secorvo
security consulting

Secorvo Security News

Januar 2016

Next Big Thing

Während Experten noch darüber streiten, was genau unter „Industrie 4.0“ zu verstehen ist, rauscht bereits die nächste große „IT-Sau“ auf das Dorf zu: das „Internet of Things“, kurz: IoT. Zwar ist die Idee nicht mehr ganz frisch: Sie basiert auf einem Aufsatz von Mark Weiser aus dem Jahr 1991 und dem „Ubiquitous computing“ – der Erwartung, dass die Miniaturisierung von Computern diese allgegenwärtig machen wird. Im Automobil ist das bereits Realität: Hunderte Steuerungs- und Diagnosesysteme sind darin verbaut. Dank des mit IPv6 ins Unvorstellbare (genauer: auf $3{,}4 \cdot 10^{38}$) vergrößerten Adressbereichs kann nun jedes Staubkorn auf unserem Planeten eine IP-Adresse erhalten – erst recht die immer kompakteren und leistungsfähigeren Miniaturrechner. Ausgestattet mit Sensoren vermessen diese nun unsere Welt: Das Einschalten von Geräten verrät unser Nutzungsverhalten, die Senderwahl im TV unsere Vorlieben, der Kühlschrank erlernt unsere Ernährungsgewohnheiten, die Armbanduhr erhebt unsere Vitaldaten, das Gaspedal erkennt unseren Fahrstil, den der Bordcomputer mit dem Ortsinformationen korreliert.

Damit sind Dienste möglich, die unsere Vorstellungskraft (noch) übersteigen: Nach intensiver Gerätenutzung könnten uns Neugeräte angeboten, das abendliche TV-Programm passgenau zusammengestellt, Nahrungsmittel geliefert, bevor der Vorrat zur Neige geht, Medikamente bei Bedarf automatisch zugestellt, Rasen und Falschparken direkt an die zuständigen Behörden gemeldet, Versicherungsprämien aus dem tatsächlichen Risiko (Zigaretten? Alkohol? Blutdruck? Riskanter Fahrstil?) berechnet und Verhaltensoptimierungen via App empfohlen (und deren Einhaltung überprüft) werden.

Derweil einigten sich die Datenschutzaufsichtsbehörden mit dem VDA am 26.01.2016, dass „... die bei der KfZ-Nutzung anfallenden Daten (...) jedenfalls dann personenbezogen (...) sind, wenn eine Verknüpfung mit (...) dem KfZ-Kennzeichen vorliegt“.

Inhalt

secorvo
security consulting

Security News

Firewalls mit Hintertür

Nachdem kurz vor Weihnachten Netzwerkgeräte von Juniper mit gleich zwei Hintertüren (sowohl im SSH-Zugang als auch im Zufallszahlengenerator für VPN-Verbindungen) für Aufsehen sorgten, zog am 12.01.2016 der bekannte Firewall-Hersteller Fortinet nach. Ein fest kodiertes „Managementpasswort" erlaubte es Angreifern jahrelang, sich per SSH an Fortigate-Firewalls anzumelden. Die Schwachstellen sind zwar behoben, ein ungutes Gefühl in der Magengegend bleibt jedoch. Beide Fälle zeigen, dass Netzwerkgeräte und Appliances kein uneingeschränktes Vertrauen verdienen.

Bei Penetrationstests entdecken wir in Netzwerkgeräten häufig vom Internet erreichbare Management-Zugänge wie SSH oder Web-Schnittstellen. Begründet wird der Zugang oft damit, dass so eine schnelle Remote-Fehlerbehebung ermöglicht werden solle – schließlich würden sichere Passwörter, Anmeldemechanismen und Protokolle eingesetzt. Die entdeckten Hintertüren sollten Anlass sein, solche Zugänge auf den Prüfstand zu stellen.

Abmahnrecht für Verbände

Bislang konnten Datenschutz-Verstöße in erster Linie von Betroffenen abgemahnt werden. Teilweise wurde dieses Recht auch Mitbewerbern zugesprochen. Mit dem am 17.12.2015 beschlossenen „Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts" kommen registrierte Verbände hinzu. Das UKlaG und das BGB werden angepasst.

Künftig können beispielsweise Verbraucherschutzzentralen per Unterlassungsklage gegen Unternehmen vorgehen, die aus ihrer Sicht Datenschutzverstöße mit Verbraucherbezug begehen. Während die meisten Datenschutz-Aufsichtsbehörden eher auf Einsicht von Unternehmen setzen, dürften Verbände weniger Beißhemmungen und vor allem mehr (personelle) Kapazitäten haben.

Besonders Betreiber von Web-Shops dürften die Auswirkungen spüren. Bisher konnten fehlende oder falsche Klauseln in AGB und Datenschutzerklärungen abgemahnt werden; nun kommen tatsächliche Datenverarbeitungen hinzu. Die Verbände werden sich Vorgänge wie Bonitätsprüfungen oder Retargeting vermutlich sehr genau anschauen. Unternehmen sollten das Gesetz zum Anlass nehmen, ihre Web-Shop-Prozesse von ihrem betrieblichen Datenschutzbeauftragten überprüfen zu lassen.

OpenSSH-Schwäche

Für das weit verbreitete OpenSSH Projekt begann das neue Jahr am 14.01.2016 mit einer gravierenden Client-Schwachstelle (CVE-2016-0777). Sie ermöglicht es, unter Ausnutzung der (experimentellen) Roaming-Funktionalität mit einem manipulierten Server-Dienst bei einer Authentisierung mit privatem Schlüssel diesen auszulesen. Damit können sich Angreifer, die einen Server übernehmen konnten, die Schlüssel der Administratoren verschaffen. Da letztere oft das gleiche Schlüsselpaar für eine große Anzahl von Servern nutzen, erhalten die Angreifer so die Credentials für alle diese Server.

Gegen derartige Angriffe können sich Nutzer durch das Deaktivieren des Roaming Supports oder durch das Einspielen eines gepatchten SSH-Clients schützen. Eine präventive Maßnahme wäre die Verwendung eines Schlüsselpaars pro Zielsystem oder der Einsatz von Smartcards gewesen.

Wie bei Heartbleed hatte hier eine Schwachstelle in einer praktisch nicht genutzten, experimentellen Funktion gravierende Auswirkungen auf die Sicherheit des gesamten Systems. Vor allem bei derart sicherheitskritischen Werkzeugen sollte man sich auf den Grundsatz besinnen: Weniger ist mehr!

Freunde finden

Der Bundesgerichtshof hat am 14.01.2016 die Funktion „Freunde finden" von Facebook für rechtswidrig erklärt und damit das Berufungsurteil des Kammergerichts Berlin vom 24.01.2014 bestätigt. Facebook verschickte über diese Funktion mittels der aus den Adressbüchern neu registrierter Nutzer ermittelten E-Mail-Adressen automatisch Einladungen zur Registrierung auch an Nicht-Mitglieder des Netzwerks. Der Verbraucherzentrale Bundesverband (VZBV) war 2010 hiergegen vorgegangen. Der BGH hat nun bestätigt, dass darin eine unzulässige, belästigende Werbung i. S. von § 7 Abs. 1 und 2 Nr. 3 UWG sowie eine Täuschung der Nutzer über die Verwendung ihrer Adressbuchdaten gelegen habe. Das Ergebnis der Revision ist wenig überraschend. Die Praxis, Adressbuchdaten ungefragt zu nutzen, hat Facebook inzwischen längst aufgegeben.

Zahlreiche weitere Soziale Netzwerke, z. B. auch Xing, bieten den Nutzern ähnliche Funktionen, um Einladungen an ihre Adressbuchkontakte zu verschicken. Nach den Kriterien des bestätigten Berufungsurteils führt die bloße technische Hilfestellung durch den Netzwerkanbieter jedoch nicht zu unerlaubter Werbung. Offen ist allerdings noch, wie der BGH automatisch generierte Erinnerungen an eine solche Einladung bewertet.

Cross Device Tracking

Dass smarte Software „nach Hause telefoniert“, um ihren Hersteller mit Nutzungsdaten zu versorgen, ist nicht neu. Neu ist, dass besonders smarte Software über Device-Grenzen via Ultraschall miteinander kommuniziert – und so ihr Wissen über das Nutzungsverhalten an PC, Smartphone, Tablet und TV verknüpfen kann. Am 16.10.2015 hatte das Center for Democracy and Technology (CDT) in einem öffentlichen Brief an die US-amerikanische Federal Trade Commission zu diesem seit mindestens Mitte 2014 bekannten Verfahren Stellung genommen.

Marktführer ist demnach die indische Firma SilverPush, die für das menschliche Ohr nicht wahrnehmbare Tonsequenzen in TV- und Browser-Werbung einblendet, die von einem in bereits mehr als 67 Apps versteckten SDK empfangen und ausgewertet werden können. Angeblich kontrolliert SilverPush auf diese Weise schon mehr als 18 Mio. Smartphones – und erfährt so, wie lange eine Anzeige oder eine TV-Werbung sichtbar ist oder ob sie weggeklickt wird. Offenbar gehören auch Google, Nestle und McDonalds zu den über 150 Kunden von SilverPush, wie Jai Vardhan am 11.11.2015 berichtete.

Tatsächlich entzieht sich diese Art des Trackings jeder technischen Gegenmaßnahme – und ist zudem nicht ohne weiteres feststellbar. Wer sich davor schützen will, dem bleibt nur, das Mikrofon seines Smartphones abzukleben – oder die „Aus“-Taste zu suchen (und zu betätigen).

Secorvo News

Wer druckt, der bleibt

Bei unserem kommenden KA-IT-Si-Event am **02.02.2016** (ausnahmsweise einem **Dienstag**) wird Ihnen Hendrik Herberger (Modox - Modern Documents GmbH) in seinem Vortrag „Übersehen und unterschätzt - Live Hacking von Druckern“ die Gefährdung Ihrer Daten durch moderne Drucker und Kopierer aufzeigen und konkrete Empfehlungen geben, wie sich diese Risiken minimieren lassen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Anmeldung unter www.ka-it-si.de.

Das T.I.S.P.-Zertifkat

Am 29.02.2016 startet die erste T.I.S.P.-Schulung 2016. Sie schließt mit der Prüfung zum T.I.S.P.-Zertifikat ab. Die Schulung gibt Ihnen einen umfassenden und themenübergreifenden Überblick über die wichtigsten Gebiete der Informationssicherheit. Vorab erhalten Sie zur Vorbereitung das Begleitbuch „Zentrale Bausteine der Informationssicherheit“. Mehr als 800 IT-Sicherheitsexperten belegen ihre Qualifikation bereits mit dem anerkannten T.I.S.P.-Zertifikat. Termin: **29.02.-04.03.2016** in Karlsruhe. Es gibt nur noch wenige freie Plätze.

Das T.E.S.S.-Zertifikat

System Security Engineering betrachtet die Sicherheit komplexer Systeme. Diese hängt nicht nur von den Sicherheitseigenschaften der beteiligten Komponenten, sondern auch von deren Zusammenwirken und den verwendeten Schnittstellen und Protokollen ab. In der Schulung T.E.S.S. lernen Sie das Zusammenspiel aller Faktoren so zu gestalten, dass das resultierende Gesamtsystem Ihren Sicherheitsanforderungen genügt. Mit dem Erwerb des T.E.S.S.-Zertifikats (TeleTrusT Engineer System Security) dokumentieren Sie Ihre Qualifikation. Termin: **04.-07.04.2016** in Karlsruhe

PKI für Experten

Wer für die Konzeption, den Aufbau oder Betrieb einer PKI zuständig ist, sei unser Praxis-Seminar-Klassiker wärmstens ans Herz gelegt. Fast 300 positive Teilnehmerbewertungen belegen, dass die Expertise und Erfahrung aus 19 Jahren PKI-Praxis ankommt. Termin: **19.-22.04.2016** in Karlsruhe

Detailbeschreibungen unserer Seminarangebote und die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite.

Krypto im Advent

In Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe realisierten wir den interaktiven Online-Adventskalender „Krypto im Advent“. Mehr als 1.100 Schülerinnen und Schülern der Klassen 3 bis 7 machten sich im Dezember 2015 täglich an die Lösung einer Knobelaufgabe aus der Welt der Kryptologie. Dabei gab es zahlreiche gesponserte Sachpreise zu gewinnen. Aufgrund der großen und begeisterten Resonanz werden wir das Adventsrätsel auch 2016 anbieten. Zum Üben gibt es alle Aufgaben aus dem vergangenen Jahr (und die Lösungen) zum Download.

Veranstaltungshinweise

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

Februar 2016	
02.02.	Wer druckt, der bleibt (KA-IT-Si, Karlsruhe)
09.-10.02.	23. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
17.-18.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)>
29.02.-04.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
März 2016	
08.-11.03.	Java Security (Secorvo, Karlsruhe)
21.-24.03.	1st IEEE European Symposium on Security and Privacy (IEEE, Saarbrücken)
29.03.-01.04.	2nd DFRWS EU Conference (DFRWS, Dublin/IE)
April 2016	
04.-07.04.	T.E.S.S. - TeleTrusT Engineer System Security (Secorvo, Karlsruhe)
11.-14.04.	CPSSE - Certified Professional for Secure Software Engineering (Secorvo, Karlsruhe)
19.-22.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)

Fundsache

Der Informatiker Carsten Eilers hat am 28.01.2016 ein (kostenfreies) E-Book veröffentlicht, in dem er alle 2015 bekannt gewordenen Router-Schwachstellen zusammengefasst hat. Eine hilfreiche Checkliste.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, 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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.