secorvo
security consulting

Secorvo Security News

August 2017

Neuland

Am 19.06.2013 äußerte Bundeskanzlerin Angela Merkel in einer Pressekonferenz mit Barack Obama, dass das Internet „für uns alle Neuland“ sei – und musste für diese Formulierung viel Hohn und Spott einstecken. Dabei ging ihr Satz weiter: Das Internet „ermöglicht auch Feinden und Gegnern unserer demokratischen Grundordnung mit völlig neuen Möglichkeiten und völlig neuen Herangehensweisen unsere Art zu leben in Gefahr zu bringen.“

Die Äußerung fiel zwar im Kontext der NSA-Überwachung, doch brachte Frau Merkel damit (wenn auch womöglich unwillentlich) eine empfindliche Wahrheit auf den Punkt: Nach wie vor treiben Hersteller mit einer erschütternden Naivität die Digitalisierung ihrer Produkte voran und schaffen mit unausgereiften und offenbar unzureichend getesteten Lösungen gefährliche neue Angriffspunkte.

Solange es sich dabei um via Internet zugängliche Überwachungskameras handelt, mag das noch als handwerkliche Ungeschicklichkeit mit Spaßfaktor durchgehen. Inzwischen erfasst die von Sicherheitsaspekten unbelastete Digitalisierung allerdings immer mehr Produkte, bei denen Angriffe eine unmittelbare Gefahr für Leib und Leben darstellen. Blieb der Angriff auf ein motorisiertes Skateboard noch eher unbeachtet, sorgte die von einem Journalisten im Selbstversuch dokumentierte Attacke auf einen Chrysler Cherokee im Juli 2015 immerhin für etwas Wirbel. Gelernt haben daraus allerdings noch lange nicht alle, wie der am 18.07.2017 bekannt gewordene Angriff auf einen Segway MiniPro zeigt.

Jeder Sicherheitsgurt, jeder Reifen und jede Stoßstange muss einen Sicherheitstest absolvieren. Aber IT-Schnittstellen, bei denen Fehler zu wesentlich dramatischeren Eingriffen in die Fahrzeugsicherheit führen können, dürfen ohne vertiefte Prüfung verbaut werden. Es fehlen sogar anerkannte, standardisierte Testverfahren, mit denen wir solche Systeme verlässlich prüfen könnten. Neuland eben.

Inhalt

secorvo
security consulting

Security News

Wie gut ist mein Passwort?

In den SSN 05/2017 haben wir über die geänderten Empfehlungen des NIST zur Wahl geeigneter Passwörter berichtet. Unter anderem wird empfohlen, Passwörter mit Listen kompromittierter Passwörter abzugleichen. Der Sicherheitsforscher Troy Hunt, bekannt durch die Bereitstellung von Listen gehackter Accounts, bietet seit dem 03.08.2017 die Online-Prüfung von Passwörtern gegen ca. 320 Millionen bekanntermaßen kompromittierter Passwörter an. Sie kann per Formular oder via API erfolgen.

Hunt warnt selbst davor, solche Webdienste mit Passwörtern zu nutzen, die in Gebrauch sind – was den Nutzwert des Angebots deutlich reduziert. Immerhin bietet er die Passwörter auch als SHA1-Hashes zum Download an. Mit etwas Programmierung (Stichwort: binäre Suche) lässt sich damit schnell ein Werkzeug erstellen, mit dem man seine Passwörter lokal überprüfen kann.

Einheitlicher Beschäftigtendatenschutz

Bereits am 08.06.2017 hat die Art. 29 Gruppe unter anderem eine Stellungnahme zum Beschäftigtendatenschutz (WP 249 – Opinion 2/2017 on data processing at work) verabschiedet. Diese aktualisiert die Stellungnahmen WP 48 und 55 aus den Jahren 2001 und 2002, ausgehend noch von der Datenschutzrichtlinie, aber mit Bezug auf die künftige Datenschutz-Grundverordnung und den aktuellen Entwurf der ePrivacy-Verordnung.

Der Beschäftigtendatenschutz wird durch die Öffnungsklausel in Art. 88 DS-GVO den Mitgliedsstaaten zur eigenständigen Regelung überlassen. Die Stellungnahme fasst Verhältnismäßigkeitserwägungen zu typischen Verarbeitungskontexten zusammen. Allgemein werden Anforderungen an die Ausfüllung von Art. 88 DS-GVO formuliert, die deutlich über den deutschen § 26 BDSG-neu (vorher § 32 BDSG) hinausgehen.

Es wird klargestellt, dass Arbeitgeber Arbeitnehmer nicht ausschließlich auf vorgegebene Social-Media-Profile verpflichten können, auch nicht, wenn diese öffentlich das Unternehmen vertreten. Es wird die Erforderlichkeit von Transparenz und dokumentierten Datenschutzrichtlinien bei IT-Nutzungsüberwachungen betont. Bezüglich Mobile Device Management Lösungen wird generell eine Datenschutz-Folgenabschätzung für erforderlich gehalten.

Gesichtserkennungstechnologien im Beschäftigungskontext werden abgelehnt. Für Einwilligungen und berechtigte Interessen des Arbeitgebers als Rechtsgrundlage wird nur ein sehr eingeschränktes Anwendungsfeld gesehen. Die Stellungnahme stellt eine hilfreiche Zusammenfassung und Orientierungshilfe dar, zumal viele aktuelle und praktische Problemstelllungen angesprochen und mit Szenarien erläutert werden.

Meinungswandel

Ob eine juristische Person (bspw. eine Firma) als externer Datenschutzbeauftragter bestellt werden kann, ist eine in der Praxis durchaus relevante, aber bislang umstrittene und nicht entschiedene Frage. Der Hessische Datenschutzbeauftrage empfiehlt nun in einem Informationspapier zum betrieblichen Datenschutzbeauftragten nach der Datenschutz-Grundverordnung vom 29.06.2017, die Bestellung einer juristischen Person bis zu einer endgültigen Klärung durch den Europäischen Datenschutzausschuss mit der zuständigen Aufsichtsbehörde lediglich abzusprechen.

Die sich abzeichnende Kehrtwende der Aufsichtsbehörden zu dieser durch den Gesetzeswortlaut weiter offenen Frage geht auf ein bereits im Dezember 2016 veröffentlichtes Arbeitspapier (WP 243) der Art. 29 Datenschutzgruppe zurück. Die Europäischen Aufsichtsbehörden halten darin die Bestellung einer juristischen Person ausdrücklich für möglich. Voraussetzung ist, dass die für die juristische Person handelnden Mitarbeiter die Qualifikationsvoraussetzungen erfüllen. Dabei wird ausdrücklich anerkannt, dass die Kombination der Qualifikationen mehrerer Einzelpersonen einer Firma die Wirksamkeit der Tätigkeit in der Praxis steigern kann.

Auch wenn eine endgültige Anerkennung des Modells noch abzuwarten bleibt, öffnet sich damit der Weg für eine praxistauglichere Bestellpraxis, die die bisherigen mühsamen Konstrukte zur persönlichen Bestellung externer Datenschutzbeauftragte überflüssig macht. Bisherige Appelle in diese Richtung waren bislang bei den Aufsichtsbehörden eher auf Ablehnung gestoßen.

Suricata extended

Bereits am 27.07.2017 erschien das robuste Network Intrusion Detection/Prevention/Security Monitoring System Suricata nach ca. 18 Monaten in der Version 4.0.0-stable. Eine wesentliche Neuerung ist die Integration der Programmiersprache RUST, dank der neben deutlich gesteigerter Geschwindigkeit auch eine sicherere Speicherverwaltung und Threats ohne Race Conditions möglich wurden.

Technisch neu sind bei TLS die Dekodierung und das Logging von STARTTLS für SMTP und FTP sowie von

TLS Session Resumptions. Hinzugekommen ist die Unterstützung für das NFS-Protokoll, welches im kommerziellen Umfeld nach wie vor eine wichtige Rolle spielt. Hinzugekommen ist mit der Implementierung des Extensible Event Format (EVE) die Möglichkeit, bei gekapseltem Netzwerkverkehr (encapsulated traffic) auch die innere und äußere IP-Adresse inklusive der zugehörigen Ports auszuwerten.

Alexas lokale Überwachung

Am 01.08.2017 stellte Mark Barnes einen Angriff auf Amazons Echo vor, der das Gerät in eine Abhörstation verwandelt. Auf der Unterseite des Geräts kann über die dortige Kontaktleiste eine SD-Karte angeschlossen werden, mit der das Gerät gebootet werden kann. Anschließend lassen sich über geeignete Skripte das interne Laufwerk ansprechen und die Firmware modifizieren. Auf diesem Weg ist es beispielsweise möglich, Mikrofon-Aufzeichnungen von Echo unbemerkt an einen Dritten zu übermitteln.

Auch wenn Barnes' Angriff nur für bis 2016 verkaufte Geräte nachweislich funktioniert und in neueren Geräten ab 2017 unterbunden wurde, sollte man die Gefahr durch Abhör-Angriffe über manipulierte Geräte mit Mikrofon nicht gering schätzen: Zwar benötigt der Angreifer Zugang zum Gerät, aber die Kosten sind vernachlässigbar.

Selbst führende Hersteller sind sich dieser Gefahr offenbar wenig bewusst, wenn sie von außen zugängliche Daten-Schnittstellen am Gerät vorsehen. Aber auch ein hermetisch verschlossenes Gerät birgt ein Restrisiko: Dass der Hersteller die mitgeschnittenen Worte nicht selbst zu anderen als den im Prospekt versprochenen Zwecken nutzt, darauf müssen Sie in jedem Fall vertrauen.

Rekall's Agent

Pünktlich zum jährlichen Rekall-Workshop auf der DFRWS 2017 ist seit dem 07.08.2017 die Version 1.7 für Windows, Linux und OSX verfügbar. Neben vielen Weiterentwicklungen bei den Plugins (z. B. iexport für NTFS-Dateiextraktion via $MFT) und der Ausweitung auf ca. 2.000 vordefinierte, spezifische Kernelprofile steht die Agenten-Komponente im Mittelpunkt, die sich nun als dauerhafter Service (Daemon) auf Endsystemen installieren lässt.

Mit diesem Release wandelt sich Rekall von einer Stand-Alone-Installation zu einem eigenständigen forensischen Client-Server Incident Response Framework und bietet Unterstützung für Echtzeitforensik auf Client-Systemen. Praktisch ist u. a. die Ausführung von WMI-Queries in Live-Systemen, um Erkenntnisse jenseits eines reinen Hauptspeicherabzugs zu erhalten.

Der Agent stößt außerdem eine spannende Entwicklung an: Client-side Plugins. Dies wird bereits durch das neue vfs_ls-Plugin ermöglicht, mit dessen Hilfe nun „Remote Timelines" auf Clients erstellt werden können – fast in Echtzeit und mit hoher Aussagekraft.

Secorvo News

BSIG-Prüfverfahrens-Kompetenz

Vier Berater und Auditoren von Secorvo haben inzwischen erfolgreich die Prüfverfahrens-Kompetenz nach § 8a (3) BSIG erworben. Sie ist Eignungsvoraussetzung für die Prüfung Kritischer Infrastrukturen und weiterer vom IT-Sicherheitsgesetz betroffener Unternehmen und Institutionen – und hilfreich beim Aufbau geeigneter Informationssicherheits-Management-Systeme.

Frisches aus der Hackerküche

Am **21.09.2017** startet die KA-IT-Si in die zweite Jahreshälfte. Benjamin Lipp und Timon Hackenjos (Fraunhofer IOSB) zeigen, wie ein im September 2016 veröffentlichter Angriff auf Windows-Anmeldeinformationen in abgewandelter Form auch heute noch funktioniert. Benny Görzig und Florian Loch (ebenfalls Fraunhofer IOSB) stellen Angriffe auf das Netzwerkauthentifizierungsprotokoll WPA2-PSK vor, das die meisten von uns in ihren privaten WLAN-Netzen benutzen. Wird die Authentifikation von einem Angreifer mitgeschnitten, liefert sie einen Hashwert, den der Angreifer für einen Angriff auf das WLAN-Passwort verwenden kann.

Im Anschluss an die Vorträge haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Secorvo-Seminare

Interessenten an unserem PKI-Seminar vom **06. bis 09.10.2017** mit einem vertieften Einblick in Public Key Infrastrukturen empfehlen wir eine baldige Buchung. Und vom **16. bis 19.10.2017** bieten wir Software Engineers das T.P.S.S.E.-Seminar mit der Möglichkeit zur anschließenden Zertifizierung als *TeleTrusT Professional for Secure Software Engineering*.

Die nächste Möglichkeit zur T.I.S.P.-Zertifizierung bieten wir Ihnen mit dem T.I.S.P.-Seminar vom **27.11. bis 01.12.2017**; das Begleitbuch „Zentrale Bausteine der Informationssicherheit" erhalten Sie vorab zur Vorbereitung.

Programme, Online-Anmeldung und weitere Termine: secorvo.de/seminare.

Veranstaltungshinweise

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

September 2017	
05.-06.09.	D • A • CH Security (GI, OCG, TeleTrusT, München)
18.09.	Sommerakademie 2017 (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel)
19.-22.09.	OWASP AppSec USA 2017 (OWASP Foundation, Orlando/US)
21.09.	Frisches aus der Hackerküche (KA-IT-Si, Karlsruhe)
26.09.	Anwendertag IT-Forensik (Fraunhofer-Institut SIT, Darmstadt)
Oktober 2017	
10.-12.10.	it-sa 2017 (Nürnberg Messe, Nürnberg)
16.-19.10.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-19.10.	IDACON 2017 (WEKA-Akademie, München)
24.-26.10.	heise devSec 2017 (dpunkt.verlag, Heidelberg)
November 2017	
06.-09.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
14.-15.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
21.-23.11.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
27.11.-01.12.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), 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