secorvo
security consulting

Secorvo Security News

August 2011

Risiko-Awareness

Bruce Schneier – ein verlässlicher Garant für originelle und scharfsinnige Einschätzungen – veröffentlichte im Februar 2007 ein bemerkenswertes Essay zur „Psychologie der Sicherheit“ (aktualisiert im Januar 2008). Darin fasst er zahlreiche Erkenntnisse der Psychologie zur Risiko-Wahrnehmung zusammen, die vor allem eines deutlich machen: Menschen schätzen Risiken immer wieder falsch ein – selbst dann, wenn sie über genügend Informationen verfügen.

Zwar geben wir vor (und bemühen uns bisweilen), Risiken nüchtern zu analysieren. Tatsächlich aber dominieren intuitive Bewertungen unser Handeln. So neigen wir dazu, spektakuläre, plötzliche und extern verursachte Risiken – wie die Gefahr einer Atomkatastrophe nach den Ereignissen in Fukushima – überzubewerten, während wir unerwünschte Risiken, die zudem nicht uns, sondern andere betreffen, unterschätzen (wie die Gefahr einer Massenpanik bei der Loveparade durch die Verantwortlichen in Duisburg).

Auch „gewohnte“ Risiken (wie die ca. 4.000 Verkehrstoten pro Jahr) werden meist unterbewertet – niemand lässt deshalb sein Auto stehen –, während bei neuen Risiken, über die gesprochen wird und die uns oder unsere Kinder direkt bedrohen – wie die EHEC/HUS-Infektion mit 50 Toten – gleich die halbe Nation den Verzehr von Gemüse einstellt.

So ergeht es uns auch mit Unternehmensrisiken. Weder ein Mehr an Information noch die Etablierung von Risikoanalyseverfahren wird daran etwas ändern – denn, wie Bruce Schneier zutreffend folgert, werden wir nur dann zu zutreffenden Risikobewertungen und angemessenen Reaktionen kommen, wenn „unser Sicherheitsgefühl mit der Sicherheitswirklichkeit übereinstimmt“.

Um das zu erreichen helfen intensive Risikodiskussionen wohl eher als trockene Analysen – und Awareness-Maßnahmen, die diffuse, anonyme, schleichende, verschwiegene und unerwünschte Risiken in unsere und die Wahrnehmung der Verantwortlichen rücken.

Inhalt

secorvo
security consulting

Security News

Mobile Keylogger

Keylogger, die Tastatureingaben protokollieren, wären auch auf Smartphones keine Überraschung – ließen sich aber auch dort recht leicht erkennen. Am 09.08.2011 zeigten jedoch zwei Forscher der University of California auf dem 6. USENIX Workshop HotSec, wie man in Android-Handys aus den Bewegungssensoren einen Keylogger macht.

Zwar verfügt Android über eine Instanz, die den Zugriff auf bestimmte Ressourcen (Adressbuch, Telefon, Netzwerk ...) regelt. Möchte ein Programm eine dieser Ressourcen nutzen, muss der Entwickler dies „anmelden". Bei der Installation der „App" erhält der Benutzer eine Liste der Ressourcen, die das Programm nutzen möchte. Erscheint die Liste dem Nutzer nicht angemessen – etwa weil ein Kartenspiel Zugriff auf das Netzwerk, das Adressbuch usw. haben möchte – kann er sich gegen eine Installation entscheiden. Die Nutzung des Bewegungssensors dürfte allerdings den meisten Nutzern unverdächtig erscheinen.

Auch bei Smartphones ist spätestens jetzt die Zeit der „erkennbar harmlosen Anwendungen" vorbei. Ohne Personal Firewalls mit cleveren Heuristiken kann man nicht davon ausgehen, dass nur der Nutzer auf Daten und Anwendungen zugreifen kann.

Kai su teknon, Facebook

Trackingdienste zur Reichweitenmessung von Websites beschäftigen bereits seit geraumer Weile die Datenschutzaufsichtsbehörden (SSN 08/2010). Nach einer nun veröffentlichten eigenen Untersuchung hat das ULD Schleswig-Holstein am 19.08.2011 eine Aufforderung an sämtliche verantwortlichen Stellen des Landes gerichtet, die Verwendung der von Facebook angebotenen Social Plugins zu unterlassen.

Grund sind die von Facebook verwendeten Cookies sowie die nachweislich erfassten Daten und vorgenommenen Verknüpfungen: Beim Aufruf von Webseiten, die z. B. den Facebook „Like-me"-Button nutzen, werden sowohl angemeldete als auch nicht angemeldete Nutzer von Facebook erfasst. Das Zusammenführen dieser Nutzungsdaten mit Facebookprofilen ist dank der Cookies über die Dauer von zwei Jahren möglich. Eine solche Verknüpfung stellt einen Verstoß gegen § 15 Abs. 3 TMG dar.

Weder die Webseiten-Anbieter noch Facebook halten hierfür ausreichende Erklärungen zum Zweck und Umfang dieser Datenerhebungen bzw. –übermittlungen vor; ein klarer Verstoß gegen § 13 Abs. 1 TMG. Nach der seit dem 25.05.2011 direkt anwendbaren Änderung von Art. 5 Abs. 3 der europäischen Datenschutzrichtlinie für elektronische Kommunikation (RL 2009/136/EG) ist zudem die Einwilligung des Nutzers vor dem Setzen solcher Cookies erforderlich, was bislang allgemein missachtet wird.

Für den Fall der Zuwiderhandlung hat das ULD ab Oktober 2011 Untersagungsverfügungen nach § 38 Abs. 5 BDSG angekündigt. Vielleicht wird so die Beachtung des Datenschutzrechts zum Wettbewerbsfaktor zwischen Social Networks. Ein erster Schritt wäre eine ausreichende Transparenz der Anbieter über ihre Datenverarbeitung.

Siemens S7 Hack

Das ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) warnte am 03.08.2011 vor Schwachstellen in S7-300 SPS-Systemen: Mit auf der diesjährigen Black Hat vorgestellten Exploits von Dillon Beresford können über einen Remote-Zugang Abläufe in der Steuerung verändert werden. Auch wenn andere SPS-Systeme wie die S7-400 von dieser Schwachstelle nicht betroffen sind, ist sehr zu empfehlen, Steuerungssysteme grundsätzlich in eigenen Netz-Segmenten zu betreiben – und schon gar nicht mit dem Internet zu verbinden.

HTML 5 Security

Noch immer sorgen viele alte Sicherheitsprobleme mit Web-Anwendungen für Probleme (siehe SSN 07/2011), da kommt mit HTML 5 neues Ungemach.

Viele der neuen Features von HTML 5 bringen gänzlich neue Angriffsvektoren ins Spiel. Mit Veröffentlichung der Studie „A Security Analysis of Next Generation Web Standards" vom 01.08.2011 sorgt die ENISA hier auf 60 Seiten für eine gute Übersicht. Neue Funktionen von HTML 5 und damit verbundene Sicherheitsprobleme werden ausführlich erläutert – eine Leseempfehlung für alle, die verstehen wollen, welchen Sicherheitsherausforderungen die Entwickler von Web-Applikationen zukünftig gegenüber stehen werden.

Tracking-Tool der IVW

Mit dem Skalierbaren Zentralen Messsystem (SZM) der Fa. INFOnline misst die Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW) seit Ende 2008 die Reichweite von Online-Medien. Der Hamburger Datenschutzbeauftragte Prof. Dr. Caspar hat in einer Presseerklärung vom 08.08.2011 die Bereitschaft der Beteiligten gewürdigt, das SZM, das auch von www.hamburg.de genutzt wurde (SSN 01/2011), hinsichtlich des Datenschutzes anzupassen. Das SZM orientiert sich nun an den Vorgaben des Düsseldorfer Kreises zur

Reichweitenmessung und kürzt das letzte Oktett der IP-Adresse. Außerdem wird ein Opt-Out für die Nutzer angeboten. Die Musterdatenschutzerklärung klärt umfassend über das IVW-Verfahren auf, bleibt allerdings bezüglich der eingesetzten Cookies vage.

Es darf jedoch bezweifelt werden, dass in dieser Sache bereits das letzte Wort gesprochen ist. Auch das SZM verwendet Cookies, die eine längerfristige Wiedererkennung ermöglichen. Es ist wahrscheinlich, dass diese durch das in Art. 5 Abs. 3 der EU-Datenschutzrichtlinie für elektronische Kommunikation (RL 2009/136/EG) geforderte Opt-In erfasst werden, da mindestens ein Identifikator dauerhaft auf dem Endgerät gespeichert wird. Zudem bleiben bislang sämtliche Lösungen der mit dem Nutzertracking verbundenen Probleme unbefriedigend, da sie entweder die meisten Nutzer nicht erreichen (Opt-Out-Cookie), zu Nutzerunfreundlichkeit führen (vorherige Einwilligung) oder die Personenbeziehbarkeit weiterer Daten neben der IP-Adresse außer acht lassen.

SIFT 2.1

Seit dem 04.08.2011 ist das generalüberholte SANS Investigative Forensic Toolkit (SIFT) für registrierte Nutzer verfügbar: ein sehr umfangreicher, hochaktueller forensischer Werkzeugkasten für Gegner einer „one click forensic", der die wichtigsten forensischen Entwicklungen der vergangenen zwölf Monate vereint.

Hervorzuheben sind die weitere Automatisierung der Zeitlinienerstellung mit log2timeline, die Vervollständigung der umfangreichen Sammlung von RegRipper-Plugins sowie die Aktualisierung des Speicheranalysewerkzeugs Volatility 2.0. Bei letzterem ist zu beachten, dass ältere Volatility-Scripts noch zu portieren sind. Thematisch wurde der Bereich Smartphones für die Analyse von iPhone, Blackberry und Android ergänzt. Allerdings genügt SIFT hier nicht allein – gerade bei iPhones ist viel Know-How für die erste Sicherung erforderlich.

SIFT sollte in keinem forensischen Arsenal fehlen; es liegt als verlässliches VMware-Image vor.

Secorvo News

T.I.S.P. – Das Buch

Mitte September wird es endlich verfügbar sein: das Begleitbuch zum T.I.S.P. Es führt, strukturiert in Anlehnung an das T.I.S.P.-Seminar, in die „Zentralen Bausteine der Informationssicherheit" ein. Neun der elf an der Erstellung beteiligten Autoren sind zugleich Referenten der nächsten T.I.S.P.-Schulung vom **17.–22.10.2011** (mit Prüfung) bei Secorvo College; alle Teilnehmer erhalten das Buch zur Vorbereitung vorab zugesandt. Es sind noch wenige Plätze verfügbar – bis zum **12.09.2011** sogar zum Frühbucherpreis.

Die Programme weiterer Seminare und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Budenzauber

Ein wirkungsvoller Informationsschutz steht und fällt mit dem sicherheitsbewussten Verhalten aller Mitarbeiter eines Unternehmens. Doch wie sensibilisiert man die Mitarbeiter nachhaltig für Informationssicherheit? Dieser Frage geht Dirk Fox auf dem kommenden KA-IT-Si-Event am **22.09.2011** im Panoramasaal der IHK Karlsruhe nach. In seinem Vortrag „Security Awareness in der Praxis" fasst er Erfahrungen aus zahlreichen Security Awareness Kampagnen großer und mittelgroßer Unternehmen der vergangenen Jahre zusammen und gibt Empfehlungen für ein wirkungsvolles Vorgehen. Die Veranstaltung beginnt um 18:00 Uhr. Um Anmeldung wird gebeten.

Security-Update 2011

„Für Hacker gibt es kaum noch Grenzen", titelte die WirtschaftsWoche am 01.08.2011. Tatsächlich kann sich heute kein erfolgreiches Unternehmen – und sei es noch so klein – vor Angriffen auf seine Infrastruktur sicher wähnen. In einem Land, das seinen wirtschaftlichen Erfolg Ideenreichtum und Wissen verdankt, setzt ein nachlässiger Umgang mit Daten jedoch die eigene Zukunft aufs Spiel.

Geschäftsführer und Vorstände wissen um diese Risiken – allerdings ändern sich Bedrohungs- und Gesetzeslage ständig. Mit dem „Sicherheits-Update 2011„ am 05.10.2011 wollen LEITWERK, Secorvo und Securiton Abhilfe schaffen: Drei Expertenvorträge geben Einblick in die wesentlichen Fragestellungen – und das anschließende Come Together die Gelegenheit zum Erfahrungsaustausch.

2. Smart Grid Symposium

Nach dem großen Erfolg des „Smart Grid Symposiums" im Februar dieses Jahres freuen wir uns, Sie zu unserem 2. Smart Grid Symposium am **29.–30.11.2011** in der Buhlschen Mühle in Ettlingen einladen zu können. Es erwarten Sie spannende Vorträge rund um den Datenschutz und die Datensicherheit im Smart Grid, u. a. vom Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundesverband der Energie- und Wasserwirtschaft (BDEW) und der EnBW. Werfen Sie einen Blick auf das Programm – wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

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

September 2011	
13.-14.09.	Cybersecurity 2011 (Handelsblatt, EUROFORUM, Berlin)
19.-23.09.	OWASP Global AppSec North America (OWASP Foundation, Minneapolis/US)
27.-29.09.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
Oktober 2011	
05.10.	Security-Update 2011 (Leitwerk/Secorvo/Securiton, Appenweier)
05.-06.10.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
11.-13.10.	it-sa (SecuMedia Verlag, Nürnberg)
17.-22.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
26.-29.10.	hashdays security & risk conference 2011 (DEFCON Switzerland, Luzern/CH)
November 2011	
11.-13.11.	FIfF Jahrestagung 2011 zur Dialektik der Informationssicherheit (FIfF e.V., München)
29.-30.11.	2. Smart Grid Symposium (Secorvo, KA-Ettlingen)

Fundsache

Die Darstellung von Herausforderungen der Web-Anwendungssicherheit muss nicht trocken daher kommen. Die zur Zeit aus drei Videos bestehende OWASP Appsec Tutorial Series informiert verständlich und unterhaltsam über aktuelle Fragestellungen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Michael Knopp, Klaus J. Müller, Jochen Schlichting

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