secorvo
security consulting

Secorvo Security News

Dezember 2019

Zauberlehrlinge

Walle! Walle manche Strecke, dass zum Zwecke Software fließe, und mit reichem, vollem Schwalle in den Rechner sich ergieße.

Das haben wir weder gewollt noch gemeint, als wir in den späten 90er Jahren regelmäßige Sicherheits-Patches forderten: Wer sich heute mit dem Internet verbindet, um einige wenige Sätze lange E-Mails abzurufen, wundert sich regelmäßig über sein rapide schrumpfendes Downloadkontingent. Denn nicht selten laden Rechner und Smartphones täglich Updates für Programme („Apps“) und Betriebssystem im Umfang von mehreren Gigabyte – je Gerät in etwa das Volumen aller täglichen Twitter-Nachrichten zusammen, weltweit.

Kein Wunder, dass Bandbreiten knapp und Netze ständig überlastet sind. Herstellern und Providern kann das wohl recht sein – der ungebändigt steigende Datenhunger nährt ihre Geschäfte, und der Kunde zahlt, ohne zu bemerken, dass es gar nicht seine Nutzung ist, die den Datenverkehr verursacht. Dabei scheint das eine das andere zu befeuern: Die Frequenz, in der Apps heute aktualisiert werden, legt nahe, dass die Hersteller es mit der Sorgfalt nicht (mehr) so genau nehmen. Warum auch, wenn man schon morgen das nächste Update nachschieben und die (Sicherheits-) Tests auf den Kunden auslagern kann?

Und so sind wir dabei, das Verhältnis von Nutzdaten zum gesamten Datenvolumen rapide zu verschlechtern. Zum Glück sind da noch die Video-Streamer, sonst wären wir wohl schon deutlich unter der Ein-Prozent-Marke. Und während unsere Kinder freitags im Namen von Umwelt und Zukunft die Schule schwänzen, verbraten ihre Smartphones und die zugehörige Netzwerkinfrastruktur über 90% der Energie für die Übermittlung von Wegwerfcode, der schon bald durch ein Update ersetzt werden wird.

Diesmal ist es mit einem „*In die Ecke, Besen! Besen! Seids gewesen.*“ des Meisters wohl nicht getan.

Inhalt

Security News

Top 25 Software Errors

Neben dem bekannten CVE-System zur eindeutigen Identifizierung von konkreten, produktspezifischen Schwachstellen bietet die weniger bekannte „Common Weakness Enumeration“ (CWE) eine detaillierte Übersicht und Kategorisierung bekannter Fehler in Software. Die gefährlichsten werden in der Liste der „Top 25 Most Dangerous Software Errors“ geführt, die am 18.09.2019 zum ersten Mal seit acht Jahren neu erstellt wurde. Dafür wurden ca. 25.000 CVE-Einträge und deren Verknüpfungen zu CWE-Einträgen aus den vergangenen zwei Jahren ausgewertet. SQL Injections fielen dabei von Platz 1 auf Platz 6 zurück, während Cross-Site Scripting (XSS) und Out-of-Bounds-Speicherzugriffe (wie z. B. „Buffer Overflows“) die neue Liste anführen.

Die detaillierten Erläuterungen der Fehlertypen mit Code-Beispielen in mehreren Programmiersprachen und Vorschlägen für Gegenmaßnahmen aus unterschiedlichen Perspektiven sind eine empfehlenswerte Handreichung für jeden Software-Entwickler.

DSGVO-Erfahrungen

Am 06.11.2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) einen Erfahrungsbericht über die DSGVO-Umsetzung verabschiedet und Anfang Dezember veröffentlicht. Darin werden die Bereiche Informationspflichten, Recht auf Unterlagenkopien, Benennungspflicht des Datenschutzbeauftragten, Vorfallsmeldungen, Zweckbindung, Sanktionspraxis, Privacy by design, Direktwerbung, Profiling und einige eher die Zusammenarbeit der Behörden betreffende Fragen diskutiert. Zu einer Reihe von Regelungen werden Änderungsvorschläge gemacht.

Dabei wird deutlich, dass es sich um Erfahrungen der Aufsichtsbehörden handelt – der radikalste Vorschlag ist die Streichung der Meldepflicht des Datenschutzbeauftragten; die Veröffentlichungspflicht reiche aus. Der ausufernde Informationskatalog des Art. 13 f DSGVO soll bei zu erwartender Verarbeitung nur auf Verlangen erteilt werden. Weiter wird der Anstieg von Bagatellmeldungen beklagt – die in vielen Fällen entbehrliche 72-Stunden-Frist wird hingegen nicht thematisiert. Zwar wird der Bedarf eines Datenschutzmanagements festgestellt, aber dessen konkrete Ausgestaltung nicht diskutiert. Für das Profiling wird eine Verschärfung des Verbots aus Art. 22 DSGVO gefordert und für Art. 25 DSGVO (Privacy by design) eine Ausdehnung auf die Hersteller als Adressaten.

Insgesamt hätte man dem Bericht mehr Mut zur kritischen Vernunft, einen weniger eingeschränkten Blick sowie einen größeren Themenumfang gewünscht.

Responsible Disclosure

Am 09.12.2019 bat die Internet Engineering Task Force (IETF) um eine letzte Kommentierung des Drafts „A Method for Web Security Policies“. Dieser Internet-Standard spezifiziert die Informationen für Sicherheitsforscher, wie gefundene Schwachstellen bei den Betreibern gemeldet werden können. Die Ablage soll in einer Datei namens „security.txt“ erfolgen, die Webseitenbetreiber auf ihrem Webserver im Verzeichnis „/.well-known/“ ablegen. Vorgesehen sind neben den üblichen Kontaktdaten (E-Mail, Telefon) auch Bug-Bounty-Programme, und zwar sowohl solche des Betreibers als auch von Plattformen wie HackerOne oder Bugcrowd. Noch vor Verabschiedung des Standards bietet der Webdienst securitytxt.org bereits eine Funktion zum Erstellen einer solchen Datei und hilfreiche Hinweise zum Thema. Es wäre erfreulich, wenn sich diese Meldewegedokumentation in der Praxis durchsetzt.

Schuld ist immer der Andere

Am 05.12.2019 hat das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein den Volltext des Urteils des Bundesverwaltungsgerichts (BVerwG) vom 11.09.2019 veröffentlicht und in einer Pressemitteilung kommentiert. Kernpunkt war die Frage, ob der Betreiber einer Facebook Fanpage datenschutzrechtlicher Verantwortlicher ist oder nicht. Der im Rahmen des Vorabentscheidungsersuchens mit dieser Frage ebenfalls befasste EuGH hatte dies bereits am 05.06.2018 bejaht (SSN 07/2018). Das BVerwG hat nun in den Urteilsgründen klargestellt, dass es beim Betrieb der Fanpages nicht nur einen Fall der gemeinsamen Verantwortlichkeit sieht, sondern dass darüber hinaus auch der Betreiber der Facebook Fanpage verantwortlich im Sinne von Art. 2 lit. d) der Datenschutzrichtlinie ist. Weiter sei auch das BDSG alter Fassung unionsrechtskonform auszulegen, und deshalb sei auch der Betreiber einer Facebook Fanpage verantwortliche Stelle im Sinne des § 38 Abs. 5 BDSG a.F., unabhängig davon, ob im Rahmen einer gemeinsamen Verantwortlichkeit die Verantwortlichen in gleichem Maße Zugriff auf die personenbezogenen Daten haben.

Das Urteil bezieht sich allerdings auf die Rechtslage im Dezember 2011. Fanpage-Betreiber werden aber auch zukünftig Adressaten von ähnlichen Verfügungen sein können. Wie die Rechtmäßigkeit der Verarbeitungen durch Facebook nach aktueller Rechtslage zu beurteilen ist, bleibt im Urteil unbeantwor-

tet. Wer eine Facebook Fanpage betreibt, sollte sich jedoch seiner desbezüglichen Verantwortung bewusst sein und die notwendigen Maßnahmen zur Information der Betroffenen ergreifen sowie den Schutz der personenbezogenen Daten ernst nehmen.

German OWASP Day 2019

Am 10.12.2019 fand der German OWASP Day in Karlsruhe statt. Die gut besuchte und sehr gut organisierte Veranstaltung bot eine Reihe spannender und interessanter Vorträge. Besonders gut gefallen haben uns die Keynote von Christoph Kerschbaumer zu den verschiedenen Schichten der Firefox-Härtung und der von Jiska Classen sehr unterhaltsam vorgetragene Hack von Vorwerk-Staubsauger-Robotern. Empfehlenswert auch die von Franziska Bühler vorgestellte Möglichkeit von "ModDevOpsSec" – ein pragmatisches Vorgehen, wie man Security bei DevOps berücksichtigen und in das Ganze auch noch eine Web Application Firewall auf Basis von ModSecurity integrieren kann. So kann die Absicherung von Web Applikationen tatsächlich gut funktionieren.

RSA-240 faktorisiert

Am 02.12.2019 informierte eine Gruppe französischer Zahlentheoretiker um Emmanuel Thomé, dass ihnen die Faktorisierung von RSA-240 (795 bit) der RSA Factoring Challenge aus dem Jahr 1991 gelungen sei. Der Aufwand lag dank verbesserter Algorithmen rund 25% unter dem der Faktorisierung von RSA-232 (768 bit) vor ziemlich genau zehn Jahren (SSN 01/2010). Die Faktorisierungserfolge machen damit eine „Seitwärtsbewegung“ – und bleiben deutlich unter unserer Prognose aus dem Jahr 2002. Mit der Faktorisierung eines 1024-bit-Schlüssels (RSA-309) ist für das Jahr 2020 also eher nicht zu rechnen. Die Faktorisierung eines doppelt so langen, 2048-bit-RSA-Schlüssels (RSA-617) dürfte nach der Prognose nicht vor 2060 gelingen – wären da nicht die Quantencomputer, denen das (zumindest theoretisch) innerhalb von acht Stunden gelingen könnte, wie von Craig Gidney und Martin Ekera am 05.12.2019 beschrieben.

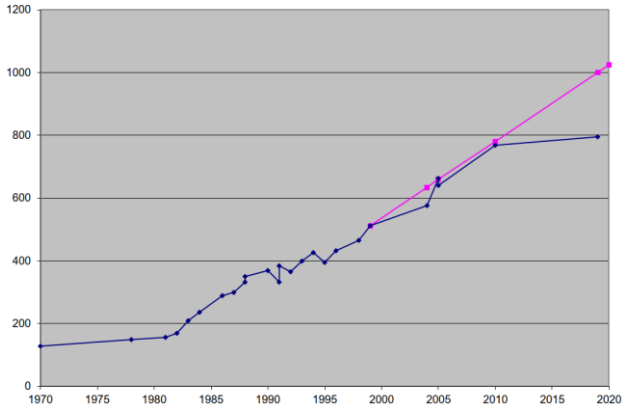

Abb.: Faktorisierungserfolge (blau), Prognose (rot)

DSGVO-konformes Win10

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat am 06./07.11.2019 ein Prüfschema zu Windows 10 veröffentlicht, das Verantwortliche in der Beantwortung der Frage unterstützt, ob Windows 10 DSGVO-konform eingesetzt wird.

Nach dem Prüfschema für Windows 10 und den zugehörigen wietergehenden technischen Hinweisen der DSK ist dafür insbesondere zu prüfen, ob eine Rechtsgrundlage für eine Übermittlung an Microsoft vorliegt. Da sich nicht alle Datenübermittlungen deaktivieren lassen, müssen erforderlichenfalls weitere technische und organisatorische Maßnahmen ergriffen werden, um unzulässige Übermittlungen zu unterbinden.

Secorvo News

... und noch nie zu fragen wagten.

Keine Novellierung des Datenschutzrechts hat eine solche Aufmerksamkeit bekommen wie die im Mai 2018 in Kraft getretene Datenschutz-Grundverordnung. Obwohl fast alles beim Alten geblieben ist, ist doch alles anders... und sind viele konkrete Fragen offen: Wann ist das Tracking von Webseitenbesuchern zulässig? Wie kann ein Unternehmen seine Informationspflichten angemessen erfüllen? Welche Datenschutzvorfälle sind meldepflichtig? Wie bestimmt sich die Höhe eines Bußgelds?

Zu diesen, weiteren und auch Ihren Fragen zur DSGVO und dem Datenschutz wird uns auf dem Jahresstart-Event der KA-IT-Si am **13.02.2019** Dr. Stefan Brink, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Rede und Antwort stehen. Wir freuen uns sehr auf diesen Termin, denn Dr. Brink ist für seine klaren Einschätzungen bekannt – und hoffen auf großes Interesse Ihrerseits.

Wir empfehlen eine frühzeitige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2020	
20.-22.01.	Omnisecure 2020 (in TIME, Berlin)
21.-24.01.	AppSec California 2020 (OWASP Foundation, Santa Monica/US)
31.01.-02.02.	ShmooCon 2020 (The Shmoo Group, Washington/US)
Februar 2020	
19.-20.02.	30. ID:SMART Workshop (Fraunhofer Institut SIT, Darmstadt)
24.-25.02.	27. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
März 2020	
09.-12.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-20.03.	GI Sicherheit 2020 (Gesellschaft für Informatik, Göttingen)
25.-26.03.	secIT 2020 (Heise Medien, Hannover)

Fundsache

Das BSI bietet im Rahmen des Services BSI für Bürger eine Reihe von Erklärvideos an. Die anschaulich animierten Kurzfilme weisen auf wichtige Aspekte der IT-Sicherheit wie Backup, Browsersicherheit, Phishing und das Löschen von Daten auf Smartphones hin. Empfehlenswert.

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Fabian Ebner, Stefan Gora, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, 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