secorvo
security consulting

Secorvo Security News

September 2024

Fantastilliarden an Schäden

Der deutsche IT-Branchenverband bitkom hat am 24.08.2024 die Ergebnisse seiner jährlichen Studie „Wirtschaftsschutz 2024“ veröffentlicht. Danach verursachte Cyberkriminalität im Vorjahr einen Schaden von 266,6 Milliarden Euro – über sechs Prozent des Bruttoinlandsprodukts 2023, fast das Vierfache des Verteidigungsetats und etwa 70 % der Summe, die die Weltbank 2023 für den Wiederaufbau der Ukraine veranschlagt hat.

Auf dem KA-IT-Si-Event „Was ko$tet die Welt?“ am 20.06.2024 haben Wiebke Reimer und Dr. Boris Hemkemeier von der Commerzbank AG gezeigt, woher die oft zitierten 5,5 Billionen Euro an weltweiten Schäden durch Cyberkriminalität pro Jahr stammen: Am Ende einer Kette von Zitaten stießen sie auf eine falsch interpretierte Schätzung des Weltwirtschaftsforums (WEF) aus dem Jahr 2014. Diese besagte lediglich, dass Cyber-Regulierung und Vorsicht der Verbraucher bis 2020 die *wirtschaftliche Nutzung innovativer Technologien* im schlimmsten Fall um drei Billionen US$ reduzieren könnten.

Die Zahlen der bitkom-Studie basieren auf einer telefonischen Befragung von Führungskräften in 1003 Unternehmen. Wie belastbar sind solche Antworten? Wie quantifiziert man beispielsweise einen Imageschaden? Offen ist auch, ob die befragten Unternehmen repräsentativ für die Gesamtwirtschaft sind. Methodisch ist es jedenfalls fragwürdig, Aussagen zu seltenen extremen Ereignissen auf die Gesamtheit der Unternehmen hochzurechnen.

Forscher von Microsoft haben bereits 2016 darauf hingewiesen, dass Umfragen ungeeignet sind, um den Gesamtschaden durch Cyberkriminalität zu ermitteln. Trotzdem werden solche Zahlen von Medien, Politik und Wirtschaft zitiert und als Grundlage für Entscheidungen herangezogen.

Warum nimmt daran niemand Anstoß?

Inhalt

secorvo
security consulting

Security News

Totgesagte leben länger

Ein Team von watchTowr beschrieb am 11.09.2024, wie es bei GlobalSign ein gültiges Zertifikat für die Microsoft-Domäne microsoft.mobi beantragen konnte. Zunächst hatte es regulär die Domäne dotmobiregistry.net erworben und darauf einen eigenen WHOIS-Server aufgesetzt. Die WHOIS-Server für die Top Level Domain „.mobi" waren zuvor von dieser Domäne zu whois.nic.mobi umgezogen – und die alte Domäne freigegeben worden. Für die Domain-Validierung des Zertifikatsantrags von watchTowr fragte GlobalSign die administrative E-Mail-Adresse des Domaininhabers jedoch noch bei der veralteten WHOIS-Adresse ab – die inzwischen watchTowr gehörte.

Nicht selten werden alte Domänen aufgegeben, ohne dass alle Dienstnutzer verlässlich darüber informiert wurden. Im Fall von dotmobiregistry.net war das verheerend, weil sicherheitskritische Funktionen darüber abgewickelt wurden. Vor der Freigabe einer nicht mehr benötigten Domain sollten kritische Dienste noch eine Weile weiter betreiben werden, bis wirklich sichergestellt ist, dass kein Dienstnutzer mehr darauf zugreift.

Kündigungsgrund Datenschutz

Dass ein Verstoß eines Arbeitnehmers gegen die DSGVO auch ein Kündigungsgrund sein kann, überrascht nicht. Das OLG München hat am 31.07.2024 festgestellt, dass ein Unternehmensvorstand mit der Weiterleitung von vertraulichen Unterlagen, die auch personenbezogene Daten beinhalteten, gegen die DSGVO verstößt. Selbst wenn die Vertraulichkeitspflichten aus § 93 Abs. 1 AktG nicht verletzt sind, kann die Übermittlung von personenbezogenen Daten sogar eine außerordentliche Kündigung rechtfertigen, falls dies einen „wichtigen Grund" (§ 626 Abs. 1 BGB) darstellt – sofern die Interessen beider Seiten gegeneinander abgewogen wurden. Die Grundsätze dieser Abwägung sind in der Bienenstich-Entscheidung des BAG festgelegt: Es müssen u. a. die Schwere der Pflichtverletzung, der Grad des Verschuldens, das Ausmaß des Schadens, die mögliche Wiederholungsgefahr, die Dauer des Arbeitsverhältnisses und dessen störungsfreier Verlauf sowie die sozialen Folgen für den Arbeitnehmer berücksichtigt werden.

Never change…

… a good password: Seit 2017 empfiehlt das NIST in seinen Vorgaben für „Authentication and Lifecycle Management" (SP 800-63B), dass weder regelmäßige Passwortwechsel noch sogenannte Komplexitätsvorgaben erzwungen werden sollten. Im ersten Entwurf der Neufassung vom Dezember 2022 wurde aus einer Unterlassens-Empfehlung ein Verbot („SHOULD NOT" wurde zu „SHALL NOT"). Die Verschärfung hat – wie der am 21.08.2024 veröffentlichte zweite Public Draft zeigt – die erste Kommentierungsphase überlebt, und es ist zu erwarten, dass das auch für die letzte Phase gilt, die am 07.10.2024 endet. Authentifizierungsdaten, die sich ein Mensch merken soll, müssen so gewählt werden, dass ein Mensch sie sich auch merken kann, ohne dass das Sicherheitsniveau dadurch sinkt. Weder erzwungene Wechsel noch feste Komplexitätsregeln genügen dieser Anforderung. Hingegen können längere Passwörter helfen – ein Thema, dass uns seit vielen Jahren beschäftigt (siehe SSN 06/2009, 06/2010, 02/2011, 05/2015 und 08/2015).

ECDSA-Seitenkanal

Am 03.09.2024 enthüllten französische Sicherheitsforscher eine Seitenkanal-Schwachstelle in der Krypto-Bibliothek für die Sicherheitschips von Infineon unter dem Namen EUCLEAK – einem Wortspiel aus „Euclid" und „Leak". Der Seitenkanal bezieht sich auf das Timing im erweiterten euklidischen Algorithmus, der bei einer ECDSA-Signatur das modulare Inverse der Nonce berechnet, die den privaten Schlüssel verschleiert. Die Nonce war schon mehrfach ein Schwachpunkt bei Angriffen auf DSA-/ECDSA-Implementierungen. Der EUCLEAK-Entdecker brach bereits 2021 auf ähnlichem Weg die ECDSA-Implementierung in Google Titan FIDO-Keys, wenn auch mit weniger medialer Aufmerksamkeit.

Die Schwachstelle wirkte sich auch auf FIDO-Token von Yubico aus, die zeitgleich ein Security-Advisory dazu veröffentlichten. Daher wurde der Angriff in der Presse auch als „YubiKey-Schwachstelle" beschrieben, obwohl auch andere Produkte (Smartcards, TPMs, FIDO-Token und Bitcoin-Wallets) angreifbar sind, die Infineon-Chips und deren Bibliothek verwenden. Seit der Veröffentlichung äußerten sich fast nur Hersteller, deren Produkte nicht betroffen sind – bei anderen ist daher eine gewisse Skepsis angebracht,

Der Angriff erfolgt mit einer Magnetfeld-Sonde, die weniger als 1 mm vom Chip entfernt platziert wird. Dafür muss beim YubiKey das Gehäuse geöffnet oder angebohrt werden. Da FIDO-Token vor allem vor Remote-Angriffen schützen sollen, ist die Gefahr begrenzt; die offizielle CVSS-Bewertung liegt deshalb auch nur bei 4.2. Wer besonders kritische ECDSA-Schlüssel verwendet, sollte dennoch handeln: YubiKeys und YubiHSMs müssen ersetzt werden, da Yubico keine Firmware-Updates erlaubt, um Angriffe über Updates auszuschließen.

Am 06.09.2024 stellten Google-Forscher auf der CHES-Konferenz ein System vor, das per Machine Learning automatisch Power-Seitenkanäle sucht und Entwicklern hilft, ihre HSMs dagegen zu härten. Auch da diente die ECDSA-Nonce als Beispiel.

Unternehmenserwerb

Die Datenschutzkonferenz (DSK) hat am 11.09.2024 die Übermittlung personenbezogener Daten vor Abschluss eines Asset Deals ohne eine Einwilligung der Betroffenen für unzulässig erklärt. Bei fortgeschrittenen Verhandlungen könne ein berechtigtes Interesse die Übermittlung bestimmter Daten rechtfertigen: So sei die Übermittlung von Kundendaten erlaubt, wenn der Veräußerer feststellt, dass die Interessen der Kunden nicht überwiegen; sie müssen jedoch über die Datenübermittlung informiert werden.

Die Übermittlung von Beschäftigtendaten ist in der Regel zulässig, wenn sie zur Erfüllung des Arbeitsvertrags durch den Käufer notwendig wird. Besondere personenbezogene Daten dürfen allerdings nur mit ausdrücklicher Einwilligung übermittelt werden.

Illegale Datenverarbeitungen

Die niederländische Datenschutzbehörde verhängte am 29.08.2024 ein Bußgeld von 290 Mio. € gegen Uber, weil das Unternehmen nach Außerkraftsetzung des Privacy Shield durch den EuGH am 17.07.2020 (SSN 7/2020) weiter personenbezogene Daten in die USA übermittelt hatte – ohne angemessene Garantien für den Schutz dieser Daten. Erst seit dem 27.11.2023 zählt Uber Technologies Inc. zu den nach dem Data Privacy Framework zertifizierten US-Unternehmen.

Ein weiteres Bußgeld über 30,5 Mio. € verhängte die Behörde am 03.09.2024 gegen Clearview AI: Das Unternehmen speichert rechtswidrig in einer Datenbank mehr als 30 Milliarden Fotos von Personen und erzeugt für jedes Foto einen einzigartigen biometrischen Code (Editorial SSN 1/2020). Die abgebildeten Personen haben nicht in die Verarbeitung eingewilligt und nicht einmal Kenntnis von der Speicherung.

Clearview AI hat keinen Sitz in Europa; dennoch müssen die nationalen Datenschutzbehörden Rechtsverletzungen gegen EU-Bürger in ihrem Zuständigkeitsbereich verfolgen. Die Datenschutzbehörden von Frankreich, Italien und Griechenland haben bereits Bußgelder in Höhe von je 20 Mio. € und Großbritannien in Höhe von 7,5 Mio. Pfund verhängt (SSN 10/2022), weil das Unternehmen wiederholten Löschaufforderungen nicht nachgekommen ist. Eine Vollstreckung der Bußgeldbescheide ist zwar (bisher) nicht möglich – aber das Signal deutlich: Europa ist keine rechtsfreie Spielwiese für amerikanische Unternehmen.

Secorvo News

Secorvo Seminare

Vom **04. bis 07.11.2024** bietet Ihnen das PKI-Seminar tiefe Einblicke in Public Key Infrastrukturen: Von den Grundlagen bis zu Planung und Betrieb Ihrer eigenen PKI. Auf unserem T.I.S.P.-Seminar vom **11. bis 15.11.2024** bereiten wir Sie in über 20 Modulen auf die anschließende Zertifikatsprüfung vor; die 4. Auflage des T.I.S.P.-Begleitbuches erhalten Sie nach Ihrer Anmeldung.

Wer lernen möchte, wie sich die Software-Entwicklung sicher(er) gestalten lässt, dem bietet unser T.P.S.S.E.-Seminar vom **25. bis 28.11.2024** ein praxisbezogenes Training mit interaktiven Workshops – und im Anschluss auch hier die Möglichkeit, sich zertifizieren zu lassen.

Werfen Sie auch gerne schonmal einen Blick in unseren Seminarkalender 2025. Wir freuen uns auf Ihre Anmeldung!

Wer hat, der kann.

Immer mehr Anwendungen verlangen eine Anmeldung, und oft sind sie ohne einen Zugriff auf andere Dienste nicht sinnvoll nutzbar. Deshalb ist moderne Authentifizierung mit OAuth-Tokens längst ein wichtiges Thema. Wer sich damit beschäftigt merkt jedoch schnell, dass es bei der technischen Umsetzung einige Hürden und Fallstricke gibt. Diese variieren je nach System, das zur Ausstellung der OAuth-Tokens verwendet wird.

Beim **KA-IT-Si-Event** im dm-dialogicum geben Eberhard Ratzel und Moritz Gabriel (dmTECH) am **17.10.2024** einen Überblick über ihre Erfahrungen und Erkenntnisse bei der Nutzung von Microsoft Entra ID zur Erstellung von OAuth-Tokens. Im Anschluss haben Sie wieder Gelegenheit zum fachlichen und persönlichen Austausch am Buffet. Hier geht's zur Anmeldung. Wir freuen uns auf Sie!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Oktober 2024	
14.-18.10.	ACM CSS 2024 (ACM SIGSAC, Salt Lake City/US)
17.10.	KA-IT-Si-Event "Wer hat, der kann." (KA-IT-Si, Karlsruhe)
22.10.	Swiss Cyber Storm 2024 (Swiss Cyber Storm, Bern/CH)
22.-24.10.	it-sa 2024 (itsa 365, Nürnberg)
November 2024	
04.-07.11.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
05.-06.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
05.-07.11.	24. IDACON 2024 (WEKA Akademie, München)
08.11.	DORA, NIS2 und CRA als Wegweiser für Informationssicherheit (GI, Frankfurt/Main)
11.-15.11.	T.I.S.P. (TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
20.-21.11.	ICSP 2024 (NIT, Jamshedpur/IND)
25.-28.11.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Dezember 2024	
09.-13.12.	Asiacrypt 2024 (IACR, Kolkata/IND)
09.-12.12.	Black Hat Europe 2024 (Black Hat, London/UK)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Ion Barza, Paul Blenderman (Editorial), Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

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