secorvo
security consulting

Secorvo Security News

Mai 2016

Vom Aushalten

Ein Login ohne Passwort? Eine EC-Karte ohne Geheimnummer? Online-Banking ohne PIN/TAN? Informationstechnik ohne Schutzmaßnahmen ist heute undenkbar.

Beim Zugriff auf Daten von Kriminellen wird aus dem Schutz jedoch ein Ermittlungshindernis. Am 21.04.2016 gestand Direktor James Comey der Washington Post, dass das Knacken des Smartphones des San-Bernardino-Mörders dem FBI über 1,3 Mio. US$ wert war – mit einem Programm, das eine Schwachstelle im iOS ausnutzte, die nur beim iPhone 5c funktionierte. Da selbst das FBI (Etat: 8,7 Mrd. US$) Hacks auf alle Smartphone-Modelle (sofern überhaupt möglich) nicht bezahlen könne, fordert Comey von den Herstellern direkten Datenzugriff. Wie könnte das funktionieren? Zwei Ansätze gibt es dafür: Entweder durch eine Hintertür in der Software oder durch Hinterlegung der kryptografischen Schlüssel.

Beide Ansätze sind keine gute Idee. Informationen über Hintertüren verbreiten sich rasch – die Listen der BIOS-Master-Passwörter zur Umgehung des Bootschutzes sind legendär. Das weiß auch das FBI: Seit Mitte 2015 kursieren 3D-Druckvorlagen der sieben Master-Schlüssel für TSA-Kofferschlösser, die angeblich nur Zollbeamten zugänglich sind. Auch gelingen immer wieder Angriffe auf hinterlegte Schlüssel – wie die Kompromittierung des SecureID-Root-Keys von RSA vor fünf Jahren (SSN 03/2011). Der 1993 von der Clinton-Regierung entwickelte *Escrowed Encryption Standard*, nach dem die Verschlüsselungsschlüssel verschlüsselt mitgesendet bzw. -gespeichert werden sollten, scheiterte an einem Protokollfehler. Die Erfahrung lehrt: Sichere Verschlüsselung muss frei von Hintertüren sein – und Schlüssel dürfen nicht zentral gespeichert werden.

Wenn wir die Sicherheit unserer Informationstechnik insgesamt nicht aufs Spiel setzen wollen, bleibt uns daher nur, es auszuhalten, dass auch Kriminelle Daten so verschlüsseln können, dass kein Strafverfolger darauf zugreifen kann.

Inhalt

secorvo
security consulting

Security News

Wette auf fallende Kurse

In letzter Zeit häufen sich wieder Meldungen zu Schwachstellen in Sicherheitssoftware: Betroffen waren u. a. Virenschutzprogramme von Symantec, (16.05.2016), SSL-Proxies von Jugendschutzfiltern mehrerer Hersteller (20.12.2015) und die Management-Software von Lenovo (26.04.2016). Diese Programme sollen die Sicherheit verbessern – schaffen aber durch Schwachstellen selbst neue Angriffspunkte.

Generell gilt: Ganz gleich, welche Art von Software man einsetzt, immer erhöht man dadurch die Wahrscheinlichkeit von Schwachstellen. Bei Sicherheitssoftware stellen sie meist eine besondere Gefahr dar, da diese oft mit privilegierten Rechten arbeitet. So mancher Benutzer wiegt sich daher mit solchen Programmen in trügerischer Sicherheit.

Schon vor zwei Jahren berichteten wir über Schwachstellen, die man sich durch den Einsatz von Virenschutz- und Monitoring-Agenten erst einhandelt (SSN 05/2014). Manchmal ist weniger mehr: Ein wenig Awareness dafür, worauf man bei der Internetnutzung achten sollte, ist womöglich eine bessere Investition als ein technischer Filter – der neue Viren ohnehin erstmal nicht erkennt und zudem womöglich Schwachstellen enthält.

Das dabei gesparte Geld sollte man vielleicht Gewinn bringend auf fallende Aktienkurse ausgewählter Hersteller von Sicherheitssoftware setzen.

Kritische Anlagen

Weitgehend unverändert ist der Referentenentwurf der ersten Verordnung zum Anwendungsbereich des IT-Sicherheitsgesetzes am 03.05.2016 in Kraft getreten. Ergänzt wurde die Behandlung von miteinander verbundenen kritischen Anlagen. Das Prinzip, den Versorgungsgrad als Maß für die Kritikalität einer Anlage heranzuziehen (SSN 02/2016), ist geblieben – die Gefährdung der öffentlichen Sicherheit durch Fehlfunktion einer Anlage bleibt bei der Einstufung weiterhin ausgeblendet.

Die Verordnung zu den Sektoren Finanzen, Transport, Verkehr und Gesundheit soll Anfang 2017 folgen. Zur Unterstützung der Entwicklung branchenspezifischer Sicherheitsstandards hat das BSI im Dezember eine Orientierungshilfe publiziert; bisher wurde jedoch noch kein Standard veröffentlicht.

Die Umsetzungsfrist für die Betreiber von in den Anhängen der Verordnung benannten Infrastrukturen läuft bis zum 03.05.2018. Bis dahin sind Investitionen in Anbieter rund um ISM-Systeme sicher keine schlechte Kapitalanlage.

Ad-hoc-Meldung

Am 03.05.2016 wurde gleich eine Handvoll schwerer Schwachstellen in der beliebten Bildbearbeitungssoftware ImageMagick veröffentlicht. Brisant sind diese Schwachstellen nicht nur wegen der Möglichkeit, beliebigen Code ausführen zu können, sondern auch, weil der ImageMagick-Code in zahlreichen Bibliotheken verwendet wird, ohne dass dies den Entwicklern bekannt sein dürfte: Nicht nur dort, wo ImageMagick draufsteht, ist ImageMagick drin.

Wer Anteile an ImageMagick hält, sollte sie nicht gleich abstoßen – denn bekanntlich ist auch schlechte Publicity gute Publicity. Aber man sollte den Fall zum Anlass nehmen, neben einem funktionierenden Patch-Management dafür zu sorgen, dass die in der Entwicklungsabteilung verwendeten (Open-Source-) Bibliotheken inventarisiert und der Umgang mit dazu veröffentlichten Schwachstellen geregelt wird.

Spionagetools statt Gold

Spätestens seit der Veröffentlichung der Panama Papers sind kreative neue Möglichkeiten der Geldanlage gefragt. Die Bundesnetzagentur will helfen und sagte am 25.04.2016 Spionagekameras den Kampf an: Seitdem ist es verboten, WLAN-Kameras anzubieten oder zu besitzen, die in Alltagsgegenständen wie beispielsweise Kugelschreibern oder Rauchmeldern versteckt sind. Die BNetzA geht gegen Hersteller, Verkäufer und Käufer vor und verlangt die Vernichtung der Gegenstände – nach eigenen Angaben bisher in rund 70 Fällen.

Nicht bekannt ist, ob auch Organisierte Kriminalität und Nachrichtendienste zu den Betroffenen zählen – und warum andere „hilfreiche" Tools wie sendende Keylogger oder spionierende Hotspots nicht unter den Bann fallen.

Dennoch ist jetzt der richtige Zeitpunkt, um schnell noch in Restbestände von Spionagekameras zu investieren und diese vom benachbarten Ausland über einschlägige, nicht-deutsche Online-Shopping-Plattformen zu vertreiben.

Investition im Keksmarkt

Cookies sind ein geliebtes Feindbild des Datenschutzes – kein Grund allerdings, Investitionen im Keksmarkt zu reduzieren. Denn die am 24.05.2016 in Kraft getretene Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, DSGVO) bringt keineswegs die vielerorts erhoffte Klarheit.

Während der Bundesinnenminister mehr Flexibilität fordert, da personenbezogene Daten schließlich „nicht um ihrer selbst willen schützenswert“ seien, weisen Experten auf strukturelle Probleme der DSGVO hin, u. a. ihre Unterkomplexität. Es bleibt eine große Unsicherheit, denn die in zwei Jahren unmittelbar geltenden Regelungen enthalten eine Vielzahl von Öffnungsklauseln. Manche stellen einen konkreten Handlungsauftrag an den nationalen Gesetzgeber: Das BDSG wird durch ein Nachfolgegesetz ersetzt werden müssen. Umgekehrt werden viele Regelungen, die Datenverarbeitungen bisher legitimieren, aufgrund fehlender Öffnungsklauseln schlicht wegfallen, so z. B. Teile des § 28 BDSG zur werblichen Nutzung personenbezogener Daten.

Da viele Datenschützer den Besuch eines der unzähligen Seminarangebote zur DSGVO einer Lektüre der 187-seitigen Broschüre der BfDI vorziehen dürften, ist in den nächsten Monaten mit einem Anstieg des Kekskonsums zu rechnen – Cookies hin oder her. Wer sich die Seminarkosten angesichts der herrschenden Unklarheit über die finale Rechtslage spart, sollte daher über eine Aufstockung seiner Investitionen im Keksmarkt nachdenken.

Haftung bleibt

Folgt man der Euphorie der Medien, ist die Störerhaftung für offene WLANs schon so gut wie begraben. Tatsächlich hat sich die Bundesregierung am 10.05.2016 auf eine Entschärfung eines vom September 2015 stammenden Gesetzesentwurfs zur Änderung des Telemediengesetzes geeinigt.

§ 8 Abs. 4 des ursprünglichen Entwurfs sah verschiedene Pflichten für Anbieter von WLAN-Hotspots vor. Diese sollen nun entfallen und Anbieter offener WLANs vollständig Zugangsanbietern gleichgestellt werden, die bereits heute nach § 8 TMG ein Haftungsprivileg genießen. Ursache des Sinneswandels ist unter anderem der Schlussantrag des Generalanwalts am EuGH vom 16.03.2016, der diese Gleichstellung auf Basis von Art. 12 der E-Commerce-Richtlinie vornimmt.

Der Schlussantrag lässt jedoch genau wie das BGH-Urteil vom 26.11.2015 den Weg zu Sperranordnungen offen. Die Rechtsprechung wendet das Haftungsprivileg zudem bislang nicht auf zukunftsgerichtete Unterlassungsansprüche an. Daran ändert auch die neue Einigung nichts. Der Schlussantrag kommt allerdings zu dem Ergebnis, dass Anbietern keine Abmahnkosten auferlegt werden dürfen. Von einer Abschaffung der Störerhaftung kann also kaum die Rede sein.

Investitionen in Musik- und Filmverlage sollte man daher nicht gleich abstoßen – hingegen lohnt es weiterhin, in Anbieter von Sperrsoftware und auf Urheberrechtsfragen spezialisierte Rechtsberatungen zu setzen.

Secorvo News

Aktuelle Entwicklungen

Auch die Informationssicherheit wird von der Schnelllebigkeit technischer Entwicklungen nicht verschont. Auf dem Seminar „IT-Sicherheit heute“ (**27.-29.09.2016**) greifen wir aktuelle Entwicklungen und neue Themen auf, um eine Hilfestellung beim Nachjustieren von Sicherheitskonzepten und Schutzmaßnahmen zu bieten. Das Programm des Seminars wird ständig aktualisiert.

T.I.S.P.

Anfang des Jahres 2017 dürfte die 1.000er-Marke fallen – so viele IT-Sicherheitsexperten haben inzwischen das T.I.S.P.-Zertifikat zum Nachweis ihrer fachlichen Qualifikation erworben. Der Erfolg des T.I.S.P. lässt sich nicht nur an der großen Nachfrage ablesen, sondern auch an der Bedeutung, die Stellenanzeigen im Bereich der IT- und Informationssicherheit dem Zertifikat einräumen.

Wer das T.I.S.P.-Seminar bei Secorvo besucht, erhält zur Vorbereitung das Begleitbuch zum T.I.S.P., ein 700seitiges Lehr- und Lernbuch sowie Nachschlagewerk zu den zentralen Themen der Informationssicherheit. Das nächste T.I.S.P.-Seminar mit freien Plätzen findet vom **21. bis 25.11.2016** statt. Programm und Online-Anmeldung unter https://www.secorvo.de/college.

8. Tag der IT-Sicherheit

Der Karlsruher Tag der IT-Sicherheit, den die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) in Zusammenarbeit mit dem CyberForum e.V. und der IHK Karlsruhe austrägt, beschäftigt sich in diesem Jahr zum achten Mal mit aktuellen IT-Sicherheitsherausforderungen für Unternehmen. Er macht deutlich, wie wichtig ein professioneller Umgang mit den Themen IT-Sicherheit und Datenschutz ist und informiert über Präventionsmöglichkeiten. Diesjähriger Keynote Speaker ist Tobias Schrödel, IT-Sicherheitsexperte und erster „Comedyhacker“. Die Fachvorträge beschäftigen sich u. a. mit den Themen Cybercrime und Industrial Security im Produktionsumfeld. Das Programm schließt mit einem Live-Hacking und bietet Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit Referenten, Teilnehmern und Ausstellern.

Die Veranstaltung findet am **22.06.2016** im Saal Baden der IHK Karlsruhe statt. Das Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

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

Juni 2016	
06.-10.06.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.06.	IT-Sicherheitsrisiken managen: Hürden und Möglichkeiten (Fachgruppe SECMGT der GI, Frankfurt)
10.-11.06.	AREA41 Security Conference (DC4131 DEFCON Switzerland, Zürich/CH)
13.-14.06.	DuD 2016 (Computas, Berlin)
15.-17.06.	Entwicklertag 2016 (VKSI, GI, ObjektForum, Karlsruhe)
22.06.	8. Tag der IT-Sicherheit (KA-IT-Si, Karlsruhe)
27.06.-01.07.	OWASP AppSec EU 2016 (OWASP Foundation, Rom/I)
Juli 2016	
30.07.-04.08.	Blackhat USA 2016 (Blackhat, Las Vegas/US)
August 2016	
04.-07.08.	DEF CON 24 (DEFCON, Las Vegas/US)
07.-10.08.	16th Annual DFRWS Conference 2016 (DFRWS, Philadelphia/US)

Fundsache

Der Landesbeauftragte für den Datenschutz Baden-Württemberg hat am 22.04.2016 einen 27-seitigen Leitfaden für Datenschutzeinstellungen bei Windows 10 herausgegeben, der empfehlenswerte Grundkonfigurationen Schritt für Schritt erläutert.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, 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