secorvo
security consulting

Secorvo Security News

November/Dezember 2023

Lernen durch Schmerzen

Also doch. Bei der Publikation der Untersuchungsergebnisse, wie Microsoft mindestens ein Entra-ID-Signierschlüssel abhanden kommen konnte, sprach das Unternehmen am 06.09.2023 noch von einer Aneinanderreihung unglücklicher, aber verzeihlicher Fehler. Die Ankündigung des stellvertretenden Vorstandsvorsitzenden Brad Smith vom 02.11.2023 klingt da schon ganz anders: Die Cyberangriffe der letzten Monate hätten Microsoft von der Notwendigkeit einer Reaktion überzeugt - der Secure Future Initiative. Es ist die Rede von einer firmenweiten Anstrengung, bei der auch KI zum Einsatz kommen soll. Das vom Marketing zunächst kleingeredete Ereignis hat das Unternehmen intern wohl doch erschüttert.

Vor allem will sich Microsoft nun um eine ordentliche Aufbewahrung von privaten Schlüsseln kümmern: Der Einsatz von Hardware Security Modules (HSMs) wird explizit erwähnt – damit bestätigt Microsoft die Vermutung von u. a. unserem PKI-Experten Hans-Joachim Knobloch (SSN 8/2023), dass die Schlüssel bisher nicht in HSMs gespeichert wurden.

Die Verlautbarung erinnert an Bill Gates' denkwürdiges Memo vom 15.01.2002, in dem er – aus ähnlichem Anlass – die Trustworthy Computing Initiative ankündigte, die bis heute bei Microsoft umgesetzt wird. Dass das von Gates beschriebene hehre Ziel allerdings in den seither vergangenen Jahr(zehnt)en noch nicht erreicht wurde, wissen wir alle nur zu gut.

Zwar macht Microsoft tatsächlich in der Cloud vieles besser als die meisten IT-Abteilungen in ihren Rechenzentren. Aber auch Microsoft kocht nur mit Wasser. Und wenn einem so großen Cloud-Anbieter Fehler unterlaufen, sind in der Regel auch die Auswirkungen erheblich größer.

By the way: Falls Sie eine eigene PKI betreiben und Ihre Root Keys bisher nicht in HSMs speichern, sollten Sie das besser ändern.

Inhalt

Microsoft ist lernfähig

Security News

Quantencomputing

Besorgniserregend

CVSS runderneuert

Zögern kostet

Umstrittenes Provisorium

Arbeitgeberhaftung

Fast täglich grüßt das Murmeltier

Angst als Schaden

KI plaudert Geheimnisse aus

Better safe than sorry?

Hoffnungslos, aber nicht ernst

Secorvo News

Weiterbildung 2024

Veranstaltungshinweise

secorvo
security consulting

Security News

Quantencomputing

Am 13.11.2023 hat das BSI die schon im August fertiggestellte Version 2.0 der erstmals im Mai 2018 verfassten Studie zum Entwicklungsstand der Quantencomputer veröffentlicht. Auf 217 Seiten bietet sie nicht nur eine hervorragende Übersicht über die aktuellen Fortschritte sondern enthält auch 42 (!) Seiten Literaturreferenzen. Die 14-seitige deutsche Zusammenfassung wurde als separates Dokument publiziert.

Nach dem derzeitigen Stand der Technik erscheint die Faktorisierung eines 2048-bit-RSA-Schlüssels mit 20 Mio. physikalischen QBits in acht Stunden möglich. Davon sind Quantencomputer derzeit weit entfernt: IBMs „Osprey" vom 14.11.2022 hat 433 QBits. Allerdings könnte bereits in zehn Jahren ein ausreichender Quantencomputer verfügbar sein, sofern es gelingt, die Algorithmen zur Korrektur der Quantenfehler deutlich zu verbessern und damit die erforderlichen physikalischen QBits zu reduzieren.

Besorgniserregend

Am 02.11.2023 hat das BSI den Bericht zur Lage der IT-Sicherheit 2023 veröffentlicht. Wem die Lektüre aller 96 Seiten zu zeitintensiv ist, dem sei zumindest das Fazit ans Herz gelegt. Die Bewertung *„Schwachstellen bei Software auf besorgniserregendem Niveau"* belegt die Publikation durch den Verweis auf die 2701 neuen Schwachstellen, die allein im Oktober 2023 veröffentlicht wurden. Das Wiki-Tool Confluence (on premise) war sogar mit zwei Schwachstellen mit maximaler Bewertung (10.0) vertreten (CVE-2023-22515 und CVE-2023-22518).

CVSS runderneuert

Das Common Vulnerability Scoring System (CVSS) ist ein De-facto-Standard zur Bewertung von Produktschwachstellen. Am 01.11.2023 löste die Version CVSS v4.0 des Forums of Incident Response and Security Teams (FIRST) die acht Jahre alte Grundlage CVSS 3 ab. Die neue Fassung legt besonderen Wert darauf, Basis-Bewertungen (Base Metrics) von erweiterten Bewertungen zu trennen und auszuweisen. Der CVSS-Calculator und die FAQ geben Hinweise darauf, wie die Bewertungen zustande kommen; hilfreiche Werkzeuge beim Umgang mit CVEs sind auch CVEDetails und OpenCVE.

Zögern kostet

Laut Arbeitsgericht Duisburg sind Auskunftsersuchen nach Art. 15 DSGVO grundsätzlich unverzüglich, also „ohne schuldhaftes Zögern" zu erteilen. Die Monatsfrist (Art. 12 DSGVO) sei lediglich eine Maximalfrist, die nicht routinemäßig ausgeschöpft werden dürfe, da der Grundsatz sonst leerlaufen würde. Bei unkomplizierten Anfragen, bei denen keine Daten im Unternehmen vorliegen, sei eine Woche als Frist ausreichend. Betroffene würden aufgrund eines temporären Kontrollverlusts einen immateriellen Nachteil erleiden, da sie bis zur Auskunft die Verarbeitung der eigenen Daten nicht prüfen und ggfs. weitere Rechte ausüben könnten. Dem Kläger wurden 750 € Schadenersatz zugesprochen.

Unternehmen sollten daher effiziente Prozesse für die Bearbeitung von Auskunftsersuchen vorsehen – und dabei die EuGH-Rechtsprechung (SSN 5/2023) berücksichtigen, nach der alle personenbezogenen Daten eines Verarbeitungsvorgangs zu beauskunften sind.

Umstrittenes Provisorium

Am 16.11.2023 hat das EU-Parlament die vorläufige Vereinbarung zur Reform der EiDAS-Verordnung veröffentlicht – und damit einen Sturm der Entrüstung ausgelöst. Kritisiert wird insbesondere Art. 45 des Entwurfs, der nach Ansicht einer Vielzahl von Wissenschaftlern und anderen Experten Privatsphäre und Sicherheit der EU-Bürger bei der Nutzung von Webbrowsern in Frage stellt. Kommt es so, wie im Entwurf vorgesehen, dann könnten staatliche Behörden selbst Zertifikate erstellen und damit beliebige Webseiten authentisch erscheinen lassen. In einem offenen Brief fordern über 550 Wissenschaftler, dass durch eine Klarstellung der Trilog-Partner die Regelung entsprechend geändert wird.

Bereits in früheren Entwürfen waren Regelungen zu den kritisierten Qualified Website Authentication Certificates (QWACs) enthalten. Der Kompromissvorschlag des EU-Parlaments berücksichtigte die Kritik, konnte sich aber offenbar in den Trilog-Verhandlungen nicht durchsetzen.

Arbeitgeberhaftung

Der Deutsche Wohnen SE war am 05.11.2019 wegen eines Verstoßes gegen die Löschpflichten der DSGVO ein Bußgeld in Höhe von 14,5 Mio. € auferlegt worden (SSN 11/2019). Nachdem zunächst das LG Berlin den Bußgeldbescheid als unwirksam angesehen hatte (SSN 03/2021), legte die Staatsanwaltschaft Berlin Rechtsmittel ein. Das Kammergericht Berlin legte daraufhin dem EuGH die Frage vor, ob eine juristische Person für von Mitarbeitern begangene DSGVO-Verstöße belangt werden kann. Der EuGH hat am 05.12.2023 entschieden, dass der Arbeitgeber auch für vorsätzlich oder fahrlässig begangene Verstöße von Mitarbeitern haftet.

Fast täglich grüßt das Murmeltier

Inzwischen mehren sich die dringenden verbindlichen Entscheidungen des Europäischen Datenschutzausschuss (EDPB) an die Irische Aufsichtsbehörde DPC (siehe SSN 12/2022 und das Editorial in den SSN 1/2023). Dieses Mal hat die Norwegische Aufsichtsbehörde einen entsprechenden Antrag auf Untersagung der Verarbeitung personenbezogener Benutzerdaten für Verhaltenswerbung im gesamten Europäischen Wirtschaftsraum (EWR) gestellt, da die DPC von sich aus nicht tätig geworden war.

Am 01.11.2023 veröffentlichte der EDPB die am 27.10.2023 angenommene Entscheidung: Meta ist es nunmehr untersagt, verhaltensbezogene Werbung zu verwenden. Die DPC muss innerhalb von zwei Wochen Maßnahmen zur Umsetzung dieser Entscheidung treffen. Die angestrebten effektiveren Regeln zur Durchsetzung der DSGVO bei grenzüberschreitenden Sachverhalten sind ganz offensichtlich dringend erforderlich – auch Studien zum Trotz, die Irland als Vorbild des Datenschutzes in der EU feiern.

Angst als Schaden

Am 26.09.2023 wollte der BGH vom EuGH wissen, ob es für einen immateriellen Schaden ausreichend ist, dass ein DSGVO-Verstoß Ärger, Unmut, Unzufriedenheit, Sorge oder Angst auslöst. Nun hat der EuGH am 14.12.2023 geurteilt, dass es ausreicht, dass eine betroffene Person bei einem Verstoß gegen die DSGVO eine missbräuchliche Verwendung ihrer Daten befürchtet. Art. 82 Abs. 1 DSGVO sei hier (sehr) weit auszulegen. Die Befürchtung muss allerdings im Einzelfall begründet sein.

KI plaudert Geheimnisse aus

Einen kuriosen Angriff, um aus Chatbots Trainingsdaten zu extrahieren, publizierten Forscher am 28.11.2023: Fordert man Chatbots auf, ein Wort endlos oft zu wiederholen, beginnen sie nach einigen Wiederholungen plötzlich damit, Trainingsdaten zu reproduzieren. Ursache für dieses Verhalten ist das Training der Sprachmodelle: Um zu signalisieren, wann ein Dokument in den Trainingsdaten endet, werden Trennsignale eingebaut. Nach dem Training wird der Chatbot einem „Alignment“ unterzogen; dabei wird der Nutzereingabe eine unsichtbare Systemeingabe vorangestellt. Durch die Wiederholung des Trennsignals „lernt“ das Sprachmodell so jedoch, häufige Wiederholungen mit einem Kontextwechsel gleichzusetzen und fängt daher an, unkontrolliert Text auszugeben, der auch Trainingsdaten enthält. Problematisch ist das, wenn mit vertraulichen Daten trainiert wurde.

Better safe than sorry?

Am 05.10.2023 berichtete Bitkom Research, dass der europäische Datenschutz nach einer Umfrage unter 500 deutschen Unternehmen von 69 % als Nachteil im internationalen Wettbewerb und von 56 % als Innovationsbremse gesehen werde. Zu einem ähnlichen Ergebnis kommt die Befragung Global Security Research (fastly) vom November 2023 unter 200 IT-Entscheidern aus Österreich, Deutschland und der Schweiz: Für 55% der Befragten beeinträchtige die IT-Sicherheitsstrategie ihre Innovativität.

Hoffnungslos, aber nicht ernst

Den zweiten „Geburtstag“ von Log4Shell am 10.12.2023 nahm Veracode zum Anlass, die aktuelle Bedrohungslage zu dieser berüchtigten Schwachstelle zu recherchieren – mit erschreckenden Ergebnissen: Insgesamt nutzen noch 38% aller untersuchten Anwendungen eine anfällige Version der Bibliothek, 32% nutzen eine, deren End-of-Life auf August 2015 datiert. Dass nicht nur in diesem Punkt dringend Handlungsbedarf für den Schutz der Software Supply Chain besteht, zeigt die Veracode-Studie State of Software Security vom 05.01.2023: Über 74% der von Veracode im vorangegangenen Jahr untersuchten Anwendungen hatten mindestens eine Schwachstelle, über 56% eine aus den Top 25 CVE. Da wirkt der grundsätzlich korrekte Appell mehrerer Sicherheitsbehörden vom 06.12.2023, auf speichersichere Programmiersprachen zu wechseln, leider realitätsfern. Wer das Problem bei der Wurzel packen möchte, dem empfehlen wir das Seminar T.P.S.S.E. zur sicheren Softwareentwicklung.

Secorvo News

Weiterbildung 2024

In das neue Jahr starten wir mit unserem „Flaggschiff“-Seminar, dem TeleTrusT Information Security Professional (T.I.S.P.) vom **11. bis 15.03.2024**, zu dem Sie nach Eingang Ihrer Anmeldung unser Begleitbuch „Informationssicherheit und Datenschutz“ erhalten.

Im April folgen die Aufbauschulung zum BSI Vorfall-Experten (**09.–11.04.2024**), das Seminar PKI – Grundlagen, Vertiefung, Realisierung (**15.–18.04.2024**) und die Schulung zum TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) (**22.–25.04.2024**).

Unser vollständiges Seminarprogramm und alle Termine 2024 finden Sie auf unseren Webseiten. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2024	
12.-14.01.	Shmoocon 2024 (The Shmoo Group, Washington/US)
22.-24.01.	Omnisecure 2024 (in TIME berlin, Berlin)
30.-31.01.	31. DFN Konferenz Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
Februar 2024	
22.02.	KA-IT-Si-Jahresauftaktevent: „HackGPT“ (KA-IT-Si, Karlsruhe)
März 2024	
05.-07.03.	secIT 2024 (Heise Medien, Hannover)
11.-15.03.	TeleTrusT Information Security Professional (T.I.S.P.) (Secorvo, Karlsruhe)
19.-22.03.	DFRWS EU 2024 (DFRWS, Zaragoza/ES)
April 2024	
09.-11.04.	BSI Vorfall-Experte – Aufbauschulung (Secorvo, Karlsruhe)
15.-18.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.04.	Blackhat Asia 2024 (Blackhat, Singapur/SG)
22.-25.04.	TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) (Secorvo, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Paul Blenderman (Editorial), Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, 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