secorvo
security consulting

Secorvo Security News

September 2007

Editorial: Über die rote Ampel

Seit nunmehr 30 Jahren soll das deutsche Datenschutzrecht den Einzelnen „unter den Bedingungen der modernen Datenverarbeitung“ vor „unbegrenzter Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten“ schützen. So gewährleistet das allgemeine Persönlichkeitsrecht des Art. 2 Grundgesetz „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf ‚informationelle Selbstbestimmung' sind nur im überwiegenden Allgemeininteresse zulässig.“ (BverfGE 65, „Volkszählungsurteil“ vom 15.12.1983)

Zwar wurde der Datenschutz im Jahr 2000 als Art. 8 in die Charta der Grundrechte der EU aufgenommen. Seit 1983 haben sich aber die „Bedingungen der modernen Datenverarbeitung“ erheblich verändert. Und erweiterte Befugnisse von Staatsorganen der Inneren Sicherheit kratzen an der Substanz dieses Grundrechts.

Am schlimmsten aber ist das herrschende Vollzugsdefizit, das auf einen verbreiteten Mangel an Respekt vor der Individualität und Persönlichkeit anderer Menschen schließen lässt. In zahlreichen Unternehmen ist die Neigung zu beobachten, unzweideutige Bestimmungen des Bundesdatenschutzgesetzes sophistisch zu verbiegen – oft mit Duldung oder gar Unterstützung der Rechtsabteilung. Da werden hemmungslos Personaldaten an amerikanische Mutterkonzerne übermittelt, Whistleblowing-Systeme ohne Rücksicht auf die Persönlichkeitsrechte anonym Verdächtigter installiert oder versteckte Videoüberwachungsanlagen eingerichtet und ohne Benachrichtigung Betroffener ausgewertet.

Diese Verstöße gegen geltendes Recht zeugen von derselben Respektlosigkeit vor der Unversehrtheit anderer Menschen, wie ein Autofahrer, der unter Inkaufnahme der Gefährdung Dritter eine Ampel bei Rot passiert. Schade nur, dass sich Datenschutzvergehen in der Regel weder „blitzen“ noch durch den Entzug einer „Verarbeitungserlaubnis“ ahnden lassen.

Inhalt

secorvo
security consulting

Security News

Security Leck in VMware

Mit dem Einsatz von Virtualisierungslösungen sind auch neue Risiken verbunden, wie beispielsweise eine am 30.07.2007 veröffentlichte Schwachstelle in VMware Workstation 6.0.0 zeigt: die mitgelieferte Library vielib.dll erlaubt es, neue Prozesse zu starten. Nach unseren eigenen Tests ist auch die Version 5.5 betroffen. Behoben wurde das Leck in der am 18.09.2007 veröffentlichten Version 6.0.1 – ein Update empfehlen wir dringend.

Zwar bietet die Virtualisierung von Server-Systemen und Test-Clients aus Sicherheitssicht einige wesentliche Vorteile, sie ist jedoch kein Allheilmittel. So werden einige Risiken nur verlagert, andere Risiken beeinflusst die Virtualisierung überhaupt nicht. Am 25.09.2007 wird Stefan Gora das Für- und Wider auf dem IT-Virtualisierungsforum 2007 vorstellen.

Passworte in Tor

Am 30.08.2007 veröffentlichte Dan Egerstad 100 E-Mail-Passwörter von Botschafts- und Regierungsangehörigen so unterschiedlicher Länder wie Iran, Usbekistan und Japan. Am 10.09.2007 enthüllte er, wie er an diese Passwörter gelangt war: Er hatte einen „Exitknoten" für das Anonymisierungsnetzwerk Tor installiert und betrieben (was man auch den Geheimdiensten von USA und China sowie kriminellen Organisationen nachsagt).

Über diesen Server konnte er Verbindungen von Tor-Nutzern weltweit beim Ausgang aus dem Tor-Netzwerk mitlesen. Denn Tor schützt zwar die Anonymität von Web-Nutzern auf TCP/IP-Ebene (und das nach heutiger Kenntnis wirksam), sorgt aber nur innerhalb des Netzwerks für Vertraulichkeit – die Verbindung bis zum Exitknoten muss man zusätzlich z.B. per TLS verschlüsseln.

Nicht auszuschließen ist allerdings, dass nicht alle betroffenen Tor-Verbindungen von Regierungsangehörigen stammten: möglicherweise waren einige Passworte längst kompromittiert, und die Angreifer nutzten Tor zur Verschleierung ihrer Spuren.

OWASP German Chapter

Am 07.09.2007 trafen sich 16 Sicherheitsexperten in Frankfurt zum Relaunch des German Chapter des Open Web Application Security Project (OWASP). Bei dieser konstituierenden Sitzung wurden die verschiedenen Erwartungen an einen deutschen Ableger diskutiert sowie die ersten Projekte mit lokalem Fokus initiiert. Interessierte sind herzlich eingeladen, sich an der Arbeit des OWASP durch Anregungen zu beteiligen (Kontakt: owasp@secorvo.de).

Germany versus Freeworld

Am 10.08.2007 wurde im Bundesgesetzblatt das Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) veröffentlicht. Der umstrittene „Hackerparagraph" §202c ist damit geltendes Recht. Jetzt erfüllen sich unsere Befürchtungen (siehe SSN 7/07): Am Tag der Veröffentlichung hat der PHP-Sicherheitsexperte Stefan Esser alle „Proof of Concept"-Exploits, die im Rahmen des Month of PHP Bugs entwickelt wurden, von seiner Webseite entfernt. Und The Hackers's Choice (THC) hat seine Aktivitäten in Deutschland eingestellt: So gibt es bei THC jetzt zwei verschiedene Webseiten: germany.thc.org und freeworld.thc.org.

Offen ist derzeit, wie die Justiz den Paragraphen in der Praxis auslegen wird. Um in diesem Punkt Rechtssicherheit zu gewinnen, hat das IT-Magzin tecchannel.de am 14.09.2007 angesichts der Verbreitung des Hacker-Tools „John the Ripper" auf der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) verbreiteten BOSS-CD Strafanzeige gegen Unbekannt wegen des Verdachts des Verstoßes gegen §202c StGB erstattet.

Kryptologen als Autoknacker

Wenn es in der Kryptologie unumstößliche Erkenntnisse gibt, dann sind dies das Kerckhoffsche Prinzip und das Mooresche Gesetz. Ersteres fordert, dass die Sicherheit eines Algorithmus nie von dessen Geheimhaltung, sondern nur von einem Schlüssel abhängen darf, letzteres, dass die Sicherheit der Schlüssellänge – dank Verdoppelung der Rechenleistung alle zwei Jahre – ständig sinkt. Aus diesem Grund aktualisiert die BNetzA jährlich den Algorithmenkatalog zum Signaturgesetz in Abstimmung mit dem BSI und zahlreichen Experten.

Dies dürfte nun auch der Hersteller gelernt haben, der das vor etwa 20 Jahren entworfene KeeLoq Verfahren in Wegfahrsperren-Chips für Autoschlüssel einsetzt. Als der geheim gehaltene Algorithmus 2006 publik wurde, begannen Kryptologen, aktuelle Analysemethoden darauf anzuwenden.

Am 21.08.2007 präsentierte eine Forschergruppe – darunter zwei Schwergewichte der Szene – auf der Rump Session der Crypto 2007 eine Methode, um binnen 48 Stunden einen Wegfahrsperrenschlüssel zu duplizieren. Erforderlich sind dafür 50 Dual-Core PCs und ca. 65 Minuten RFID-Kontakt zum Autoschlüssel des Fahrers, beispielsweise mit einem präparierten Stuhl im Wartezimmer. Schlimmer noch: Stimmt die vermutete Schlüsselableitung, sind so gleich die Wegfahrsperren der ganzen Fahrzeugserie gebrochen.

secorvo
security consulting

Herausforderung Gütesiegel

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) ist um seine selbst gewählte Herausforderung nicht zu beneiden: Wie überzeugt man die Menschheit von einem Datenschutz-Gütesiegel, wenn man nur für Behörden des Landes Schleswig-Holstein zuständig ist?

Da die bereits 2001 im BMI-Gutachten „Modernisierung des Datenschutzrechts" geforderte gesetzliche Produktzertifizierung auf sich warten lässt, hat das ULD nun Europa für das Gütesiegel begeistert: Im Projekt European Privacy Seal (EuroPriSe) werden ab November 2007 unter der Leitung des ULD europäische Pilot-Zertifizierungen durchgeführt.

Aber ein Gütesiegel braucht auch prominente Träger. Mit der Verleihung an Microsofts Update Service landete das ULD im Februar 2007 einen Medien-Coup (siehe SSN 3/07). Das damit betretene Eis ist aber dünn: Dies wurde bei der Verleihung des Gütesiegels für den Lizenzprüfdienst WGA von Windows XP am 03.09.2007 deutlich. Der Schutz der personenbezogenen Daten stützt sich teilweise (bei Fälschungsverdacht) auf rein organisatorische Maßnahmen bei Microsoft – eine Maßnahme, die weder für den Betroffenen nachvollziehbar (nur ein Kurzgutachten ist öffentlich) noch kontrollierbar ist. Auch ist wie bei Sicherheitszertifikaten die Zertifizierung von Teildiensten inhaltlich zumindest fragwürdig, denn das „pars pro toto"-Denken beim Verbraucher kann nicht verhindert werden. Dass hier nicht Microsoft oder Windows ein Datenschutzgütesiegel erhalten haben, sondern ein winziger Dienst des Betriebssystems XP, wird so differenziert nur von einer Minderheit wahrgenommen. Dies könnte mittelfristig das Vertrauen in das Gütesiegel selbst gefährden.

Neues Sicherheitszertifikat

Das International Software Quality Institute (iSQI) hat gemeinsam mit u.a. SAP, Secunet, Virtual Forge und Secorvo die Entwicklung eines Zertifizierungsstandards für Softwareentwickler („Certified Professional for Secure Software Engineering") initiiert. Secorvo wird seine Erfahrungen mit dem Seminar „Sichere Softwareentwicklung" in dieses Zertifikat einbringen.

Sichere Software bei eco

Wer die gut besuchte Veranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zu sicherer Software-Entwicklung am 28.06.2007 verpasst hat, dem sei die Sitzung des Arbeitskreises Sicherheit des eco – Verband der deutschen Internetwirtschaft e.V. am 26.09.2007 in Frankfurt ans Herz gelegt. Die Teilnahme ist kostenlos, eine Online-Anmeldung erforderlich.

Secorvo News

Secorvo College aktuell

In das vierte Quartal startet Secorvo College mit vollem Programm und vollen Seminaren – noch wenige Plätze gibt es für das PKI-Seminar am **09.-12.10.2007**, das Seminar Information Security Management am **16.-19.10.2007** und die T.I.S.P.-Schulung am **05.-09.11.2007**.

Auch die Seminare Sichere Software-Entwicklung am **13.-15.11.2007** und IT-Sicherheitsaudits in der Praxis am **04.-06.12.2007** füllen sich bereits.

Programme und Online-Anmeldung unter
http://www.secorvo.de/college

Sicherheitspreis

Am 14.09.2007 wurde im Rahmen der Security-Fachmesse Safekon in Karlsruhe die Security Awareness-Kampagne „Mission Security" der T-Systems Enterprise Services GmbH, die von Secorvo und der Agentur Südpol konzipiert und unterstützt wurde, als eines von vier beispielhaften Projekten zum Schutz vor Wirtschaftsspionage und Konkurrenzausspähung von Innenminister Heribert Rech mit dem erstmals verliehenen „Sicherheitspreis Baden-Württemberg" ausgezeichnet (zweiter Preis).

Der Innenminister lobte in seiner Laudatio das „psychologisch einfühlsam aufbereitete Konzept" der Kampagne, in der der fiktive Mitarbeiter James Bit als Leitfigur und Vorbild diente (Motto: „Mir ist es nicht egal!").

Weitere KA-IT-Si-Events

Angesichts der großen und wachsenden Resonanz, der sich die Events der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) erfreuen, sind für 2007 noch drei Veranstaltungen geplant. Zwei Termine sollten Sie sich bereits vormerken:

- **Leben in der Schlangengrube**
  Am 27.09.2007 gewährt Angel Jodra (Kaspersky Labs) einen Einblick in die zu erwartende Entwicklung der Bedrohung durch Viren, Trojaner und andere Malware (Anmeldung).

- **Wer wird FIDUCIA Security Champ?**
  Am 18.10.2007 ist die FIDUCIA IT AG Gastgeber der KA-IT-Si und wird ihre mit dem Sicherheitspreis Baden-Württemberg 2007 (2. Preis) ausgezeichnete Security-Awareness-Kampagne vorstellen. Das sollten Sie nicht verpassen ...

Veranstaltungshinweise

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

September 2007	
25.-27.09.	ISSE 2007 (TeleTrusT et al., Warsaw/PL)
26.09.	Sichere Softwareentwicklung (eco AK Sicherheit, Frankfurt)
27.09.	Leben in der Schlangengrube (KA-IT-Si, Karlsruhe)
Oktober 2007	
04.-05.10.	3rd European Conference on Computer Network Defense (FORTH-ICS & ENISA, Heraklion/GR)
09.10.	Verdeckte Online-Durchsuchung (a-i3, Bochum)
09.-12.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.10.	Information Security Management – von A(udit) bis Z(ertifizierung) (Secorvo, Karlsruhe)
18.10.	Wer wird FIDUCIA Security Champ? (KA-IT-Si, Karlsruhe)
November 2007	
05.-09.11.	T.I.S.P. Schulung (Secorvo, Karlsruhe)
13.-15.11.	Sichere Software-Entwicklung (Secorvo, Karlsruhe)

Fundsache

Auf den Punkt gebracht werden zahlreiche Sicherheitsthemen auf der Cartoon-Seite SecurityCartoon.com. Eine thematische Gliederung erleichtert die Recherche. Deren nichtkommerzielle Nutzung – z. B. zur gestalterischen Aufwertung einer Security-Intranet-Seite – ist mit Quellenangabe zugelassen.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting, 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