

Unternehmen vernachlässigen Backup

Viele Unternehmen vernachlässigen ihre Sicherheitskonzepte, wie eine Acronis Studie zu Backupgewohnheiten in europäischen Unternehmen ergab. 56 Prozent der befragten deutschen Unternehmen benötigen für das Anfahren ihrer Systeme nach einem Systemausfall zwischen einem Tag und einer Woche. Vergleichbare Werte ermittelte die Studie für die französischen Nachbarn. Noch schlechter sind die Werte in England. 70 Prozent der Interviewten benötigten bis zu einer Woche für einen Start ihrer Systeme. Nur wenige IT-Verantwortliche vertrauen ihren Systemen. Nur 9 Prozent äußerten sehr geringe oder keine Erwar-

tungen, einen Hardwareschaden oder Virenbefall ohne Verlust zu überstehen. Weitere 22 Prozent sehen einer Wiederherstellung von Daten weder besonders zuversichtlich oder pessimistisch entgegen. Acronis befragte für die Studie europaweit 600 IT-Verantwortliche von kleinen und mittleren Unternehmen.

Fazit: Die Investition in vorbeugende Maßnahmen ist – auch wenn der Mehrwert nicht sofort sichtbar ist – ein Schritt zur Erhaltung der Handlungsfähigkeit des Unternehmens. ■ NSCH

Internet: www.acronis.com

Stichworte: Backup-Strategie, Wiederanlauf, Notfallplanung

Studie: Datenpannen sind teuer

Unternehmen wägen häufig im Rahmen einer Risikoanalyse die Kosten für präventive datenschutzrechtliche Maßnahmen gegen die Kosten eines Datenschutzvorfalls ab. Besondere Schwierigkeiten bereitet die Einschätzung der Kosten einer Datenschutzverletzung. Die „Jahresstudie 2009: Kosten von Datenpannen“ zeigt: die durchschnittlichen Investitionen der deutschen Unternehmen nach einer Datenpanne sind im Vergleich zum Vorjahr um 7 Prozent gestiegen (DSB 4/09, Seite 15). Zahlten die Unternehmen im Jahr 2008 noch 2,41 Millionen Euro pro Fall für die Schadensbehebung, waren es im Jahr 2009 schon 2,58 Millionen Euro. Ein noch stärkerer Anstieg war bei kompromittierenden Datensätzen zu verzeichnen. So mussten im Jahr 2009 bereits 132 Euro pro Datensatz im Vergleich zu 112 Euro im

Vorjahr investiert werden. Oft verursachen Fehler von externen Dienstleistern die Datenpannen. Lag der Wert im Jahr 2008 noch bei 17 Prozent, so waren es im Jahr 2009 schon 36 Prozent. Die zunehmende Sensibilisierung der Kunden im Umgang mit ihren Daten führt für die Unternehmen bei Datenpannen zu Umsatzverlusten. Der Anteil des entgangenen Umsatzes an den Gesamtkosten pro kompromittierten Datensatz lag im Jahr 2009 bei 46 Euro von 132 Euro. Die Studie des Ponemon Institutes basiert auf realen Fakten und Zahlen, die sich aus Datenpannen und anschließenden Fällen von Datenmissbrauch in 22 deutschen Unternehmen ergeben haben. ■ NSCH

Internet: www.encryptionreports.com

Stichworte: Datenpannen, Kosten

Botnetze - (k)eine Gefahr?

Botnetze sind ein wichtiges Verbreitungsinstrument für Spam-Nachrichten. Eine Studie des E-Mail Sicherheitsanbieters eleven zeigt, dass 97 Prozent des deutschen Spam-Aufkommens durch Botnetze generiert werden. Doch viele PC-Nutzer sind sich dieser Problematik nicht bewusst. 62 Prozent der Befragten hielten es für unwahrscheinlich, dass ihr Rechner durch ein Botnetz infiziert werden könnte. Gleichwohl wussten 91 Prozent der Befragten von der Existenz von Botnetzen; 45 Prozent waren bereits Opfer einer Virusattacke. 52 Prozent der Interviewten gaben an, dass sie schon einmal Spam-E-Mails geöffnet hatten. Unternehmen sollten sich bei ihren Maßnahmen nicht alleine auf technische Lösungen verlassen. Die Technik kann gut informierte Mitarbeiter nicht ersetzen. ■ NSCH

Internet: www.eleven.de

Stichworte: Spam-E-Mails, Botnetze

Authentifizierung via Handy

VASCO, ein Anbieter von Authentifizierungsmöglichkeiten, ermöglicht mit dem Digipass Pack für Remote Authentication ein Komplettpaket zur Authentifizierung. Ab sofort können Handys für die Zwei-Faktor-Authentifizierung und die digitale Signatur eingesetzt werden. ■ NSCH

Internet: www.vasco.com

Stichworte: Authentifizierung, Handy

Datenschutzaufsichtsbehörden sind umzustrukturieren

Die Aufsichtsbehörden für den Datenschutz sind aufgrund der föderalen Struktur in Deutschland unterschiedlich aufgebaut. Teilweise sind sie als Datenschutzbeauftragte eingerichtet, die vom Parlament gewählt werden, teilweise sind sie bei Regierungspräsidien oder im Innenministerium vorgesehen. Diese Struktur ist von der Europäischen Datenschutzkommission kritisiert und zum Gegenstand eines Vertragsverletzungsverfahrens gemacht worden. Am 9. März 2010 hat der Europäische Gerichtshof un-

ter dem Aktenzeichen C-518/07 daraufhin Deutschland verurteilt, „völlig unabhängige“ Aufsichtsbehörden für den Datenschutz zu schaffen. Jede rechtliche Kontrollmöglichkeit eines Ministers über die Datenschutzaufsicht sei mit der Europäischen Datenschutzrichtlinie von 1995 nicht vereinbar. Die Maßnahmen der Aufsichtsbehörden dürften allein durch die Gerichte kontrolliert werden.

Diese Entscheidung führt dazu, dass sich die Datenschutzver-

antwortlichen in den Behörden nun ergänzend zu ihrem normalen Arbeitspensum auch mit Fragen der datenschutzkonformen Gestaltung einer Datenschutzaufsichtsbehörde beschäftigen müssen. Der Datenschutz-Berater wird über die sich in Zukunft ergebenden Änderungen berichten. ■ PK

Internet: <http://curia.europa.eu>

Stichworte: EuGH, Datenschutzaufsichtsbehörden

Studie: Schutz von Betriebsgeheimnissen

Der Schutz von Betriebsgeheimnissen steht nicht im Mittelpunkt der Investitionen der Unternehmen. In der Studie „The Value of Corporate Secrets“ gaben 90 Prozent der befragten Unternehmen an, dass Ausgaben für Datenschutzregeln, Compliance mit PCI-DSS (Payment Card Industry Data Security Standard) und den Schutz vor Sicherheitslücken priorisiert sind. Für diese Bereiche werden 30 Prozent der Unternehmensetats ausgegeben.

Allerdings bestehen 62 Prozent aller vorgehaltenen Daten aus Betriebsgeheimnissen, während compliancebezogene Daten nur 38 Prozent ausmachen. Forrester Consulting befragte für die Studie im Auftrag von Microsoft, RDS und der Sicherheitsabteilung von EMC weltweit 305 Entscheidungsträger für IT-Sicherheit. Spätestens mit dem Verkauf mehrerer Steuersünder-CDs ist die öffentliche Diskussion um den

Schutz von Betriebsgeheimnissen wieder entbrannt. Das Know-how vieler Unternehmen – insbesondere im mittelständischen Bereich – ist deren Kapital.

Doch der Schutz dieser Daten wird vernachlässigt. So sind etwa die besten Zutrittskontrollsysteme zu Forschungsbereichen nutzlos, wenn der Datenabzug in einem äußerlich geschützten Bereich bequem über offene USB-Schnittstellen möglich ist. Eine Verbesserung dieser Situation kann nur durch einheitliche Schutzkonzepte erreicht werden. ■ NSCH

Internet: www.microsoft.com

Stichworte: Betriebsgeheimnisse

Sozialdatenschutz-Novelle

Die Bundesregierung hat einen Gesetzentwurf vorgelegt, der Teile der BDSG-Novelle II auf den Sozialdatenschutz im Zehnten Buch Sozialgesetzbuch (SGB X) erstreckt (Bundesrats-Drucksache 152/10 vom 26. März 2010). Für die Auftragsverarbeitung von Sozialdaten nach § 80 SGB X soll künftig der Katalog der zehn Pflichtinhalte ebenso gelten wie das Prinzip der zwingenden Erst- und Folgekontrollen. Neu ist die Security Breach Notification nach § 83a SGB X-RegE für Sozialleistungsträger. Einerseits würde die Melde- und Benachrichtigungspflicht damit erstmals auf öffentliche Stellen erstreckt werden; andererseits soll sie auf besondere Arten personenbezogener Daten, also insbesondere Gesundheitsdaten der Sozialversicherungsträger beschränkt sein. ■ SHA

Stichworte: Sozialdatenschutz, SGB X, Sozialleistungsträger, Gesundheitsdaten

Der Datenschutzbeauftragte informiert:

Sicher einkaufen im Internet

Verbraucher übermitteln bei Einkäufen im Internet ihre Daten zur Abwicklung der Kaufverträge. Die Vertrauenswürdigkeit des Geschäftspartners kann nur in seltenen Fällen durch die Käufer überprüft werden. Mit Hilfe der neuen EV-Zertifikate (Extend Validation) können nun auch unerfahrene PC-Nutzer zwischen vertrauenswürdigen Webseiten und Angeboten mit betrügerischen Absichten unterscheiden. Die Zertifikate informieren darüber, ob das hinter der Homepage stehende Unternehmen existiert und ordnungsgemäß registriert ist. Sie erkennen die Zertifizierung des Online-Shops an folgenden Kriterien: (1) die Adressleiste der Webseite – mittels der vertrauliche Informationen ausgetauscht werden sollen – färbt sich ganz oder teilweise grün, (2) der Betreiber der Homepage und die Zertifizierungsstelle werden genannt. ■ NSCH

Internet: www.trustcenter.de

Stichworte: Online-Shops, EV-Zertifikate

Angriffe auf Online-Gamer

Cyberkriminelle haben Online-Gamer als Ziel von neuen Phishing-Attacken ausgewählt. So werden Spieler von „World of Warcraft“ oder „Aion“ mittels eines Links in einer E-Mail auf eine gefälschte World of Warcraft-Webseite geleitet. Dort werden vertrauliche Account-Daten abgefragt, die später auf einer Online-Auktionsplattform versteigert werden.

Der Angriff via Spam-Mail ist – auch für erfahrene Gamer – kaum erkennbar. Die Mails weisen keine sprachlichen Fehler auf und die Phishing-Seite verfügt über ein täuschend echt aussehendes Design, so Kaspersky Lab.

Bitte informieren Sie auch Ihre Angehörigen über diese potentielle Gefahrenquelle. ■ NSCH

Internet: www.kaspersky.com

Stichworte: Phishing, Online-Games

Achtung Kostenfalle!

Manche Eigentümer von Windows-Smartphones sehen sich in diesen Tagen mit erhöhten Telefonrechnungen konfrontiert. Die Ursache hierfür kann in dem kostenlosen First-Person-Shooter „3D Anti-Terrorist-Action“ liegen. Cyberkriminelle haben in dem Spiel einen Trojaner versteckt und bieten es auf verschiedenen Webseiten zum Download an. Das Schadprogramm führt unangefordert und selbstständig Telefonate mit kostenintensiven, internationalen Mehrwertdiensten durch, so der IT-Sicherheitsanbieter F-Secure.

Bitte nutzen Sie nur vertrauenswürdige Webseiten für den Download von kostenlosen Spielen. Ein Antivirenprogramm bietet zusätzlichen Schutz für Ihr Smartphone. ■ NSCH

Internet: www.f-secure.de

Stichworte: Smartphone, 3D-Anti-Terrorist-Action

Für unsere Leser: Diese Texte können Sie zur eigenen Verwendung abrufen unter: redaktion@glisskramer.de.

Umfrage: Vertrauenswürdigkeit beim Schutz persönlicher Informationen

Die Deutschen bescheinigen den Unternehmen für die Vertrauenswürdigkeit beim Schutz persönlicher Informationen schlechte Noten. Im Rahmen einer Umfrage des Emnid-Instituts bewerteten die Befragten die Vertrauenswürdigkeit des öffentlichen

Sektors mit der Bestnote 2,9. Schlusslichter des Vertrauensrankings sind Telekommunikationsdienstleister mit der Note 4,2 und Online-Shops mit der Note 4,4. Im Mittelfeld bewegen sich Finanzsektor, Transport, sowie Einzelhandel. Die Studie, zu der

1.000 Bürger befragt wurde, hat Symantec beauftragt. ■ NSCH

Internet: www.symantec.com

Stichworte: Umfrage, Vertrauenswürdigkeit