Secorvo Security News

August 2023

Wayback Machine

Sie erinnern sich zweifellos: Es war ein Monat weltbewegender Ereignisse. Bundesverteidigungsminister Rudolf Scharping wurde von Gerhard Schröder entlassen, die Bahn eröffnete die Schnelltrasse Frankfurt-Köln und MCI WorldCom geriet in die Insolvenz. Michael Schuhmacher wurde zum fünften Mal (und vorzeitig) Formel-1-Weltmeister, Serena Williams gewann Wimbledon vor ihrer Schwester und die deutsche Fußballnationalmannschaft musste im Finale der Weltmeisterschaft Brasilien den Vortritt lassen. Chang Sang wurde erste weibliche Premierministerin in Südkorea und George Bush errichtete als Reaktion auf die Terroranschläge von 9/11 ein Ministerium für „Homeland Security".

Sie ahnen es: Es geht um den Juli 2002, den Monat, in dem die erste Ausgabe der Secorvo Security News das Licht der Welt erblickte. Seitdem schlägt sie Monat für Monat eine „Schneise in die Informationsflut", wie wir es uns in der Erstausgabe vor 21 Jahren vorgenommen haben. Inzwischen sind exakt 250 Ausgaben erschienen – mit einem Umfang von je vier Seiten, einem Editorial, relevanten Nachrichten zu IT-Security und Datenschutz aus dem vorausgegangenen Monat und aktuellen Terminhinweisen.

1000 Seiten „SSN" sind so zusammengekommen, die wir Ihnen zur Feier dieses Jubiläums in einem „Großen Buch der Security News" zum Download zusammengefasst haben. Eine (gar nicht so kurze) Geschichte der IT-Sicherheit, gespickt mit zahlreichen Déjà-vus. Da mischt sich das eine oder andere Schmunzeln in die Erinnerung – aber auch die ernüchternde Einsicht, wie häufig Fehler wiederholt werden und wie selten aus der Geschichte gelernt wird.

Wir freuen uns auf viele weitere Ausgaben der Security News, in denen wir die weitere Entwicklung der IT-Sicherheit und des Datenschutzes begleiten werden. Und über ein Feedback von Ihnen – und natürlich Ihre begeisterte Weiterempfehlung.

Security News

Verlorener Generalschlüssel

Den am 11.07.2023 von Microsoft veröffentlichten Angriff auf Office-365-Instanzen von mindestens 25 Unternehmen durch eine chinesische Hackergruppe hatte nicht Microsoft, sondern eine amerikanische Bundesbehörde entdeckt. Seit dem 15.05.2023 besaßen die Hacker einen gültigen Signierschlüssel für Authentifikationstoken der Azure-Cloud – einen Generalschlüssel, den Microsoft offenbar nicht in einer geschützten Hardware, sondern auf einem Rechner gespeichert hatte. Bei einem Systemabsturz war er bereits im April 2021 (!) im Snapshot eines Crash-Dumps gelandet – der in das „Debugging Environment" verschoben worden war. Dort konnten die Hacker über

den Account eines Mitarbeiters eindringen und den Crash Dump analysieren – so die Ergebnisse der am 06.09.2023 veröffentlichten Untersuchung von Microsoft.

Die – teilweise pikanten – technischen Details des Angriffs hat Hans-Joachim Knobloch (Secorvo) analysiert und in der iX 9/2023 beschrieben.

Wir lernen daraus: Bei Azure ist es keinesfalls selbstverständlich, dass die Generalschlüssel in Hardware Security Modules liegen – bei PKIs ist das normalerweise der Standard. Generalschlüssel, die nicht mehr benötigt werden, werden bei Microsoft auch nicht unverzüglich gesperrt; stattdessen können sie in Crash Dumps auftauchen. Und auf die haben Angreifer Zugriff, die sich anscheinend ungestört im Entwicklernetz von Microsoft tummeln.

Zum Glück ist Cloud Computing sicher.

Gefährliche Altlasten

Mehrere englischsprachige Cybersecurity Agencies haben am 03.08.2023 ein gemeinsames Cybersecurity Advisory (2022 Top Routinely Exploited Vulnerabilities) veröffentlicht, in dem sie vor im Jahr 2022 besonders häufig von Angreifern genutzten Schwachstellen warnen. Allein von den 12 kritischsten CVEs stammen eines aus dem Juni 2019 und sechs weitere aus dem Jahr 2021. Offenbar ist noch immer bei zahlreichen Behörden und Unternehmen ein systematisches Patch-Management keine Selbstverständlichkeit.

Backdoor Browserweiterung

Ein wichtiger Schritt zur Verringerung des Angriffsrisikos war vor einigen Jahren, Windows-Benutzern die lokalen Administrationsrechte zu entziehen, damit sie nicht mehr alles installieren können, was im Internet glänzt. Daher bieten inzwischen Softwarehersteller (und Angreifer) vermehrt Installationen im Benutzerkontext an.

Das betrifft auch Chrome- und Edge-Extensions sowie Firefox-Add-ons. Zwar verhindert Firefox seit Jahren die Ausführung von bekannt problematischen Erweiterungen – die Sperrliste hat bereits eine beachtliche Länge. Und Google kündigte am 16.08.2023 an, Chrome-Anwender zumindest vor solchen Erweiterungen zu warnen. Entfernen oder wenigstens abschalten müssen die Nutzer sie allerdings selbst. Vor allem aber kann man bei allen drei Browsern per Policy festlegen, welche Erweiterungen Anwender installieren dürfen. Das zentrale Management von zulässigen Erweiterungen ist inzwischen ebenso zu empfehlen wie der noch immer wichtige Entzug der lokalen Administrationsrechte.

Excel Disclosure

Täglich tauschen Organisationen untereinander Millionen Excel-Dateien aus. Doch das Dateiformat ist tückisch: So können ausgeblendete oder schlicht übersehene Kommentare, Spalten, Zeilen oder ganze Arbeitsblätter enthalten sein: Die Berechnung im Angebot könnte die Marge, ein Kommentar im Vertragstext den vorhandenen Spielraum verraten. Das BSI widmete diesem Problem im Februar 2020 sogar

einen eigenen Grundschutz-Baustein. Besonders heikel wird es, wenn Excel- (oder andere Office-) Dateien veröffentlicht werden. Diese Aufgabe sollte man daher geschulten Mitarbeitern übertragen.

Bei der Polizei von Nordirland scheint das noch nicht angekommen zu sein: Am 08.08.2023 beantwortete eine Nachwuchskraft eine Anfrage nach dem Informationsfreiheitsgesetz mit einer Datei, die außer den angefragten Daten auch Nachname und Initialen, Position, Rang, Standort und Abteilung sämtlicher Mitarbeiter enthielt. Brisante Daten in einem Land, in dem vor allem katholische Polizisten um ihre Sicherheit bangen müssen. Die Datei war zwar nur drei Stunden abrufbar, hat aber in dieser Zeit den Weg in die Welt gefunden. Nun verfolgt die irische Polizei Einzelpersonen, die im Besitz einer Kopie der Datei sind – ein eher aussichtsloses Unterfangen.

Vor solchen unerwünschten Preisgaben bewahren geeignete DLP-Verfahren und -Systeme, oder die Verwendung des weniger verfänglichen PDF-Formats.

Verschlüsselte Backups

Der kleine dänische Webhoster CloudNordic wurde am 18.08.2023 Opfer eines Ransomware-Angriffs, bei dem auch die Backups verschlüsselt wurden. Daraufhin erklärte man den Kunden auf einer provisorischen Homepage: *Leider hat es sich als unmöglich erwiesen, weitere Daten wiederherzustellen, und die meisten unserer Kunden haben alle Daten bei uns verloren.* Es folgt noch der Hinweis, der Kunde könne, sofern er kein eigenes lokales Backup habe, seine Webseiteninhalte möglicherweise der Wayback Machine entnehmen.

Dort findet man übrigens auch die Version der CloudNordic-Webseite vom Juni 2023, auf der der Hoster erklärt, alle Grundsätze der ISO 27001 zu befolgen und sich auf eine Zertifizierung vorzubereiten. Angeblich waren auch Maßnahmen ergriffen worden, die verhinderten, dass Angreifer von der Produktionsumgebung auf Management- oder Backupsysteme zugreifen konnten – wegen eines Umzugs waren sie jedoch vorübergehend deaktiviert worden. Eine Gelegenheit, auf die die Angreifer offenbar gewartet haben.

Und die Moral? Glauben Sie nicht blind den Sicherheitsversprechen Ihrer Dienstleister – denn auch Profis können mal schwächeln. Ein eigenes Backup ist daher eine gute Idee: Better safe than sorry.

NIST CSF 2.0

Am 08.08.2023 hat das NIST das Cybersecurity Framework (CSF) 2.0 als Initial Public Draft veröffentlicht. Zur Diskussion stehen neue Versionen des Frameworks selbst sowie des Framework Cores. Wie in der Vorversion 1.1 beschäftigt sich das erste Dokument mit der Anwendung, das zweite beschreibt Anforderungen mit Umsetzungsbeispielen.

In der neuen Version wurden die Bezüge des CSF zu anderen NIST-Standards mit ihren eigenen Sichten auf die Informationssicherheit in das Cybersecurity and Privacy Reference Tool ausgelagert. Zudem wird der Anwendungsbereich von Unternehmen der kritischen

Infrastrukturen auf alle Unternehmen ausgeweitet. Bei den Anforderungen finden sich – ähnlich wie in der neuen Version der ISO 27002 – einige Reorganisationen und Umstrukturierungen.

Die vielleicht wichtigste Neuerung ist, dass mit „Governance" eine alle Phasen des Entwicklungszyklus umfassende Schicht mit eigenen Anforderungen hinzugekommen ist.

Der DSA kommt

Ab dem 17.02.2024 müssen Anbieter digitaler Dienste den Anforderungen des Digital Services Act (DSA) genügen (SSN 05/2022). Dazu zählen, dass illegale Inhalte unverzüglich zu löschen und Nudging und Dark Pattern verboten sind. Auch die Nutzung von Werbeprofilen, die auf besonderen Kategorien personenbezogener Daten (wie der sexuellen Orientierung, politischen Überzeugung oder der ethnischen Herkunft) beruhen, ist unzulässig. Zum Erhalt des Prinzips der freien Rede darf kein allgemeines Content Monitoring betrieben werden. Am 25.04. 2023 hatte die EU-Kommission 19 sehr große Plattformen und Suchmaschinen (sog. VLOPs) festgelegt, die die Regelungen bereits seit Ende August erfüllen müssen.

Verstöße gegen Bestimmungen des DSA haben empfindliche Bußgelder zur Folge – sie können bis zu 6% des weltweiten Jahresumsatzes betragen. Die EU hat am 25.04.2032 eine „Questions & Answers"-Seite zum DSA bereitgestellt, die die Umstellung unterstützen soll.

Secorvo News

Secorvo Seminare

Im Oktober starten unsere Seminare in die goldene Herbstsaison. Mit der Teilnahme am Seminar „BSI-Vorfall-Experte – Aufbauschulung" vom **17.–19.10.2023** erfüllen Sie eine wesentliche Voraussetzung für die entsprechende BSI-Zertifizierung zum Vorfall-Experten. Oder Sie sichern sich noch einen der wenigen freien Plätze im letzten T.I.S.P.-Seminar des Jahres vom **13.–17.11.2023**: Krönen Sie Ihre Kenntnisse in der Informationssicherheit mit einem anerkannten Zertifikat und werden Sie Teil der engagierten „T.I.S.P.-Community".

Das inhaltlich gründlich überarbeitete und didaktisch neu konzipierte T.P.S.S.E.-Seminar startet **vom 27. bis 30.11.2023** in die erste Runde. Für Software-Entwickler definitiv ein „Must-have" – gelebte Informationssicherheit. Profitieren Sie vom Frühbucherrabatt. Wir freuen uns auf Ihre Anmeldung!

Authenticate. Generate. Repeat.

Das nächste KA-IT-Si-Event widmet sich dem Einsatz von PKIs in der Industrie. Tamás Horváth von Nexus wird einen Überblick über IoT-typische Bedrohungen und die entsprechenden Sicherheitsziele geben. Gemeinsam mit der Firma STIHL wird er am Beispiel des internetfähigen Mähroboters iMow zeigen, wie die Provisionierung digitaler Identitäten mit Hilfe einer autonomen Factory CA gelingt. Im Anschluss an den

Vortrag haben Sie wie immer Gelegenheit zum intensiven Buffet-Networking.

Wir freuen uns auf Sie am **14.09.2023** um 18 Uhr in den Räumen der IHK Karlsruhe (Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2023	
11.-13.09.	heise devSec 2023 (dpunkt.verlag, heise, Karlsruhe)
14.09.	Authenticate. Generate. Repeat. (KA-IT-Si, Karlsruhe)
27.-29.09.	Informatik 2023 (GI, Hamburg)
28.09.	IT-Sicherheitsrechtstag 2023 (Swiss Cyber Storm Association, Bern/CH)
Oktober 2023	
10.-12.10.	it-sa 2023 (NürnbergMesse GmbH, Nürnberg)
12.10.	Ransomware as a Service (KA-IT-Si, Karlsruhe)
17.-19.10.	BSI Vorfall-Experte – Aufbauschulung (Secorvo, Karlsruhe)
24.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
November 2023	
07.-09.11.	IDACON 2023 (WEKA-Akademie, München)
08.-09.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
13.-17.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
26.-30.11.	ACM CCS 2023 (ACM/SIGSAC, Copenhagen/DNK)
27.-30.11.	T.P.S.S.E. (TeleTrusT Professional for Secure Software Engineering) (Secorvo, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Dirk Fox (Editorial), Christian Blaicher, Paul Blendermann, Robert Eitel, Stefan Gora, 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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.