Secorvo Security News

April 2020

Imagine

Stellen Sie sich einmal vor – rein hypothetisch – ein neuer Virus bräche aus. In China. Ein Computervirus, meine ich.

Und stellen Sie sich weiter vor, er besäße unschöne Eigenschaften: Er ist hochansteckend und besitzt eine Inkubationszeit von einigen Tagen, in denen er sich aber weiter verbreitet. Bricht er aus, dann richtet er bei 5-10 % der befallenen Geräte erhebliche Schäden an – von der Löschung des Datenbestands und der installierten Software bis hin zu irreparablen Hardware-Defekten. Jüngere Geräte sind offenbar weniger stark betroffen.

Dabei nutzt er alle Schwächungen des „Immunsystems" wie sicherheitskritische Fehler in veralteter Software oder unbedachte Konfigurationen. Offenbar verwendet er alle Arten von Kontakten mit anderen Rechnern zur Verbreitung: USB-Sticks, SD-Karten, Bluetooth-, WLAN- und Internetverbindungen. Befallene Rechner können bisher nur über die Symptome identifiziert werden; da der Virus sein Erscheinungsbild ändert, ist er für Virenscanner „unsichtbar".

Da sich der Virus nun auch in Deutschland ausbreitet, Sicherheitsexperten zur Schadensbegrenzung knapp sind und bisher keine wirksamen Schutzmaßnahmen zur Verfügung stehen, sperrt die Bundesregierung internationale Datenverbindungen. Rechner dürfen Räume nur noch in unvermeidlichen Fällen verlassen und nur innerhalb des Unternehmens oder der eigenen Wohnung miteinander verbunden werden (LAN). Sie müssen einen Mindestabstand von 1,5 m zu anderen Rechnern einhalten und außerhalb geschlossener Räume in Metallbehältern transportiert werden...

Das klingt ein wenig wie Selbstmord aus Angst vor dem Tod. Und selbst wenn der Vergleich mit der aktuellen Situation hinkt (denn schließlich geht es dort um den Schutz von Leib und Leben): Ein wenig mehr Paranoia hier und etwas mehr Augenmaß dort könnten keinesfalls schaden.

Inhalt

secorvo
security consulting

Security News

MASVS 1.2

Nach zahlreichen Überarbeitungen wurde am 17.03.2020 Version 1.2 des Mobile Application Security Verification Standard (MASVS) von OWASP gleich in acht Sprachen veröffentlicht. Analog zum etablierten ASVS für Web-Anwendungen definiert der MASVS einen Sicherheitsstandard aus verschiedenen Anforderungen an mobile Apps. In Anbetracht der häufigen Berichterstattung über verwundbare Apps war ein solcher Standard überfällig.

Der MASVS unterscheidet drei aufeinander aufbauende Prüf-Niveaus/Level: Der Basis-Level 1 wird in Level 2 um Defense-in-Depth-Anforderungen und in Level „R" um Maßnahmen gegen Reverse Engineering erweitert. Je nach Schutzbedarf der App sollte der gewünschte Level entsprechend festgelegt werden. In acht Bereichen wird im Standard beschrieben, welche Anforderungen beispielsweise an Architektur, Datenschutz und sichere Kommunikation gestellt werden.

Ergänzt wird der MASVS zukünftig um die Version 1.2 des Mobile Security Testing Guide (MSTG). Der MSTG beschreibt Prüfpunkte für die Sicherheitsanforderungen des MASVS und kann somit im Rahmen eines Pentests eingesetzt werden. Da Apps meist mit Web-Services im Backend kommunizieren und deren Sicherheit im Rahmen des MASVS nicht betrachtet wird, sollte die Prüfung des Gesamtsystems auch die Web-Services umfassen. Hierbei empfiehlt sich eine Vorgehensweise auf Basis des OWASP Testing Guide und Prüfung der API Security Top 10.

CWE für Hardware-Schwächen

Bisher war die Common Weakness Enumeration (CWE) eine Sammlung und Kategorisierung häufiger Fehler in Software, die zu Sicherheitsschwachstellen führen können (SSN 12/2019). Am 24.02.2020 sind mit Version 4.0 häufige Fehler im Hardware-Design neu hinzugekommen; zusätzlich gibt es eine für die sichere Softwareentwicklung wertvolle „Software Development"-Sicht auf die Schwächen, welche die vorherigen Architektur- und Entwicklungs-Sichten kombiniert.

Aus Sicherheitssicht besonders zu begrüßen ist die Integration von Hardware-Schwächen in die CWE. Dieser Schritt unterstreicht eine Entwicklung, die wir in der vergangenen Zeit vermehrt beobachten konnten: Nachdem Software-Sicherheit sich inzwischen als ein wichtiges und zunehmend höher priorisiertes Qualitätsmerkmal etabliert hat, wird der Allgemeinheit die Fehlbarkeit von Hardware immer bewusster – nicht zuletzt aufgrund von medial wirksamen Schwachstellen wie Meltdown und Spectre (SSN 02/2018). Bisher spielte die Sicherheit bei der Entwicklung von Hardware eher eine untergeordnete Rolle. Wichtigere Parameter waren Performance, Effizienz und Kosten. Dass Hardware-Fehler unter Umständen alle anderen Sicherheitsmaßnahmen kompromittieren können, haben verschiedene Schwachstellen eindrucksvoll demonstriert. Beispielsweise war ein Fehler im Nvidia Tegra Prozessor in frühen Nintendo Switch Konsolen dafür verantwortlich, dass diese ohne eine Möglichkeit zur Behebung mit Homebrew-Firmware bespielt werden konnten. Auch Apple hat in jüngster Vergangenheit Bekanntschaft mit Hardware-Schwachstellen gemacht: Der checkra1n-Exploit für iPhones wurde inzwischen auf den in Macs zu findenden T2-Chip „portiert". Und Intels „Converged Security and Management Engine" (CSME) ist ebenfalls von einer nicht behebbaren Schwachstelle betroffen. Wir empfehlen daher auch bei Hardware-Entwicklung die Nutzung der CWE und die Durchführung expliziter Risikobetrachtungen.

Gefährliche Browser-Helfer

Als kleine Alltagshelfer erleichtern „Browser Extensions" und andere Plugins vielerlei Aufgaben. Doch merke: Erweiterungen sind Computerprogramme und können Schaden anrichten. Sie dürfen zudem meist mit nur wenigen Klicks auch von niedrig privilegierten Nutzern installiert werden und stammen oft aus intransparenten Quellen.

Wie Brian Krebs am 03.03.2020 berichtete, war eine Browser Extension verantwortlich dafür, dass die Webseite des „Blue Shield of California" von verschiedenen Sicherheitsprodukten als bösartig eingestuft wurde. Ein Mitarbeiter, der die Webseite aktualisierte, hatte in seinem Webbrowser die Erweiterung „Page Ruler" installiert. Als einst nützliches Tool mit über 400.000 Installationen wurde sie vor wenigen Jahren vom Entwickler verkauft und injiziert seitdem im Hintergrund bösartigen JavaScript-Code in Webseiten, während diese über ein CMS wie WordPress oder Joomla gepflegt werden.

Wie häufig das Problem bösartiger Erweiterungen ist, zeigt ein Blick auf Googles Chrome Web Store: Im Februar 2020 wurden 500 bösartige Erweiterungen entfernt, im April 2020 nochmals fast 50 – und das ist wahrscheinlich nur die Spitze des Eisbergs. Wie schon beim Umgang mit Docker-Images und Programmbibliotheken (SSN 03/2019) empfehlen wir auch bei Plugins einen minimalistischen Ansatz: Installieren Sie nur solche Plugins, die Sie unbedingt benötigen und die von vertrauenswürdigen Entwicklern aus offiziellen Quellen stammen. In größe-

ren Umgebungen empfiehlt sich ein Whitelisting-Ansatz: Konfigurieren Sie Webbrowser so, dass nur erlaubte Plugins installierbar sind. Eine vollständige Deaktivierung von Plugins sollte hingegen gut abgewogen werden, da viele Plugins Ihre Sicherheit und Privatheit im Web verbessern.

Neu im Telemediengesetz

Am 03.04.2020 hat die Bundesregierung mit dem Gesetzesentwurf zur Umsetzung der 2018 überarbeiteten Richtlinie über audiovisuelle Mediendienste (AVMD-RL) im Telemediengesetz das Gesetzgebungsverfahren eröffnet; jetzt ist der Bundesrat am Zug. Der Entwurf verankert neben dem bisherigen Telemedienrecht neue Pflichten für Anbieter von Webseiten zum Abruf von Video-Sendungen und Videosharing-Plattformen in den neuen §§ 10a ff TMG. Dazu gehören ein Beschwerdeverfahren, das Videosharing-Plattform-Anbieter ihren Nutzern bereitstellen müssen, und ein entsprechendes Abhilfeverfahren bezüglich rechtswidriger Inhalte. Weiter werden eine Verpflichtung zum Einsatz von Nutzungsbedingungen und eine Datenschutzregelung für den Umgang u. a. mit Altersverifikationsdaten eingeführt.

Auch wenn Ziel des Gesetzes die Richtlinienumsetzung ist, überrascht doch, dass trotz wiederholter TMG-Änderungen seit Geltung der DSGVO noch immer keine Anpassung der §§ 13 ff TMG erfolgt, obwohl diese schon lange von Aufsichtsbehörden und Lehre als unzureichend angesehen werden.

Dauerbrenner DS-Erklärung

Das Spannungsverhältnis zwischen Transparenz und Verständlichkeit von Datenschutzerklärungen erhält weiteres Futter. Der Erwägungsgrund 39 der DSGVO verlangt Verständlichkeit in einer klaren und einfachen Sprache. Aufsichtsbehörden und Gerichte scheinen sich jedoch derzeit eher in Richtung Detaillierung zu bewegen. So wandte sich die dänische Datenschutzaufsichtsbehörde am 11.02.2020 in einer Entscheidung gegen das Dänische Meteorologische Institut gegen gängige Cookie-Banner: Die Einwilligung über ein einheitliches „Akzeptieren“ oder „Ok“ sei nicht ausreichend für eine freiwillige Einwilligung. Vielmehr müsse in unterschiedliche Verarbeitungszwecke granular und einzeln eingewilligt werden. Das Angebot einer detaillierten Auswahl nach einem weiteren Klick sei intransparent. Auch müsse eine Gesamtablehnung mit einem Klick möglich und genauso schnell auffindbar sein. Mit anderem Bezug, aber möglicherweise richtungsweisend urteilte das OLG Köln am 19.02.2020, dass allein der 80seitige Umfang der AGB bei einem komplexen Geschäftsmodell wie PayPal nicht zur Intransparenz und mangelnder Einbeziehung führe. Bei Internetgeschäften sei es dem Nutzer überlassen, wie lange er sich mit den Bedingungen befasse.

Für Datenschutzerklärungen (56 Seiten von Samsung) wurde dies auch schon umgekehrt bewertet (SSN 06/2016). Die „Wahrheit“ dürfte wohl in der Mitte liegen.

Corona-Orientierungshilfe

Der Europäische Datenschutzausschuss (EDSA) hat in seiner 24. Sitzung am 24.04.2020 seine bisherigen Empfehlungen zum Umgang mit Gesundheitsdaten während einer Pandemie ergänzt und Orientierungshilfen zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken im Kontext des Covid-19 Ausbruchs angenommen.

Eine erste Ergänzung betrifft die Erleichterung internationaler Datentransfers zu Forschungszwecken in Drittstaaten. Hier soll auf die Ausnahmen des Art. 49 DSGVO zurückgegriffen werden, wenn andere Garantien des Datenschutzniveaus nicht zur Verfügung stehen.

Bezüglich der Tracking-Tools zur Ausbreitungsüberwachung verweist der EDSA auf die Flexibilität der DSGVO, die den Datenbedarf zur Epidemie-Bekämpfung bereits vorsehe. Die Orientierungshilfe setzt sich intensiv mit der Gestaltung erforderlicher Einwilligungen auseinander. Weitere Anforderungen betreffen Anonymisierung und Löschfristen sowie den angemessenen Schutz der Daten, wenigstens durch Pseudonymisierung oder Verschlüsselung.

Insgesamt betont der EDSA, dass trotz der Ausnahmesituation die Datenschutzbestimmungen der DSGVO umgesetzt werden können und müssen.

Secorvo News

Wiederaufnahme des Seminarbetriebs

Den aufgrund der Pandemie-Verordnungen des Landes Baden-Württemberg bis Ende Mai eingestellten Seminarbetrieb werden wir nach der Sommerpause wieder aufnehmen. Da viele Teilnehmer ihre Anmeldung verschoben haben, ist die Mindestteilnehmerzahl schon jetzt bei einigen Seminaren erreicht – wir empfehlen daher eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Hinweis: Wegen der derzeitigen Pandemie-Einschränkung finden einige der genannten Veranstaltungen möglicherweise nicht oder in anderer Form statt.

Mai 2020	
06.-07.05.	BvD Verbandstag 2020 (BvD e.V., Berlin)
12.-15.05.	European Identity & Cloud Conference 2020 (KuppingerCole Ltd., München)
13.-14.05.	21. Datenschutzkongress (EUROFORUM, Berlin)
Juni 2020	
02.-03.06.	a-i3/BSI-Symposium 2020 (a-i3, Bochum)
15.-16.06.	DuD 2020 (COMPUTAS, Berlin)
Juli 2020	
14.-18.07.	PETS 2020 (University of Minnesota, Montréal/CAN)
19.-21.07.	DFRWS USA 2020 (DFRWS, Memphis/US)

Fundsache

Privacy Captcha gibt es zwar schon seit 2014, aber seit Spätsommer 2019 in neuem Gewand und gerade derzeit für einen sicheren Versand schützenswerter Daten bei unsicheren Kommunikationskanälen zu empfehlen.

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Michael Knopp, Sarah Niederer, Christian Titze

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