secorvo
security consulting

Secorvo Security News

November 2007

Editorial: Quod licet Jovi...

Der Streit um die datenschutzrechtliche Zulässigkeit der Speicherung von Zugriffsdaten auf Web-Angebote fußt auf der Kernfrage, ob es sich bei IP-Adressen um personenbezogene Daten handelt. Dazu liegt inzwischen ein einschlägiges Urteil vor: Das Landgericht Berlin hat am 23.11. 2006 festgestellt, dass IP-Adressen auch dann als personenbeziehbar (und damit als personenbezogene Daten) gelten, wenn zwar nicht die speichernde Stelle, wohl aber ein Dritter den Personenbezug herstellen kann. Die Konsequenz ist klar: Ohne Einwillligung der Betroffenen ist damit jede Speicherung unzulässig, die für den Betrieb des Web-Angebots nicht erforderlich ist. Auf dieser Grundlage untersagte das Landgericht Berlin am 27.03.2007 dem Bundesjustizministerium (sic!) die Speicherung von Zugriffsdaten über das Ende des Nutzungszeitraums hinaus, da dies das Persönlichkeitsrecht der Betroffenen verletze.

In der Antwort der Bundesregierung vom 30.10. 2007 auf eine kleine Anfrage von FDP-Bundestagsabgeordneten und einer Antwort vom 07.11.2007 auf eine Anfrage der Linksfraktion wurde nun bekannt, dass das Bundeskriminalamt (BKA) seit Juli 2001 die IP-Adressen von Besuchern der BKA-Webseite „Militante Gruppen“ nicht nur registriert, sondern bei „signifikanter Zugriffsfrequenz“ eine „Anschlussinhaberfeststellung über den Provider gemäß § 100g StPO“ vornimmt.

Bemerkenswert ist daran die datenschutzrechtliche Position der Bundesregierung: Eine „Aussage zur Gesamtmenge der überprüften IP-Adressen“ sei nicht möglich, da datenschutzkonform gelöscht werde; eine Information der Betroffenen erfolge nicht. Und: „Inwieweit IP-Adressen personenbezogene Daten darstellen, ist nicht abschließend geklärt.“ Da möchte man der Bundesregierung doch die Lektüre der Entscheidung des BVerfG vom 23.10.1952 zum SRP-Verbot ans Herz legen: „Zu den grundlegenden Prinzipien dieser Ordnung sind mindestens zu rechnen: die Achtung (...) vor allem vor dem Recht der Persönlichkeit auf Leben und freie Entfaltung, (...) die Gesetzmäßigkeit der Verwaltung (...).“ Schön wär's.

Inhalt

secorvo
security consulting

Security News

GSM-Hacking

Auf dem diesjährigen Chaos Communication Camp in Berlin präsentierten David Hulton und Joshua Lackey am 10.08.2007 Angriffe auf GSM-Verbindungen. Sie stellten einen „GSM Traffic Sniffer" und eine Implementierung des Cyphertext Only Angriffs (siehe SSN 09/2003) von Eli Biham, einem der weltweit führenden Kryptologen vom Israel Institute of Technology in Haifa, auf den Verschlüsselungsalgorithmus A5 vor, mit der sie kürzeste SMS- oder Telefonie-Verbindungen innerhalb von 3-5 Minuten mit einem handelsüblichen PC entschlüsseln können. Der Vortrag ist als einstündiger Film abrufbar; auch gibt es umfangreiche Hintergrundinformationen zum A5 Cracking Projekt wie die Original-Veröffentlichungen aller Angriffe, sehr viele Beispielprogramme und einen Überblick über die weltweite Nutzung des A5 in GSM-Netzen.

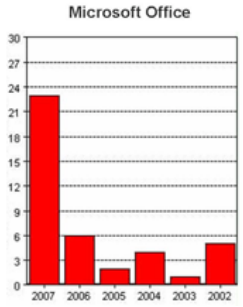
Damit hat der von den meisten GSM-Netzbetreibern genutzte Verschlüsselungsalgorithmus A5 ein unrühmliches Ende gefunden. Immerhin: Nun gibt es einen prominenten weiteren Beleg dafür, dass die Nutzung proprietärer und geheim gehaltener Verschlüsselungsverfahren in der Regel der Anfang vom Ende der Vertraulichkeit ist. Bleibt zu hoffen, dass die Lehre ankommt.

ISF Good Practice

Am 16.10.2007 veröffentlichte das Information Security Forum (ISF) eine neue Version des "Standard of Good Practice for Information Security". Die 372 Seiten umfassende Neufassung wurde an die jüngsten Standards in der Informationssicherheit wie ISO/IEC 27002:2007 und COBIT v4.1 angepasst. Da auch aktuelle Entwicklungen wie Virtualisierung und EuroSOX, die in den Unternehmen derzeit eine große Rolle spielen, berücksichtigt wurden, hilft das Dokument, den derzeitigen Stand der „Best Practice" in der Informationssicherheit zu bestimmen.

SANS Top 20

Am 28.11.2007 publizierte SANS die aktuelle Version der „TOP-20"-Liste der größten Security Risiken. Viele Positionen blieben unverändert, wie die der Web-Applications auf Platz 1 der Server-seitigen Verletzlichkeiten. Auffällig ist allerdings die signifikante Zunahme hochkritischer Sicherheitslücken in Office-Anwendungen von Microsoft: Patchen dringend anzuraten.



Denial of Car Service

Eine ganz neue Klasse von Denial of Service (DoS) Angriffen könnte uns zukünftig bevorstehen. So wurde am 01.11.2007 in einem Parkhaus in Kent (GB) als Verursacher einer seit mehreren Wochen andauernden Störung von Dutzenden Fahrzeugen das Familienauto eines Pendlers identifiziert. Es gab periodisch Signale ab, die in einem Umkreis von 50 m die Bordelektronik anderer Automobile verwirrten. Die dadurch verursachten Effekte reichten von einer Selbstauslösung der Diebstahl-Alarmierung über die Blockierung der Zentralverriegelung bis zur Sperrung der Zündung. Wenn das schon unbeabsichtigt so wirksam funktioniert – mit welchen Wirkungen ist dann erst bei gezielten „DoCS"-Angriffen zu rechnen?

Vorratsdatenspeicherung

Am 09.11.2007 hat der Bundestag die Telekommunikationsüberwachung neu geregelt. Damit wurden unter anderem die Zugriffsmöglichkeiten der Strafverfolgungsbehörden auf Verkehrsdaten erheblich ausgeweitet. So sind TK-Provider nun verpflichtet, im manuellen Auskunftsverfahren (§ 113 TKG), d. h. auch ohne Vorlage eines richterlichen Beschlusses, zu einer dynamischen IP-Adresse mit Zeitangabe den Namen des Anschlussinhabers preiszugeben.

Auch wurde die Pflicht zur Benachrichtigung Betroffener nach Abschluss einer Maßnahme (§ 101 StPO) erheblich abgeschwächt: Der neue Absatz 7 erlaubt, mit Zustimmung des Gerichts von einer Benachrichtigung abzusehen, wenn sie für insgesamt fünf Jahre zurückgestellt worden ist und die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden.

Schließlich macht der neue § 113a TKG eine sechsmonatige Vorratspeicherung aller Verkehrsdaten demjenigen zur Pflicht, der „öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt". Die bei Telefondiensten, Internet-Nutzung und E-Mail-Diensten jeweils zu speichernden Verkehrsdaten sind vollständig aufgeführt – und schließen explizit auch nicht zu Stande gekommene Verbindungsversuche ein; Mobilfunknetzbetreiber haben den Standort aller Funkzellen und die zugehörigen Hauptstrahlrichtungen vorzuhalten.

Mit dieser Regelung bricht der Gesetzgeber ein zentrales Grundprinzip des Datenschutz- und Strafrechts: Eine verdachts- und anlassunabhängige Erhebung und Speicherung von Verkehrsdaten galt bisher als unvereinbar mit den Prinzipien einer freiheitlichen Ordnung.

Die Neuregelungen treten am 01.01.2008 in Kraft – sofern der Bundespräsident dieser erheblichen Ausweitung sicherheitsbehördlicher Eingriffsbefugnisse nicht seine Unterschrift verweigert. Dann bleibt nur noch, auf einen Erfolg der Initiative gegen die Vorratsdatenspeicherung zu hoffen, die eine Sammel-Verfassungsbeschwerde initiiert hat. Eine Beteiligung daran ist noch bis 24.12.2007 möglich.

Leitfaden IT-Sicherheit

Am 25.10.2007 gab das BSI eine aktualisierte Fassung des "Leitfaden IT-Sicherheit" heraus. Darin werden die 50 wichtigsten organisatorischen und technischen Maßnahmen insbesondere für kleinere und mittelständische Unternehmen sowie Behörden als „IT-Grundschutz kompakt" anschaulich zusammengefasst. Der Leitfaden bietet eine gute Übersicht und Checklisten zur (Selbst-) Überprüfung.

Pikanterweise haben sich die Autoren darin gegenüber der Version vom September 2003 (siehe SSN 10/2003) sang- und klanglos vom Begriff „... Härten in der IT-Sicherheit ..." verabschiedet. Vielleicht lassen sich ja so die Grundschutzanforderungen an Behörden im Kontext des Umsetzungsplans Bund (UP Bund) besser erfüllen.

Anstieg der IuK-Straftaten

Das Bundeskriminalamt (BKA) veröffentlichte am 20.11.2007 die offizielle Statistik der Entwicklung von „IuK-Straftaten" im Jahr 2006. Einschließlich Warenkreditbetrug stieg die Gesamtfallzahl um 40% auf über 165.000 Straftaten. Zur „IuK-Kriminalität im engeren Sinne" zählte das BKA knapp 30.000 Fälle – ein Plus von knapp 10 %. Dabei verzeichneten die „Fälschung beweiserheblicher Daten und Täuschung im Rechtsverkehr bei der Datenverarbeitung" und das „Ausspähen von Daten" (Plus von 140 % bzw. 26 %) die höchsten Zuwachsraten.

Tag des Informationsrechts

Eine spannende Veranstaltung zur Online-Durchsuchung des Zentrums für Angewandte Rechtswissenschaft in Kooperation mit den Jungen Juristen Karlsruhe e.V. ist für den „Karlsruher Tag des Informationsrechts" am 10.12.2007 geplant. Neben Gerhart Rudolf Baum, Bundesinnenminister a.D. und einer der Beschwerdeführer vor dem Bundesverfassungsgericht, werden der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar und der BKA-Präsident Jörg Ziercke zu der dreistündigen Veranstaltung in der Städtischen Galerie beim ZKM erwartet. Die Teilnehmerzahl ist begrenzt, eine Anmeldung erforderlich.

T.I.S.P.-Boom

Die wachsende Bedeutung des T.I.S.P.-Zertifikats verdeutlichte das erste T.I.S.P.-Community-Treffen am 15.-16.11.2007 in Karlsruhe. Neben Fachvorträgen zu „Security bei SAP", „IT won't happen to me" und „Abhörschutz" wurden Workshops zu den Themen „Awarenesskampagnen", „Herausforderungen im Arbeitalltag" und „Projektleitung und IT-Sicherheit" geboten. Gelegenheit zu Erfahrungsaustausch und Networking, u. a. beim abendlichen Dinner, rundeten die gut besuchte Veranstaltung ab.

Dr. Günther Welsch, Geschäftsführer von TeleTrusT Deutschland e.V., erwartet für Ende 2007 mehr als 200 zertifizierte T.I.S.P.-Absolventen – eine Verdoppelung innerhalb eines Jahres. Diese Entwicklung belege die steigende Akzeptanz und Bedeutung des T.I.S.P. als beruflicher Qualifikationsnachweis.

Secorvo News

Secorvo College aktuell

Eine letzte Weiterbildungsgelegenheit in 2007 bietet Secorvo College mit dem Seminar IT-Sicherheitsaudits in der Praxis am **04.-06.12.2007**. Alle Seminare und Termine für das kommende Jahr finden Sie im noch druckfrischen Jahresprogramm 2008.

Auf Grund der großen Nachfrage bietet Secorvo College die Möglichkeit zur T.I.S.P.-Zertifizierung im Jahr 2008 insgesamt vier Mal an. Termin des ersten T.I.S.P.-Seminars ist der **25.-29.02.2008**.

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

"Wie dick ist Ihr Bunker?"

Für den 22.11.2007 hatte die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zu Vortrag und Diskussion über physikalische Gefährdungen von Rechenzentren und den damit verbundenen Haftungsrisiken geladen. Prägnant und eindrucksvoll spannten Prof. Dr. Michael Bartsch (Bartsch und Partner) und Hans-Jürgen Frase (Litcos) den Bogen von der Verantwortung des Managements für die Risikovorsorge bis zu den konkreten Bedrohungen der IT-Verfügbarkeit durch Überhitzung, Stromausfall, Feuer und Wasser sowie einem systematischen Vorgehen zur Entwicklung von Schutzmaßnahmen. Die Unterlagen der Referenten sind online abrufbar.

Veranstaltungshinweise

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

Dezember 2007	
04.-06.12.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
10.12.	Tag des Informationsrechts: Onlinedurchsuchung (ZAR, Karlsruhe)
27.-30.12.	The 24th Chaos Communication Congress (24C3) (Chaos Computer Club, Berlin)
Februar 2008	
10.-13.02.	Fast Software Encryption Workshop (FSE 08) (IACR, Lausanne/CH)
11.-14.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
13.-14.02.	15. DFN CERT & PCA Workshop - Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
19.-20.02.	Identity Management Symposium 2008 (vps & Secorvo, Karlsruhe)
25.-29.02.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)

Fundsache

Der seit dem 13.07.2007 öffentliche Aufsatz "Fast-Flux Service Networks" des Honeynet Projects erläutert die immer ausgefeilteren Methoden von Angreifern zur Verschleierung des Ursprungs von Viren-, Würmer- und Spam-E-Mails oder Phishing-Angriffen. Kern der Analyse ist eine neue Technologie namens "Fast Flux", mit der Angreifer ihre DNS-Einträge sowie die zugeordneten IP-Adressen regelmäßig – teilweise im Minutentakt – ändern, um unentdeckt zu bleiben.

Impressum

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

ISSN 1613-4311

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