secorvo
security consulting

Secorvo Security News

März 2011

Krisenmanagement

Die entsetzliche Naturkatastrophe in Japan hat die Industrienationen dieser Welt in einen Schockzustand versetzt. Mehr noch als die gerne verdrängte Einsicht, dass lange drohende Naturkatastrophen eben doch eines Tages eintreten, erschreckt die Erkenntnis, dass das Krisenmanagement eines so hoch entwickelten und in Qualitätsfragen vorbildlichen Landes wie Japan geradezu hilflos wirkt.

So hielten die Hochhäuser dank präventiver Maßnahmen dem gewaltigen Erdbeben der Stärke 9 stand, nachdem das mit 20 Sekunden deutlich kürzere und schwächere Beben der Stärke 7 vor 16 Jahren in Kobe Häuser und Brücken wie Streichhölzer einknicken ließ.

Die Notfallvorsorge hingegen versagte. Stimmen die Berichte, dann haben Mängel in der Versorgung der Überlebenden des gigantischen Tsunami weitere Todesopfer gekostet. Angesichts der Kritik am Krisenmanagement nach der Kobe-Katastrophe erscheint dies wie ein Déjà-vu. Inzwischen ist zudem bekannt, das der Betreiber des havarierenden Kernkraftwerks zahlreiche Inspektionen versäumt hatte – darunter die des Kühlsystems. Möglicherweise waren die Notstromaggregate also bereits vor dem Tsunami defekt.

Notfallvorsorge bedeutet, sich auf den Umgang mit einem Ereignis vorzubereiten, dessen Eintritt man zugleich durch präventive Maßnahmen zu verhindern sucht. Das ist ein „mentaler Spagat", der oft zu Lasten der Notfallvorsorge ausgeht, da Menschen dazu neigen, die Wirksamkeit ihrer präventiven Maßnahmen zu überschätzen – weil „nicht sein kann, was nicht sein darf".

Dafür gibt es auch in der IT-Sicherheit zahlreiche Beispiele – wie Backup-Bänder, deren Rückspielbarkeit nicht regelmäßig überprüft wird oder Notfallpläne, die auf falschen Annahmen beruhen (wie der Verfügbarkeit von Strom, Telefon oder Internet). Zwar geht es hier meist nicht um „Leib und Leben". Dennoch gilt: Wer die Krisenreaktion nicht übt, wird sie im Ernstfall nicht beherrschen.

Inhalt

secorvo
security consulting

Security News

Datenschutzkonformes Webtracking

Wer die Zugriffsstatistiken seiner Webseitenbesucher datenschutzkonform auswerten wollte, musste sich lange Zeit mühen, eine brauchbare Alternative zu Google Analytics zu finden. Zwar hat Google als Reaktion auf den „Bann" der deutschen Aufsichtsbehörden (SSN 08/2010) im vergangenen Jahr eine Möglichkeit geschaffen, IP-Adressen der Seitennutzer so zu kürzen, dass sie nicht mehr zurückverfolgt werden können. Die Datenverarbeitung in den USA ohne angemessenen Schutz verhinderte jedoch nach wie vor einen rechtskonformen Einsatz in Deutschland. Die Datenschutz-Aufsichtsbehörden nahmen dies zum Anlass, den Einsatz von Google Analytics und anderer Tracking-Tools zunehmend abzumahnen – nicht immer mit glücklicher Hand (SSN 01/2011).

Als Alternative zu Google Analytics wird seit einer Weile das Open-Source-Tool PIWIK diskutiert. Für einen datenschutzkonformen Einsatz muss es allerdings angepasst werden – und genau dafür hat am 15.03.2011 das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) nach einer aufsichtsbehördlichen Analyse eine Arbeitshilfe publiziert. Unternehmen, die weiterhin Google Analytics auf ihren Webseiten nutzen, haben nun nicht einmal mehr eine schlechte Ausrede, wenn sie ein Bußgeldbescheid der Aufsichtsbehörde erreicht.

Legalisierte PIN-Weitergabe?

Am 09.03.2011 hat das Bundeskartellamt nach Auskunft der Payment Network AG eine Stellungnahme zu der am Landesgericht Köln anhängigen Klage der Giropay GmbH abgegeben. Darin wirft Giropay dem Betreiber von sofortüberweisung.de wettbewerbswidriges Verhalten durch die Anstiftung zum Verstoß gegen die Muster AGB der Banken vor. Hintergrund ist das in diesen AGB verankerte Verbot, die Authentifizierungsmittel für das Online-Banking (Login-ID, PIN und TAN) an Dritte weiterzugeben. Genau dies ist jedoch erforderlich, um im Rahmen von Internetgeschäften eine von sofortüberweisung.de unterstützte, in den Kaufprozess eingebundene Überweisung vorzunehmen. Das Bundeskartellamt sieht nach den eingeleiteten Ermittlungen Hinweise darauf, dass durch das Verbot der Weitergabe der Authentisierungsmittel bankenunabhängigen Direktüberweisungsverfahren der Marktzutritt verwehrt wird.

Noch ist offen, wie das LG Köln und die vermutlich folgenden Instanzen den Sachverhalt bewerten werden. Allerdings erscheint fraglich, dass das Bundeskartellamt die Klausel der AGB in ihrer Bedeutung richtig erfasst hat. Für die Sicherheit des Online-Bankings ist die Geheimhaltungsklausel berechtigt, und es darf bezweifelt werden, dass ein Geschäftsmodell, das die Herausgabe der für einen persönlichen Authentisierungsprozess verwendeten Geheimnisse an Dritte erfordert, überhaupt kartellrechtlichen Schutz genießen kann.

Desaster I

Mehrere Security-Unternehmen wurden in den vergangenen Wochen Opfer von viel beachteten Angriffen. Dabei betreffen die Angriffe auf RSA und Comodo auch die Sicherheit der Kunden und weiterer Anwender.

RSA – Hersteller der SecurID Einmalpasswort-Token und inzwischen Teil von EMC – teilte am 17.03.2011 mit, dass das Unternehmen Opfer eines längerfristigen gezielten Angriffs (Neusprech: APT) geworden war. Aus der Mitteilung geht hervor, *dass* ein Schaden für SecurID eingetreten ist – lässt aber offen, *worin* dieser genau besteht und *wie* er sich auswirkt. Dem Vernehmen nach informiert RSA derzeit seine großen Kunden einzeln und unter NDA über Details. Spekulationen zufolge könnte zumindest ein Teil der Datenbank mit den Seed-Werten, aus denen sich alle One-Time-Passwörter aller registrierten Token rekonstruieren lassen, den Angreifern in die Hände gefallen sein. Dann würde nur noch ein Austausch der betroffenen Token helfen.

Desaster II

Am 15.03.2011 wurde eine für die Prüfung von SSL-Zertifikatsanträgen zuständige Registration Authority (RA) der von Comodo (Claim: „Creating Trust Online") betriebenen CA UTN-UserFirst-Hardware kompromittiert. Der vorgeblichlich iranische Angreifer konnte mit deren Zugangsdaten fingierte Zertifikate für Domains wie Google.com und Yahoo.com beziehen – ein Blankoscheck für Phisher. Comodo informierte am 23.03.2011 darüber und veröffentlichte den zugehörigen Incident Report.

Bereits zuvor hatten viele Browserhersteller Patches erstellt, um die falschen Zertifikate unabhängig von den üblichen PKI-Sperrmechanismen zurückzuweisen. Besondere Übung hierin hat Microsoft, das bereits seit 22.03.2001 zwei fingierte „Microsoft Corp." Code-Signing-Zertifikate auf diese Weise aus Windows aussperrt. Falls die Angreifer allerdings wie behauptet noch weitere, nicht identifizierte Zertifikate oder Zugangsdaten erbeutet haben, bliebe letztlich nur, die betroffenen CAs komplett als Vertrauensanker zu entfernen – mit unschönen Konsequenzen auch für alle legitimen Zertifikate.

Beide Fälle belegen, dass selbst in sicherheitskritischen Branchen noch nicht alle Unternehmen ver-

standen haben, dass das langfristige Vertrauen von Kunden und Anwendern in einem solchen Fall nur mit Offenheit, Kulanz und schneller Schadensbegrenzung zurück gewonnen werden kann – und nicht mit vagen Andeutungen, Geheimniskrämerei oder Verharmlosung. Gerade von Anbietern im Bereich der IT-Security sollte man zudem erwarten dürfen, dass sie Notfallpläne für „ihr" Worst-Case-Szenario in der Schublade liegen haben.

Schwierige Trennung

Am 23.03.2011 hat das Bundesarbeitsgericht die vorangegangenen Urteile zum Umfang des Kündigungsschutzes eines betrieblichen Datenschutzbeauftragten bestätigt. Kern des Streits war der gesetzliche Kündigungs- und Widerrufsschutz des betrieblichen Datenschutzbeauftragten aus den §§ 4f Abs. 3 BDSG, 626 BGB einerseits und das Bestreben eines Unternehmens, konzernweit einen einheitlichen externen Datenschutzbeauftragten statt des internen zu etablieren andererseits. Sämtliche Instanzen haben den Wunsch nach einer Neuorganisation des Datenschutzes ebenso wie mögliche Konflikte durch die gleichzeitige Zugehörigkeit zum Betriebsrat nicht als wichtigen Grund gemäß § 626 BGB anerkannt.

Wie das klagende Unternehmen zu Recht vorgetragen hat, hat diese – auch schon zuvor in der einschlägigen Literatur vertretene – Rechtsauffassung zur Folge, dass ein unbefristet bestellter interner Datenschutzbeauftragter ohne sein Mitwirken praktisch nicht mehr abgelöst werden kann.

Rückkehr der Dialer

Bei der Sicherheit von VoIP wird der Fokus gern auf Vertraulichkeit, Integrität und Authentizität gelegt. Diese Sicherheitsziele sind meist jedoch weniger kritisch, solange VoIP nur hausintern betrieben wird. Eine erhebliche Gefahr ist hingegen der Gebührenbetrug. Durch die Vereinigung von Daten- und TK-Netzen werden Angriffe möglich, die die längst totgeglaubten Dialer wieder zum Leben erwecken. Insbesondere Softphones sind stark gefährdet.

So berichtete Mark Collier am 09.03.2011 in seinem VoIP Security Blog von einem Fall, in dem durch die Installation von Dialern acht Millionen US-Dollar „erwirtschaftet" wurden. Der Urheber dieses Betruges wurde ermittelt und zu sieben Jahren Haft verurteilt. Solche Dialer können lange unbemerkt bleiben, wenn der Betrüger nicht zu gierig wird, denn gelegentliche kurze Anrufe an Servicenummern dürften in der Praxis kaum auffallen.

Bei Softphones kommen zudem zwei Angreiferwelten zusammen: Sofern es die Browser-Konfiguration zulässt, wird ein SIP-URI in einem HTML-Dokument an das Softphone weitergereicht – ein Himmelreich für Phisher. Von solchen Angriffen sind auch Smartphones betroffen, wie ein am 28.02.2011 bekannt gewordenes Android-App belegt.

Angesichts der geringen Aufmerksamkeit für diese Bedrohung steht zu befürchten, dass die schmerzlichen Lektionen mit herkömmlichen Endgeräten ignoriert und erneut gelernt werden müssen.

Secorvo News

PKI lesen und erleben

Seit dem 01.03.2011 stehen auf der Secorvo-Webseite zwei neue Whitepaper zum Download bereit: Eine Einführung in „Public Key Infrastrukturen" von Petra Barzin und eine Schritt-für-Schritt-Anleitung zur Realisierung einer „PKI von der Stange" von Hans-Joachim Knobloch. Vom **10.–13.05.2011** können Sie auf dem viertägigen Secorvo College Seminar „PKI – Grundlagen, Vertiefung, Realisierung" beide Autoren persönlich kennen lernen. Sie bieten Ihnen einen detaillierten und praxisorientierten Einblick in Konzeption, Implementierung und Nutzung von PKIs.

Alle IT-Sicherheit geht von Karlsruhe aus

Vor mehr als 25 Jahren wurden an der Universität Karlsruhe – dem heutigen KIT – die ersten Vorlesungen zu Kryptographie, technischem Datenschutz und Informationssicherheit in Deutschland gehalten. Zahlreiche Lehrstühle an deutschen Hochschulen und Unternehmen im Gebiet IT-Sicherheit haben ihre Wurzeln in Karlsruhe, ebenso wie das „Europäische Institut für Systemsicherheit (EISS)".

Am 28.02.2011 wurde das EISS/KIT vom Bundesforschungsministerium zum „**K**ompetenzzentrum für **a**ngewandte **S**icherheits-**Te**chno**l**ogie" ernannt. Was KASTEL in der Zukunft zur IT-Sicherheit in und aus der Region Karlsruhe beitragen wird, stellt Prof. Dr. Jörn Müller-Quade, Leiter des EISS, auf dem kommenden KA-IT-Si-Event am **14.04.2011** vor. Beginn: 18 Uhr im Schlosshotel Karlsruhe, mit anschließendem Buffet-Networking (Anmeldung).

SSN-Symposium

Nach dem überschwänglichen Feedback zu unserem „Security News Symposium" im vergangenen Jahr freuen wir uns, Sie heute zu unserem zweiten SSN-Symposium am **31.05.–01.06.2011** in die Buhlsche Mühle einladen zu können – mit spannenden Vorträgen und Diskussionen zu Security- und Datenschutzfragen rund um VoIP, IPv6, Webtracking, Skimming und Online-Banking. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2011	
12.-13.04.	a-i3/BSI-Symposium 2011 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
Mai 2011	
10.-13.05.	Public Key Infrastrukturen (PKI) (Secorvo College)
10.-12.05.	12. Deutscher IT-Sicherheitskongress (BSI, Bonn)
12.-15.05.	Swiss Cyber Storm 3 Security Conference (Compass Security AG, Rapperswil/CH)
17.-20.05.	12. Datenschutzkongress (Euroforum, Berlin)
24.-27.05.	ISSECO Certified Professional for Secure Software Engineering - CPSSE (Secorvo College)
31.05.-01.06.	2. Security News Symposium (Secorvo, Karlsruhe/Ettlingen)
Juni 2011	
06.-07.06.	DuD 2011 (Computas, Berlin)
06.-11.06.	T.I.S.P.-Schulung und -Prüfung (Secorvo College)
06.-11.06.	OWASP Global AppSec Europe (OWASP Foundation, Dublin/IE)
28.-30.06.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)

Fundsache

Anfang März publizierte das US-amerikanische NIST die 88seitige Special Publication 800-39 zum Thema „Managing Information Security Risk“ – ein lesenswerter systematischer und aktueller Überblick.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Karin Schuler

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de