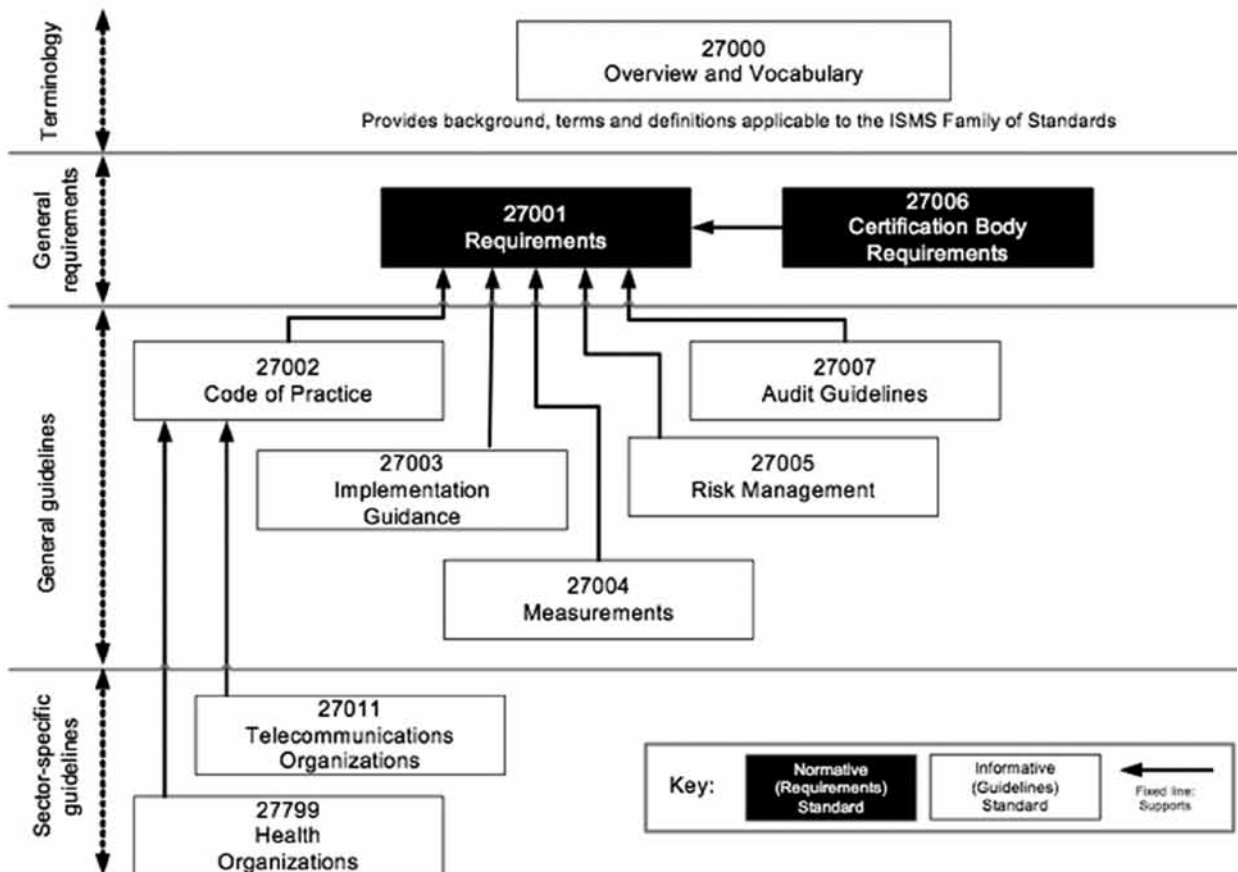
Die Einrichtung eines Information-Security-Management-Systems

(ISMS) bietet Verantwortlichen in Unternehmen und Organisationen gleich mehrere Vorteile:

1. Erkennen von bislang verborgenen Sicherheitslücken im Prozess: Bereits während der Einrichtung des ISMS werden Unternehmensprozesse umfassend erfasst und dokumentiert. Somit können Fehler im Prozess wie ein fehlendes 4-Augen-Prinzip bei einer kritischen Applikation direkt erkannt und behoben werden.
2. Dauerhafte Transparenz für Prozesse: Durch die Prozessdokumentation werden alle Prozesse transparent. Notwendige Prozessänderungen lassen sich schnell umsetzen.
3. Kennzahlen zur schnellen Kontrolle: Bei der Einrichtung eines ISMS werden Kennzahlen zur Prozesskontrolle eingeführt. Die

Verantwortlichen müssen nur ein Minimum an Arbeit aufwenden, um die Ordnungsmäßigkeit der Prozesse zu überwachen. Die Kontrolle der Kennzahlen ermöglicht bereits eine gute Prozessüberwachung ohne ins Detail zu gehen.

4. Substanzielle Schadensbegrenzung und -reduzierung durch Früherkennungssystem: Durch die Verwendung von Kennzahlen können Risiken, Prozessfehler, Datenverluste und Manipulationen schneller erkannt und Gegenmaßnahmen ergriffen werden. Zusätzlich werden durch regelmäßige Reviews und Kennzahlenabgleiche über einen längeren Zeitraum unternehmensspezifische Vergleichswerte ermittelt. Das ISMS verbessert somit selbst die Aussagekraft der Kennzahlen, da auch kleinste Abweichungen von den Standards sofort erkannt werden.



Beziehung der ISO 27xxx Standards untereinander

5. Kostenreduktion durch nachweisbare Reduktion von Schadensfällen und Unternehmensrisiken: Da die Einrichtung eines ISMS im Allgemeinen mit einer ISO 27001 Zertifizierung durch unabhängige Dritte abgeschlossen wird, erhält die Organisation einen anerkannten Nachweis zur Sicherstellung der Informationssicherheit. Dieser kann unter anderem gegenüber den Haftpflichtversicherern zur Reduktion von Versicherungspolicen verwendet werden.
6. Positive Außenwirkung: Die ISO 27001 Zertifizierung stellt ein allgemein anerkanntes Gütesiegel dar und eignet sich gegenüber Geschäftspartnern und Kunden als „Verkaufsargument“. Bei Ausschreibungen im eHealth Markt wird die Einführung eines ISMS (oder darauf aufsetzend eine ISO 27001 Zertifizierung) häufig als Selektionskriterium verwendet.
7. Reduzierung des Haftungsrisikos für Führungskräfte: Schnelleres Erkennen von Fehlern und demzufolge schnelleres Eingreifen mindert die Haftungsrisiken für Prozessverantwortliche und Führungskräfte. Zusätzlich stellt die Einrichtung eines ISMS und die ISO 27001 Zertifizierung einen Nachweis darüber dar, dass die Führungskraft ihrer Pflicht zur Sicherung der Informationssicherheit bestmöglich nachgekommen ist. Falls dennoch Schadensfälle eintreten sollten, können die Verantwortlichen nachweisen, dass sie ihrer Sorgfaltspflicht nachgekommen sind und bestmöglich Maßnahmen ergriffen haben, um diesen Schadensfall zu verhindern.

Schritte zur ISO Zertifizierung

Der Focus von ISO 27001 liegt darauf, die Rahmenbedingungen zu definieren, nach welchen ein ISMS

aufgesetzt und betrieben werden muss, um darauf basierend die ISO 27001 Zertifizierung erfolgreich zu durchlaufen. Der ISO 27001 Standard liefert damit einen Kriterienkatalog für die „Zertifizierung“ eines ISMS. Spricht man davon, dass sich ein Unternehmen nach ISO 27001 zertifizieren lassen will, so verbirgt sich dahinter nichts anderes als der Aufbau eines ISMS, welches später von unabhängigen Dritten nach festgelegten Kriterien geprüft und bestätigt wird. Bei erfolgreicher Prüfung und Bestätigung des ISMS ist die ISO 27001 Zertifizierung das Resultat.

Der Aufbau eines ISMS bildet das Herzstück einer ISO 27001 Zertifizierung. Im Zusammenhang mit Informationssicherheit spricht man in der Regel vom ISO 27001 Standard. Dies gibt jedoch genau betrachtet nur einen Teilaspekt wieder. Der Standard ISO 27001 wird durch eine ganze Reihe weiterer Standards ergänzt. ISO 27001 alleine ist im Grunde überhaupt nicht anwendbar. Daher spricht man häufig auch von der ISO 27000 Familie oder von ISO 2700x.

ISO 27001 definiert die Grundanforderungen an ein ISMS. Bei Konzeption und Umsetzung des ISMS fällt schnell auf, dass einige Teilaspekte in weiteren ISO Standards näher spezifiziert sind. Unter anderem existiert ISO 27002, ein Leitfaden zur Implementierung von ISMS. Er definiert verschiedene Zielsetzungen und Kontrollziele, welche durch das ISMS erreicht werden müssen. Aktuell sind sieben Standards für den Aufbau eines ISMS von Bedeutung.

ISO Richtlinien sind grundsätzlich branchenneutral gefasst. Sie definieren aus der Vogelperspektive welche Prozesse, Kennzahlen, Kontrollzahlen und ähnliches herangezogen werden sollen, um die Informationssicherheit langfristig zu gewährleisten. Prozesse und Kennzahlen hingegen sind meist

branchenspezifisch geprägt. Daraus ergibt sich, dass jede Branche selbstverständlich auch ihre „eigenen“ kritischen Prozesse und Kennzahlen hat. Derjenige, der eine ISO 27001 Zertifizierung leitet und den Aufbau des ISMS realisiert, muss zwingend über umfangreiche ISO-bezogene Branchenkenntnisse verfügen. Dabei ist es wichtig, dass die Personen Kenntnisse und praktische Erfahrungen aus der Umsetzung einer ISO 27001 Zertifizierung in der jeweiligen Branche gesammelt haben. Nur so können die kritischen Prozesse identifiziert und durch das ISMS abgedeckt werden.



Die IT-Security-Messe

Nürnberg
19.-21. Okt. 2010

Erleben Sie mit der it-sa in Nürnberg vom 19.-21. Oktober 2010 eine Messe, die sich exklusiv auf das Thema IT-Sicherheit konzentriert

- Lösungen zu Informations-Sicherheit, Storage- und Netzwerksicherheit, Datenschutz, Hardware-Sicherung, Security-Awareness
- Non-Stop-Vortragsprogramm auf drei großen Foren mit Kurzreferaten, Podiumsdiskussionen und Live-Demos
- Guided Tours von unabhängigen Consultants
- Topic-Routen zu Trendthemen, Basis-Lösungen
- Seminare, Security-Tagungen, Workshops

Jetzt informieren: www.it-sa.de
SecuMedia Verlags-GmbH
Postfach 12 34, 55205 Ingelheim
Telefon +49 6725 9304-0
Fax +49 6725 5994

Der Wert der Ware „Daten“

Wirtschaftskriminalität nimmt zu

Elmar Török, bits+bites

Immer mehr deutsche Unternehmen sehen sich durch Wirtschaftskriminalität bedroht. Das zeigt eine Studie der Wirtschaftsprüfungsgesellschaft KPMG. Vor allem der Mittelstand unterschätzt die Gefahr, ergab die Umfrage.

In den vergangenen Jahren ist der Anteil der Unternehmen, die wirtschaftskriminelle Handlungen als ernsthaftes Problem betrachten, auf 80 Prozent gestiegen, bei Großunternehmen sogar auf 90 Prozent. Das ermittelten die Wirtschaftsprüfer von KPMG in der aktuellen Studie „Wirtschaftskriminalität in Deutschland 2010“ unter 300 Führungskräften aus allen Bereichen. Laut KPMG haben viele Firmen inzwischen ein umfassendes Fachwissen über wirtschaftskriminelle Handlungsmuster aufgebaut. So setzen 91 Prozent im Rahmen der Aufklärungsarbeit auf interne Kräfte, das ist ein Anstieg um 20 Prozentpunkte gegenüber der letzten Befragung.

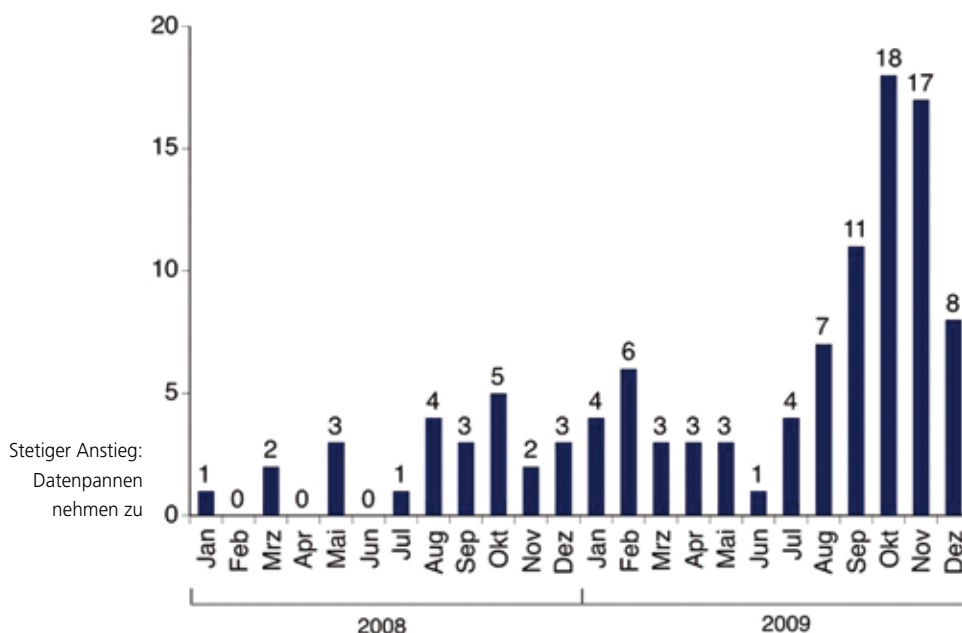
Trotzdem hat sich in vielen Firmen kein ausreichendes Problembewusstsein etabliert. So unterschätzt der Mittelstand noch immer die Bedrohung durch wirtschaftskriminelle Handlungen. Viele dieser Unternehmen wännen sich weniger gefährdet als Großkonzerne. Sie vernachlässigen aufgrund des Vertrauensverhältnisses zu ihren Mitarbeitern oft interne Kontrollsysteme. Alarmierend ist in diesem Zusammenhang, dass nur die Hälfte der befragten Unternehmen in den letzten drei Jahren verstärkt Maßnahmen zur Verhinderung des Verlustes von sensiblen Informationen ergriffen hat.

Unternehmen in der Pflicht

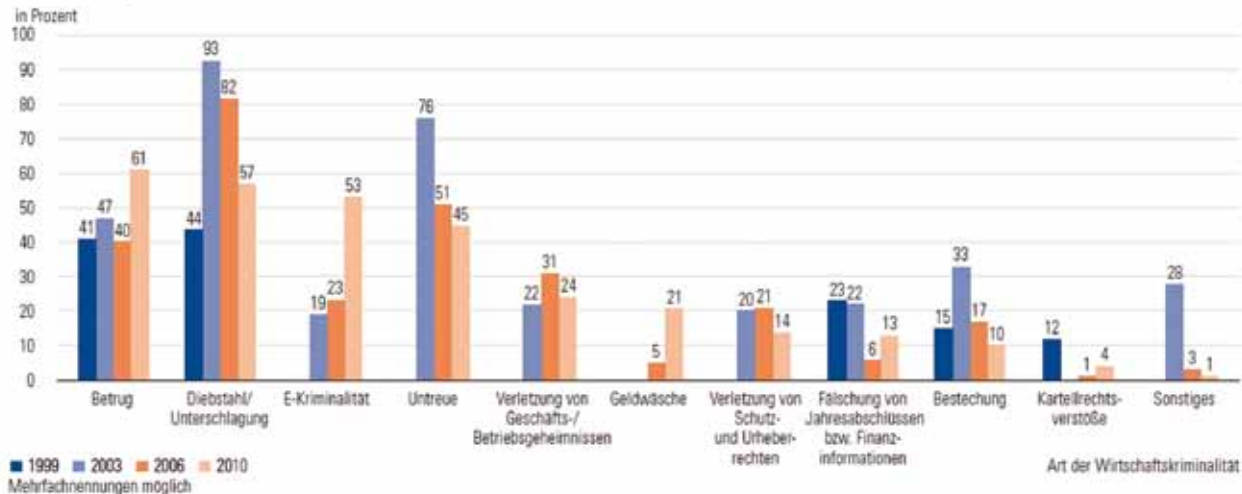
Das Ergebnis kann man an der extrem hohen Zahl von Datenpannen erkennen, in denen Informationen gestohlen oder verloren wurden. Auf dem Portal projekt-datenschutz.de wurden mehr als dreimal so viele gravierende Vorfälle wie im Vorjahr verzeichnet. Insbesondere im Oktober und November 2009 kam es zu einem besonders starken Anstieg der Fälle. Das dürfte der Ansicht der bayerischen Justizministerin Beate Merk zuwider laufen, die jüngst in einem Interview mit der Aussage zitiert wurde, dass „Daten anders als Autos oder Handys keine Sachen sind, daher kann man sie nicht stehlen.“ Sicherlich sind zahlreiche Vorkommnisse auf menschliches Versagen zurück zu führen und haben keine Profiterzielung als Ursache. Doch ein nicht unerheblicher Teil der Probleme entsteht, weil persönliche Daten heute selbstverständlich einen messbaren finanziellen Wert darstellen.

Immer wieder tauchen sensible beziehungsweise private Daten von Bürgern oder Kunden ungesichert im Internet auf. Oft wurden die Daten entwendet, häufig einfach unberechtigt weiter gegeben. So ließen Finanzdienstleister den Abfluss Tausender von Kundeninformationen zu, soziale Netzwerke erlaubten Zugriffe auf vertrauliche Mitgliederdaten und Telekomprovider und Webshops schickten private Daten an fremde Personen.

Wiederholt waren auch Ämter und Behörden an den Datenpannen beteiligt, so etwa Stadtverwaltungen, Gemeindeämter, Amtsgerichte und die Bundesagentur für Arbeit. Etliche Unternehmen und Organisationen fielen sogar mehrfach auf, darunter AWD, Kabel Deutschland, die Deutsche Bank, Libri, Kik, die Deutsche Telekom oder die Postbank.



Die Anzahl der von projekt-datenschutz.de ermittelten Datenschutzvorfälle 2008 und 2009



Häufigkeit und Arten von Wirtschaftskriminalität

Zahlen steigen an

Gegenüber dem Jahr 2008 ist eine überaus starke Zunahme zu konstatieren: Die Gesamtzahl der bekannt gewordenen Vorfälle lag 2009 um rund 350 Prozent über der des Vorjahrs. Der Anstieg über zwei Jahre ist überaus deutlich - für fast jeden Monat wurden erheblich mehr Vorfälle verzeichnet als im Vorjahr.

Auf Grund der negativen Entwicklung muss damit gerechnet werden, dass auch 2010 die Anzahl von Pannen und Missbrauchsfällen nicht zurückgeht, sondern eher steigen wird. Dafür spricht insbesondere, dass es den für die Pannen Verantwortlichen nach wie vor an Einsicht mangelt. Ein offener, transparenter Umgang mit Datenmissbrauch und -pannen ist nicht erkennbar. Stattdessen werden die Vorfälle so lange wie möglich vertuscht oder heruntergespielt. Für zahlreiche Unternehmen und öffentliche Stellen scheint Datenschutz erst relevant zu werden, wenn ein Fall publik wird.

Konsequenterweise geht die starke Zunahme in der zweiten Jahreshälfte nicht auf die nach den Änderungen des BDSG seit September 2009 bestehende Meldepflicht zurück. Die einzelnen Fälle wurden nicht von den verursachenden Unternehmen und Organisationen, sondern meist von den Betroffenen oder von den Medien aufgedeckt. „Die von

projekt-datenschutz.de dokumentierte Entwicklung lässt sich nur umkehren, wenn Wirtschaftsunternehmen und Behörden für ihren Bereich ein funktionierendes Datenschutzmanagement aufbauen“, sagt Dr. Thilo Weichert, Datenschutzbeauftragter des Landes Schleswig-Holstein. „Das heißt, sie müssen einen Datenschutzbeauftragten bestellen, die datenschutzrelevanten Prozesse dokumentieren und prüfen und nachhaltige Verfahren zur Sicherung der Compliance einrichten.“

Vielfältige Formen der Kriminalität

Die Studie von KMPG umfasste neben klassischen Problemen der IT-Sicherheit natürlich auch IT-fremde wirtschaftskriminelle Handlungen wie Unterschlagung oder Bilanzbetrug. Unternehmen sollten sich bei der Bekämpfung von Wirtschaftskriminalität nicht ausschließlich auf die klassischen Bereiche wie Einkauf und Vertrieb konzentrieren. Auch die Rechnungslegung oder das Kreditmanagement sind immer stärker betroffen. Im Fokus bei der Betrugs- und Korruptionsbekämpfung stand bislang die Aufdeckung und Aufklärung wirtschaftskrimineller Handlungen. Allerdings vernachlässigen viele Unternehmen ihre Reaktionsfähigkeit auf konkrete Fälle sowie den Umgang mit

Verdachtsfällen. Dadurch steigt die Gefahr von Reputationsschäden.

Viele Unternehmen verlassen sich zu sehr auf die eingeführten technischen Maßnahmen und präventiven Kontrollen. Oft passen sie diese Systeme nicht an ein sich veränderndes Umfeld an. Prävention wird eher als „Rundumschlag“ betrieben, anstatt Verhaltens- und Betrugsmuster zu analysieren und auf dieser Basis die Maßnahmen gezielt zu planen.

Häufig befinden sich Unternehmen mit Kunden und Lieferanten in einer eng verzahnten Lieferkette. Innerhalb dieser Kette bildet Wirtschaftskriminalität häufig ein Risiko für das eigene Unternehmen. Die meisten Firmen sind auf diese Risiken kaum ausreichend eingestellt: Lediglich 29 Prozent der Befragten gaben an, Integritätskriterien in die Lieferantenbewertung beziehungsweise -entwicklung aufzunehmen.

Wie prominente Skandale gezeigt haben, können Maßnahmen zur Prävention von wirtschaftskriminellen Aktivitäten Gefahren bergen. Besonders wenn Mitarbeiterdaten in eine Prüfung einbezogen werden, kann der Grat zum Gesetzesverstoß oft sehr schmal sein. Offensichtlich haben jedoch viele Firmen die Gefahren in dem Spannungsfeld „Kontrolle und Aufklärung versus Datenschutz“ noch nicht erkannt.

Freud und Leid mit dem GSTOOL

Interview Claus Möhler, Applied Security GmbH

Elmar Török, bits+bites

Claus Möhler beschäftigt sich seit elf Jahren beruflich mit der Abwehr von IT-Angriffen. Bei Applied Security ist er als Berater für Informationssicherheit tätig. Seine Spezialgebiete sind das IT-Risikomanagement bei Outsourcings sowie die Risikobewertung von Anwendungen und komplexen Infrastrukturen. Darüber hinaus betreut er Kunden bei der Vorbereitung für eine Zertifizierung nach IT-Grundschutz.

IT-Grundschutz: Herr Möhler, Sie bereiten Kunden unter anderem für die Zertifizierung nach IT-Grundschutz vor. Wie erleben Sie den Prozess in der Praxis?

Möhler: Wenn der Auditor vor Ort prüft, ist das sicherlich eine Stresssituation für unsere Kunden. Im Vorfeld ist viel Zeit und Energie hineingeflossen, klar, dass im Moment der Wahrheit mit großer Spannung auf das Ergebnis gewartet wird. Aber durch den Standard 100-2 ist der Weg bis zum Audit sehr klar vorgegeben, große Abweichungen, so eine Art „Themaverfehlung“ kann eigentlich nicht vorkommen, wenn man sich an den Standard 100-2 hält.

IT-Grundschutz: Welche Tools nutzen Sie, um den Prozess zu begleiten und zu dokumentieren?

Möhler: Neben einigen selbst entwickelten Hilfsmitteln ist natürlich das GSTOOL des BSI das Werkzeug der Wahl. Ich habe die Erfahrung gemacht, dass daran kein Weg vorbei führt, wenn man am Ende eine Zertifizierung anpeilt. Auch wenn es durchaus andere Werkzeuge auf dem Markt gibt, ist das GSTOOL unverzichtbar, weil es optimal zum Ablauf der Zertifizierung passt.

IT-Grundschutz: Wenn Sie so stark auf das GSTOOL angewiesen sind, haben Sie sicherlich umfangreiche Erfahrungen damit gemacht. Was ist Ihr genereller Eindruck des Softwarewerkzeugs?

Möhler: Es ist sicherlich so, dass das BSI mit dem GSTOOL ein sehr universelles Hilfsmittel anbietet. Es passt für jedes Einsatzszenario oder kann dafür passend gemacht werden. Das unterstützt mich in meiner täglichen Praxis natürlich sehr, ich muss ja als Berater ständig bei wechselnden Kunden mit wechselnden IT-Sicherheitskonzepten und IT-Umgebungen zurecht kommen.

IT-Grundschutz: Passt der universelle Ansatz wirklich in jedem Fall? Oder gibt es durch die Allgemeintauglichkeit auch Verluste beim Fokus?

Möhler: Also, für die Basissicherheitschecks ist das GSTOOL wirklich sehr gut geeignet. Der lässt sich ohne Probleme durchführen und wird auch durch das Tool sehr gut begleitet. Aber was überall passt, kann natürlich nicht in jeder Situation die gleiche Abdeckung und Passgenauigkeit bieten. Das führt im einen oder anderen Szenario dazu, dass die Begleitung einer Zertifizierung durch das GSTOOL etwas weit vom Kunden entfernt ist.

IT-Grundschutz: Wie kann so eine Situation aussehen?

Möhler: Was ich immer wieder erlebe, sind Probleme in der Rollenbehandlung. Im IT-Grundschutz sind die Rollen der Personen im Unternehmen klar definiert und natürlich wird auch in der Zertifizierung dediziert nach den Rollen und deren Aufgaben gefragt. Aber



Claus Möhler, Berater für Informationssicherheit bei der Applied Security GmbH (apsec)

im GSTOOL gibt es keine einfache Möglichkeit, nach den Rollen und den für sie relevanten Fragen zu filtern.

IT-Grundschutz: Gibt es typische Beispiele, denen Sie in der Praxis immer wieder begegnen?

Möhler: Sicher. Nehmen Sie den Baustein Router/Switch. Die Fragen im Rahmen des Basis-Sicherheits-Checks, die Sie mit dem Kunden im Vorfeld klären, sind zu 70 oder 80 Prozent technischer Art. Der Rest betrifft andere Themen, die beispielsweise den Beschaffer betreffen. Der ist in größeren Firmen eine andere Person, sitzt in einer anderen Abteilung und oft auch in einem anderen Gebäude.

IT-Grundschutz: Aber wer dafür verantwortlich ist, können Sie doch im Vorfeld klären.

Möhler: Natürlich, aber es ist ja nicht damit getan, dass ich ihm die Fragen des Bausteins Router/Switchstelle. Es gibt in praktisch jedem Baustein eine ähnliche Aufteilung mit vielen technischen und einigen nichttechnischen Fragen. Es wäre sehr sinnvoll, wenn Sie im GSTOOL alle Fragen für eine Rolle filtern und zusammenfassen könnten, egal in welchem Baustein sie sich befinden. Sonst tauchen immer wieder Überbleibsel auf, für die Sie viel Zeit investieren müssen, nur um die richtigen Leute zu finden.

IT-Grundschutz: Wie lösen das andere Anbieter, ist es dort einfacher?

Möhler: Es gibt andere Hersteller, die in ihrer Umsetzung komplett auf das Rollenmodell gesetzt haben. Dort ist es natürlich einfacher, die relevanten Fragen für die richtigen Personen zu finden.

IT-Grundschutz: Wäre das keine Alternative zum GSTOOL?

Möhler: Nein, meiner Erfahrung nach kommt man um das GSTOOL nicht herum, sofern eine Zertifizierung angestrebt wird – auch wenn das für mich bedeutet, dass ich den Antworten auf die letzten paar Fragen verhältnismäßig lange hinterherlaufen muss. Dafür, und das muss man auch erwähnen, ist die Aktualität der Inhalte natürlich perfekt an die Grundschutzkataloge angepasst, das ist bei den anderen Tools nicht immer so eindeutig geregelt. Es gibt schon einen Grund, warum bei der großen Mehrheit der Zertifizierungsprojekte das GSTOOL verwendet wird, trotz seiner Schwächen. Für Teilbereiche der IT-Grundschutz-Vorgehensweise, zum Beispiel bei der ausschließlichen Bearbeitung des Basis-Sicherheits-Checks, sind alternative Tools durchaus nutzbar.

IT-Grundschutz: Was fehlt Ihnen im GSTOOL, über das andere Tools verfügen?

Möhler: Ich habe schon mit Werkzeugen gearbeitet, die komplett Web-basiert aufgesetzt waren und auch eine reibungslos funktionierende und einfache Mehrbenutzerumgebung ermöglichten. Das ist bei uns manchmal ein Problem, wenn ich mit Kollegen an einem Projekt arbeite und wir beide im GSTOOL Einträge vornehmen. Oder wenn auch der Kunde selbst im GSTOOL arbeitet. Die vorgesehene Lösung über den Export ist zu wenig praxisgerecht.

IT-Grundschutz: Wie lösen Sie das Problem?

Möhler: Zum Glück müssen wir das nur sehr selten machen, denn die wenigsten Kunden wollen selbst im GSTOOL Hand anlegen. Es gibt doch eine recht steile Lernkurve bei der Bedienung, selbst wenn man die Grundschutzthematik kennt und mit ihr vertraut ist. Das Tool erschließt sich nicht von selbst. Und so bleibt es in der Regel bei uns als Dienstleister, der mit dem Programm umgeht. Darum ist es auch nicht so gravierend, dass es bislang nur eine Windows-Version davon gibt. Wir sind in erster Linie Windows-zentrisch wenn es um die Tools für die Zertifizierung geht.

IT-Grundschutz: Gibt es von Seiten Ihrer Kunden Nachfragen nach einer Linux-Version?

Möhler: Das kommt vor, allerdings sehr selten. Wie gesagt, bislang war das kein Problem. Schwerer wiegt die recht eingeschränkte Exportfunktion der Dokumente in ein HTML-Format. Ich benötige oft Auszüge aus Listen oder Dokumenten, die ich dann entweder für die Beantwortung der Fragen beim Kunden oder für die interne Dokumentation nutze. Das, was das GSTOOL hier bietet ist nicht mehr zeitgemäß. Exportierte Dokumente muss ich viel zu aufwändig nacharbeiten. Das gilt übrigens auch für das Berichtswesen. Eigentlich nutzen wir das nur noch zum Prüfen, ob Papierdokumentation und GSTOOL synchron sind.

IT-Grundschutz: Die Erstellung von Berichten ist mit dem GSTOOL durchaus möglich. Woran scheitert es?

Möhler: Formate und Inhalte sind einfach nicht ausreichend für unsere Anforderungen. Es wirkt wie Stückwerk, nicht aus einem Guss. Wir pflegen die Daten eigentlich nur noch, weil sie bei der Zertifizierung geprüft werden, aber eine Hilfe sind sie nicht.

IT-Grundschutz: Wenn Sie dem BSI eine Wunschliste für Änderungen oder Erweiterungen des GSTOOL vorlegen könnten, was wären Ihre Top-Prioritäten?

Möhler: Neben der Rollenthematik fehlt mir vor allem etwas, das nicht direkt mit dem Tool zu tun hat. Ich vermisse das schnelle Eingehen auf Entwicklungen bei grundschutzrelevanten Produkten. So ist Vista erst ab dieser Ergänzungslieferung mit dabei, Windows Server 2008 R2 fehlt ganz. Die allgemeinen Themen sind gut abgedeckt, aber bei den Produkten reagiert das BSI meiner Ansicht nach zu langsam. Wenn es den Prozess beschleunigen würde, wäre ich auch gern bereit auf die Printausgabe zu verzichten.

IT-Grundschutz: Trotz aller Schwächen: Sie sagten eingangs, dass es keine Alternative zum GSTOOL gibt.

Möhler: Ja, ganz klar: wir arbeiten mit dem GSTOOL nicht nur, weil es vom BSI kommt, sondern - weil es nach wie vor das beste Werkzeug für den Job ist. Es passt für viele Anforderungen und in viele Umgebungen, für uns als Dienstleister ist das essenziell. Und viele Funktionen sind ja auch sehr gut umgesetzt. So sind zahlreiche Kunden froh über die integrierte Zeitplanung. Damit kann man wunderbar Projektschritte definieren und behält Zeit- und damit auch das Kostenbudget gut im Blick. Das ist, wie der Großteil der Funktionen des GSTOOL eine wertvolle Hilfestellung während der Vorbereitungen.



IT-Grundschutz Wegweiser

Audits



TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD

ISO/IEC 27001 (auch auf der Basis von IT-Grundschutz) und BS 25999-2:

- Kompetenz auf Senior-Level in Auditierungs- und Zertifizierungsverfahren
- Management Coaching, Project Supervising und Training
- Ausbildung von ISMS-Auditoren
- Pre-Checks, Gap-Analysen, Assessments
- Auditierung und Zertifizierung

www.tuvit.de

Beratung

»Mit Sicherheit gute Geschäfte«

»secaron

Ihr Partner in Sachen IT-Sicherheit und Informationsschutz.

www.secaron.de
info@secaron.de
0811-9594-0

»IT-Sicherheit nach Maß«



Ausbildung / Schulung



Wir setzen auf **Qualität**.
Setzen Sie sich zu uns.



Hochwertige
Security-
Schulungen

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

DuD 2010 – Datenschutz und Datensicherheit
Das Treffen der Datenschutzbeauftragten
7. und 8. Juni 2010 in Berlin
www.computas.de



Die IT-Security-Messe

19.-21. Okt. 2010, Nürnberg
Ihr bookmark für IT Security:
www.it-sa.de/newsletter

Awareness



8COM

IT SECURITY

Awareness Kampagnen, Pentests,
Sicherheitsanalysen, Sicherheitskonzepte,
LIVE-Hacking Vorträge

8com GmbH & Co. KG

Telefon: +49 (0) 6327 976 428-0

Mail: info@8com.de, Web: www.8com.de

Beratung / Consulting

secunet

Sicherheitskonzepte - Planung und
Realisierung nach IT-Grundschutz

secunet Security Networks AG
Kronprinzenstraße 30, 45128 Essen
Tel.: +49 (0) 201 5454-0

E-Mail: info@secunet.com

www.secunet.com

Datenschutz

**Ist Datenschutz für Sie
ein Drahtseilakt?**

„Das Security Forum 2010 in Frankfurt, Hannover
und München – Aktuelle Informationen von Security-
Experten zum Thema Datensicherheit“ mehr
Infos zu den kostenlosen Veranstaltungen unter
<http://events.secude.com>



**Datenschutz kompakt
und verständlich**

Eine praxisorientierte Einführung

246 Seiten, 23,95 €

<http://buchshop.secumedia.de>

E-Mail-Verschlüsselung

Z1 SecureMail

- Server-basierte E-Mail-Verschlüsselung u. -Signatur
- Automatisiertes Key- u. Zertifikatsmanagement
- Governikus-zertifiziert
- Security-Policies
- Z1 Appliance wirtschaftlich einsetzbar, auch „Virtual Appliance“ für VMware oder Xen



zertificon
www.zertificon.com solutions

Veranstaltungen

- Seminare
- Workshops
- Messen
- Kongresse

zum Thema IT-Grundschutz:

www.grundschutz.info

**Ihr Kontakt zur
Anzeigenabteilung**

Informationsdienst
IT-Grundschutz
Birgit Eckert
Tel. +49 6725 9304-20
anzeigenleitung@secumedia.de
www.grundschutz.info

**Ihr Kontakt zum
Leserservice**

Informationsdienst
IT-Grundschutz
Max Weisel
Tel. +49 6725 9304-27
vertrieb@secumedia.de