secorvo
security consulting

Secorvo Security News

April 2014

Was jetzt zählt

Nicht jeder IT-Sicherheitsverantwortliche wird dieses Editorial lesen können – denn der eine oder andere wird noch mit den Aufräumarbeiten nach „Heartbleed“ beschäftigt sein. Dennoch sollte in der unvermeidlichen operativen Hektik nicht übersehen werden, was genau dieser JAB (*Just Another Bug*) uns eigentlich lehren müsste.

IT-Sicherheit hat viel mit Vertrauen zu tun. Das ist aber mehr Not als Tugend – denn wünschen würden wir uns, dass wir uns von der Vertrauenswürdigkeit einer Soft-, Hard- oder Cloudwarelösung, der wir unsere Kommunikation oder unsere Daten anvertrauen, zuverlässig überzeugen könnten.

Leider funktioniert das meistens nicht. So steht der Aufwand für die Analyse oft in keinem realistischen Verhältnis zum Schutzbedarf der Daten – oder bedroht gar die Wirtschaftlichkeit des Geschäftsmodells des Nutzers. Zudem ist jede Analyse immer nur eine Momentaufnahme: Jede Änderung am System (Konfiguration, Firmware, Hardware, Software, ...) kann ein zunächst positives Urteil in sein Gegenteil verkehren. Was bleibt ist bestenfalls ein strenger Vertrag mit dem Anbieter, das Einspielen von Patches und die fromme Hoffnung, dass die eigene Infrastruktur verschont bleibt.

Allerdings gibt es Bereiche, in denen wir uns nicht mit solcherart halbblindem Vertrauen begnügen dürfen: den „Herzstücken“ unserer IT-Sicherheitsinfrastrukturen – zu denen angesichts der weiten Verbreitung und zentralen Bedeutung zweifellos OpenSSL gezählt werden muss. Es hilft auch nicht, wie nach dem Bekanntwerden von Prism gebetsmühlenartig nach „Security made in Germany“ zu rufen – denn unglücklicherweise war es gerade ein deutscher Programmierer, dem die Welt nun Heartbleed verdankt.

In den zentralen Organen unserer Infrastrukturen brauchen wir mit Methoden der sicheren Softwareentwicklung erzeugten und nachprüfbar verifizierten Code. Sich dabei lediglich auf die Offenheit des Sourcecodes zu verlassen, ist schlicht unverantwortlich.

Inhalt

secorvo
security consulting

Security News

Persilschein für Office 365

Mit seiner Cloud-Kollaborationslösung Office 365 will Microsoft seine Kunden von komplizierten Lizenzverträgen befreien. Die neuen nutzerbezogenen Lizenzmodelle können dabei zu hohen Einsparungen führen. Um das Angebot datenschutzrechtlich abzusichern, hat Microsoft ein Vertragskonstrukt entworfen, welches eine Vereinbarung zur Auftragsdatenverarbeitung mit Microsoft Irland (Standort des europäischen Rechenzentrums) vorsieht. Da die Lizenzverwaltung und der Support durch Microsoft USA erfolgen, ist außerdem der Abschluss von EU Model Clauses erforderlich. Die Vertragsvorlagen können über das Office 365 Trust Center bezogen werden.

Mit Schreiben vom 29.11.2011 hatte das Bayerische Landesamt für Datenschutzaufsicht bereits die grundsätzliche Eignung der Microsoft-Verträge bestätigt. Nach intensiven Diskussionen liegt nun mit Datum vom 02.04.2014 eine weitere Bestätigung der Artikel-29-Gruppe vor, die Microsoft seit dem 10.04.2014 als Persilschein nutzt. Dabei sollte man allerdings nicht vergessen, dass man für die Übermittlung im Rahmen von EU Model Clauses nach wie vor eine Rechtsgrundlage benötigt. Ob es zudem ratsam ist, einen erheblichen Teil der Unternehmensdaten in die Hand eines (US-) Dienstleisters zu legen, steht auf einem anderen Blatt.

XP ist tot...

Mit dem Sicherheitsupdate MS14-020 veröffentlichte Microsoft am 08.04.2014 die letzten Patches für Windows XP und Microsoft Office 2003. Beide Produkte erfreuen sich jedoch weiterhin großer Beliebtheit. Die britische Regierung, das Land Niedersachsen und weitere Großkunden schlossen daher Verträge über ein weiteres Jahr Support für ihre Systeme ab. Den meisten Nutzern der beiden Softwarepakete werden jedoch weitere Updates verwehrt bleiben.

Voraussichtlich wird die Zahl der Schwachstellen und Exploits ansteigen – auch weil Windows XP und Office 2003 sich mit den neueren Versionen große Teile des Quellcodes teilen. So lassen sich aus zukünftigen Sicherheitsupdates mit einfachen Reverse Engineering-Techniken wie binären Diff-Tools die behobenen Schwachstellen ausfindig machen – von dort ist der Weg zum funktionierenden XP-Exploit nicht mehr weit.

Immerhin: Eingebettete Alt-Systeme wie Bankautomaten sind von dem Problem meist nicht betroffen, da sie überwiegend Windows XP Embedded verwenden – und das wird bis 2016 mit Updates versorgt.

Ende der Verantwortungsabschiebung

In einem mit Spannung erwarteten Urteil hat der Europäische Gerichtshof am 08.04.2014 die Richtlinie zur Vorratsdatenspeicherung (RL 2006/24/EG) rückwirkend für ungültig erklärt. Die europarechtliche Pflicht zur Einführung einer Vorratsdatenspeicherung ist damit entfallen.

Der EuGH folgt in seinem Urteil weitgehend der Argumentation, die bereits das Bundesverfassungsgericht seinem Urteil zu Grunde gelegt hatte: Der schwerwiegende Eingriff in Art. 7 und 8 der Charta der Grundrechte der Europäischen Union sei nur verhältnismäßig, wenn die Verwendung der Daten anhand klarer Kriterien begrenzt, die Datensicherheit durch strikte Regeln gewährleistet und die Speicherdauer anhand objektiver Kriterien auf das absolut Notwendige beschränkt werde. Auch schreibe die Richtlinie keine Speicherung im Unionsgebiet vor, so dass nicht sichergestellt sei, dass die Umsetzung der Datensicherheitsanforderungen durch eine unabhängige Stelle der EU überwacht werden könne.

Zwar berührt auch nach Auffassung des EuGH die Vorratsdatenspeicherung nicht den Wesensgehalt der Chartagrundrechte. Doch kann sich jetzt keine Regierung eines Mitgliedsstaats mehr bei der Einführung einer Vorratsdatenspeicherung hinter einer europäischen Umsetzungspflicht verstecken.

Schutz durch Big Data

Am 25.03.2014 stellte Mark Hammell auf der Webseite der Facebook-Sicherheitsinitiative „protectthegraph“ vor, wie Facebook Security-Informationen automatisiert verarbeitet – mit hauseigenen Big Data-Techniken.

Die Komponente Feeds sammelt ständig sicherheitsnahe Informationen aus freien und abonnierten externen und eigenen Quellen und reichert diese mit Kontextdaten wie Ort und Zeit an. Dies können Daten von Malware-Diensten sein, Hinweise aus Infoportalen, Security-Blogs oder Informationen der eigenen Security-Teams.

Diese Daten werden jeweils als Thread-Datum im Hieve, dem Hadoop-Datawarehouse von Facebook archiviert. Das für Massendaten entwickelte Analysewerkzeug Scuba untersucht jedes neue Thread-Datum auf Trends oder Muster und startet Reaktionsprozesse – Blacklisting gefährlicher URLs, Benachrichtigung von Nutzern oder Alarmierung des Security-Teams.

In internen Tests habe dieses System die eingesetzten Antiviren-Produkte geschlagen. Dieses Ergebnis steht und fällt jedoch mit aktuellen externen Informationen, wie von Lösungsanbietern kritisiert wurde. Es deutet aber daraufhin, dass das Teilen von Information z. B. über erkannte Angriffsmuster oder eigene Vorfälle für alle Beteiligten – außer dem Angreifer natürlich – Vorteile bietet.

Innerhalb einiger Branchen gibt es dieses kooperative Vorgehen bereits. Was fehlt ist allerdings ein einheitliches Datenformat. Dessen Spezifikation wäre einmal eine sinnvolle Aufgabe für eine der zahlreichen Cybersecurity-Initiativen.

Open Source-Desaster

Gleich mehrere verbreitete Open Source-Lösungen standen in den vergangenen Wochen im Rampenlicht. Zunächst sorgte bekanntlich am 07.04.2014 das Security Announcement von OpenSSL, inzwischen als Heartbleed bekannt, für Furore (siehe Editorial). Die Schwachstelle ermöglicht das (spurlose) Auslesen von 64 kByte großen Speicherbereichen eines SSL-Servers. Der Programmierfehler wurde weder während des Reviews noch in den zwei darauffolgenden Jahren bemerkt, bis Neel Mehta von Google ihn entdeckte und dem OpenSSL-Team meldete.

Mit den Updates für iOS 7.1 vom 23.03.2014 und iOS 7.1.1 sowie die Safari Browser 6.1.3 und 7.0.3 vom 22.04.2014 behob Apple einen weiteren, als „Triple Handshake" bezeichneten Bug in der SSL/TLS-Implementierung sowie zahlreiche Schwachstellen in der Open-Source-HTML-Engine WebKit, die von Safari und vielen weiteren Browsern genutzt wird. Von den 27 Schwachstellen in WebKit wurden 26 durch Programmierfehler verursacht, die den Datenspeicher korrumpieren: Beim Besuch manipulierter Webseiten kann damit Code vom Angreifer auf dem Rechner des Opfers ausgeführt werden.

Das Google Chrome Security Team fand 18 der 26 Schwachstellen, da Chrome die Engine Blink verwendet, die im April 2013 aus dem Sourcecode von WebKit abgespaltet worden war. Dabei konnte Google 8.8 Millionen Codezeilen entfernen. Möglicherweise schlummern noch immer etliche Bugs in WebKit, die Google bereits in Chrome beseitigt hat – bis Apple sie eines Tages findet.

Schließlich erschien am 14.04.2014 der Bericht über den ersten Teil des Source-Code-Audits zu TrueCrypt. Er dokumentiert eine gründliche Prüfung des Bootloaders und des Kernel-Treibers. Zwar wurden keine gravierenden Schwachstellen aufgedeckt; dennoch gibt die Bewertung „*Overall, the source code for both the bootloader and the Windows kernel driver did not meet expected standards for secure code*" zu denken.

Zur Vermeidung von gravierenden Schwachstellen in so grundlegenden Bausteinen der Sicherheit sollte die Offenheit des Codes mit der gebotenen Professionalität beim Entwickeln und prüfen kombiniert werden (siehe SSN 01/2014). Hierzu bedarf es entsprechender Anreize und Ressourcen. Initiativen wie das Open Crypto Audit Project zeigen einen möglichen Weg dafür auf.

Secorvo News

PKI für Profis

Seit den späten 90er Jahren realisiert Secorvo PKI-Projekte. Der dabei entstandene, Produkt unabhängige Erfahrungsschatz in Sachen Konzeption, Aufbau, Betrieb und Weiterentwicklung wurde für das Seminar „PKI – Grundlagen, Vertiefung und Realisierung" in einem viertägigen Programm verdichtet. Die fünf Referenten des Seminars bringen zusammen über 90 Jahre Berufserfahrung in der IT-Sicherheit mit. Für den Einsteiger bietet die Schulung eine grundlegende, Produkt unabhängige Einführung, für den Profi eine vertiefende Auseinandersetzung mit den Möglichkeiten von Public Key Infrastrukturen. Nächster Seminartermin ist der 24. bis 27.06.2014.

Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Live Hacking

Live-Hacking-Demos haben gelegentlich vor allem Show-Charakter – die vorgestellten Angriffe betreffen entweder längst ausgemusterte IT-Systeme oder führen für einen praktischen Angriff eher ungeeignete Spezialschwachstellen vor.

Nach dem großen Erfolg der Live-Vorführung eines äußerst wirkungsvollen WLAN-Angriffs auf der vergangenen Anti-Prism-Party am 12.02.2014 im Karlsruher ZKM werden Kai Jendrian und Jörg Völker von Secorvo den Angriff und einige einfache und elementare Maßnahmen zum Schutz der Privatsphäre auf der kommenden Veranstaltung der KA-IT-Si am **05.06.2014** erneut vorstellen (18 Uhr im Panoramasaal der IHK Karlsruhe).

Nach Vortrag und Diskussion haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" – diesmal über den Dächern von Karlsruhe. Weitere Informationen und die Möglichkeit zur Anmeldung auf www.ka-it-si.de.

Veranstaltungshinweise

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

Mai 2014	
05.-09.05.	CPSSE (Certified Professional for Secure Software Engineering) – Schulung und Prüfung (Secorvo College, Karlsruhe)
07.-09.05.	1st DFRWS EU Conference (DFRWS, Amsterdam/NL)
11.-15.05.	Eurocrypt 2014 (IACR, Kopenhagen/DK)
12.-14.05.	IMF 2014 (Fraunhofer IAO, Münster)
14.-16.05.	15. Datenschutzkongress (Euroforum, Berlin)
16.05.	Jahrestagung "Datenschutz im digitalen Zeitalter – global, europäisch, national" (Institut für Rundfunkrecht an der Universität zu Köln, Köln)
19.-20.05.	a-i3/BSI-Symposium 2014 (Arbeitsgruppe Identitätenschutz im Internet/BSI, Bochum)
21.-22.05.	BvD Datenschutztage (BvD e. V., Berlin)
21.-23.05.	Entwicklertag 2014 (VKSI, GI, Objekt-Forum, Karlsruhe)
Juni 2014	
23.-24.06.	DuD 2014 (Computas, Berlin)
23.-26.06.	OWASP AppSec EU 2014 (OWASP, Cambridge/UK)

Fundsache

Damn Vulnerable iOS App ist eine App, die alle gängigen Sicherheitslücken von iOS-Anwendungen enthält – sie ist „verdammt verwundbar". Diese App bietet Sicherheitsinteressierten eine Plattform, auf der sie iOS-Penetrationtests legal durchführen können.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, André Domnick, Kai Jendrian, Michael Knopp, Sven Köhler, 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