secorvo
security consulting

Secorvo Security News

Oktober 2007

Editorial: Angehört

Ein Erlebnis der besonderen Art war die Anhörung des Bundesverfassungsgerichts zur „Online-Durchsuchung“ am 10.10.2007. Mit beeindruckender Konzentration folgte der erste Senat vor vollen Besucherbänken der Erörterung wichtiger Fragen, die für die Bewertung der Verfassungsmäßigkeit einer Online-Durchsuchung eine Rolle spielen dürften. Diskutiert wurden u. a. die Eingriffstiefe von Online-Durchsuchung und „Quellen-Telekommunikationsüberwachung“ sowie die Frage, ob sich beides technisch unterscheiden lässt. Kritisch beleuchtet wurde auch, ob eine Online-Durchsuchung zielgerichtet möglich ist: Wie kann sicher gestellt werden, dass das „richtige“ System durchsucht wird? Entlarvend die Antwort eines BKA-Vertreters: Das wisse er erst, „wenn die Daten zu ihm sprechen“.

Die Stellungnahmen der fünf geladenen sachkundigen Auskunftspersonen Bogk (CCC), Fox (Secorvo), Prof. Freiling (Uni Mannheim), Prof. Pfitzmann (TU Dresden) und Prof. Sieber (MPI Freiburg) sind inzwischen online verfügbar.

Deutlich wurde, dass das NRW-Gesetz kippen wird – schon aufgrund der mangelnden Normenklarheit. Nach den Ausführungen des Bevollmächtigten der NRW-Landesregierung, Prof. Heckmann, fragte Verfassungsgerichtspräsident Prof. Papier dezent süffisant: „Sprechen wir über dasselbe Gesetz?“. Auf die Erwiderung Heckmanns, das Gesetz sei „auslegungsfähig“, konterte Papier, die Auslegung sei „ansprechend“, das Gericht habe jedoch „nicht die Auslegung eines Prozessbevollmächtigten zu beurteilen, sondern den Wortlaut des Gesetzes.“ Das für 2008 erwartete Urteil dürfte wegweisend ausfallen – vergleichbar dem "Volkszählungsurteil" von 1983, das die "Informationelle Selbstbestimmung" prägte. Möglicherweise wird das BVerfG den Schutz des Kernbereichs privater Lebensgestaltung neu definieren, und zweifellos wird eine Online-Überwachung an hohe Hürden geknüpft, mindestens an die einer G10-Ermächtigung.

Solange wir solche Verfassungsrichter haben, können stümperhafte Gesetzgeber zum Glück nur begrenzten Schaden anrichten.

Inhalt

Editorial: Angehört

Security News

Last Orders, please!

Risiko Kreditkarte

SQL-Nahkämpfer

Material zum Bundestrojaner

BBA 2007

Nichts zu verbergen

iPhone out of Jail

Secorvo News

Secorvo College aktuell

Spionage für Anfänger

Virtuelle IT-Sicherheit

Wie dick ist Ihr Bunker?

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Last Orders, please!

Am 01.11.2007 beginnen die deutschen Einwohnermeldeämter mit der Erfassung von Fingerabdrücken für den neuen Reisepass („ePass"). Allen Sicherheitsbedenken zum Trotz werden jedem Antragsteller zwei Fingerabdrücke abgenommen, die als weiteres biometrisches Merkmal – zusätzlich zu dem bereits 2005 eingeführten digitalen Passbild – auf einem im Pass befindlichen RFID-Chip gespeichert werden.

Dabei hat sich offenbar bei den Behörden noch nicht herumgesprochen, dass das Auslesen der RFID-Chips geradezu trivial ist (siehe SSN 08/2007): sogar das Bundesinnenministerium behauptet auf seinen Informationsseiten: „*Schon die elektronischen Pässe der ersten Generation sind durch einen wirkungsvollen Mechanismus gegen unberechtigtes Auslesen geschützt.*" Vertrauensbildung sieht anders aus. Wer schnell handelt, sichert sich noch eine zehnjährige Karenzzeit.

Risiko Kreditkarte

Am 04.10.2007 hat der amerikanische Großhändlerverband NRF die Kreditkartenorganisationen aufgefordert, auf die Verpflichtung zur Speicherung der vollständigen Kreditkartendaten beim Händler gemäß den Best-Practice-Vorgaben des Payment Card Industry Security Standards Council zu verzichten. Danach müssen die Daten 12 bis 18 Monate für laufende Abfragen bereit gehalten werden.

Auch wenn das nicht das einzige Motiv der NRF sein dürfte, verringert die Reduktion sensibler Daten zweifellos die Gefahr unerwünschten Datenabflusses. Just an eben diesem 04.10.2007 waren dem Eintrittskarten-Shop Kartenhaus.de Kreditkartendaten von ca. 66.000 Kunden der vergangenen 12 Monate gestohlen worden.

Vorfälle dieser Art täuschen jedoch darüber hinweg, dass Kreditkartenbetrug in der Regel „klassisch" erfolgt: Angeblich finden 70% aller Kreditkartenbetrügereien der USA in Restaurants statt. Selbst wenn die Kreditkarte nicht vom Personal mitgenommen wird, ist es mit geeigneten Lesegeräten trivial, den Magnetstreifen unbemerkt am Tisch auszulesen – und die Karte später zu „klonen".

SQL-Nahkämpfer

Am 08.10.2007 wurde Version 0.2.1 des SQL-Angriffswerkzeugs SQLNinja veröffentlicht. Das auf Microsofts SQL-Server spezialisierte Open-Source-Tool versucht, bekannte SQL-Schwachstellen auszunutzen und kann bei Penetrationstests zur Analyse von Webapplikationen eingesetzt werden.

Die Angriffsoptionen reichen von der Informationsbeschaffung bis zur Durchführung von Bruteforce-Attacken auf Datenbank-Accounts. Im „besten" Fall startet SQLNinja eine remote shell auf dem betroffenen System. Im Mai 2007 wurde es in die Top 15-Liste der kostenfreien SQL Injection Scanner aufgenommen.

Material zum Bundestrojaner

In den vergangenen Wochen wurden einige erhellende Dokumente zum Thema „Online-Durchsuchung" veröffentlicht, allen voran zwei Stellungnahmen des BMI vom 22.08.2007 zu einem Fragenkatalog des BMJ und einem Fragenkatalog der SPD-Bundestagsfraktion. Eine gute Übersicht enthält auch der in HRRS erschienene Beitrag von Ulf Buermeyer. Nach Überzeugung von Prof. Hartmut Pohl (Beitrag in DuD 9/2007) wurden vom Bundesnachrichtendienst Online-Durchsuchungen unter Verwendung von „Less-Than-Zero-Day-Exploits" durchgeführt – unabhängig von dem dafür erforderlichen Aufwand ein gefährlicher Ansatz, wird durch die Geheimhaltung von Sicherheitslücken doch zugleich der Zeitraum verlängert, in dem Systeme von Unternehmen, Behörden und Bundesbürgern angreifbar sind.

Inzwischen sind auch die Stellungnahmen der fünf vom Bundesverfassungsgericht befragten und zur Anhörung am 10.10.2007 geladenen sachkundigen Auskunftspersonen Bogk (CCC), Fox (Secorvo), Prof. Freiling (Uni Mannheim), Prof. Pfitzmann (TU Dresden) und Prof. Sieber (MPI Freiburg) online.

BBA 2007

In Deutschland erstmals im Jahr 2000 ausgelobt wurden sie am 12.10.2007 zum achten Mal verliehen: die „Big Brother Awards", unerwünschte Auszeichnungen für Datenkraken. Erstmals überstieg die Zahl der Nominierungen die Marke 500, so dass die Jury in diesem Jahr zahlreiche Auswahlrunden zu bewältigen hatte, ehe die endgültigen acht Preisträger fest standen.

In der Kategorie „Arbeitswelt" siegte die Novartis Pharma GmbH mit der Bespitzelung des eigenen Außendienstes, der Öffnung von Betriebsratspost und der Missachtung der Vertraulichkeit von Mitarbeiterumfrageergebnissen. Die internationalen Hotelketten in Deutschland – stellvertretend Hyatt, Marriott und Intercontinental – errangen den Award in der Kategorie „Verbraucherschutz" für die heimliche Erfassung und Speicherung von Gastdaten (Trink- und Essgewohnheiten, Pay-TV-Nutzung, Allergien, Kontaktadressen, Kreditkartendaten, Sonderwünsche und Beschwerden) sowie deren rechtswidrige Übermittlung in die USA.

In der Kategorie „Politik“ setzte sich Bundesfinanzminister Peer Steinbrück mit seiner lebenslangen „Steuer-ID“ durch.

Für die hochwirksame Schärfung des Datenschutzbewusstseins in der Öffentlichkeit (mittels zahlloser Vorschläge zur Einschränkung von Freiheitsrechten zu Gunsten wirksamerer Terrorismusbekämpfung) wurde Bundesinnenminister Wolfgang Schäuble die Ehrenmitgliedschaft in der Deutschen Vereinigung für Datenschutz (DVD) angetragen.

Nichts zu verbergen

Was ist Privatsphäre, warum ist diese schützenswert, und ist es so, dass wir wirklich nichts zu verbergen haben? Mit diesen Fragestellungen beschäftigt sich das am 12.07.2007 veröffentlichte Essay 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy von Professor Daniel J. Solove. In dem 25-seitigen Papier entkräftet der Autor anhand grundsätzlicher Überlegungen und zahlreichen Beispielen die verbreitete, undifferenzierte „Ich-habe-nichts-zu-verbergen“-Haltung sowie die simplifizierende Gegenüberstellung von Sicherheitsinteressen und dem Schutz von Privatsphäre.

iPhone out of Jail

Seit dem 08.10.2007 können Besitzer infizierter iPhones wieder die alleinige Kontrolle über ihr Eigentum zurück erlangen. Die Portierung eines seit 2006 bekannten Buffer Overflows der TIFF library (libtiff), der – im Kontext des Browsers Mobile Safari erfolgreich ausgeführt – Root-Berechtigungskontext gewährt, bedrohte iPhones bis Version 1.02.

Die Gefährdung mobiler Geräte durch eben diesen Bug wurde bereits Anfang 2006 an Sonys Playstation demonstriert. Bedenklich, dass ein führender Hersteller sein mobiles Äpfelchen nicht besser vor der Root-Fäule schützt – fachkundige, lesbare Impfanleitungen für gesundes Obst gibt es mindestens seit 2002 von Forschern wie Steven M. Bellovin.

Sollte die Sicherheit von Embedded Systems nicht bald ebenso ernst genommen werden wie die Sicherheit von Servern und Arbeitsplatzrechnern, werden in den SSN demnächst wohl Hersteller von intelligenten IP-Kühlschränken gegen Navigationssysteme antreten.

Secorvo News

Secorvo College aktuell

Drei Weiterbildungsgelegenheiten bietet Secorvo College noch in 2007: die T.I.S.P.-Schulung am **05.–09.11.2007** (mit anschließender Prüfung) sowie die Seminare Sichere Softwareentwicklung (**13.–15.11.2007**) und IT-Sicherheitsaudits in der Praxis (**04.–06.12.2007**). Weitere Seminare und Termine finden sich im druckfrischen Jahresprogramm 2008.

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

Spionage für Anfänger

Auf Einladung der Firma Vollack und der „badischen Wirtschaftswoche“, dem Magazin econo, gewährt Secorvo am 15.11.2007 ab 18:30 Uhr in der Vollack Culturwerkstatt (Karlsruhe, Fettweisstraße 42) einen Einblick in Techniken der Wirtschaftsspionage – und zeigt an Beispielen die Bedeutung von IT-Sicherheit für den Mittelstand auf; typische Bedrohungen werden live demonstriert. Im Anschluss gibt es Gelegenheit zur Diskussion am Buffet. Eintritt 30 Euro, Anmeldung bis 08.11.2007 an Frau Cornelia Braun, cbraun@vollack.de (0721/4768126).

Virtuelle IT-Sicherheit

Virtualisierungslösungen besitzen aus der Perspektive der IT-Sicherheit zahlreiche Vor-, aber auch einige Nachteile. Stefan Gora stellte auf dem Forum IT-Virtualisierung 2007 im September die wichtigsten Aspekte gegenüber. Zum selben Thema wird er auf dem Forum IT-Revision am 06.-07.11.2007 vortragen.

Wie dick ist Ihr Bunker?

So aktiv war die Karlsruher IT-Sicherheitsinitiative noch nie: Fünf Events zu spannenden Themen in 2007 mit mehreren hundert Teilnehmern – und ein sechstes Event in Vorbereitung: Unter der Leitfrage „Wie dick ist Ihr Bunker?“ werden am 22.11.2007 (18 Uhr) die physischen Gefährdungen von Rechenzentren und die damit verbundenen Haftungsrisiken diskutiert.

Die Unternehmen Lampertz und Rittal werden zusammen mit Professor Bartsch von der Kanzlei Bartsch und Partner die besonderen Herausforderungen des Rechenzentrumsbetriebs aus technischer und rechtlicher Perspektive beleuchten. Anschließend gibt es Gelegenheit zum Networking am Buffet (bitte um Anmeldung bis 20.11.2007).

Die Vortragsunterlagen des KA-IT-Si-Events „Trau, schau, wem“ am 18.10.2007 bei der FIDUCIA IT AG, auf dem die mit dem Sicherheitspreis Baden-Württemberg 2007 ausgezeichneten Security Awareness Kampagnen der FIDUCIA IT AG und der T-Systems Enterprise Services GmbH präsentiert wurden, sind inzwischen vom Server der KA-IT-Si abrufbar.

Veranstaltungshinweise

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

Oktober 2007	
23.-26.10.	4. Black Hat Japan Briefings & Training 2007 (Tokyo)
November 2007	
05.-09.11.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
06.-07.11.	Forum IT-Revision (IIR, Frankfurt)
09.11.	Security Symposium (TelekomForum, Hamburg)
13.-15.11.	Sichere Softwareentwicklung (Secorvo College, Karlsruhe)
15.11.	Wirtschaftsspionage für Anfänger (Vollack Culturwerkstatt, Karlsruhe)
15.-16.11.	1. T.I.S.P.-Community-Workshop (TeleTrusT/Secorvo College, Karlsruhe)
22.11.	Wie dick ist Ihr Bunker? (KA-IT-Si, Karlsruhe)
Dezember 2007	
04.-06.12.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)

Fundsache

Das am 17.09.2007 publizierte 35seitige SAP-Whitepaper SSO mit Windows und SAP stellt die unterschiedlichen Authentifizierungsverfahren von Microsoft (IIS, .NET, MOSS, WCF) und SAP NetWeaver (SAP GUI, ICM, PAS, JAAS), die Kopplungsmöglichkeiten mit externen Verfahren (LDAP) sowie die unterschiedlichen Mechanismen – von ID/Passwort bis zum Client-Zertifikat – vor. Dabei werden unterschiedliche Szenarien für die gegenseitige Nutzung der Mechanismen – von Windows zu SAP ebenso wie von SAP-Applikationen zu Windows-Services – präsentiert.

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