

Hans Gliss

Fallstudie Datendiebstahl

Stichwort

Compliance
Datendienstahl
Insidertäter
Datenabfluss

Die Gefahr, Opfer von Datenabflüssen zu werden, wird allgemein unterschätzt. Eine Studie liefert Hinweise. Das mit IT-Sicherheit befasste US-Unternehmen Symantec veröffentlichte am 15. Dezember 2011 die Ergebnisse einer empirischen Studie zum Verhalten interner Datendiebe. Es wurde gezielt nach der „Bedrohung von innen“ gefragt. Hackerbedrohungen von außen, die schon wegen zahlreicher spektakulärer Fälle eher wahrgenommen werden, waren kein Gegenstand der Untersuchung.

Aus der Veröffentlichung geht leider nicht hervor, wie viele Befragungen tatsächlich durchgeführt wurden. Eine der zitierten Quellen spricht von 550 Befragungen. Man darf also trotz dieses methodischen Fehlers davon ausgehen, dass die Studie – in den Vereinigten Staaten durchgeführt – breit angelegt war und die Aussagen repräsentativ sind. Die Ergebnisse dürften damit auch auf Europa übertragbar sein.

Täterstruktur

Die Studie definiert die internen Datendiebe als meist in technisch orientierten Jobs angesiedelt, zweite Hälfte Dreißig, also da, wo man sich auf die Midlifecrisis vorbereitet und überlegt, wie man sein Insiderwissen gewinnbringend vermarkten kann. Dass sie auf Geheimhaltung verpflichtet sind, ist den Tätern schnuppe, wenn das schnelle Geld lockt. Systemtechnische Wege zum

Datenabfluss sind beliebt, weil man mit diesen Dingen umzugehen gewohnt ist. Hier setzt die Kritik an den Betreibern ein, die es Datendieben allzu leicht machen, sich der Kommunikationsmechanismen zu bedienen, die eigentlich für Firmenbelange installiert sind.

Besonders anfällig sind Mitarbeiter, die sich „innerlich verabschiedet“ haben. Die Studie behauptet, dass 65 Prozent der Innentäter zum Zeitpunkt des Datendienstahls bereits einen Vertrag mit einem anderen Unternehmen hatten, das vom Verrat profitierte. Auch die Zahl der ermittelten Zugangsmöglichkeiten ist erschreckend: In 75 Prozent der Fälle hatten Mitarbeiter Zugang zu Daten, mit deren Umgang sie vom Arbeitsplatz her autorisiert waren. Ausspionieren fand also kaum statt. Man bediente sich einfach an dem, was man ohnehin einsehen und kopieren durfte (bei der Frage des Kopierens hört eigentlich der Spaß auf, hier geht es um strenge Berechtigungskonzepte).

Wer sich mit Korruptionsbekämpfung befasst und den Spagat zwischen Datenschutz (streng limitierte Auswertung von Daten) und existenzbedrohlichen Informationsabflüssen bewältigen muss, sollte sich die Studie näher ansehen. Zumindest dient sie zur Sammlung von Fakten für Entscheidungsträger, die Datenschutzbeauftragte in diesem schwierigen Geschäft zu beraten haben.

Internet

www.symantec.com/content/en/us/about/media/pdfs/symc_malicious_insider_whitepaper_Dec_2011.pdf?om_ext_cid=biz_soc_med_de_pv_061211_symantec_socialmedia_MaliciousInsiderWP

Nicole Schmidt

The Right to Privacy

Stichworte

Recht auf Privatheit

Bereits im Jahr 1890 entwickelten Samuel D. Warren und Louis D. Brandeis in einem Aufsatz das Recht auf Privatheit. Ursächlich dafür waren die Erfindungen und Geschäftsmethoden der Presse der damaligen Zeit. Die Autoren forderten die Möglichkeit des Schutzes des Einzelnen vor

dem Eindringen der Zeitungen in das Privatleben und damit die Unterbindung des Geschäfts mit den Informationen. Der Beitrag wurde nun durch die Leitung des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein ins Deutsche übersetzt.

Internet

www.datenschutzzentrum.de/allgemein/20111219-Warren-Brandeis-Recht-auf-Privatheit.html

Nicole Schmidt

Bedrohungsszenarien 2012

Das Risiko der IT-Bedrohungen wird auch in 2012 nicht sinken. Nachfolgend sind auszugswise die Ausblicke von zwei IT-Security-Unternehmen aufgeführt. Die vollständigen Prognosen finden Sie unter den angegebenen Links.

Das Information Security Forum (ISF), eine der weltweit größten unabhängigen Organisationen für Informationssicherheit, sieht die folgenden Bedrohungen: (1) Consumerisation der IT. Mitarbeiter wollen mit ihren privaten mobilen Endgeräten auf geschäftliche Informationen zugreifen. Auf den Arbeitsplatzrechnern werden vielfach Webanwendungen mit ungetesteten Codes vorgehalten, die die Unternehmenssicherheit gefährden. Lokalisierungsdaten von GPS-fähigen Geräten können missbraucht werden. (2) Cyber (In)security. Das Gefahrenpotential des vernetzten Datenaustauschs und die damit einhergehenden Möglichkeiten der Wirtschaftsspionage, der Verletzung von Persönlichkeitsrechten und der negativen Beeinflussung von IT-Infrastruktur wird zunehmen. (3) Cloud-Sicherheit. Im

kommenden Jahr werden sich die IT-Verantwortlichen mit der Datensicherheit in der Datencloud beschäftigen. (4) Datenverlust. Informationsaustausch über soziale Netzwerke, Open Source-Applikationen oder Wikis bieten Hackern einfache Angriffspunkte und müssen gesichert werden.

Imperva, ein Anbieter von Datensicherheitssystemen, sieht folgende Trends: (1) Die Anzahl der Attacken auf das https-Protokoll wird zunehmen. (2) Cyberkriminelle werden ihre Malware verstärkt in Browser-Sicherheitslücken ablegen. (3) Die Onlinetäter werden effektivere Denial of Service (DDoS)-Angriffe starten und auch die Anwendungs- und Geschäftslogikebene angreifen. (4) Die Nutzung von NoSQL stellt eine Gefahr dar, es gibt zu wenige Sicherheitsexperten hierfür. (5) Informationen in sozialen Netzwerken können Ziel von automatisierten Angriffen werden. (6) Ein neu geschaffener „Hacking-Mittelsmann“ (Broker) wird die Vermittlung von Verkäufer und Käufer von gestohlenen Daten übernehmen.

Stichworte

Bedrohungsszenarien
Informationssicherheit

Nicole Schmidt

UK: Bußgelder gegen County Council

Das Information Commissioner's Office (ICO) hat Bußgelder gegen den North Somerset Council und den Worcestershire County Council wegen Verletzungen des Datenschutzrechts verhängt. Beide Institutionen haben sehr sensible persönliche Informationen an die falschen Empfänger weitergegeben. Das Worcestershire County Council verschickte eine E-Mail mit hoch sensiblen persönlichen Informationen an 23 unbeabsichtigte Adressaten. Das ICO setzte eine Strafe von £ 80.000,- fest und bemängelte das Fehlen

eines Mitarbeitertrainings und von Zugangsbeschränkungen zu Informationen. Das North Somerset Council muss £ 60.000,- zahlen. Ein Beschäftigter versendete fünf E-Mails an einen unzuständigen National Health Service-Mitarbeiter; zwei E-Mails enthielten sensible, vertrauliche Angaben über ein Kind. Besonders prekär: Nach der Aufdeckung des Sachverhalts wurde die E-Mail noch dreimal an die falschen Empfänger verschickt. Das ICO bemängelte auch hier die mangelnde Datenschuttschulung.

Stichworte

UK
Bußgelder
Datenpanne

Internet

[www.ico.gov.uk/
what_we_cover/
taking_action/dp_pecr.
aspx#monetarypenalties](http://www.ico.gov.uk/what_we_cover/taking_action/dp_pecr.aspx#monetarypenalties)

Stefan Felixberger

Online-Dialogmarketing

Der Technologieanbieter Artecic AG fasst in einem Whitepaper das Thema „Datenschutzkonforme Profilierung von Reaktionsverhalten im Online Dialogmarketing“ zusammen. Es geht

vor allem um den rechtskonformen Aufbau von Kundenprofilen mit verhaltensbezogenen Reaktionsdaten und den Einsatz der Privacy Admission Control® Funktion der Lösung ELAINE FIVE.

Stichworte

Online-Marketing
Dialogmarketing
Artecic

Internet

[www.artecic.net/files/0,0/1111/
artecic_whitepaper_privacy_
admission_control_web.pdf](http://www.artecic.net/files/0,0/1111/artecic_whitepaper_privacy_admission_control_web.pdf)

Nicole Schmidt

Stichwort
mobile Endgeräte

Studie: Mobile Endgeräte als Risiko

IT-Verantwortliche sehen in der Einbindung von mobilen Endgeräten in die Unternehmensnetzwerke ein erhebliches Risiko. Das zeigt die Studie „Mitigating Risk in a Mobile World“ von IDG Research Services und Symantec. 59 Prozent der Befragten gaben an, dass sie keine oder nur mäßig effektive Mittel gegen die – durch mobile

Endgeräte verursachten Gefahren – vorhalten. Lediglich 44 Prozent sagten, dass Applikationen die Anwender an der Verletzung von internen Nutzungsvorgaben hindern. Für die Studie wurden 115 IT-Verantwortliche befragt.

Internet
www.csoonline.com/whitepapers/symantecmobile

Nicole Schmidt

Stichworte
Google Translate

Schwachstelle in Google Translate API v2

IceWrap, ein Anbieter von Messaging-Lösungen, hat eine Schwachstelle in dem kostenpflichtigen Übersetzungsdienst „Google Translate API V2“ entdeckt. Cyberkriminelle können die Software einfach kapern und unerwünschte Gebühren für den ahnungslosen Anwender auslösen. Allerdings

muss der User vorher seine Zugangsdaten in eine öffentlich zugängliche Javascript-Datei einfügen. IceWarp hat die Google Applikation in ihr Programm „LiveWebAssist“, einen mehrsprachigen Business-Chat-Dienst integriert und den Sicherheitsfehler behoben.

Internet
www.icewarp.com

Nicole Schmidt

Stichwort
Dokumentenmanagement

Externes Dokumentenmanagement

Die neu gegründete REISSWOLF Köln Archivservice GmbH bietet Lösungen im externen Dokumentenmanagement an. Dazu zählen das Digitalisieren von physischen Akten, die Einlagerung von Dokumenten in Sicherheitsarchiven und die

Anlieferung von angeforderten Unterlagen nebst der anschließenden Wiedereingliederung in das Archiv. Der Auftraggeber kann die Aktenbewegung über das Internet verfolgen.

Internet
www.reisswolf-koeln.de

Nicole Schmidt

Stichworte
Phishing

Der Datenschutzbeauftragte informiert: Phishing-Versuch

Cyberkriminelle regionalisieren vermehrt ihre Phishing-Kampagnen; dadurch versprechen sie sich eine höhere Erfolgsquote. Zu diesem Ergebnis kommt der eleven E-Mail Security Report 2011. So täuschen die Täter als Absender ein regionales Kreditinstitut vor und erhoffen durch die Verwendung von sprachlich verbesserten Texten die Eingabe von vertraulichen Bank- und Kreditkartendaten auf ihren Phishing-Seiten. Entsprechend trat die Deutsche Bank in Erscheinung. Die Täter lockten die Opfer mittels eines Links in der E-Mail auf eine Seite mit der URL: „meine.deut-

sche-bank.de“. Das äußere Erscheinungsbild entsprach dem originalen Layout, auch werden Teile der Website aus der Originalseite geladen. Im Gegensatz dazu verwies der entscheidende Login-Link auf eine Seite der Phisher; der User sollte im Rahmen einer Kontobestätigung vertrauliche Daten eingeben. Anschließend erfolgte eine Weiterleitung auf die richtige Seite der Deutschen Bank. Zu den weiteren Opfern von Phishing-Kampagnen gehören: Postbank, Mastercard, Visa und PayPal.

Internet
www.eleven.de/eleven-security-reports-reader/items/eleven-e-mail-security-report-dezember-2011.html