secorvo
security consulting

Secorvo Security News

Dezember 2014

Im Überwachungsstaat

Es war ein Jubiläum, das niemand beging – 30 Jahre nach „1984“, dem Jahr von Orwells Überwachungsstaat. Wirkte der Schreck über Snowdens Veröffentlichungen so nach, dass uns das Feiern verging? Oder ist die Ursache beunruhigender: Sind wir Frösche im Kochtopf, dessen Wasser schleichend erwärmt wird? Fragen wir uns vielleicht: Können wir überhaupt (noch) etwas tun? Oder blenden wir die allgegenwärtige Überwachung aus und reden uns (immer noch) ein, dass wir nichts zu verbergen haben? Es ist ja noch nichts passiert (zumindest haben wir nichts gemerkt), und böse Tyrannen gibt es ohnehin nur in Geschichtsbüchern und Nachrichten aus fernen Ländern.

Wenn wir die Realität nicht zumindest teilweise ausblenden, wird es unangenehm. Wer mag WhatsApp, GMail oder Facebook noch nutzen, wenn er ständig daran denkt, dass jede Nachricht und jeder „Like“-Klick, jeder Chat und jede Internet-Suche mitgeschnitten, beobachtet und zu einem Bild von uns verdichtet wird, das nie mehr gelöscht und jederzeit ausgewertet werden kann? Aber das Smartphone ausschalten? Dann ist man nicht erreichbar! E-Mails verschlüsseln? Dann kann man sie nicht mehr mit jedem Client abrufen! Auf das Navi verzichten? Wer hat denn heute noch einen Autoatlas? („Papi, was ist ein Autoatlas?“)

Derweil schrumpft der Bereich, in dem unser Verhalten nur im Gedächtnis unserer Mitmenschen vergängliche Spuren hinterlässt. „Car-IT“ analysiert Fahrverhalten und Regelverstöße, „SmartHomes“ steuern Heizung und Beleuchtung, und abends erfreut „SmartTV“ mit individualisiertem Programmangebot. Vielleicht war es richtig, sich nicht an „1984“ zu erinnern. Denn was uns wirklich bevorsteht, hat Ray Bradbury („Fahrenheit 451“) 1953 zutreffender vorausgesehen: Wir leben in einem technologischen Wunderland, rundumversorgt und perfekt unterhalten, bei umfassender Kontrolle (zu unserer eigenen Bequemlichkeit) – und haben vor lauter Unterhaltungsglück vergessen, wie Freiheit und Erkenntnis schmecken.

Inhalt

secorvo
security consulting

Security News

Und wieder SSL...

Am 08.12.2014 veröffentlichte der Security Engineer Adam Langley ein weiteres Poodle-Dilemma, von dem diesmal TLS betroffen ist. Das Protokoll füllt beim blockweisen Verschlüsseln den letzten Block per Padding auf. Der Empfänger muss die Gesamtlänge des Paddings prüfen – Load-Balancer von F5 und A10 Networks sowie einige Cisco-Geräte prüfen jedoch nicht und sind daher anfällig für Poodle. Wahrscheinlich ist die Wiederverwendung alter SSL-Funktionen die Ursache. F5 und A10 haben bereits Patches veröffentlicht.

Mit dem SSL Server Test von Ivan Ristić (Qualys) kann man die Verwundbarkeit des eigenen Servers testen. Grundsätzlich empfiehlt sich die Umstellung auf die aktuelle TLS-Version 1.2 mit AEAD-Blockverschlüsselung. Den Entwicklern der anfälligen Implementierungen empfehlen wir vor der Wiederverwendung von Security-Code sorgfältige Funktionstests.

Ein Klick für mehr Datenschutz

Social Plugins, die kleinen Spione der sozialen Netzwerke, die viele Betreiber von Internetseiten allzu freiwillig in ihren Quellcode einbinden, sind seit langem ein Dorn im Auge der Datenschützer. 2011 stellte Heise eine 2-Klick-Lösung für mehr Datenschutz vor (SSN 1/2012): Baute man den Code-Schnipsel in seine Seite ein, konnten die Social Plugins nicht ungefragt Daten übertragen. Stattdessen wurde der Benutzer über einen gesonderten Hinweis (erster Klick) gefragt, ob er z. B. eine „Like"-Meldung an das soziale Netzwerk übermitteln will. Erst nach seiner Bestätigung (zweiter Klick) wurde das Skript des Plugins aktiviert.

Zwei Klicks auf einer Internetseite sind eine Hürde, daher setzte sich die Heise-Lösung nicht flächendeckend durch. Mit Shariff hat Heise am 27.11.2014 nun einen Nachfolger in den Ring geschickt, bei dem nur noch ein Klick nötig ist. Die neuen Buttons sind einfache HTML-Links, die via CSS individuell gestalten werden können; sie müssen nicht mehr umständlich eingebettet werden.

IM Encryption for the Masses

Am 18.11.2014 hat Open Whisper Systems, der Spezialist für Verschlüsselungslösungen für Instant Messaging, seine Zusammenarbeit mit WhatsApp bekannt gegeben. In den letzten sechs Monaten hat man an einer Integration des TextSecure Protokolls gearbeitet. Die neueste Version von WhatsApp auf Android nutzt das Protokoll bereits transparent im Hintergrund. Auch wenn noch wichtige Funktionen wie die Verifikation der Schlüssel von Kommunikationspartnern, die Unterstützung von Gruppenchats und die Unterstützung anderer Plattformen fehlen, ist die Implementierung einer Ende-zu-Ende-Verschlüsselung ein Schritt in die richtige Richtung. Hoffentlich folgt der notwendige Rest...

Türsteuerung gibt Zugang preis

Am 01.12.2014 publizierte das RedTeam ein Advisory zur Schwachstelle in der Türsteuerung EntryPass N5200 – über die Konfigurationsoberfläche konnte die Kennung und das Passwort des Administrators in Erfahrung gebracht werden. Die – insbesondere bei der Timeline recht unterhaltsame – Schwachstellenmeldung zeigt, was man nicht tun sollte: So gibt der auf dem System betriebene simple Webserver recht freizügig Informationen preis. Woraus wir lernen können: Auch bei einem physischen Sicherheitssystem darf man die Sicherheit des IT-Anteils nicht ignorieren. Es muss immer das Gesamtsystem betrachtet werden.

Bei Angriffsmöglichkeiten kann man nicht voraussetzen, dass Systeme in einem separierten Management-Netz betrieben werden. Sofern ein System über einen netzseitigen Zugang verfügt, muss der auch entsprechend abgesichert werden. Debug-Meldungen oder sonstige Informationen, die einem Angreifer helfen können, darf das System im Auslieferungszustand nicht mehr ausgeben.

Strafverfolgungspfründe

Der U. S. District Court, S. D. New York hat am 31.10.2014 eine gerichtliche Weisung gegen einen Mobilfunkbetreiber bestätigt, der die Durchsuchung eines Mobiltelefons durch Hilfestellung bei der Entschlüsselung des Speicherinhalts unterstützen sollte. Die Weisung stützt sich auf ein über 225 Jahre altes Gesetz, nach dem ein US-Gericht Dritte zur Mitwirkung verpflichten kann, wenn diese in einer Position sind, in der sie auch als Unbeteiligte den Erfolg einer gerichtlichen Maßnahme verhindern könnten.

Aus dieser Entscheidung könnte abgeleitet werden, dass Mobilfunkbetreiber nach US-Recht verpflichtet sind, sich die Möglichkeit zur Entschlüsselung bei von ihnen vertriebenen Geräten offen zu halten. Das wäre ein weiterer Rückschlag für US-Anbieter, die gerade dabei sind, verlorenes Vertrauen ausländischer Kunden nach dem NSA-Skandal zurückzugewinnen. Jedenfalls lassen die Strafverfolgungsbehörden keine Gelegenheit aus, um zu verhindern, dass Daten ihrem Zugriff entzogen werden.

Ob Turing das gewollt hätte?

Ohne den Turing-Test durch CAPTCHAs (SSN 2/2008) würden viele Kontakt- und Registrierungsformulare, Foren und Downloadangebote im Internet von Bots überrollt. Allerdings werden CAPTCHAs auch für den Nutzer immer herausfordernder (und nerviger), weil Maschinen die Aufgaben zunehmend besser lösen können als wir (SSN 4/2009).

Wie ein verfrühtes Weihnachtsgeschenk kam am 03.12.2014 eine neue Methode von Google namens No CAPTCHA reCAPTCHA daher. Google berechnet dabei schon vor der Eingabe des CAPTCHA-Codes mithilfe der IP-Adresse, der Verweildauer auf der Seite und der Mausbewegungen im CAPTCHA-Feld, wie wahrscheinlich es ist, dass der Besucher ein Mensch ist. Dieser muss dann keinen Code mehr lösen, sondern nur noch einen Haken setzen. Auf Smartphones funktioniert die Methode mangels Mausbewegungen nicht – hier muss man „lustiges" Tier-Memory spielen.

Doch halt: IP-Adresse übermitteln? Mausbewegungen auswerten? War da nicht etwas mit Datenschutz? Nicht erst „No CAPTCHA", schon der Einsatz des reCAPTCHA-Dienstes bedarf der vorherigen Einwilligung der Seitenbesucher. Schließlich werden dabei personenbezogene Daten an Google übermittelt. reCAPTCHA kann man nicht einmal per Browser-Plugin blockieren. Unterhalb des Radars der meisten Datenschützer hat sich reCAPTCHA massenweise ausgebreitet. Datenschutzkonform und benutzerkompatibel ist einzig eine selbst gehostete CAPTCHA-Lösung.

Internationaler Datenverkehr

Mit ihrem am 26.11.2004 veröffentlichen Arbeitspapier 226 hat die Art. 29-Gruppe ein Verfahren in Kraft gesetzt, das Zuständigkeitskonflikte und bürokratische Hindernisse bei der Verwendung von EU-Standardvertragsklauseln vermeiden soll, wenn bspw. eine internationale Unternehmensgruppe für den konzerninternen Datenverkehr die an sich unveränderlichen Standardvertragsklauseln aufgrund nationalem Recht ergänzt und hierzu eine Genehmigung benötigt. Nun kann die anfragende Stelle eine führende Aufsichtsbehörde vorschlagen, die für alle übrigen Stellen die Rechtskonformität prüft. Alle anderen zuständigen Behörden prüfen nur noch die Voraussetzungen des nationalen Rechts.

Das Papier bekräftigt, dass die Standardvertragsklauseln um weitere Regelungen ergänzt werden können. Auch wenn zunächst nicht viele betroffene Stellen von dem neuen Verfahren Gebrauch machen werden, ist dies eine wichtige Klarstellung.

Secorvo News

Zertifizierter Datenschutzkoordinator

Für Datenschutzbeauftragte gibt es Weiterbildungsangebote wie Sand am Meer. Dünner wird die Luft bei Angeboten für Datenschutzkoordinatoren, die ihrem Datenschutzbeauftragten zuarbeiten. Am 28. bis 29.04.2015 bieten wir die Weiterbildung zum „Geprüften Datenschutzkoordinator im Unternehmen" an. Mit Bestehen der Abschlussprüfung kann der Datenschutzkoordinator anschließend seine Qualifikation mit einem Zertifikat belegen.

Der T.I.S.P. entwickelt sich zu dem am weitest verbreiteten deutschen Personenzertifikat für Informationssicherheit. 700 T.I.S.P.-Absolventen gibt es inzwischen, die sich in einer eigenen Community regelmäßig zum Erfahrungsaustausch treffen. Die nächste Möglichkeit, eine unserer T.I.S.P.-Schulungen zu besuchen, bieten wir Ihnen Mitte März.

Anfang März bringt Sie das Seminar IT-Sicherheit heute in drei Tagen auf den aktuellen Stand – Sie erfahren, was Sie als IT-Sicherheitsverantwortlicher über die aktuelle Sicherheitslage wissen sollten.

Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Krönungsfest

Es ist der höchstdotierte, privat gestiftete Preis Deutschlands: der deutsche IT-Sicherheitspreis, ausgelobt von der Horst Görtz Stiftung und seit 2006 alle zwei Jahre verliehen. Der Preis würdigt mit Preisgeldern in Höhe von insgesamt 200.000 € herausragende deutsche Innovationen in der IT-Sicherheit. Im Jahr 2014 ging der erste Preis über 100.000 € an Herrn Professor Müller-Quade (KASTEL/KIT) und die Karlsruher Firma WIBU-Systems für die Entwicklung der Blurry-Box – einer zukunftsweisenden Lösung für den Softwareschutz, die nicht auf der Geheimhaltung des Verfahrens beruht.

Nicht genug, dass damit Professor Müller-Quade nach seiner Auszeichnung im Jahr 2008 bereits zum zweiten Mal Träger des ersten Preises ist: der KA-IT-Si-Partner WIBU-Systems erhielt die Auszeichnung pünktlich zum 25. Unternehmensjubiläum. Gründe genug für die KA-IT-Si, um Ihnen vorzustellen, was in Karlsruhe möglich ist – und diese Krönung unseres IT-Sicherheitsstandorts bei unserer nächsten KA-IT-Si-Veranstaltung am **15.01.2015** im Informatik-Gebäude des KIT mit Ihnen zu feiern. Anmeldung unter www.ka-it-si.de.

Veranstaltungshinweise

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

Januar 2015	
15.01.	Krönungsfest (KA-IT-Si, Karlsruhe)
16.-18.01.	ShmooCon 2015 (The Shmoo Group, Washington/US)
20.-22.01.	Omnicard 2015 (in TIME berlin, Berlin)
Februar 2015	
04.-05.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
24.-25.02.	22. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2015	
03.-05.03.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen & Schutzmechanismen (Secorvo, Karlsruhe)
09.-13.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
23.-26.03.	2nd DFRWS EU Conference (DFRWS, Dublin/IE)

Fundsache

Im November 2014 wurde auf der CCS 2014 eine Studie zur Aussagekraft von Webseiten-Prüfsiegeln vorgestellt (siehe auch Placebo-Zertifikate, SSN 11/2014). Dabei fanden praktisch alle Prüfverfahren bei einer präparierten Webseite nur einen Bruchteil der Schwachstellen. Auch wurden zahlreiche Webseiten im Netz gefunden, die trotz Prüfsiegel Schwachstellen aufwiesen. Hier wird dem Besucher der Website ein Sicherheitsniveau vorgegaukelt, das eher zu einer Sicherheitsgefährdung aufgrund falschen Vertrauens als zu einem Sicherheitsgewinn führt.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Sven Köhler, Christoph Schäfer.

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