secorvo
security consulting

Secorvo Security News

März 2015

Hobbyistensicherheit

Die zentrale Verschlüsselungsinfrastruktur des Internets hängt an 447.247 Programmzeilen von 147 Programmierer-Aktivisten: OpenSSL. Die geschützte Remote-Administration der wahrscheinlich meisten Systeme der Welt basiert auf 64.813 Zeilen C-Code von 92 unabhängigen Entwicklern: OpenSSH. Und die meisten (deutschen) PGP-Verschlüsselungen erledigt die Open-Source-Software GnuPG, entwickelt von 14 enthusiastischen Codern.

Manchmal ist die Abhängigkeit vielleicht nicht offensichtlich, weil sich der Open-Source-Code in einem Produkt „versteckt". Und ja, manche Open-Source-Projekte werden (teil-)finanziert von einem Unterstützer oder erhalten öffentliche Mittel.

Dennoch muss die Situation für jemanden außerhalb der „IT-Szene" ziemlich skurril anmuten. Das dürfte in etwa so wirken, als ob wir die Statik von Brücken durch Hobby-Architekten berechnen, ABS und Airbags von engagierten Bastlern konstruieren und Flugzeuge von Freizeitschraubern warten ließen.

Zwar muss das Ergebnis nicht schlecht sein – im Gegenteil: Wenn viele Engagierte eigeninitiativ und professionell zusammenarbeiten, kann sich das Resultat oft sehen lassen. Zu denken geben sollte uns diese Entwicklung trotzdem: Hat jemand einmal ausgerechnet, wie viel es volkswirtschaftlich kostet, wenn alle Unternehmen, die bspw. TrueCrypt zur Verschlüsselung einsetzen, auf BitLocker wechseln müssen, weil die Initiatoren es nicht weiterführen? Oder wenn eine GPG-Installation durch S/MIME ersetzt werden muss, weil der Hauptentwickler die Code-Pflege aufgibt?

Schließlich hat die Geschichte von OpenSSL gezeigt, dass Open Source nicht dasselbe ist wie „geprüfter" Code – sondern eben nur „prüfbarer" Code. Wäre es nicht angemessen, bei den zentralen Komponenten unserer Sicherheitsinfrastruktur für eine stabile Finanzierung und vor allem regelmäßige Code-Analysen zu sorgen?

Inhalt

secorvo
security consulting

Security News

Stromortung

Am 11.02.2015 veröffentlichten vier Forscher der Stanford University und des *National Research and Simulation Center* eine empirische Analyse zur Standortbestimmung über den Stromverbrauch eines Smartphones. Da das Senden und Empfangen von Daten den meisten Strom verbraucht und dieser stark schwankt (abhängig von der Entfernung zum Sendemast und der Signalstärke, die sich durch Hindernisse wie Häuser, Bäume oder Menschen schnell verändert), kann man jedem Ort einen spezifischen Verbrauch zuordnen. In aktuellen Smartphones sind die Strom- und Spannungswerte uneingeschränkt zugänglich; eine App kann diese also zyklisch an einen Server übermitteln, der die Werte mit bereits ausgemessenen Routen korreliert. Die Forscher konnten so innerhalb von zwei Minuten acht von zehn Teilstrecken erkennen.

Für einen flächendeckenden Einsatz erfordert die Technik zwar ausgemessene „Landkarten". Die Sperrung der GPS-Daten im Smartphone lässt sich damit jedoch umgehen. Wegen des geringen Verbrauchs ist ein Verschleiern der Werte durch das Starten vieler Apps keine wirksame Gegenmaßnahme; helfen würde allein eine Ausdehnung des Rechtemanagements auf die Stromverbrauchsdaten.

Kompatibilitätsbug

2010 patchte Microsoft gegen Stuxnet und Fanny – nur leider fehlerhaft. Das belegt die nach Hinweisen von Michael Heerklotz vom Januar initiierte Untersuchung von HP, deren Ergebnisse Dave Weinstein am 10.03.2015 veröffentlichte.

So missbrauchte Stuxnet CPL-Dateien (DLLs mit anderem Namen, also ausführbaren Code), indem er über Icons für Windows-Verknüpfungen (.lnk) eigenen Code aus mitgebrachten CPLs zur Ausführung brachte. Seit dem Patch im Jahr 2010 lädt Microsoft diese Windows-Urgesteine nur noch aus einer CPL-Whitelist. Der Schutz lässt sich allerdings durch geschickte Änderungen des Dateinamens der .lnk-Datei aushebeln: Das Icon wird zusammen mit dem Angriffscode in einen Speicherbereich mit Ausführberechtigung geladen – und Stuxnet ist fünf Jahre nach dem Patch wiederbelebt.

Die kompatibilitätserhaltende Pflege von Architekturschwächen (wie das Laden von Icons in Executable Memory) ist immer wieder ein Einfallstor. Eine ernsthafte Erhöhung des Sicherheitsniveaus erfordert es jedoch, gelegentlich die Rückwärtskompatibilität auf dem Altar der Sicherheit zu opfern.

Sozialadäquate Straftat

In den SSN 2/2015 wiesen wir darauf hin, dass Berufsgeheimnisträger wie Ärzte, Rechtsanwälte und Steuerberater grundsätzlich keine Dienstleister mit der Verarbeitung personenbezogener Daten beauftragen dürfen: Sie müssen die ihnen anvertrauten Geheimnisse schützen (§ 203 Abs. 1 StGB).

Diese (zugegebenermaßen betagte) strafrechtliche Vorschrift empfanden die Anwaltskammern als nicht zeitgemäß und versuchten sie mit dem am 11.11.2014 (sic!) beschlossenen Entwurf zur neuen Berufsordnung (BORA) auszuhebeln: Um künftig Aktenvernichter, Schreib- und Clouddienste einsetzen zu dürfen, soll ein Rechtsanwalt sich nicht mehr strafbar machen, wenn das Outsourcing „im Rahmen der Arbeitsabläufe der Kanzlei einschließlich der Inanspruchnahme von Leistungen Dritter erfolgt und objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht (Sozialadäquanz)." Auf Deutsch: Alle schieben ihre Daten in die Cloud – dann muss das der Rechtsanwalt doch auch dürfen.

Dieser eigenmächtigen Strafbefreiung schob der Bundesjustizminister jetzt einen Riegel vor und stellte am 04.03.2015 klar, dass die Berufsordnung das Strafgesetzbuch nicht aufweichen kann. Nicht alles, was technisch machbar ist, darf auch zulässig sein: Schließlich verarbeiten Berufsgeheimnisträger besonders schützenswerte Daten.

Angriffsanalyse

Auf dem USENIX Security Symposium wurden am 21.08.2014 die Ergebnisse einer Analyse gezielter, systematischer Angriffe auf eine China kritische Nichtregierungsorganisation vorgestellt, die Rückschlüsse auf typische Angriffsmethoden erlauben – das dürfte auch der Grund für die Einladung der Autoren als Keynote der diesjährigen 22. DFN-Konferenz gewesen sein.

In der Analyse wurden 1.500 verdächtige E-Mails von ca. 700 unterschiedlichen Absenderadressen untersucht; bei über 1.100 wurde Schadsoftware gefunden. Alle betroffenen E-Mails waren mit für die Empfänger plausiblem individuellen Kontext versehen. Bemerkenswert sind die folgenden Erkenntnisse: Es handelte sich um einen Langzeitangriff, der mindestens von 2009 bis 2013 dauerte und ggf. weiter andauert. Die meisten Empfänger, die Opfer der Angriffe wurden, erhielten erst nach dem Eintritt von Praktikanten in die Organisation infizierte E-Mails. Genutzt wurden keine Zero-Day-Exploits, sondern frei verfügbare Schadsoftware, wobei die Zeitspanne zwischen Veröffentlichung des Exploits und der maliziösen E-Mail meist sehr kurz war. Als „Wirtsdatei" wurden zunächst meist PDF-

Dokumente verwendet, die nach Einführung von Sandboxing in Acrobat Reader (ab 2010) von Microsoft Office-Dokumenten abgelöst wurden.

Daraus können wir Verschiedenes lernen. Erstens: Angreifer haben einen langen Atem. Zweitens: Schnelles Patchen von Sicherheitslücken wird immer wichtiger – „Aufpassen" schützt nicht. Und Drittens: Bei einer Häufung von Schadsoftware-Vorfällen könnte ein gezielter Angriff dahinterstecken – daher ist eine systematische Auswertung wichtig.

Rechts(un)sicherer WLAN-Betrieb

Das Bundesministerium für Wirtschaft und Energie hat am 11.03.2015 einen Gesetzesentwurf für ein zweites Gesetz zur Änderung des Telemediengesetzes vorgelegt. Damit will das Ministerium Rechtssicherheit für WLAN-Anbieter schaffen. Bislang drohen diesen bei missbräuchlicher Nutzung Unterlassungsansprüche (SSN 6/2014). Gleichzeitig will man die Störerhaftung von Plattformanbietern erleichtern, deren Plattformen hauptsächlich für rechtswidrige Handlungen genutzt werden, und das bisherige telemedienrechtliche Haftungsprivileg einschränken.

Diese Ziele soll eine Definitionsergänzung in § 2 TMG für drahtlose lokale Funknetze (= WLAN) ermöglichen. In drei neuen Absätzen des § 8 TMG, dem Haftungsprivileg für Access-Provider, wird klargestellt, dass auch die Störerhaftung ausgeschlossen sein soll. Voraussetzung ist, dass die Anbieter bestimmte Sorgfaltspflichten erfüllen: die Verschlüsselung des Zugangs zum Ausschluss unberechtigter Nutzer und die Beschränkung auf Nutzer, die zuvor erklären, keine Rechtsverletzungen über den Zugang zu begehen. Nicht geschäftsmäßige Anbieter sollen zudem den Zugang auf namentlich bekannte Nutzer beschränken.

Entgegen der in der Rechtsprechung zuletzt erkennbaren Tendenz, das Haftungsprivileg endlich uneingeschränkt auf WLAN-Anbieter anzuwenden, werden nun mit den Sorgfaltspflichten europarechtswidrige, wirkungslose Einschränkungen geschaffen. Erklärungen allein werden Rechtsverletzungen nicht verhindern, das Abmahnrisiko bei einer unzureichenden Umsetzung der Sorgfaltspflichten steigt dagegen. Im Interesse der Rechtssicherheit und einer Verbesserung der WLAN-Verfügbarkeit ist zu hoffen, dass dieser Entwurf gar nicht erst den Bundestag erreicht.

Secorvo News

Sichere Systeme

Für die Entwicklung sicherer Systeme genügt es nicht, nur die Sicherheit der einzelnen Komponenten zu betrachten – in deren Zusammenspiel und an der Schnittstelle zum Benutzer können unerwartet neue Risiken entstehen. Wie sich auch in komplexen Systemen Security by Design erreichen lässt, erfahren Sie auf unserem Seminar T.E.S.S. – Sichere Systeme dank System Security Engineering vom 14. bis 19.06.2015 mit anschließender Zertifizierung als T.E.S.S. (TeleTrusT Engineer for System Security).

Der T.I.S.P., das deutsche Personenzertifikat für Informationssicherheit, umfasst alle grundlegenden Themenbereiche der Informationssicherheit. In unseren T.I.S.P. Schulungen erhalten Sie in fünf Tagen einen kompakten Überblick – und vorab unser T.I.S.P.-Begleitbuch zur Vorbereitung. Für die Schulung vom 22. bis 26.06.2015 gibt es noch wenige freie Plätze. Die nächste Möglichkeit zur Zertifizierung bieten wir im September und November. Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/college.

7. Tag der IT-Sicherheit

Der Tag der IT-Sicherheit am **19.05.2015** in Karlsruhe, eine Kooperationsveranstaltung der KA-IT-Si mit der IHK Karlsruhe, dem CyberForum und KASTEL, beschäftigt sich mit aktuellen IT-Sicherheitsherausforderungen für Unternehmen. Das Landesamt für Verfassungsschutz Baden-Württemberg informiert in einer Keynote über die aktuelle Bedrohungslage. Es folgen Fachvorträge zu den Themen Netzwerksicherheit, Datenschutz und Mobile Computing. Die Veranstaltung schließt mit einem Live-Hacking, das Sicherheitslücken von Webseiten aufzeigt. Zwischendurch gibt es Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit Referenten, Teilnehmern und Ausstellern. Wir freuen uns auf Ihre Anmeldung!

„No Blackout"

Am **12. und 13.05.2015** veranstaltet Secorvo anlässlich der bevorstehenden Verabschiedung des IT-Sicherheitsgesetzes und der daraus folgenden Verpflichtungen von Betreibern kritischer Infrastrukturen das Symposium „No Blackout – IT-Sicherheit für die Energieversorgung" in der Buhlschen Mühle in Ettlingen. Die Veranstaltung richtet sich nicht nur an Unternehmen und Institutionen aus dem Bereich der kritischen Infrastrukturen – sie bietet wertvolle Informationen für alle Unternehmen, die den Aufbau eines ISMS planen oder vorbereiten. Unter anderem werden die Stadtwerke Ettlingen über den „fx-Hack" und die Folgen berichten, und wir werden etwas über die IT-Sicherheit in Kernkraftwerken erfahren. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

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

April 2015	
14.-15.04.	Datenschutztage 2015 (FFD Forum für Datenschutz, Wiesbaden)
21.-24.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
22.-23.04.	Security Forum 2015 (Hagenberger Kreis, Hagenberg/AT)
23.-24.04.	8. GDD-Fachtagung "Datenschutz International" (GDD e.V., Berlin)
26.-30.04.	Eurocrypt 2015 (IACR, Sofia/BG)
Mai 2015	
04.-07.05.	CPSSE (Certified Professional for Secure Software Engineering) (Secorvo, Karlsruhe)
06.-07.05.	16. Datenschutzkongress (EUROFORUM, Berlin)
11.-12.05.	BvD Verbandstag 2015 (BvD e. V., Berlin)
12.-13.05.	No Blackout – Symposium IT-Sicherheit für die Energieversorgung (Secorvo, Ettlingen)
18.-20.05.	IMF 2015 (Fraunhofer IAO, Magdeburg)
18.-21.05.	OWASP AppSec EU 2015 (OWASP Foundation, Amsterdam/NL)
19.-21.05.	14. Deutscher IT-Sicherheitskongress (BSI, Bonn)
19.05.	7. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
20.-22.05.	Entwicklertag 2015 (VKSI, ObjektForum, Karlsruhe)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Michael Knopp, Sven Köhler, Christoph Schäfer, 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