secorvo
security consulting

Secorvo Security News

September 2016

Die Tür

Wer in den vergangenen Jahren die Nachrichten verfolgt, dem drängt sich leicht der Eindruck auf, dass gegen alle diese Cracks – ob in staatlichem Auftrag, aus krimineller Motivation oder schlichtem Spieltrieb – einfach kein Kraut gewachsen ist. Warum also überhaupt diesen ganzen Aufwand treiben? Wieso nicht einfach alle Daten in die billigste Cloud verlegen, jede hilfreiche App auf das preisgünstigste Smartphone laden – und das gesparte Geld statt in Schutzmaßnahmen in Aktien investieren? Wenn der Datengau ohnehin früher oder später jeden trifft, dann hat man bis dahin wenigstens am Vermögen gearbeitet... So ähnlich klang kürzlich der Fatalismus zwischen den Zeilen eines Gesprächspartners, dem der Schreck über einige von mir vorgestellten Angriffswege noch anzusehen war.

Da kam mir eine Geschichte in Sinn, die schon einige Jahre zurückliegt. Bei unseren Nachbarn war eingebrochen worden – am hellichten Tag, mit nicht mehr als einem langen Schraubenzieher als Hebel. Es wurde wenig entwendet, aber der Schock saß tief.

Unvermeidlich unterzog ich unsere Haustür einem kritischen Blick – und musste feststellen, dass auch sie einem solchen Angriff nicht standgehalten hätte. Also holte ich mir Rat bei einem erfahrenen Kriminalisten. Der besah sich die Tür und beäugte mich amüsiert, als ich ihn fragte, was ich tun müsste, um so einen Einbruch zu verhindern. Falsche Frage, meinte er: „Es geht nicht darum, *ob* jemand einbrechen kann – sondern *wie lange* er dafür braucht." Genau das sei der Punkt. Jede Tür ließe sich öffnen – oft mit überraschend wenig Aufwand, und wenn es sein muss, mit schwerem Gerät. Entscheidend sei der Aufwand: Je mehr Zeit ein Einbrecher benötige und je mehr Lärm er verursache, desto größer sei die Entdeckungsgefahr. Wie bei der IT-Sicherheit: Je aufwändiger und langwieriger ein Angriff, desto höher Kosten und Risiko. Darum helfen Schutzmaßnahmen – gegen Einbrecher ebenso wie gegen Cracker.

Inhalt

secorvo
security consulting

Security News

Flüsterangriff auf Smartphones

Auf dem diesjährigen 25th USENIX Security Symposium wurde am 11.08.2016 ein unkonventioneller Angriff auf Smartphones vorgestellt: Ein Smartphone mit aktivierter Spracherkennung lässt sich von für ein menschliches Ohr unverständlichen Sprachbefehlen steuern. Denn die Geräuschfilterung ist erstaunlicherweise so gut, dass ein Smartphone manche Befehle wie "Öffne URL xyz" erkennt und ausführt, während der Besitzer dies aufgrund von Umgebungsgeräuschen nicht mitbekommt. Bei Tests wurde ein verschleiertes "OK Google" zu 95% vom Smartphone, aber nur von 22% der Probanden verstanden.

Einige Beispiele solcher „Hidden Voice Commands" für Android-Smartphones haben die Autoren auf ihrer Webseite zusammengestellt. Dort finden sich auch Tests, bei denen den Forschern Details zum Spracherkennungssystem vorlagen. Wer sicher gehen möchte, dass sein Smartphone keine Fremdsteuerung ermöglicht, sollte die Sprachsteuerung deaktivieren – oder zumindest so konfigurieren, dass sie im gesperrten Zustand nicht reagiert.

Hacker-Stecker

Ein einheitlicher Micro-USB-Stecker ist bei Smartphones (bis auf wenige Ausnahmen) mittlerweile Standard – und ab 2017 gesetzlich vorgeschrieben. Neben dem Laden des Akkus und dem Datenaustausch mit einem Computer bietet der Anschluss dank OTG meist nahezu die gleichen Möglichkeiten wie jeder USB-Port eines Computers. Durch den immer größeren Funktionsumfang der Schnittstelle entstehen jedoch auch neue Angriffsflächen, wie Brian Markus auf der Hacking-Konferenz DEF Con vom 04. bis 07.08.2016 demonstrierte. Bei seinem als „VideoJacking" bezeichneten Angriff wird ein externer Monitor oder ein Aufnahmegerät über einen Splitter mit dem Ladekabel verbunden. Darüber kann das auf dem Smartphone angezeigte Bild gespiegelt und abgegriffen werden. Betroffen sind alle mit dem Feature *Mobile High-Definition Link* (MHL) ausgestatteten Smartphones.

Für einen Nutzer ist grundsätzlich nicht ersichtlich, ob das über den Micro-USB-Port angeschlossene Gerät auch das ist, was es zu sein vorgibt. Fremde Ladegeräte sollten daher gar nicht oder nur mit einer dazwischen gesteckten Datenaustauschsperre (wie z. B. dem USB-Kondom) genutzt werden.

WLAN-Haftung

Der rechtliche Rahmen für Hotspots und Gäste-WLANs ist seit langem umstritten und mit großer Unsicherheit behaftet. Nach dem Vorstoß des deutschen Gesetzgebers (siehe SSN 7/2016) hat nun der EuGH am 15.09. 2016 sein Urteil im Fall Tobias McFadden ./. Sony Music verkündet. Der Beklagte hatte in seinen Verkaufsräumen ein ungesichertes WLAN betrieben und sich anlässlich einer Abmahnung von Sony wegen einer Urheberrechtsverletzung auf Art. 12 der Richtlinie 2000/31/EG und deren deutsche Umsetzung in § 8 TMG (das „Providerprivileg") berufen. Der EuGH hat nun entschieden, dass eine Schadensersatzhaftung des Anbieters gegen die Richtlinie verstoße und von dem Anbieter keine über die Richtlinie hinaus gehenden Maßnahmen verlangt werden dürften. Der Anbieter könne aber auf Unterlassung in Anspruch genommen werden und müsse hierfür die Kosten tragen. Er dürfe zum Schutz des WLANs durch ein Passwort und zur Nutzeridentifikation verpflichtet werden.

Die (ohnehin voreilige) Euphorie über den neuen § 8 Abs. 3 TMG dürfte damit verflogen sein. Die Richtlinie lässt die Störerhaftung in Art. 12 Abs. 3 ausdrücklich zu, das Urteil ist daher nachvollziehbar. Passwortschutz und Identifikation alleine reichen jedoch zur Umsetzung des Unterlassungsanspruchs nicht aus, daher hat das Urteil nicht zur Klarheit über die tatsächlichen Pflichten des Anbieters beigetragen – ein weiteres in der langen Reihe unglücklicher WLAN-Entscheidungen.

IoT-Krypto-Camouflage

Am 06.09.2016 veröffentlichte das Unternehmen SEC Consult eine Untersuchung der Sicherheit der Implementierung kryptographischer Verfahren in IoT-Geräten. Schon im November 2015 war SEC Consult in eine Studie zu dem Ergebnis gekommen, dass die Verwendung von privaten Schlüsseln in verbreiteten Geräten bei weitem nicht dem Stand der Technik entspricht. Die aktuellen Ergebnisse legen nahe, dass sich die Situation in den vergangenen neun Monaten eher verschlimmert hat. Vielfach erlauben falsch verwendete Schlüssel und Zertifikate Zugriff auf Geräte oder vertrauliche Informationen. Betroffene Schlüssel und Zertifikate wurden inzwischen auf Github veröffentlicht; darunter finden sich auch einige Schlüssel von AVM Fritzboxen. Auf die offizielle Meldung des US CERTs reagierte offenbar bisher fast keines der betroffenen Unternehmen. Der Kauf von billiger Kryptographie kann die Nutzer also teuer zu stehen kommen.

OPM-Hack

Fast wie ein Krimi lesen sich die 217 Seiten des am 07.09.2016 veröffentlichten offiziellen Untersuchungsberichts mit dem prägnanten Titel „The OPM

Data Breach: How the Government Jeopardized Our National Security for More than a Generation“ zu den Angriffen auf das *U.S. Office of Personnel Management* (OPM) in den Jahren 2014 und 2015, bei denen sehr persönliche Daten aus Sicherheitsüberprüfungen, darunter auch Fingerabdrücke, von mehr als 21,5 Millionen Amerikanern entwendet wurden. Das OPM war Ende 2014 als die Behörde mit den schwächsten Authentifikationsverfahren gerügt worden und betrieb zentrale Server (die später kompromittiert wurden) vorschriftswidrig ohne Security Assessment. Bereits im März 2014 war das OPM vom US-CERT auf einen Hackerangriff hingewiesen worden; die Aktivitäten des Hackers wurden vom OPM jedoch lediglich über zwei Monate beobachtet. Mangelhafte Schutzmaßnahmen, unvollständige Logs und unangemessene Reaktionen sieht der Bericht als Ursachen des (verhinderbaren) Datenabzugs. Ein abschreckendes Beispiel für falsche Prioritätensetzung beim Umgang mit Informationssicherheit.

Smart-Meter-Regulierung

Am 01.09.2016 ist das am 08.07.2016 vom Bundesrat verabschiedete Gesetz zur Digitalisierung der Energiewende im Bundesgesetzblatt veröffentlicht worden und am 02.09.2016 in Kraft getreten. Kernstück ist das ‚Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen‘ (Messstellenbetriebsgesetz – MsbG). Es regelt den Übergang zu modernen Messstellen in zukünftigen Energienetzen.

Technische Vorgaben an die Datensicherheit werden in den §§ 19 ff. MsbG geregelt. Konkrete Anforderungen an Interoperabilität und Anbindungssicherheit vor allem der Smart-Meter-Gateways finden sich in bereits vorliegenden technischen Richtlinien. Die Erfüllung der Anforderungen durch die Geräte ist mit einer Zertifizierung nachzuweisen. Nicht den Anforderungen entsprechende Geräte dürfen nur noch bis Ende 2016 verbaut und anschließend maximal acht Jahre genutzt werden.

Die Datenerhebung und –verarbeitung wird umfangreich in 25 Paragraphen (§§ 49 ff. MsbG) geregelt, darunter finden sich auch Löschpflichten und sogar konkrete Löschfristen. Die aus Datenschutz- und Datensicherheitsanforderungen resultierenden Umsetzungspflichten sind komplex und umfangreich; sie werden von Herstellern und Betreibern mehr als einen Blick über den Tellerrand erfordern, um den Zertifizierungsanforderungen genügen zu können.

Secorvo News

Von und für Experten

Vierzig Jahre liegt die wegweisende Veröffentlichung von Whitfield Diffie und Martin E. Hellman („New Directions in Cryptography“) inzwischen zurück – und noch immer sind Aufbau und Betrieb einer PKI eine Herausforderung. Wie so oft liegt der Teufel in den Details – Zertifikatsgültigkeiten, Key Usage, Prozesse und Policies sind geeignet festzulegen und umzusetzen. Wie das geht, zeigen wir in Theorie und Praxis auf unserem PKI-Seminar vom **14. bis 17.11.2016** (Programm und Anmeldung).

Bis Mitte des Jahres 2016 wurden 850 T.I.S.P.-Zertifikate ausgestellt. Sofern Sie drei Jahre Berufserfahrung im Gebiet Informationssicherheit mitbringen, können Sie noch in diesem Jahr Teil dieser schnell wachsenden Experten-Community der *Information Security Professionals* werden: Vom **21. bis 25.11.2016** findet in Karlsruhe die nächste T.I.S.P.-Schulung mit anschließender Zertifikatsprüfung statt, durchgeführt von den Autoren des T.I.S.P.-Buchs (detaillierte Agenda und Online-Anmeldung).

Live Hacking

Kaum etwas ist wirkungsvoller als die Anschauung – das gilt auch für die IT-Sicherheit. Daher haben wir in den vergangenen Monaten zahlreiche Live-Hacking-Vorführungen entwickelt, die verbreite Einfallstore zeigen. Alle Live Hacks kommen ohne „Hokuspokus“ wie Spezialversionen einer anfälligen Soft- oder Hardware aus; gezeigt wird, was ohne größere Investitionen in die Ausrüstung heute möglich ist. Wenn Sie einen solchen Live Hack buchen möchten, nehmen Sie bitte mit uns Kontakt auf.

IT-Grundschutz-Zertifizierung

Zertifizierung eines großen Rechenzentrums – nach IT-Grundschutz? Kann das mit vertretbarem Aufwand und in überschaubarer Zeit funktionieren? Sascha Grund, IT Compliance Manager der Globalways AG, stellt auf dem kommenden KA-IT-Si Event am **10.11.2016, 18 Uhr** in den Räumen des CyberForum e.V. vor, dass und wie das geht – und gibt praktische Tipps zur Umsetzung.

Im Anschluss an den Vortrag haben Sie wie gewohnt die Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Anmeldung und weitere Informationen unter www.ka-it-si.de.

Veranstaltungshinweise

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

Oktober 2016	
04.10.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
11.-14.10.	OWASP AppSec USA 2016 (OWASP Foundation, Washington DC/US)
18.-20.10.	it-sa 2016 (NürnbergMesse GmbH)
19.10.	Swiss Cyber Storm 6 (Swiss Cyber Storm Association, Luzern/CH)
26.-28.10.	IDACON 2016 (WEKA-Akademie, München)
November 2016	
01.-04.11.	Black Hat Europe 2016 (Blackhat, London/UK)
08.-11.11.	DeepSec In-Depth Security Conference 2016 Europe (DeepSec, Wien/AT)
10.11.	IT-Grundschutz-Zertifizierung (KA-IT-Si, Karlsruhe)
10.-11.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
14.-17.11.	PKI (Secorvo, Karlsruhe)
17.-18.11.	40. DAFTA (GDD, Köln)
21.-25.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Die 40seitige Publikation „Offenes Geheimnis – Mythen und Fakten zu Überwachung und digitaler Selbstverteidigung“ der Rosa Luxemburg Stiftung gibt eine Übersicht über Hintergründe und Schutzmöglichkeiten für Endanwender.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp.

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