secorvo
security consulting

Secorvo Security News

August 2019

Digitale Blockwarte

Manchmal kommen selbst dramatische Paradigmenwechsel verhuscht um die Ecke. So wissen wir zwar längst, dass ein Gerät, das seinen Standort über Satellitenortung oder WLAN-Accesspoints bestimmen kann, diese Information auch gelegentlich weitergibt. Natürlich dient das nie der Erstellung von Bewegungsprofilen, sondern ausschließlich anderen, unverdächtig nützlichen Zwecken, wie der Bestimmung der Verkehrsdichte, der exakten Berechnung der richtigen Kochzeit für das Frühstücksei oder der behütenden Aufsicht über den Nachwuchs. Charmant obendrein: Ortungsfunktion oder Gerät lassen sich ausschalten (ja, tatsächlich!), und schon sind wir zurück in steinzeitlicher Freiheit.

Damit könnte es allerdings bald endgültig vorbei sein. Wenn die Idee hinter Apples „Apple Tag" (angekündigt für iOS 13 auf der Entwicklerkonferenz am 03.06.2019) Schule macht, ist die Steinzeit abgelaufen. Und die Freiheit mit ihr. Wie so oft kommt die Überwachung im Schafspelz daher: Elektronische Geräte ohne Ortungs- und Mobilfunk-Chipsatz sollen von anderen, kommunikations- und GPS-fähigen Geräten via Bluetooth kontaktiert, die übermittelte Geräte-ID mit aktueller Ortsinformation angereichert und an Apple geschickt werden – damit verlorene oder gestohlene Devices einfacher und schneller wiedergefunden werden.

Welch zauberhafte Vorstellung: Dank Millionen digitaler Blockwarte müssen wir unsere Schlüssel, Hunde, Zahnbürsten oder Rasierapparate nie mehr suchen oder uns über entwendete Gadgets grämen – einfach ins Netz gucken, und schon wissen wir, wo sie sind. Und auch der Standort der Blockwarte ist jederzeit dokumentiert.

Schade nur, dass die Entwicklung ziemlich genau 30 Jahre zu spät kommt. Wie viel volkswirtschaftliches Vermögen hätte man damit im Ministerium für Staatssicherheit sparen können...

Und die Geschichte wäre vielleicht ganz anders verlaufen.

Inhalt

secorvo
security consulting

Security News

Bluetooth-Downgrade

Ex- und Import von Verschlüsselungslösungen stießen in den 90er Jahren noch auf zahlreiche Restriktionen. Daher verwenden Bluetooth-Verbindungen bis heute getrennte Schlüssel für Integritätsschutz und Verschlüsselung. Während ersterer immer 128 bit lang ist, kann letzterer auf bis zu 8 bit verkürzt werden. Fast 20 Jahre dauerte es, bis ein internationales Forscherteam eine diesen Umstand nutzende Downgrade-Attacke entdeckte und am 14.08.2019 veröffentlichte: Ein Angreifer, der sich in die Schüsselaushandlung einschaltet, kann die Kommunikationspartner dazu bringen, einen 8 Bit Schlüssel zu verwenden und so die übertragenen Daten entschlüsseln.

Wer vertrauliche Daten (wie die Anschläge einer Tastatur oder Dokumente zum Drucken) und nicht nur die aktuelle Playlist via Bluetooth überträgt, sollte prüfen, ob die Hersteller beider Geräte Patches bereitstellen – oder doch zu einer kabelgebundenen Übertragung zurückkehren.

Kreditkarten-Upgrade

Auch bei einem am 29.07.2019 veröffentlichten Kreditkartenangriff mischt sich der Angreifer in die Aushandlung seiner beiden Opfer ein. So ermöglicht Visa inzwischen, am Point-of-Sale durch einfaches Auflegen der Kreditkarte zu bezahlen. Das Missbrauchsschäden bei gestohlenen Karten begrenzende Zahlungslimit (in Großbritannien £ 30) kann dabei durch die Man-in-the-Middle-Attacke auf ein Vielfaches erhöht werden.

Trotz des Proof-of-Concept will Visa nicht sofort etwas gegen die Schwachstelle unternehmen. Zwar kann ein Einzelschaden leicht im drei- oder vierstelligen Bereich liegen, doch dass organisierte Kriminelle zahlreiche Komplizen mit der erforderlichen Elektronik vor Ort auf „Einkaufstour" schicken, erscheint eher unwahrscheinlich. Daher dürfte Visa erst bei einem ohnehin fälligen Wechsel von Karten und Terminals eine sicherere Version ausrollen.

Heiße Schwachstelle

Eingebettete Systeme sind die jüngste Achillesferse der IT-Sicherheit. Da liegt es nahe, Betriebssysteme zu verwenden, die mit Fokus auf Sicherheit und Zuverlässigkeit entwickelt wurden, wie beispielsweise Wind Rivers marktführendes VxWorks. Umso schockierender ist daher eine Nachricht wie die vom 09.08.2019: Elf Schwachstellen wurden in VxWorks 6.9 gefunden, veröffentlicht unter anderem unter CVE-2019-12256. Besonders schlimm: Anwender wissen häufig gar nicht, ob sie betroffen sind oder nicht, denn bei vielen Lösungen wird das genutzte Betriebssystem nicht genannt.

Von vielen Herstellern werden bereits Updates zur Verfügung gestellt. Sie sollten, sofern die Systeme über Netzwerke erreichbar sind, dringend eingespielt werden. Und bei der Beschaffung neuer IoT-Geräte sollte zukünftig auf die Angabe der verwendeten IT-Komponenten geachtet werden.

Komplexinetes

Von Oktober bis Dezember 2018 wurde Version 1.13.4 der Open-Source-Anwendung Kubernetes einem Sicherheitsaudit unterzogen. Den Abschlussbericht veröffentlichte Kubernetes am 06.08.2019 im GitHub-Repository. Code-Qualität und Dokumentation der Container-Orchestrierungs-Lösung erhalten darin keine besonders gute Bewertung. So wurde beispielsweise die gleiche Programmlogik wiederholt implementiert anstatt auf zentrale Mechanismen zu setzen. Insgesamt wird Kubernetes als sehr komplex und reich an Abhängigkeiten eingestuft, was den Code wiederum besonders fehleranfällig macht. Daher überrascht es wenig, dass die Auditoren 37 Sicherheitslücken entdeckten, von denen fünf als hoch kritisch eingestuft wurden.

Das Beispiel zeigt erneut, dass übermäßig komplexe Lösungen ein Sicherheitsrisiko darstellen – und dass Open Source nicht automatisch bedeutet, dass existierende Schwachstellen von der Community selbst aufgedeckt werden. Korrekturen, die die Komplexität der Anwendung signifikant verringern, sind nachträglich nur schwer umsetzbar, da jene häufig aus grundsätzlichen Entwurfsentscheidungen resultiert. Ein Grund mehr, Security-Aspekte schon beim Design zu berücksichtigen.

EuGH-Trend

Der Europäische Gerichtshof (EuGH) hat am 29.07.2019 über die Verantwortung bei der Einbindung von Social Media Plugins entschieden (Rs. C-40/17). Ein Webseitenbetreiber war wegen eines Facebook Like-me Buttons und der daraus resultierenden Übermittlungen an Facebook Irland abgemahnt worden. Auch wenn es sich noch auf die EG-Datenschutz-Richtlinie und die Datenschutzrichtlinie für elektronische Kommunikation (RL 95/46/EG und 2002/58/EG) bezieht, bestätigt das Urteil einen bereits in der Entscheidung C-210/16 zu Facebooks Fanpages anklingenden Trend: Veranlasst oder ermöglicht der Webseitenbetreiber eine Datenverarbeitung durch einen Plattform- oder Dienstanbieter, tendiert der EuGH zur Annahme einer gemeinsamen Verarbeitung. Die daraus folgende

gemeinsame Verantwortung soll jedoch nur die Verarbeitungsphasen umfassen, für die Mittel und Zwecke gemeinsam bestimmt werden. Beide Beteiligte benötigen eine eigenständige Rechtsgrundlage, wobei der EuGH von der Erforderlichkeit einer durch den Webseitenbetreiber einzuholenden Einwilligung ausgeht. Informieren muss der Webseitenbetreiber nur über die gemeinsam verantwortete Verarbeitung.

Die Entscheidung ist insbesondere für Tracking-Pixel hochrelevant. Für Webseitenbetreiber ist die dargestellte Verantwortungsverteilung eine gute Nachricht. Offen bleibt, wie der Social-Media- oder Tracking-Anbieter seine über die gemeinsame Verarbeitung hinausgehende Nutzung begründen kann.

Spiegelreflex-Trojaner

Am 11.08.2019 zeigte Eyal Itkin auf der Defcon, wie sich der Markt für ein funktionierendes kriminelles Geschäftsmodell vergrößern lässt. So gelang es ihm unter Kombination mehrerer Schwachstellen einen Verschlüsselungstrojaner auf die Bilder von Canon-Kameras loszulassen (Demo). Dabei nutzte er die WLAN-Verbindung und das Picture Transfer Protocol (PTP). Nutzern der betroffenen Kameramodelle mit WLAN-Schnittstelle sei daher die Aktualisierung der Firmware und die Deaktivierung der WLAN-/NFC-Schnittstelle bei Nichtgebrauch ans Herz gelegt.

DSGVO-konforme Kamerafahrten

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) informierte am 30.07.2019 über die von Apple seit Juli 2019 auch in Deutschland vorgenommenen Aufnahmen von Straßenzügen und Gebäudefronten zur Aufwertung des Apple-eigenen Kartendienstes. Die damit einhergehenden datenschutzrechtlichen Fragen wurden erstmals mit dem vergleichbaren Dienst Google Streetview vor rund 10 Jahren beleuchtet.

Zur Sicherstellung der Betroffenenrechte wurden Maßnahmen eingeführt, die nun auch bei Apple umgesetzt werden, wie bspw. die vorherige Ankündigung von geplanten Kamerafahrten, die automatische Verpixelung von Gesichtern und Kfz-Kennzeichen, die Möglichkeit der Unkenntlichmachung des eigenen Hauses, die Widerspruchsmöglichkeit gegen die Verarbeitung sowie die Angabe von Beschwerdestellen für Betroffene. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) bewertet das Vorgehen als datenschutzkonform. Eine selten gelungene datenschutzrechtliche Zusammenarbeit zwischen einem amerikanischen Unternehmen und einer deutschen Aufsichtsbehörde.

Forever Young

Backdoors sind alte Bekannte (siehe SSN 12/2007 und SSN 01/2016) – und mächtige Ansatzpunkte für Angriffe. Bereits am 03.11.2003 wurde ein spektakulärer Ansatz für eine Backdoor im Linux-Kernel öffentlich, und erst kürzlich, am 26.07.2019, berichtete Bruce Schneier über die Verurteilung eines Mitarbeiters, der bei Siemens „logic bombs“ in Code eingebaut hatte.

Am 15.08.2019 wurde nun unter der CVE-2019-15107 die Existenz einer Hintertür in den Versionen 1.900 bis 1.920 des beliebten Admin-Tools webmin bekannt. Die Besonderheit gerade dieser Schwachstelle: Sie bestand offenbar seit April 2018 – und stattete Angreifer, die sie ausnutzten, mit hoch privilegierten Rechten aus. Ein weiteres Beispiel, dass gerade verbreitete Open Source-Lösungen besonders attraktiv (und zugleich anfällig) für derartige Angriffe sind.

Secorvo News

Seminare

Nach der Sommerpause startet das Seminarangebot von Secorvo in der letzten Septemberwoche (**23.–26.09.2019**) mit dem Zertifizierungsseminar TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.), IT-Sicherheit heute (**22.–24.10.2019**) und PKI (**18.–21.11.2019**). Für den T.I.S.P. (**14.–18.10.2019**) gibt es noch einen freien Platz; das nächste T.I.S.P.-Seminar folgt in der 48. Woche (**25.–29.11.2019**). Programme und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Hallo, hier spricht Deine Zahnbürste.

Ob zu Hause, in Fahrzeugen, Industrieanlagen oder Agrarbetrieben: IoT-Anwendungen sind heute nicht mehr wegzudenken und halten in nahezu allen Bereichen Einzug in unser Leben. Bis 2020 sollen laut Gartner 20 Milliarden vernetzte Geräte im Einsatz sein. Das Internet of Things eröffnet vielfältige Chancen, jedoch mangelt es häufig an Bewusstsein für Sicherheitsaspekte. Die sichere Kommunikation der unzähligen vernetzten Dinge untereinander ist dabei die größte Herausforderung.

Warum es für Unternehmen existentiell ist, ihre IoT-Devices und den Zugriff auf ihre IoT-Plattformen abzusichern und welche aktuellen Technologien dafür zur Verfügung stehen, erläutert beim kommenden KA-IT-Si-Event am **19.09.2019** Thorsten Gahrmann von der Nexus Group. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch bei unserem „Buffet-Networking“ – diesmal wieder mit Blick über die Dächer von Karlsruhe (zur Anmeldung).

Veranstaltungshinweise

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

September 2019	
17.09.	Anwendertag IT-Forensik (Fraunhofer Institut SIT, Darmstadt)
19.09.	Hallo, hier spricht Deine Zahnbürste. (KA-IT-Si, Karlsruhe)
22.-24.09.	FIfFKon 2019 (FIfF e.V., Berlin)
23.-26.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.09.	Datenschutztag 2019 (COMPUTAS, Köln)
24.-27.09.	heise devSec 2019 (dpunkt.verlag, heise Developer, heise Security, Heidelberg)
Oktober 2019	
08.-10.10.	it-sa 2019 (NürnbergMesse GmbH, Nürnberg)
14.10.	Night of the Living Labs (FZI, Karlsruhe)
14.-18.10.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
15.10.	Swiss Cyber Storm 2019 (Swiss Cyber Storm Association, Bern/CH)
22.-24.10.	IDACON 2019 (WEKA-Akademie, München)
22.-24.10.	IT-Sicherheit heute - praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)

Fundsache

Am 24.07.2019 hat Netflix unter dem Titel „The Great Hack“ eine Dokumentation des Cambridge Analytica / Facebook-Skandals veröffentlicht.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Stefan Gora, Hans-Joachim Knobloch, Michael Knopp, Sarah Niederer, 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