secorvo
security consulting

Secorvo Security News

Juni 2014

Die Vertrauensattacke

Während das US-amerikanische Repräsentantenhaus am 23.06.2014 mit überwältigender Mehrheit (293:123 Stimmen) der NSA untersagte, Hintertüren in US-amerikanische IT-Produkte einzubauen und die Internet-Aktivität amerikanischer Bürger ohne Gerichtsbeschluss zu überwachen, blieben wichtige Aspekte der Geheimdiensttätigkeit ungeregelt.

Vor dem Hintergrund der amerikanischen Überwachungsaktivitäten der vergangenen 20 Jahre wird ein bedenkliches Gesamtbild erkennbar. In den 90er Jahren versuchte die NSA vergeblich, sich den Zugriff auf verschlüsselte Daten zu sichern: Schwache Verschlüsselungsverfahren, wie der auf Drängen der NSA von 128 auf 56 bit Schlüssellänge verkürzte DES, waren durch öffentlich evaluierte, starke Verfahren wie den AES ersetzt worden. Und das „Law Enforcement Access Field" (LEAF), mit dem sie sich eine Entschlüsselungsmöglichkeit erhalten wollte, scheiterte 1994 an einer blamablen Protokollschwäche.

Danach verlegte sich die NSA auf eine verdeckte Universalstrategie – und attackierte jeden möglichen Angriffspunkt der entstehenden, auf SSL basierenden Vertrauensinfrastruktur:

- SSL-Serverbetreiber, deren geheimer SSL-Schlüssel die Entschlüsselung mitgeschnittener Kommunikation ermöglichte,
- Zertifizierungsinstanzen, die Schlüsselpaare erzeugten (und damit auch Zugang zu geheimen SSL-Schlüsseln besaßen),
- Zertifizierungsinstanzen, die der NSA falsche SSL-Zertifikate für Man-in-the-Middle-Angriffe ausstellten,
- möglicherweise auch (Open)SSL-Implementierungen, um Hintertüren in Soft- oder Firmware zu verankern und
- Standardisierungsgremien, um Zufallszahlengeneratoren mit Vorhersagemöglichkeit für die NSA zu etablieren (SSN 11/2013).

Das Ergebnis ist ein Scherbenhaufen: Vertrauensverlust in SSL, amerikanische Anbieter und die Standardisierung. Wer wird das kitten?

Inhalt

secorvo
security consulting

Security News

Sicherer im Netz mit Tails

Am 10.06.2014 wurde Version 1.0.1 des Live-Betriebssystems Tails veröffentlicht. Tails kann von einem USB-Stick gestartet werden und eröffnet den Internetzugang standardmäßig über das Tor-Netzwerk. Weitere Maßnahmen zum Schutz der Privatsphäre sind die Veränderung der MAC-Adresse sowie die GPG-Unterstützung des E-Mail-Clients. Um Angriffswege zu reduzieren ist zudem in der Grundeinstellung der Root-Account deaktiviert.

Im Test lief Tails auf verschiedenen Laptops einwandfrei, mit ordentlicher Bildschirmauflösung und WLAN-Unterstützung – ohne dass die Grundkonfiguration angepasst werden musste. Will man eine dauerhafte Datenpartition auf dem Stick anlegen, sollte man Tails von einem bereits laufenden Tails – beispielsweise von DVD gestartet – kopieren. Auf der verschlüsselten Partition können dann eigene Dateien abgelegt werden. Tails hinterlässt keine Spuren auf dem genutzten Rechner.

Tails macht einen durchdachten Eindruck und ist ein möglicher Weg, einen „ergrauten" XP-Rechner mit einem aktuellen Betriebssystem auszustatten – das gelingt sogar im „XP-Look", wenn man diese Option beim Starten auswählt.

Dämmer im Dunkel

TK-Unternehmen haben Transparenzberichte als Mittel entdeckt, um ihrer juristischen Machtlosigkeit gegenüber staatlichen Zugriffen zumindest ihren guten Willen zum Schutz der Kundendaten entgegenzusetzen. So bestätigt Vodafone in einem am 06.06.2014 veröffentlichen Bericht, in 29 Staaten Behörden Zugriff auf Telekommunikationsdaten gewähren zu müssen.

Dabei werden deutliche Unterschiede in Art und Umfang der Zugriffe erkennbar. In Deutschland müssen TK-Anbieter auf Grundlage von § 5 des Artikel 10-Gesetzes, § 110 Abs. 1 Nr. 5 TKG und § 27 TKÜV staatlichen Stellen Zugriff auf die bei ihnen gespeicherten Daten gewähren. Dazu speichern sie die relevanten Daten in einer so genannten *interception copy* („Überwachungskopie"), die dem Nachrichtendienst übergeben wird. Vorher werden die Daten nach vorgegebenen Suchbegriffen gefiltert – und nicht relevante Teile gelöscht.

Ein solch umständliches Vorgehen ist in zumindest sechs Staaten, die Vodafone nicht namentlich benennt, nicht erforderlich: Dort müssen TK-Anbieter Direktzugriffe gewähren. In Albanien, Ägypten, Indien, Malta, Katar, Rumänien, Südafrika, Türkei und Ungarn darf zudem nicht darüber berichtet werden, wie und in welchem Umfang Überwachungsmaßnahmen erfolgen. Auch ohne weitere Snowdens wissen wir nun immerhin, wer sich neben den USA noch an unseren TK-Daten bedient.

Cyberabwehr in der Kritik

Das holperige Kürzel ist Programm: Irgendwie ist niemand mit dem seit dem 01.04.2011 tätigen Nationalen Cyberabwehrzentrum (NCAZ) so recht glücklich. Die einen wundern sich, dass Deutschland mit zehn Mitarbeitern im „Cyberwar" bestehen will. Verfassungsrechtler schlagen Alarm, da die vorgeschriebene Trennung zwischen Nachrichtendiensten und Polizei durch das NCAZ ad absurdum geführt werde – immerhin arbeiten ihm das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Verfassungsschutz (BfV), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundeskriminalamt (BKA), die Bundespolizei (BPol), das Zollkriminalamt (ZKA), der Bundesnachrichtendienst (BND) sowie die Bundeswehr zu. Vernichtend äußert sich der Bundesrechnungshof in einem nicht öffentlichen Bericht, aus dem die Süddeutsche am 07.06.2014 zitierte: Danach sei das NCAZ „*nicht geeignet, die über die Behördenlandschaft verteilten Zuständigkeiten und Fähigkeiten bei der Abwehr von Angriffen aus dem Cyberraum zu bündeln.*" Der Nutzen der Einrichtung sei fraglich. Der Bundesrechnungshof rät, das „*Abwehrzentrum (...) mit eigenen Aufgaben und Kompetenzen für die Abwehr von Cyberangriffen*" auszustatten.

Allein das BMI sieht das NCAZ als Erfolgsgeschichte: Bis März 2013 habe es 900 nationale und internationale IT-Sicherheitsvorfälle bewertet. Sensationelle 1,2 Vorfälle pro Tag.

Ende der WLAN-Störerhaftung

Endlich hat der Bundesgerichtshof die Urteilsbegründung zu seinem am 08.01.2014 verkündeten Urteil zur Störerhaftung des Anschlussinhabers bei Urheberrechtsverletzungen veröffentlicht. Das Urteil schließt an die Entscheidung „Sommer unseres Lebens" an, in dem die Haftung bejaht worden war (SSN 06/2010). Im aktuellen Fall verwies der Beklagte auf die WLAN-Mitnutzung volljähriger Familienangehöriger, und der BGH verlangte lediglich eine überzeugende Darlegung, dass es weitere (familienangehörige) WLAN-Nutzer gäbe. Auch bei einer unzureichenden Sicherung könne eine Vermutung der Täterschaft des Anschlussinhabers nicht greifen. Schließlich ergebe sich selbst eine Überwachunspflicht von Minderjährigen (SSN 11/2012) erst bei Anzeichen für eine missbräuchliche Nutzung.

In einem ähnlichen Fall wies das AG Hamburg am 10.06.2014 die Haftung des Betreibers eines

Ferienhotels zurück, der seinen Mietern ein WLAN zur Nutzung anbot: Es erkannte ihn als Dienste-anbieter an, womit der Haftungsausschluss des § 8 TMG greift. Nach dieser Rechtsprechung sinkt das Risiko von Abmahnungskosten für Anschluss-inhaber, die Mieter oder Familienangehörige als Mitnutzer zulassen.

E2E-Verschlüsselung in Chrome

Am 03.06.2014 hat Google die Alpha-Version von „End-to-End“ angekündigt, eines Verschlüsselungs-tools für den Chrome-Browser. Überraschender-weise soll es nicht den S/MIME-Standard, sondern OpenPGP unterstützen und damit einen mit PGP und GnuPG kompatiblen, verschlüsselten E-Mail-Austausch ermöglichen.

Die Implementierung erfolgte in JavaScript. Es werden ausschließlich ECC-Schlüssel erzeugt; RSA-Keys können aber aus einem anderen Schlüsselring importiert werden.

Einige wichtige Fragen rund um die Implementie-rung beantwortet Google in einer FAQ. Nach der Testphase soll die End-to-End-Erweiterung im Google Web Store bereitgestellt werden. Jetzt wird es vor allem von der Bedienungsfreundlichkeit der Browser-Erweiterung abhängen, ob sich diese Lösung bei Privatnutzern durchsetzen kann.

Folgen des Suchmaschinenurteils

Als Reaktion auf das Suchmaschinenurteil des EuGH (SSN 05/2014) stellte Google ein Löschantragsfor-mular bereit, von dem bereits rege Gebrauch ge-macht wurde. Inzwischen hat Microsoft angekün-digt, mit seiner Suchmaschine Bing nachzuziehen.

Die Blockierung der Suchergebnisse erfolgt jedoch nur gegenüber europäischen Suchmaschinennut-zern; allen anderen werden die Ergebnisse weiter angezeigt. Da der EuGH in seinem Urteil Google Inc. als verantwortliche Stelle spanischem Datenschutz-recht unterworfen hat, reicht die regional begrenzte Sperrung jedoch nicht aus; sie muss für den gesamten Dienst des Betreibers erfolgen.

Zudem stellt die Authentifizierung der Antragsteller ein ungelöstes Problem dar. In der ersten Version des Formulars hatte Google rechtswidrig die Vorlage einer Personalausweiskopie verlangt; die aktuelle Version fordert eine Kopie eines „identifizierenden Dokuments“ – keine geeignete, Missbrauch aus-schließende Identifizierungsform. Für die Prüfung behält sich Google die Einschaltung der Aufsichts-behörden vor. Wie Anträge geprüft werden sollen, zu denen eine Begründung verlangt wird, ist derzeit noch offen.

Secorvo News

Das Buch, der T.I.S.P. und das Zertifikat

Mitte Juni haben wir die erweiterte, aktualisierte und überarbeitete Ausgabe unseres Grundlagen-buchs „Zentrale Bausteine der Informationssicher-heit“ fertiggestellt. Das auch für die Vorbereitung auf eine T.I.S.P.-Zertifizierung geeignete, 700 Seiten starke Begleitbuch ist bereits als E-Book (pdf) verfügbar; die gebundene Fassung ist noch im Druck, kann aber schon bestellt werden und wird voraussichtlich in der zweiten Julihälfte geliefert.

Die nächste Gelegenheit zur Vorbereitung auf das T.I.S.P.-Zertifikat bieten wir vom **22.–27.09.2014**., alternativ können Sie sich auf dem Seminar „IT-Sicherheit heute“ (**30.09.–02.10.2014**) auf den aktuellen Stand bringen lassen.

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

6. Tag der IT-Sicherheit

Bereits zum sechsten Mal findet am **09.07.2014** der „Tag der IT-Sicherheit“ statt, den die KA-IT-Si jährlich gemeinsam mit dem CyberForum e.V., der IHK Karlsruhe und KASTEL veranstaltet. Frau Dr. Birte Mössner, Leiterin Corporate Compliance und Daten-schutz der EnBW beleuchtet in ihrer Keynote die Relevanz des Datenschutzes im Compliance-Kon-text. Während TechniData auf das nicht immer einfache Verhältnis von IT-Managern und Sicher-heitsverantwortlichen und Secorvo auf die daten-schutzrechtlichen Fallstricke im Marketing eingeht, steht bei 1&1 die technische Sicherheit im Mittel-punkt. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

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

Juli 2014	
09.07.	6. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
August 2014	
02.-07.08.	Blackhat USA 2014 (Blackhat, Las Vegas/US)
03.-06.08.	14th Annual DFRWS Conference 2014 (DFRWS, Denver/US)
07.-10.08.	DEF CON 21 (DEFCON, Las Vegas/US)
17.-21.08.	Crypto 2014 (IACR, Sanata Barbara/US)
20.-22.08.	23rd USENIX Security Symposium (Usenix, San Diego/US)
25.-25.08.	Sommerakademie (ULD Schleswig-Holstein, Kiel)
September 2014	
16.-19.09.	OWASP AppSec USA 2014 (OWASP Foundation, Denver/US)
16.-17.09.	D • A • CH Security (GI, OCG, BITKOM, SI, TeleTrusT, Graz/AT)
18.09.	Informationstag "Elektronische Signatur" 2014 (TeleTrust, Berlin)

Fundsache

Die Agentur der Europäischen Union für Grundrechte, der Europarat und die Kanzlei des Europäischen Gerichtshofs für Menschenrechte haben am 05.06.2014 ein gut strukturiertes, 220 Seiten starkes Handbuch zum Europäischen Datenschutzrecht in fünf Sprachen herausgegeben.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Michael Knopp, 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