secorvo
security consulting

Secorvo Security News

Februar 2014

Zwischenbilanz

Neun Monate nach den ersten Enthüllungen Edward Snowdens über die Überwachungstätigkeit der NSA zeichnet sich die zukünftige Entwicklung ab. In seiner Rede vom 17.01.2014 machte Präsident Obama deutlich, dass sich allein bei der Überwachung amerikanischer Bürger und ausgewählter Staatsoberhäupter etwas ändern wird. Und RSA-CEO Art Coviello erklärte in seiner Keynote am 25.02.2014 unzweideutig: Auch amerikanische Sicherheitsunternehmen arbeiteten mit der NSA zusammen – und werden es auch künftig tun, wenn es um die (Sicherheits-) Interessen der USA geht. Selbst die Kritik namhafter Kryptologen vom 24.01.2014 zielt in erster Linie auf die Überwachung amerikanischer Bürger und die Schwächung von Sicherheitstechnologie ab. Vor diesem Hintergrund und den dank Snowden bekannten Fakten können wir daher dreierlei festhalten:

1. Trust the Math: Wie Bruce Schneier bereits am 06.09.2013 schrieb, gibt es keine Hinweise darauf, dass die NSA in der Lage ist, kryptografische Verfahren zu brechen, die von Kryptologen als ausreichend sicher angesehen werden. Wer „ausgemusterte" Verfahren und kurze Schlüssellängen meidet, liegt daher mit kryptografischem Ende-zu-Ende-Schutz immer richtig.
2. Misstraue der Implementierung: Auch gute kryptografische Verfahren lassen sich so implementieren, dass ein Angreifer leichtes Spiel hat – dank einer schwachen Schlüsselerzeugung (Pseudo-Zufall), einer Hintertür (Backdoor) oder einem Programmierfehler. Deutschen Herstellern und überprüfter oder zertifizierter Software gebührt diesbezüglich ein Vertrauensbonus.
3. Misstraue den Vertrauensankern: Sicherheit gibt es nicht aus dem Nichts – so wie man sich nicht am eigenen Schopf aus dem Sumpf ziehen kann, benötigt auch Sicherheit einen Vertrauensanker wie z. B. den Aussteller eines SSL-Zertifikats. Statt blindem Vertrauen ist hier eine kritische Prüfung Pflicht.

Inhalt

secorvo
security consulting

Security News

Zeit zum Wechsel

Die Ankündigung von Facebook, den Instant-Messaging-Dienst WhatsApp für 19 Mrd. US$ zu übernehmen, hat am 19.02.2013 für viel Wirbel gesorgt. Dieser Deal hat bei zahlreichen Nutzern das Interesse an sicheren Alternativen zu WhatsApp geweckt; auch die Stiftung Warentest stufte WhatsApp in einem am 26.02.2014 veröffentlichten Vergleichstest als „sehr kritisch" ein. Die stolze Nutzerzahl von ca. 450 Mio. könnte daher schon bald erodieren.

Bereits auf der ersten Karlsruher Anti-Prism-Party am 05.09.2013 stellten wir die aus der Schweiz stammende Alternative Threema vor. Zu einer weiteren Alternative könnte sich der Open-Source Messenger Surespot entwickeln. Die Offenheit des Quellcodes ist ein Plus für Surespot – Threema kann hingegen bei der Implementierung des Schlüsselaustausches punkten. Neben den Instant-Messengern mit Zwischenspeicherung von Daten bleibt die Nutzung von OTR über Jabber-basierte Chat-Dienste eine sichere Alternative – hierbei müssen allerdings beide Gesprächspartner online sein.

Die Downloads zur Anti-Prism-Party umfassen eine Installations- und Konfigurationsanleitung sowie weitere Informationen zur sicheren Nutzung von Internet-Diensten.

Facebook rechtswidrig

Die Berufungsentscheidung des Kammergerichts Berlin vom 24.02.2014 bestätigte Facebook, dass an Nicht-Mitglieder versandte Einladungen zur Registrierung wettbewerbswidrig und die AGB sowie die Datenschutzbestimmungen u. a. hinsichtlich der Gewinnung der Adressen rechtswidrig sind. Auch die unbestimmte, vergütungsfreie und vollständige Rechteübertragung der Inhalte an Facebook verstößt gegen geltendes AGB-Recht. Dasselbe gilt für die einschränkungslosen Änderungs- und die einseitigen Beendigungsklauseln. Die Entscheidung zum *Friend Finder* folgt der Rechtsprechung zu Empfehlungs-E-Mails (SSN 1/2014) und stellt fest, dass die Beteiligung des Nutzers bei der Versendung von Registrierungseinladungen an Dritte für die Einstufung als belästigende Werbung unmaßgeblich und die diesbezügliche Nutzereinwilligung in die Datenverwendung unwirksam ist.

Besonders brisant – und im Widerspruch zum Schleswig-Holsteinischen Verwaltungsgericht (SSN 2/2013) – wird die Anwendbarkeit deutschen Rechts bejaht: Als 100%ige Gesellschafterin habe ungeachtet aller Verträge Facebook Inc., USA, die Entscheidungsmacht. Eine Auftragsdatenverarbeitung käme in dieser gesellschaftsrechtlichen Konstellation nie in Betracht. Dieser Satz dürfte die meisten Konzerngesellschaften mit zentralen Verarbeitungsprozessen und ausländischer Muttergesellschaft mit Entsetzen erfüllen.

Kleiner Bug – große Wirkung

Die Zeilen 631 und 632 der Datei sslKeyExchange.c sehen eher harmlos aus – wird dort doch nur das eingerückte Statement „goto fail" wiederholt. Allerdings hat diese Einrückung weitreichende Wirkung – wie Apple am 21.02.2014 in einem Security Update mitteilen musste. Die offenbar bei der Entwicklung von OS X 10.9 eingeführte Änderung öffnet Man in the Middle-Angriffen auf Apple-Betriebssysteme Tür und Tor. Nach 46 Jahren werden damit Dijkstras Befürchtungen zur bitteren Realität – ein unverzügliches Update von OS X 10.9, iOS 7.0 und iOS 6.1 wird daher dringend empfohlen.

Durchsuchungsverbot

Mit einem nun ausführlich veröffentlichten Urteil vom 20.06.2013 hat das Bundesarbeitsgericht die Anforderungen an das Vorgehen bei Verdachtsmomenten gegen Beschäftigte weiter konkretisiert und den besonderen Rechtfertigungsbedarf für heimliche Überwachungsmaßnahmen verdeutlicht.

In dem entschiedenen Fall war ein Spind aufgrund eines Diebstahlsverdachts unter Einbeziehung des Betriebsrats, aber ohne Beteiligung des Betroffenen durchsucht worden. Dies führte im anschließenden Kündigungsschutzprozess wegen der Unverhältnismäßigkeit der Maßnahme zu einem Beweisverwertungsverbot.

Diese Entscheidung unterstreicht einmal mehr, dass das Vorgehen bei derartigen Untersuchungen klar geregelt und der Betroffenenbeteiligung und -information ein hoher Stellenwert eingeräumt werden sollte, um am Ende belastbare Feststellungen zu erhalten.

Gefahr aus dem IoT

Zunehmend werden Alltagsgegenstände mit eingebetteten Computern ausgestattet und über das Internet vernetzt, wie Babyphones, Videoüberwachungsanlagen oder Heimnetzwerksteuerungen. Das „Internet der Dinge" (*Internet of Things* – IoT), Mark Weisers Vision einer vernetzten Welt aus dem Jahr 1991, wird langsam Realität. Leider sind auch die damit verbundenen Gefahren inzwischen real. Symantec berichtete am 21.01.2014 über einen Linux-Wurm, der auf das IoT zielt. Der Wurm existiert für typische Chiparchitekturen des IoT.

Darauf ist das IoT jedoch nicht vorbereitet. Dort stehen wir bei der Sicherheit da, wo wir vor zwanzig Jahren bei PCs standen: Sicherheitsschwachstellen wurden nicht veröffentlicht, und falls Hersteller Patches bereitstellten, wussten die Benutzer nicht, wie diese zu installieren waren. Schlimmer noch: Soft- oder Firmware der Geräte sind im IoT oft älter als diese. Ist der Quellcode nicht vollständig verfügbar, kann nicht einmal ein Patch erzeugt werden.

Zudem sind die Geräte des IoT ständig mit dem Internet verbunden. Sie lassen sich mit der Suchmaschine Shodan sogar gezielt suchen. Dennoch werden auch solche Geräte mit einem Default-Passwort ausgeliefert. Da die Geräte meist keinen automatischen Update-Mechanismus besitzen, besteht die Gefahr, dass mit vermeintlichen Updates aus nicht autorisierter Quelle Firmware mit Hintertüren eingeschleust wird – wie bei dem am 18.02.2014 bekannt gewordenen Fall der intelligenten Haushaltsgeräte von Belkin Wemo.

Erweiterter Process Explorer

Am 29.01.2014 wurde der Process Explorer von Microsoft um eine hilfreiche Funktion ergänzt: Version 16 unterstützt nun VirusTotal-Abfragen für laufende Prozesse und die von diesen bei jedem Programmstart zahlreich hinzugeladenen Dynamic Link Librarieres. Ist die Funktion aktiviert, werden MD5-Summen gebildet und mit den Erkenntnissen von 50 verschiedenen Virenscannern bei VirusTotal abgeglichen. Ein blauer (‚gut') oder roter (‚böse') Zahlenwert weist dann auf „kritische Erkenntnisse" hin. Ein blaues Ergebnis ist allerdings eher eine „Tendenzaussage", schließlich gibt es Schadsoftware, die von diesem Werkzeug und vielen Antivirusprogrammen in einer Live-Umgebung nicht gefunden wird.

Bei der Aktivierung wird man um die Zustimmung zur Nutzungsvereinbarung von VirusTotal gebeten – in der man alle Verwertungsrechte für hochgeladene Daten an VirusTotal abtritt. Ach ja: Seit 2012 gehört VirusTotal zu Google.

DIN-Norm Datenlöschung

Im Dezember 2012 stellte Secorvo die DIN-Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten vor, die auf großes Interesse stieß. Ende 2013 startete daher ein von den Unternehmen Blancco, DATEV, Deutsche Bahn, Secorvo und Toll Collect gefördertes Projekt, in der die Leitlinie nun zu einer DIN-Norm weiterentwickelt wird. Am 12.02.2014 beschloss der DIN-Arbeitskreis für Identitätsmanagement und Datenschutz-Technologien (AK 05 im NIA 27) die Aufnahme eines Normungsprojekts.

Die Norm für Löschkonzepte soll bis zum Herbst 2015 verabschiedet werden. Die veröffentlichte Leitlinie gibt bereits heute wesentliche Hilfestellung für die Entwicklung eigener Löschkonzepte.

Secorvo News

System Security

Security Engineering – die Entwicklung inhärent sicherer Systeme – ist eine vergleichsweise junge Disziplin. In den vergangenen Jahren ist jedoch aus zahlreichen Erfahrungen und *Best Practices* ein sinnvolles Vorgehensmodell entstanden. Dabei wird die Sicherheit eines Systems aus unterschiedlichen Blickwinkeln betrachtet, um die vielfältigen Abhängigkeiten und externen Einflüsse bereits beim Systemdesign zu berücksichtigen.

In dem Seminar Security Engineering – Sichere Systeme durch Security by Design legen wir dar, wie Sicherheit in die Prozesse und Lebenszyklen der Systementwicklung integriert werden kann. Sie haben die Möglichkeit, Ihre erworbenen Kenntnisse anschließend mit dem T.E.S.S. zertifizieren zu lassen (12.-15.05.2014). Und falls Sie – schnell entschlossen – zuvor noch ein T.I.S.P.-Zertifikat erwerben wollen: vom 24. bis 28.03.2014 haben Sie die Gelegenheit dazu, es gibt noch einige wenige freie Plätze. Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Herkunft verpflichtet.

In modernen Informationssystemen (Stichwort *Data Warehouse* oder *Big Data*) erreicht die Verarbeitung von personenbezogenen Daten eine Komplexität, die die Umsetzung datenschutzrechtlicher Transparenzanforderungen erheblich erschwert. *Data Provenance* (Bestimmung der Datenherkunft) kann dabei unterstützen, die Herkunft und die Bearbeitung von personenbezogenen Daten sowie den Zugriff auf diese nachvollziehbar zu gestalten. Beim nächsten KA-IT-Si Event am 03.04.2014 um 18 Uhr in den Räumen des Fraunhofer IOSB in Karlsruhe zeigt Christoph Bier (Fraunhofer IOSB) in seinem Vortrag „Data Provenance. Auch Daten haben ihre Geschichte", wie die Datenschutzauskunft der Zukunft aussehen könnte.

Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

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

März 2014	
24.-29.03.	T.I.S.P.-Schulung und -Prüfung (Secorvo College, Karlsruhe)
April 2014	
03.04.	Herkunft verpflichtet. (Karlsruher IT-Sicherheitsinitiative, Karlsruhe)
08.-10.04.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen, Schutzmechanismen (Secorvo College, Karlsruhe)
Mai 2014	
05.-09.05.	CPSSE (Certified Professional for Secure Software Engineering) – Schulung und Prüfung (Secorvo College, Karlsruhe)
07.-09.05.	1st DFRWS EU Conference (DFRWS, Amsterdam/NL)
11.-15.05.	Eurocrypt 2014 (IACR, Kopenhagen/DK)
12.-16.05.	Security Engineering – Schulung & T.E.S.S.-Prüfung (Secorvo College, Karlsruhe)
12.-14.05.	IMF 2014 (Fraunhofer IAO, Münster)
14.-16.05.	15. Datenschutzkongress (Euroforum, Berlin)

Fundsache

Das Portal Netzpolitik.orG verschenkt seit dem 19.02.2014 das im November 2013 erschienene Buch „Überwachtes Netz“ mit spannenden Beiträgen von Autoren wie Constanze Kurz, Frank Rieger, Markus Beckedahl, Peter Schaar, Bruce Schneier und Richard Stallman. Das Buch ist erhältlich als ePub, AZW3 oder PDF.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, 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