

Dr. Philipp Kramer

Stichwort
Videoüberwachung

Miterfassung des Bürgersteigs bei betrieblicher Videoüberwachung zulässig

Häufig möchten Unternehmen ihre Beschäftigten und ihre Firmenwerte schützen, vor allem gegen Straftaten und Überfälle sowie Vandalismus. Ein probates Mittel dafür ist der Einsatz der Videoüberwachungstechnik. Da Videoüberwachung Menschen und deren Gesichter erfassen kann und gegebenenfalls aufzeichnet, liegt eine Datenverarbeitung im Sinne des Bundesdatenschutzgesetzes vor. Erfassen die Kameras auch öffentliche Bereiche, also Bereiche, die von jedermann betreten werden können, muss die Überwachung erforderlich sein und die Güterabwägung zugunsten der überwachenden verantwortlichen Stelle ausgehen (§ 6b BDSG). Hält sich das überwachende Unternehmen an die Beschränkung auf das erforderliche Maß, namentlich durch Schwärzung irrelevanter Bereiche, und dokumentiert es seine Prozesse ordentlich, muss ein zufällig vorbeigehender Passant es hinnehmen, wenn er unvermeidlich erfasst wird. Auch das unter Umständen persönliche Empfinden, „sich überwacht zu fühlen“, steht der Videoüberwachung nicht entgegen. Das Unternehmen ist nicht verpflichtet, alternativ auf den Einsatz von Wachpersonal zurückzugreifen. Auch einer Popularklage von Jedermann wurde eine Absage erteilt. Das sind die Aussagen des Urteils des Landgerichts München I vom 21. Oktober 2011 (20 O 19879/10; anzufragen unter redaktion@gliss-kramer.de). Es liegt damit auf einer Linie mit dem Amtsgericht Berlin-Mitte (18. Dezember 2003, 16 C 427/02). Das Amtsgericht hatte die Überwachung eines ein Meter breiten Streifens – von der Gebäudeaußenwand gerechnet – für zulässig befunden, sofern es sich nicht eindeutig um einen typischen Bereich spontaner sozialer Kommunikation handele.

hender Passant es hinnehmen, wenn er unvermeidlich erfasst wird. Auch das unter Umständen persönliche Empfinden, „sich überwacht zu fühlen“, steht der Videoüberwachung nicht entgegen. Das Unternehmen ist nicht verpflichtet, alternativ auf den Einsatz von Wachpersonal zurückzugreifen. Auch einer Popularklage von Jedermann wurde eine Absage erteilt. Das sind die Aussagen des Urteils des Landgerichts München I vom 21. Oktober 2011 (20 O 19879/10; anzufragen unter redaktion@gliss-kramer.de). Es liegt damit auf einer Linie mit dem Amtsgericht Berlin-Mitte (18. Dezember 2003, 16 C 427/02). Das Amtsgericht hatte die Überwachung eines ein Meter breiten Streifens – von der Gebäudeaußenwand gerechnet – für zulässig befunden, sofern es sich nicht eindeutig um einen typischen Bereich spontaner sozialer Kommunikation handele.

Internet
www.jurpc.de/rechtspr/20040199.htm

Nicole Schmidt

Stichworte
Studie
Informationssicherheit
(Studie)

Studie: Risiken für Datensicherheit

Die Risiken für die Datensicherheit in Großunternehmen steigen fortlaufend, bedingt durch die technische Weiterentwicklung. Zu diesem Ergebnis kommt die Studie „2011 Global Information Security Survey“ der Wirtschaftsprüfungs- und Steuerberatungsgesellschaft Ernst & Young. Etwa 75 Prozent aller Befragten geben an, dass das Sicherheitsrisiko durch das erhöhte Aufkommen von externen Bedrohungen ansteigt. Weitere 56 Prozent aller befragten Unternehmen

sind der Auffassung, dass sie ihre Datenschutzsicherheitsstrategien untersuchen oder optimieren müssen. Ein besonderes Augenmerk liegt auf den Gefahren, die durch soziale Netzwerke verursacht werden. 53 Prozent der Großunternehmen haben den Zugriff ihrer Mitarbeiter auf die Seiten gesperrt oder stark eingeschränkt; in 46 Prozent der Fälle erfolgte eine Anpassung der Richtlinien. Für die Studie wurden 1.700 Fachkräfte für Informationssicherheit aus 52 Ländern befragt.

Internet
[www.ey.com/Publication/vwLUAssets/Into_the_cloud_out_of_the_fog-2011_GISS/\\$FILE/Into_the_cloud_out_of_the_fog-2011%20GISS.pdf](http://www.ey.com/Publication/vwLUAssets/Into_the_cloud_out_of_the_fog-2011_GISS/$FILE/Into_the_cloud_out_of_the_fog-2011%20GISS.pdf)

Nicole Schmidt

Stichworte
Android
Malware

Schadprogramme attackieren Android-Betriebssystem

Das mobile Betriebssystem Android wird zunehmend durch Schadprogramme attackiert. Laut Kaspersky Lab stieg die Anzahl der neuen Android-Malware im September 2011 um 30 Prozent an. Besonders auffällig ist: 46 Prozent aller mobilen Schadprogramme greifen das System Android an. Die Täter haben es zunehmend auf den Diebstahl

von persönlichen Informationen abgesehen; 34 Prozent der Android-Malware wird entsprechend programmiert und teilweise im offiziellen Android-Market eingestellt. Die Cyberkriminellen tarnen die Trojaner beispielsweise als App für das Herunterladen von Klingeltönen.

Internet
www.kaspersky.com/de/news?id=207566494

Nicole Schmidt

Datenpanne bei Gesundheitsdaten: Organisatorische Mängel

Über einen längeren Zeitraum waren medizinische Befunde und psychologische Dokumentationen von etwa 3.600 psychisch erkrankten Personen aus den Jahren 2002 bis 2011 im Internet einsehbar. Der Server ist zwischenzeitlich abgeschaltet. Nach Angaben des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein (ULD) war eine Kombination von schwer-

wiegenden organisatorischen Mängeln zwischen mehreren Einrichtungen beziehungsweise Stellen für die Datenpanne ursächlich. So waren weder die Arbeitsverhältnisse und die Verantwortlichkeiten klar geregelt noch erfolgte eine Qualitätskontrolle der IT. Auch die Sicherheit der eingesetzten Software war anscheinend nie ernsthaft hinterfragt worden, so das ULD.

Stichworte

Datenpanne
Psychiatriedaten

Internet

www.datenschutzzentrum.de/presse/20111107-psychatrie-daten.htm

Nicole Schmidt

Der Datenschutzbeauftragte informiert: Europäische Kreditkartendaten

Europäische Kreditkartendaten sind auf dem Schwarzmarkt sehr begehrt. Die Täter verkaufen die Daten auf dem Schwarzmarkt, nachdem sie die Karte entwendet haben oder die Informationen auf dem Magnetstreifen in krimineller Absicht ausgelesen haben. US-amerikanische Daten sind dagegen geringer bewertet. Die höhere Anzahl von Kreditkarten wirkt sich negativ auf dem Schwarzmarktwert aus. Daneben wird stetig die Sicherheit der Kreditkartendaten in Europa erhöht. Bedingt durch die Einführung der Sicherheitschips auf den Kreditkarten sinkt die Anzahl der für die Cyberkriminellen „brauchbaren“ Kre-

ditkarteninformationen. Die Kreditkartenunternehmen MasterCard und Visa erhöhen den Druck auf die Annahmestellen. Sofern die Eigentümer die Geldautomaten nicht entsprechend fristgemäß auf die Akzeptanz der „Sicherheitschipkarten“ umstellen, sind sie verantwortlich für den Betrug, der durch ihre Maschinen begangen wird.

Bitte beachten Sie die Sicherheitshinweise Ihres Kreditkartenunternehmens und kontrollieren Sie täglich, ob Sie noch im Besitz Ihrer Kreditkarte sind.

Stichwort

Kreditkartenbetrug

Internet

www.blog.imperva.com/2011/10/current-value-of-credit-cards-on-the-black-market-part-ii.html

Nicole Schmidt

Schweden: Hacker veröffentlichen Passwörter

Hacker haben mehrere hunderttausend Passwörter im Klartext veröffentlicht. Betroffen sind 210.000 Login-Daten, einschließlich der persönlichen Identifikationsnummern von Journalisten, Abgeordneten und Prominenten. Mindestens 90.000 Passwörter des bekannten Blogs „Blogtoppen.se“ wurden über einen gehackten Twitter-Account eines Politikers bekannt gegeben. Darüber hinaus wurden 57 Webseiten gehackt,

sodass die Cyberkriminellen die größte Sicherheitslücke in der schwedischen Geschichte verursacht haben. Der Hacker sc3a5j gab gegenüber der Zeitung „Expressen“ unter anderem zu seinen Motiven an: Nutzer sollen wissen, dass sie nie die gleichen Passwörter für verschiedene Dienste im Internet verwenden sollen. Die Polizei in Stockholm untersucht den Vorfall.

Stichworte

Passwort
Schweden

Internet

www.theregister.co.uk/2011/10/26/logins_details_dumped_in_sweden/

Nicole Schmidt

Stichwort
Fachkräftemangel

Studie: Fachkräftemangel in der IT-Sicherheit

Schon heute sind erste Auswirkungen des Fachkräftemangels im Umfeld der IT-Sicherheit erkennbar. Zu diesem Ergebnis kommt die weltweite Umfrage „2011 Threat Management Survey“ von Symantec. 57 Prozent der Unternehmen geben an, dass die Reaktionszeit der IT-Security-Verantwortlichen bei neuen Bedrohungen zu

langsam ist. Als Ursache hierfür sehen 46 Prozent der Befragten die unzureichende personelle Ausstattung. Daneben mangelt es nach der Auffassung von 45 Prozent der Interviewten an dem notwendigen Zeitbudget für die Bewältigung der Aufgaben; 35 Prozent beklagen den fehlenden Sachverstand der Fachkräfte.

Internet
www.symantec.com/content/en/uk/about/media/pdfs/symc-threat-mangement-survey-global.pdf

Nicole Schmidt

Stichworte
Duqu
Stuxnet

Duqu - ein neuer Stuxnet-Schadcode

Offensichtlich haben Cyberkriminelle einen Nachfolger des Stuxnet-Wurms (siehe dazu DSB 11/10) programmiert. Der Duqu-Wurm wurde nach Angaben von Kaspersky Lab insgesamt viermal im Iran und Sudan entdeckt. Die Infektionswege der Computer sind noch unklar. Duqu kann Sicherheitsprogramme so beeinflussen, dass

er nicht erkannt wird. Die besondere Gefährlichkeit ist darin zu sehen, dass die Malware entsprechend dem späteren Zielobjekt modifiziert werden kann. Duqu ist komplexer als Stuxnet und könnte für den Diebstahl von Informationen aus Unternehmen oder politischen Organisationen entwickelt worden sein.

Internet
www.securelist.com/en/blog/208193197/The_Mystery_of_Duqu_Part_Two
www.securelist.com/en/blog/208193182/The_Mystery_of_Duqu_Part_One

Nicole Schmidt

Stichwort
Authentifizierung

Authentifizierungslösung

Authentifizierungslösungen sollen Schäden durch den Identitätsdiebstahl vorbeugen und gleichzeitig die Anwender in ihrer Nutzung nicht behindern. Das neue FT2011 Modell der 4TRESS Authentication Appliance verfügt über eine komplette

mehrschichtige Authentifizierung. Das Modul erkennt Betrugsversuche und weist Funktionen für Sicherheit in der Cloud sowie mehr als 15 unterschiedliche starke Authentifizierungsmethoden auf.

Internet
www.actividentity.com

Nicole Schmidt

Stichworte
Online-Marketing
E-Mail-Werbung
Checkliste

Checkliste: E-Mail und Recht

Der E-CRM Anbieter artegic hat in Zusammenarbeit mit der Anwaltskanzlei Bird&Bird eine kostenlos erhältliche Checkliste veröffentlicht, die in leicht verständlicher Frage-und-Antwort-Form auf 22 Rechtsfragen zum E-Mail-Marketing eingeht. Behandelt werden unter anderem folgende Themen: Wie lässt sich die Einwilligung des

Empfängers rechtssicher nachweisen? Sind Anmelde-Links für weitere Abos aus einer E-Mail heraus eine ausreichende Einwilligung? Darf ich in Service- und Transaktions-E-Mails werben? Darf ich die Daten meiner Kontakte aus Social Networks herunterladen und damit meine Daten anreichern?

Internet
www.artegic.de/eCRM/Downloads/E-Mail_und_Recht_-_Fragen_und_Antworten/mv.html

Dr. Philipp Kramer

EuGH gegen präventive Kontrolle von Datenaustausch im Internet

Stichworte

EuGH
Internetprovider
IP-Adressen
SABAM
Urheberrecht

Der Europäische Gerichtshof hat in seinem Urteil vom 24. November 2011 (C 70/10) die Rechte von Internet Providern gestärkt und im Ergebnis gegen die belgische Urheberrechtsschutzvereinigung SABAM (vergleichbar mit der deutschen GEMA) entschieden. Die Entscheidung präzisiert auch die Datenschutzrechte von Internetnutzern und äußert sich zum Personenbezug von IP-Adressen.

Die SABAM wendet sich gegen das bekannte Filesharing bei urheberrechtlich geschützter Musik. Internetnutzer verwenden dazu eine Software (Peer-to-Peer-Programm), um die Musik vom Rechner eines anderen Nutzers herunterzuladen. SABAM hatte in einem Urheberrechtsstreit einen Internet-Service-Provider zwingen wollen, den Datenaustausch seiner Kunden zu kontrollieren. Der Provider sollte zum Schutz von Urheberrechten auf eigene Kosten ohne zeitliche Beschränkung für sämtliche Kunden generell und präventiv ein Filtersystem für alle eingehenden und ausgehenden elektronischen Nachrichten, die mittels seiner Dienste, insbesondere unter Verwendung von Peer-to-Peer-Programmen durchgeführt werden, einrichten. Es sollten solche Datenpakete herausgefiltert und blockiert werden, die ein Musikwerk, ein Filmwerk oder audiovisuelles Werk enthalten, für welches SABAM Rechte vertritt.

Die Richter halten eine solche Filterung zur Ermittlung von Urheberrechtsverletzungen für un-

zulässig. Sie wiederholen ihre Beurteilung aus vorangegangener Entscheidung, dass nationale Vorschriften unter den EU-Richtlinien einen Provider nicht verpflichten dürften, sämtliche Daten jedes einzelnen Kunden aktiv zu überwachen, um jeder künftigen Verletzung von Rechten des geistigen Eigentums vorzubeugen. Solche Totalüberwachungen seien unzulässig.

Zwar würde das Urheberrecht einen hohen Schutz genießen. Dieser Schutz sei jedoch nicht unbedingt, sondern unter Achtung anderer Grundrechte zu gewährleisten. Der Schutz der unternehmerischen Freiheit, die Wirtschaftsteilnehmern wie den Providern zukomme, würde zu wenig beachtet, wenn sie ein solches totales Filtersystem einrichten müssten.

Außerdem würden die Datenschutzrechte der Kunden des Providers unangemessen eingeschränkt. Dabei argumentiert der EuGH zugleich mit der Einordnung der IP-Adresse als personenbezogenes Datum („[...] IP-Adressen der Nutzer [...], wobei es sich bei diesen Adressen um personenbezogene Daten handelt, da sie die genaue Identifizierung der Nutzer ermöglichen.“) Allerdings bezieht sich diese Aussage im Urteil auf die Identifizierbarkeit durch den Provider. Die endgültige gerichtliche Klärung der Frage, wann IP-Adressen personenbezogene Daten sind, bleibt weiterhin aus.

Nicole Schmidt

Ungarn verschärft Datenschutzrecht

Mit Wirkung zum 1. Januar 2012 wird Ungarn das nationale Datenschutzrecht verschärfen. Die Datenschutzaufsichtsbehörde erhält stärkere Be-

fugnisse, der Verwaltungsaufwand für die Unternehmen steigt und die Sanktionsmöglichkeiten bei Datenschutzverletzungen nehmen zu.

Stichworte

Ungarn
Datenschutzgesetz

Internet

www.privacylaws.com/int_eneews_August11

Anzeige

Hans Gliss

StichworteSchadenstiftende Software
Social Engineering
Internet-Betrug

Der Datenschutzbeauftragte informiert: Betrug im Internet dramatisch zugenommen - Warnung vor neuen Tricks

Die Überlistung gutgläubiger Internetnutzer hat gewaltig zugenommen, wie das auf Internetsicherheit spezialisierte Unternehmen Kaspersky jüngst berichtet. In der Fachwelt des Internet nennt man dies „Social Engineering“: Durch Vorgaukeln eines seriösen Hintergrunds soll der Geschädigte zu Handlungen bewegt werden, die dem Angreifer entweder die Kontrolle des attackierten PC oder direkten Zugriff auf sein Geld oder seine schätzenswerten Daten verschaffen. Dergleichen kann am Arbeitsplatz wie zuhause relevant sein. Deshalb informiere ich Sie über die jüngsten Tricks.

Bettelbriefe aus Afrika, die an das Mitleid appellieren, werden inzwischen „gestuft“ abgeschickt, die Texte werden immer dramatischer. Löschen und auf keinen Fall Anhänge öffnen!

„Offizielle“ Mails von Behörden oder Banken sollen Sachverhalte vortäuschen, auf die anscheinend zu reagieren wäre. Auch hier: Ungesehen löschen! Behörden und Banken wenden sich niemals per E-Mail an Bürger oder Kunden.

Dann gibt es immer wieder Aufforderungen zur Zusammenarbeit. Einem Kölner Datenschutzbeauftragten wurde am 11.11. (!) ein Geschäft von einem Bankier in Hongkong angetragen, wo es um 44,5 Mio Dollar gehen sollte; 50 Prozent davon sollte der Partner erhalten. Solche aberwitzigen Angebote entlarven sich von selbst. Aber subtiler kann es vielleicht klappen: Internetnutzer bekommen unter der angeblichen Adresse von McDonald's das Angebot, 80 US-\$ auf ihr Kreditkartenkonto gutgeschrieben zu bekommen, wenn sie sich an einer Umfrage des Unternehmens be-

teiligten. Klar, dass es hier um die Abschöpfung der Kreditkartennummer ging. Kein seriöses operierendes Unternehmen käme auf die Idee, eine derartige „Umfrage“ zu starten.

Was auch zu beobachten ist: Man bekommt von einer Adresse, die man kennt, eine Mail, in der es um einen Link geht, den man anklicken möge. Hände weg! Internet-Adressen können durch Eindringen in einen PC gekapert werden, dazu die Liste der Korrespondenzpartner. Nun kann sich jemand als Korrespondenzpartner darstellen, um die PC der Partner ebenfalls zu kapern. Das ist der Anfang eines Netzes zum Versenden von Spam oder krimineller Attacken. Besonders schlimm: Diejenigen, deren Mail-Adresse missbraucht wurde, können nicht beweisen, dass die Schadenssoftware fremdgesteuert verschickt wurde. Und dann ist man möglicherweise zivil- und strafrechtlich haftbar.

Meine Bitte: Seien Sie am Arbeitsplatz wie zuhause misstrauisch und vorsichtig. Wenn jemand, dessen Adresse Sie kennen, Ihnen Seltsames schickt, kontaktieren sie ihn auf einem anderen Weg, um zu erfahren, ob die Mail von ihm stammt. Und bedenken Sie: Betriebliche Firewalls schirmen vieles ab, was verdächtig ist. Wenn es jemand auf Sie und Ihr Wissen abgesehen hat, wird er sich eher Erfolg versprechen, wenn er versucht, Sie auf der privaten Ebene zu erwischen. Hier verschwimmen die Grenzen zwischen betrieblicher und privater Sphäre – und das ist Internetgaunern durchaus bekannt.

Ihr Datenschutzbeauftragter

www.datenschutz-berater.de

Der Datenschutz-Berater erweitert kontinuierlich seinen Internetauftritt unter www.datenschutz-berater.de. Alle Leser (auch Nicht-Abonnenten) können die Suchfunktion des Online-Archivs nutzen; für Abonnenten sind alle Beiträge im Volltext zugänglich. Die Suchmaschine (mit Volltextsuche) erlaubt eine einfache Recherche in allen DSB-Ausgaben seit dem Jahr 2000.

» Die in vielen Beiträgen angegebenen Internetlinks können in den PDF-Dateien des Archivs angeklickt werden und verlinken direkt auf die jeweils angegebene URL.