secorvo
security consulting

Secorvo Security News

Oktober 2011

Untragbar unerträglich

Gelegentlich ist es unerfreulich, mit einer Prognose richtig gelegen zu haben. Die Erkenntnisse um die vom Chaos Computer Club mit der am 08.10.2011 publizierten Analyse eines „Staatstrojaners“ ausgelösten Recherchen übertreffen jedoch die schlimmsten Befürchtungen. Da ist zunächst das Unternehmen, das die Überwachungssoftware im Auftrag von LKAs und BND entwickelte: Dessen früherer Geschäftsführer wurde nach Erkenntnissen des Handelsblatts 2002 wegen Bestechung zu 1,5 Mio. € Geldbuße und 21 Monaten auf Bewährung verurteilt, und zumindest von Web-Sicherheit versteht es nicht allzu viel. Dann ist da die Software: Sie verschlüsselt die zu übermittelnden Daten mit einem immer gleichen AES-Schlüssel und kann über nachladbare Module sowohl zur Quellen-TKÜ als auch zur Online-Durchsuchung eingesetzt werden. Für letztere hat das BVerfG in seinem Urteil vom 27.02.2008 sehr hohe materielle Zulässigkeitsvoraussetzungen formuliert: „*Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.*“ Anders als bei einer (Quellen-) TKÜ genügen z. B. Verstöße gegen das Betäubungsmittelgesetz diesem Kriterium nicht.

Dass es keine gute Idee ist, die Entscheidung über den Funktionsumfang in die Hand der Strafverfolgung zu legen, zeigt das Urteil des LG Landshut vom 20.01.2011: Bei der Umsetzung eines Quellen-TKÜ-Beschlusses des Amtsgerichts wurden von den bayerischen Strafverfolgungsbehörden mit der Software im 30-Sek.-Takt rechtswidrig 66.000 Screenshots erzeugt. Möglicherweise kein Einzelfall.

In einem Rechtsstaat ist auch die Exekutive an Gesetz und Verfassung gebunden – vor allem das unterscheidet ihn von einer Willkürherrschaft. Ein Landesinnenminister, der einen solchen Rechtsbruch verteidigt, ist daher nicht nur unerträglich, sondern untragbar.

Inhalt

secorvo
security consulting

Security News

Bepper-Trojaner

Immer häufiger werden QR-Codes (zweidimensionale Barcodes) als Link zu weiterführenden Informationen in Zeitschriften, auf Plakaten, Webseiten oder Eintrittskarten angegeben. Diese Grafik kann mit einem Handy oder Smartphone abfotografiert und weiterverarbeitet werden, so dass der interessierte Nutzer auf der darin angegebenen Website landet, ohne eine URL eintippen zu müssen.

Am 30.09.2011 berichtete Denis Maslennikov von Kaspersky Labs über einen Angriff, bei dem auf über QR-Codes referenzierten Webseiten dem Smartphone-Benutzer – ähnlich wie bei einem SMS-Trojaner – eine mit Schadsoftware angereicherte Version eines mobilen ICQ-Clients untergeschoben wird. Theoretisch war ein solcher „Bepper-Trojaner" (umgangssprachlich für „Aufkleber") bereits einige Wochen zuvor beschrieben worden.

Ein gutes Beispiel dafür, wie aus einem ergonomischen Feature eine Angriffsmöglichkeit wird. Wer QR-Codes nutzt, sollte auf keinen Fall Software oder Apps auf diesem Weg beziehen.

Grundschutz EL 12

Seit dem 11.10.2011 steht die aktualisierte und erweiterte Version der BSI-Grundschutzkataloge in der 12. Ergänzungslieferung (EL) im PDF-Format mit dokumenteninternen Sprungmarken online zur Verfügung. Die HTML-Version, die von freien Werkzeugen wie z. B. verinice genutzt wird, bleibt vorerst jedoch auf dem Stand der 11. EL. Für das GSTOOL 4.7 wurde indes bereits eine Aktualisierung (Servicepack 3 und zugehörige Metadaten) für November und Dezember 2011 angekündigt, Version 5.0 soll im 2. Quartal 2012 verfügbar sein.

Zeitgleich mit der Ergänzungslieferung wurden auch eine aktualisierte „Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz" sowie die Formblätter und Kreuzreferenztabellen, die viele Unternehmen als Grundlage für eigene Arbeitswerkzeuge nutzen, vom BSI bereitgestellt. Neben neuen Bausteinen wie „Virtualisierung" (B 3.304) und „Terminalserver" (B 3.305) wird für ein produktunabhängiges Vorgehen bei Webservern in der 12. EL nur noch der generische Baustein „Webserver" (B 5.4) genutzt. Ein richtiger Schritt angesichts der sich schnell ändernden Technologie. Ein Hinweis auf die OWASP-Top 10 wäre dort allerdings sinnvoll gewesen.

CAINE erneuert

Seit dem 19.09.2011 ist die frei nutzbare Live-CD-Forensikdistribution CAINE (Computer Aided INvestigative Environment), die auf Ubuntu basiert, in der überarbeiteten Version 2.5 verfügbar. Auch gibt es eine spezielle USB-Stick-Version.

Besonders hilfreich sind die stark erweiterten NAUTILUS-Scripts für das direkte Einsehen von Dateiinformationen von z. B. gelöschten Dateien und Bilddaten. Ein besonderes Schmankerl ist das unscheinbare Script „FileInfo", welches über die Option „Metadatenextraktion" die Inhalte von SQLite-Datenbanken ausliest, die z. B. von Firefox, Nokia OVI, Skype und Apples iPhones genutzt werden. Abgerundet wird der positive Eindruck durch das Werkzeug frag_find, mit dem z. B. Dokumententeile über identische Sektoren-Hashwerte gefunden und nachgewiesen werden können, vorausgesetzt, dass bei einer Untersuchung das nachzuweisende Dokument digital vorliegt.

Risiken der Überwachung

Das Landgericht Lüneburg hatte am 28.3.2011 über die Rechtmäßigkeit der Beschlagnahme der GPS-Überwachungsanlage eines Privatdetektivs zu entscheiden. Die Anlage wurde zur lückenlosen Verfolgung des Aufenthaltsortes u. a. von Arbeitnehmern beim Verdacht missbräuchlicher Krankschreibungen eingesetzt. Zu diesem Zweck wurde sie an den Fahrzeugen der Zielpersonen angebracht. Dagegen hatte der niedersächsische Landesdatenschutzbeauftragte Strafanzeige gestellt.

Das Landgericht sah darin den Anfangsverdacht einer entgeltlichen unbefugten Erhebung und Verarbeitung personenbezogener Daten (§ 44 i.V.m. § 43 Abs. 2 Nr. 1 BDSG). Sollte die Entscheidung eines anschließenden Strafverfahrens der des Landgerichts folgen, die nicht die erste mit ähnlicher Tendenz ist, dürfte dies sowohl dem Auskunfteigewerbe als auch Auftraggebern privater Überwachungsmaßnahmen deutliche Grenzen setzen.

Immer wieder Facebook

Auf der Entwicklerkonferenz f8 am 22.09.2011 stellte Facebook neue Funktionen vor. So ermöglicht Facebook Timeline dem Nutzer nun, zurückliegende Erlebnisse oder Ereignisse an einer übersichtlichen Zeitleiste – wie eine persönliche „Chronik" – einzustellen. Und unter der Bezeichnung „frictionless sharing" kann man durch einmalige Einverständniserklärung gegenüber Facebook Webdiensteanbietern und Smartphone-Apps erlauben, alle eigenen Aktivitäten an Facebook zu melden. Dieses „Tracking" des gesamten digitalen Lebens (Welche Musik kaufe ich gerade? Auf welcher Seite surfe ich? Welches Online-Spiel habe ich eben gestartet?) kann dann mit Freunden geteilt werden.

In Europa sind mit diesen Diensten die nächsten Rechtsstreitigkeiten vorprogrammiert. Wie bislang wird es auch dabei nicht darum gehen, ob der Nutzer seine Daten in dieser Form der Welt oder Facebook preisgeben darf, sondern dass nach deutschem Datenschutzrecht die Diensteanbieter verantwortliche Stelle für die Übermittlung der Nutzungsdaten sind. Daher benötigen sie als Folge von § 15 TMG jeweils separate Einwilligungen, bei denen sie – deutlich weitergehend als in den Datenverwendungsregeln von Facebook – über Zweck und Art der Nutzung dieser Daten werden aufklären müssen. Dies gilt zumindest für alle europäischen Diensteanbieter und solche, die gezielt in Deutschland anbieten.

Solange sich Facebook außerdem Zweckänderungen und umfangreiche eigene Verarbeitungen vorbehält, selbst nicht umfassend aufklärt und keine ausreichende Einwilligung einholt, ist zudem Facebooks eigene Verarbeitung der Nutzerdaten rechtswidrig. Der Aktivist Max Schrems hat daher gegen Facebooks europäische Niederlassung in Irland wegen 22 Verstößen gegen europäisches Datenschutzrecht Anzeige erstattet.

Der Streit um und mit Facebook steht exemplarisch für die zahlreichen grundsätzlichen Missachtungen der Persönlichkeitsrechte im Internet – und des geltenden deutschen und europäischen Rechts.

Security Theatre in der Cloud

Am 04.10.2011 kündigte Amazon an, dass ab sofort Daten im Amazon Web Service (AWS) S3 durch eine serverseitige Verschlüsselung (SSE) geschützt werden können - eine Meldung, die in der deutschen Presse viel Resonanz gefunden hat. Diese Verschlüsselung erlaubt die „transparente Absicherung" von Daten in der Cloud – durch Amazon, inklusive der Erzeugung, Verwaltung und Vernichtung von Schlüsseln. Da stellt sich die Frage: Was genau wird hier eigentlich geschützt? SSE bewahrt die auf Amazon-Rechnern gespeicherten Daten vor Preisgabe bei einem Diebstahl der Datenträger aus dem Rechenzentrum. Damit schützt Amazon mit viel Wirbel gegen ein eher kleines Risiko.

Einen deutlich besseren Schutz bietet die Client-seitige Verschlüsselung mit dem AWS JDK for Java. Vielleicht möchte Amazon diesen Mechanismus aber gar nicht so gerne bewerben – schließlich macht er die Anwendungsentwicklung aufwändiger. Und die amerikanischen Sicherheitsbehörden sind dabei auch ausgesperrt.

Secorvo News

Kaminlektüre

Über vier Jahre haben wir daran geschrieben, und nach nur sechs Wochen war es so weit: Die erste Auflage des Secorvo-Buchs „Zentrale Bausteine der Informationssicherheit", auch als Begleitbuch zum T.I.S.P. geeignet, ist ausverkauft. Auflage zwei ist bereits im Druck und voraussichtlich ab der ersten Novemberwoche verfügbar. Wem also noch eine Kaminlektüre für die langen Winterabende fehlt, dem sei das Werk ans Herz gelegt. Bei einer Anmeldung zum T.I.S.P.-Seminar (nächster Termin: 07.-11.05.2012) ist das Buch inklusive und wird vorab zugesandt.

Seminare

Für alle Kurzentschlossenen bietet Secorvo noch drei Weiterbildungschancen (mit garantierter Durchführung) im Jahr 2011:

- Das Seminar PKI – Grundlagen, Vertiefung, Realisierung vom 08.-11.11.2011 bietet Ihnen einen Einblick in die Konzeption, Implementierung und Nutzung von PKIs.
- Ihre IT-Security-Grundlagenkenntnisse können Sie beim Seminar IT-Sicherheit heute vom 15.-17.11. 2011 auffrischen.
- Eine praxisorientierte Einführung in die sichere Softwareentwicklung bekommen Sie beim Seminar ISECCO Certified Professional for Secure Software Engineering (CPSSE) vom 22.-24.11.2011 mit anschließender Zertifikatsprüfung.

Sichern Sie sich jetzt einen der noch freien Plätze. Die Programme aller Seminare, die Möglichkeit zur Online-Anmeldung und das Jahresprogramm 2012 finden Sie unter http://www.secorvo.de/college. Wir freuen uns auf Ihre Anmeldung!

Durch die Hintertür

Die Erbringung von IT-Dienstleistungen erfordert in wachsendem Umfang den Fernzugriff auf IT-Systeme. Wie kann man sich dabei aber gegen Zugriffe unberechtigter Dritter und einen unkontrollierten Datenabfluss schützen? Was ist bei der Fernwartung heute „state-of-the-art" – und von welchen Techniken sollte man besser die Finger lassen?

Diese und weitere Fragen rund um die Absicherung von Wartungszugriffen beantwortet Dr. Böttger (Leiter CONNECT-SupportCenter) in seinem Vortrag auf dem kommenden Event „Wer kommt da durch die Hintertür?" der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 17.11.2011 um 18 Uhr im Schlosshotel Karlsruhe. Um Anmeldung wird gebeten.

Veranstaltungshinweise

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

November 2011	
08.-11.11.	PKI (Secorvo College, Karlsruhe)
11.11.	Outsourcing und Vendor Security (Gesellschaft für Informatik/Fachgruppe SECMGT, Frankfurt)
15.-17.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
17.11.	Wer kommt da durch die Hintertür? (KA-IT-Si)
22.-25.11.	CPSSE (Secorvo College, Karlsruhe)
Dezember 2011	
05.-06.12.	IsSec/ZertiFA 2011 (Computas, Berlin)
Januar 2012	
17.-19.01.	OMNICARD 2012 (in TIME berlin, Berlin)
24.-26.01.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
Februar 2012	
08.-09.02.	22. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.-22.02.	19. DFN Workshop „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)

Fundsache

Das NIST veröffentlichte am 27.09.2011 den Draft einer überarbeiteten Fassung der Special Publication SP 800-121 „Bluetooth Security“, die nun auch die Bluetooth-Standards 3.0 und 4.0 (Low Energy) berücksichtigt. Die Security-Checkliste ist auf 34 Empfehlungen angewachsen und ersetzt die Listen für Headsets und Smart Card Reader der Vorfassung.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Michael Knopp, 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