secorvo
security consulting

Secorvo Security News

Januar 2023

Datenparadies Irland

Gegen die europäischen Niederlassungen mehrerer Meta-Unternehmen hatte Max Schrems' Initiative noyb wegen Umgehung der Einwilligungspflicht bei personalisierter Werbung sowie mangelnder Transparenz bei verschiedenen europäischen Aufsichtsbehörden mehrere Datenschutz-Beschwerden eingereicht – pünktlich zum Inkrafttreten der DSGVO am 25.05.2018.

Angelockt von niedrigen Steuern haben viele amerikanische „Big Tech"-Konzerne wie Microsoft, Meta, Google oder Apple ihre europäische Hauptniederlassung in Irland. In Datenschutzfragen ist damit die irische Datenschutzbehörde DPC zuständig.

Jahrelang verschleppte die DPC die Entscheidungen über die Beschwerden. Zunächst hatte die DPC sogar versucht, eine Leitlinie des Europäischen Datenschutzausschusses (EDSA) zu beeinflussen, um die Umgehung der Einwilligung durch Meta zu legitimieren. In einem ersten Entscheidungsentwurf vom 06.10.2021 ging die DPC nur auf die Transparenzverstöße ein, ließ das Vertragsmodell unberücksichtigt und empfahl ein Bußgeld von 28 bis 36 Mio. €. Nach Einsprüchen mehrerer europäischer Aufsichtsbehörden hob der EDSA am 05.12.2022 die vorläufigen Bußgeldbescheide der DPC gegen Facebook über 17 Mio. € (15.03.2022) und Instagram über 265 Mio. € (28.11.2022) auf und erhöhte die Bußgelder von Facebook, Instagram und WhatsApp auf insgesamt 390 Mio. € (SSN 12/2022).

Keine europäische Aufsichtsbehörde stellte sich dabei auf die Seite der DPC. Die Ankündigung der DPC, gegen den verbindlichen Beschluss des EDSA vorzugehen, spricht Bände. Dabei ist die DPC trotz eines Jahresbudgets von 19 Mio. € die Aufsichtsbehörde Europas mit den mit Abstand meisten unerledigten Fällen: Von 164 Beschwerden mit europaweiter Bedeutung wurden erst vier erledigt, wie ein Bericht des Irish Council for Civil Liberties vom 13.04.2022 aufzeigt. Die Geduld des EDSA ist nun hoffentlich zu Ende.

Inhalt

secorvo
security consulting

Security News

Detailfrage

Mit seinem Urteil vom 12.01.2023 hat der EuGH auf ein Vorabentscheidungsersuchen des Obersten Gerichtshofs Österreichs eine wichtige Auslegung des Art. 15 Abs. 1 lit. c DSGVO (Datenschutz-Auskunftsersuchen) geklärt: Danach muss der Verantwortliche (im vorliegenden Fall die Österreichische Post AG) die Identität der (Daten-) Empfänger so konkret wie möglich benennen, um dem Transparenzgrundsatz zu genügen und dem Betroffenen eine weitere Rechtsausübung überhaupt erst zu ermöglichen. Ist dem Verantwortlichen dies (noch) nicht möglich, darf er sich darauf beschränken die Kategorien der betreffenden Empfänger mitzuteilen.

Eine Auskunft kann verweigert werden, wenn ein Antrag offenkundig unbegründet oder exzessiv ist; das muss der Verantwortliche jedoch nachweisen.

iCloud-Verschlüsselung

Apple hat am 23.01.2023 auch in Deutschland die Möglichkeit freigeschaltet, unter iOS 16.2 und macOS 13.1 den erweiterten Datenschutz zu aktivieren. Damit lassen sich fast alle Daten in der iCloud Ende-zu-Ende verschlüsseln. Die Funktion muss vom Nutzer ausgewählt werden.

Die US-Bundespolizei FBI kritisiert die Ende-zu-Ende Verschlüsselung; im Rahmen von Ermittlungen bekommt sie nun nur noch eingeschränkten Zugriff auf die Daten in der iCloud. Gemäß Apples jüngstem Transparenzbericht von 2021 wurden in fast 4000 Fällen iCloud-Daten an Behörden herausgegeben – darunter auch iCloud Backups.

iCloud Mail, Kalender und Kontakte sowie zahlreiche Metadaten wie Dateinamen, Checksummen und Safari-Lesezeichen werden allerdings weiterhin nicht Ende-zu-Ende verschlüsselt. Die Lösung hat daher noch Luft nach oben.

NIS2

Am 14.12.2022 wurde die so genannte NIS2-Richtlinie über „Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union“ (EU 2022/2555) im EU-Amtsblatt veröffentlicht. Ziel der Richtlinie ist ein einheitlicheres Niveau der IT-Sicherheit kritischer Infrastrukturen innerhalb der EU. Sie muss bis Oktober 2024 in nationales Recht umgesetzt werden. In Deutschland ist vieles bereits im IT-Sicherheitsgesetz 2.0 geregelt (siehe SSN 5/2021).

Die Richtlinie gilt für Unternehmen in kritischen Infrastrukturen mit mindestens 50 Mitarbeitern und 10 Mio. € Umsatz. Teile der digitalen Infrastruktur und der öffentlichen Verwaltung sollen unabhängig von der Größe reguliert werden. Die Unternehmen müssen „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen“ nach dem „Stand der Technik“ ergreifen, die sie nach einer „systemischen Analyse“ festlegen. Zuständig für die Umsetzung der Maßnahmen ist die Geschäftsführung. Die getroffenen Maßnahmen sind systematisch mit Hilfe eines implementierten Risikomanagementsystems zu dokumentieren.

Bei Verstößen können Bußgelder verhängt werden, deren Höhe an die der DSGVO angelehnt wurde: bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes bei wesentlichen und 7 Mio. € bzw. 1,4 % des Jahresumsatzes bei wichtigen Einrichtungen. Das kann teuer werden, da im schlimmsten Fall auch noch ein Bußgeld wegen Verstoßes gegen die DSGVO hinzukommen kann.

Verbannt

Am 25.11.2022 machte die US-Regierung ernst: In einer aktualisierten Auslegung des Secure Equipment Act vom 11.11.2021 (H.R.3919) verbot sie die Zulassung von chinesischen Telekommunikations- und Videoüberwachungseinrichtungen, da sie eine Gefahr für die nationale Sicherheit darstellten. Damit dürfen Komponenten von Huawai, ZTE und anderen chinesischen Herstellern zukünftig nicht mehr in Mobilfunkeinrichtungen oder Routern verbaut werden; auch Smartphones könnten betroffen sein.

Zwar gilt auch diese Regelung nicht ohne Ausnahmen und spielten sicher auch wirtschaftliche Interessen bei der Entscheidung eine Rolle. Doch macht sie deutlich, dass die USA die Gefahr einer technischen „Unterwanderung“ der IT-Infrastrukturen ernst nimmt. Anders als die Bundesregierung, die von einer entsprechenden Regelung in § 9b IT-Sicherheitsgesetz bisher keinen Gebrauch macht.

Teure Wahlkampfhilfe

Am 22.12.2022 stimmte Meta einem Vergleich zu: Der Konzern zahlt 725 Mio. US$ an Betroffene für die rechtswidrige Weitergabe der Daten von 87 Mio. Facebook-Nutzern an Cambridge Analytica. Das Unternehmen hatte die Daten 2016 im Wahlkampf von Donald Trump und für die britische Brexit-Kampagne genutzt. Nach Bekanntwerden des Skandals musste Cambridge Analytica am 02.05.2018 Insolvenz anmelden (siehe SSN 4+5/2018). Im Juli 2019 hatte Facebook bereits ein Bußgeld der US-Verbraucherschutzbehörde in Höhe von 5 Mrd. US$ akzeptiert. 660 € pro Datensatz – ein teurer Spaß für die Aktionäre. Auch in diesem Sinne kann sich Datenschutz auszahlen.

IT-Grundschutz-Kompendium

Am 01.02.2023 hat das BSI die Edition 2023 des IT-Grundschutz-Kompendiums vorgestellt. In der aktuellen Version finden sich 10 neue Bausteine, darunter ein Baustein zum allgemeinen IT-Betrieb, dem nun versionsunabhängigen Baustein „Windows Server“ sowie die vollständige Überarbeitung der Bausteine zur Nutzung und dem Anbieten von Outsourcing. Bei 21 Bausteinen gab es Änderungen, die das BSI in einem eigenen Dokument zusammengefasst hat. Das Kompendium steht in den Formaten PDF und XML zur Verfügung.

Für alle Unternehmen und Einrichtungen, die sich nach IT-Grundschutz zertifizieren lassen, sind ab dem 01.02.2023 die Versionen 2022 und 2023 verbindlich. Aber auch für alle anderen Unternehmen bietet das Kompendium gute Anregungen für die Implementierung von Maßnahmen der Informationssicherheit.

Cookie-Chaos

Cookie-Banner sind ein Ärgernis für Webseitenbesucher, Datenschützer und Webseitenbetreiber – wenn auch aus jeweils anderen Gründen. Zwar sind die gesetzlichen Anforderungen klar: Wer personenbezogene Daten ohne Vertrag oder andere gesetzliche Grundlage verarbeiten möchte (hier: Tracking von Webseitenbesuchern) benötigt eine Einwilligung der Betroffenen.

Wie aber ist eine solche Einwilligung auf einer Webseite rechtskonform zu gestalten? Da gehen die Auffassungen schon seit vielen Jahren (siehe z. B. SSN 2/2015) erheblich auseinander. Am 14.03.2022 hatte sich das European Data Protection Board (EDPB) auf eine Richtlinie zu „Dark Patterns“ geeinigt (SSN 4/2022), mit denen Seitenanbieter versuchen, Besucher zur Zustimmung zu verleiten.

Das ist aber nur ein Teil des Problems. Angesichts der Schwemme der Beschwerden über vorgeblich rechtswidrige Cookie-Banner haben die Datenschutz-Aufsichtsbehörden daher eine „Taskforce Cookie Banner“ eingerichtet, die am 17.01.2022 ihren Bericht vorgelegt hat. Er enthält zahlreiche bereits durch einschlägige Urteile bestätigte Klarstellungen (wie die Forderung, dass ein Tracking erst nach der expliziten Zustimmung erfolgen, die Zustimmung nicht vorausgewählt sein und optionale Cookies nicht als „erforderlich“ deklariert werden dürfen), bleibt aber beispielsweise hinsichtlich der Gestaltung eines „alles Ablehnen“-Knopfs unscharf. Wer Cookies und Tracking wirksam verhindern möchte, bleibt daher bis auf weiteres auf Browser-Plugins wie Privacy Badger der EFF (SSN 12/2017) oder uBlock Origin angewiesen (SSN 10/2022).

Secorvo News

Secorvo auf der DFN-Konferenz

Auf der diesjährigen 30. DFN-Konferenz Sicherheit in vernetzten Systemen (08.-10.02.2023) referierten unsere Datenschutzexperten Friederike Schellhas-Mende und Christian Blaicher zu „E-Mail-Tracking und -Profiling“, und der Krypto-Experte Hans-Joachim Knobloch beschrieb den „Kampf gegen Goldene Zertifikate“ und wie man sich vor Angriffen über die ‚Certifried'-Schwachstelle schützen kann. Die Beiträge erschienen im Konferenzband.

Seminare

Das Seminar BSI Vorfall-Experte vom **07.03.** bis **09.03.2023** bietet Ihnen eine Vorbereitung nach dem Curriculum des Bundesamts für Sicherheit in der Informationstechnik (BSI) auf die Zertifizierung zum BSI-Experten.

Das Seminar IT Security Insights – T.I.S.P. Update vom **21.03.** bis **22.03.2023** frischt Ihren Wissensstand rund um die Themen Informationssicherheit und Datenschutz auf. Und kurz vor Ostern (**27.03.–31.03.2023**) bieten wir Ihnen mit dem T.I.S.P.-Seminar die Möglichkeit, Ihre IT-Security-Kenntnisse nicht nur zu vertiefen, sondern auch zertifizieren zu lassen – zur Vorbereitung erhalten Sie nach Ihrer Anmeldung unser T.I.S.P.-Buch „Informationssicherheit und Datenschutz“ (erschienen im dpunkt-Verlag).

Die Seminarprogramme und weitere Informationen zu unseren Seminaren finden Sie auf unserer Website. Wir freuen uns auf Ihre Anmeldung.

Phish me, if you can

Ein weltweit agierendes Kollektiv anarchischer Hacker hat sich, getrieben von anarchistischen Freiheitsidealen zum Ziel gesetzt, die vorherrschenden Gesellschaftsstrukturen zu destabilisieren und in totales Chaos zu stürzen. Ihr erstes Ziel ist die Energiewirtschaft.

Beim Jahreseröffnungsevent der KA-IT-Si am **16.03.2023** berichtet Jan Tomasch, Information Security Awareness Manager der EnBW, in seinem Vortrag „Security Awareness Kampagne mit Gamification“, wie die Mitarbeitenden der EnBW als Cyber-Interventionsteam ihre Verteidigungslinie aufbauen, um den Hackern das Handwerk zu legen.

Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2023	
13.-16.02.	OWASP 2023 Global AppSec (OWASP Foundation, Dublin/IRL)
März 2023	
07.-09.03.	BSI Vorfall-Experte (Secorvo, Karlsruhe)
14.-16.03.	secIT 2023 (Heise Medien, Hannover)
16.03.	Phish me, if you can (KA-IT-Si, Karlsruhe)
21.-22.03.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
21.-24.03.	DFRWS EU 2023 (DFRWS, hybrid)
27.-31.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
April 2023	
23.-27.04.	Eurocrypt 2023 (IACR, Lyon/FR)
24.-27.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-27.04.	Datenschutztage 2023 (WEKA, virtuell)
25.-26.04.	Security Forum 2023 (Hagenberger Kreis, Hagenberg/AT)

Fundsache

Die DSK hat am 24.11.2022 Version 3.0 des Standard-Datenschutzmodells beschlossen. Diese Methode zur Datenschutzberatung und -prüfung erleichtert die Umsetzung der rechtlichen Anforderungen der DSGVO in konkrete technische und organisatorische Maßnahmen.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher (Editorial), Stefan Gora, Kai Jendrian, 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

secorvo
security consulting

Secorvo Security News

Februar 2023

Leichen im Keller

Jede App, die personenbezogene Daten verarbeitet, muss diese Verarbeitung in einer Datenschutzerklärung erläutern. Nur so ist eine „faire und transparente" Verarbeitung der Daten – wie von der DSGVO gefordert – möglich, da für einen Nutzer beispielsweise nicht offensichtlich ist, ob eine App die Verarbeitung lokal durchführt oder einen Cloud-Dienst in Anspruch nimmt.

Geht die Verarbeitung über den eigentlichen Anwendungszweck der App hinaus, weil der Anbieter zusätzliche Daten für eigene (bspw. Marketing-) Zwecke erhebt, wie zur Bildung von Nutzerprofilen, oder gar Daten an Dritte (beispielsweise verbundene Unternehmen) weitergibt, ist eine Einwilligung der Betroffenen erforderlich – und die ist nur rechtswirksam, wenn sie *informiert* erfolgt. Eine am 23.02.2023 veröffentlichte Forschungsstudie der Mozilla Foundation zeigt, dass zahlreiche Unternehmen hier „Leichen im Keller" haben: Von den 40 Apps mit den höchsten Download-Zahlen des Google Play Store stimmten bei fast 80% die Angaben in der Datenschutzerklärung nicht mit den Angaben der Entwickler in Googles Data Safety Form überein, die im Google Play Store angezeigt werden. Bei 40% der Apps waren die Abweichungen gravierend – so weisen beispielsweise weder TikTok noch Twitter ihre Datenweitergaben an Werbeplattformen aus. Eine auf solchen unvollständigen Informationen beruhende Einwilligung in die Verarbeitung ist damit unwirksam – und die Verarbeitung der Daten somit rechtswidrig.

Die Zahlen sind erschreckend, denn die Studie untersuchte nur die Abweichung der Datenschutzerklärung von den Angaben der Entwickler im Play Store – welche Daten von den Apps (und den dahinter liegenden Plattformen) *tatsächlich* verarbeitet und an Dritte weitergegeben werden, wurde nicht untersucht. Nach einer Langzeitstudie von ARD und ZDF verbrachten die Deutschen 2021 rund 3,4 h pro Tag mit dem Smartphone. Die dabei anfallenden Daten liefern ein Verhaltensprofil aller Deutschen.

Inhalt

secorvo
security consulting

Security News

Tesla reagiert

Am 22.02.2023 veröffentlichte die niederländische Datenschutz-Aufsichtsbehörde (DPA) ihr Untersuchungsergebnis des „Wächter-Modus" in Tesla-Fahrzeugen. Danach hat Tesla erfreulicherweise auf die vielfach geäußerte Kritik (siehe SSN 07/2022 und SSN 08/2022) reagiert: Möchte der Fahrzeuginhaber den „Wächter-Modus" nutzen, muss er ihn nun zunächst aktivieren. Die Aufnahmen werden nur noch für die Dauer von zehn Minuten und ausschließlich im Fahrzeug gespeichert; so wird eine Dauerüberwachung der Fahrzeugumgebung vermieden. Zudem filmen die Kameras nur, wenn das Fahrzeug berührt wird. Eine Anzeige im Fahrzeug und die Innenbeleuchtung signalisieren Betroffenen, dass Videoaufnahmen stattfinden. Die DPA hat deshalb von der Verhängung eines Bußgelds gegen Tesla abgesehen und weist darauf hin, dass der Fahrzeughalter datenschutzrechtlich für die Videoaufnahmen verantwortlich ist. Grundsätzlich gelten für in Fahrzeugen verbaute Kameras die gleichen Regelungen wie für jede andere Kamera.

Vorgaben für S/MIME-Zertifikate

Trust Center, die Zertifikate anbieten, die von Browsern akzeptiert werden sollen, müssen sich an die Vorgaben des 2005 gegründeten CA/Browser-Forums (CAB) halten. Am 01.01.2023 veröffentlichte das CAB nun die von einer Arbeitsgruppe über gut zwei Jahre entwickelten Mindestanforderungen an S/MIME-Zertifikate. 84 Seiten füllen die Vorgaben, die am 01.09.2023 in Kraft treten. Danach müssen Zertifikatsaussteller die Identität des Antragstellers bei Personenzertifikaten genauer prüfen und diese Prüfung dokumentieren. Die Kriterien für die Auditierung der PKI werden noch diskutiert und zu einem späteren Zeitpunkt veröffentlicht.

Die Identitätsprüfung ist bei S/MIME-Zertifikaten zweifellos ein (sicherheits)kritischer Punkt – das Vertrauen in Personenzertifikate dürfte daher durch die neuen Vorgaben steigen. Allerdings könnten auch die bestehenden Registrierungsprozesse in Unternehmen, die öffentliche S/MIME-Zertifikate beziehen, von den Vorgaben betroffen sein – schlimmstenfalls ist beim nächsten Zertifikatswechsel die Registrierung zu wiederholen.

It's not a bug

Am 08.02.2023 wurde eine kontrovers diskutierte Schwachstelle im verbreiteten Passwort-Manager KeePass behoben. Konkret ging es um eine für Automatisierungsprozesse eingebaute Funktion, mit der die Passwort-Datenbank nach dem Entsperren durch den Anwender unverschlüsselt exportiert werden kann. Das (vermeintliche) Problem: Kann ein Angreifer die Konfigurationsdatei von KeePass ändern, dann kann er diese Funktionalität ohne Wissen des Benutzers aktivieren und darüber die Passwörter auslesen.

Der Fall lässt Parallelen zur Schwachstelle Log4Shell erkennen, bei der eine Funktion, die die meisten Anwender nicht erwarteten, letztlich zu einem Sicherheitsproblem führte. Auch wenn bei KeePass die Auswirkungen deutlich geringer sind: Eine automatisierte Exportfunktion werden hier nur die wenigsten Anwender erwartet haben.

Doch ein Angreifer mit Schreibzugriff auf die Konfigurationsdatei von KeePass kann weitaus mächtigere Angriffe durchführen. Das erläutert KeePass selbst schon seit einigen Jahren auf der eigenen Website. Mit den Worten der KeePass-Entwickler: „KeePass cannot magically run securely in an insecure environment."

Die neue Version 2.53.1 verlangt nun grundsätzlich bei einem Datenbankexport die erneute Eingabe des Master-Passworts.

Leitlinien gegen Irreführung

Nach elfmonatiger öffentlicher Kommentierungsphase veröffentlichte der Europäische Datenschutzausschuss (EDSA) am 14.02.2023 seine Leitlinien zu irreführenden und DSGVO-widrigen Design-Elementen auf Social-Media-Plattformen als Version 2.0. In dem 74-seitigen Dokument werden zahlreiche Irreführungen beschrieben, mit denen Plattformbetreiber versuchen, Benutzer zu verleiten, gegen besseres Wissen ihre Zustimmung zu Tracking und anderen Datenerhebungen zu erteilen. Die verschiedenen Methoden werden in sechs Kategorien strukturiert und anhand 61 konkreter Beispiele veranschaulicht. Einige der beschriebenen irreführenden Design-Elemente finden sich auch auf anderen Plattformen.

Es ist zu erwarten, dass die im Dokument beschriebenen Methoden von den Datenschutz-Aufsichtsbehörden zukünftig bei der Prüfung von Portalen auf Datenschutzverstöße herangezogen werden.

Spyware auf Diensthandys

Nach mehreren Warnungen und dem Verbot der Installation und Nutzung von TikTok, der Videoplattform des chinesischen Bytedance-Konzerns, auf Dienst-Handys der amerikanischen Bundesbehörden haben nun die EU-Kommission (am 28.02.2023) und das EU-Parlament (am 01.03.2023) die

Installation und Nutzung des Dienstes auf Dienst-Handys untersagt.

Tatsächlich sind Apps mit großer Verbreitung perfekte Einfallstore für Spionage-Software: Die Geräte sind „always on“, kennen den Aufenthaltsort und die Kontaktdaten des Benutzers sowie sein Nutzungsverhalten und können, wenn der Benutzer es zulässt, auf Mikrofon und Kameras zugreifen. Zusätzliche Funktionen lassen sich (bei Bedarf sogar „zielgruppenspezifisch“) in Updates unterbringen, an deren ständigen Download sich Smartphone-Nutzer bereits gewöhnt haben. Zwar verhindern Schutzmechanismen der Betriebssysteme, dass eine App auf beliebige Daten und Sensoren zugreift; die erteilten Berechtigungen genügen aber meist, um ein Smartphone in ein Überwachungsgerät zu verwandeln.

Solche Angriffe sind für einen Nutzer bestenfalls an einer kürzeren Laufzeit des Geräts oder erhöhtem Internet-Traffic zu erkennen. Zwar kann man sie temporär außer Gefecht setzen, indem man den GPS-Sensor deaktiviert und die Internet-Verbindung kappt – damit deaktiviert man allerdings auch (fast) alle anderen Anwendungen auf dem Gerät.

Da viele Anbieter nicht einmal die von ihnen verarbeiteten Daten korrekt offenlegen (siehe Editorial), bleibt derzeit nur der Rückgriff auf Apps wie Gardion, die den Netzwerkverkehr des Smartphones nach Vorgaben filtern. Denen muss man allerdings vertrauen.

E-Mail-Tracking & Profiling

In ihrem Vortrag auf der 30. DFN-Konferenz am 09.02.2023 gingen Friederike Schellhas-Mende und Christian Blaicher auf die rechtskonforme Gestaltung von E-Mail-Tracking und Profiling ein. Denn nicht nur im Browser und in Apps wird das Nutzerverhalten analysiert, sondern zunehmend auch über Newsletter. Aber auch hier gelten UWG, DSGVO und TTDSG.

Damit bedürfen Newsletter mit Werbung nicht nur einer Einwilligung nach § 7 Abs. 2 Nr. 2 UWG. Protokollieren sie das Nutzerverhalten, benötigen sie außerdem eine Einwilligung nach § 25 TTDSG. Wenn zudem Benutzerprofile erstellt werden, ist obendrein eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO erforderlich. Eine Volltextveröffentlichung finden Sie auf der Secorvo-Webseite.

Da das Tracking in E-Mail-Newslettern gerne US-amerikanischen Tools (wie klaviyo und Mailchimp) überlassen wird, sollte man sich in einem solchen Fall angesichts der derzeitigen Abmahnungen besonders um eine rechtskonforme Gestaltung kümmern.

Secorvo News

Was sind „Goldene Zertifikate“?

Auf der Heise-Konferenz secIT in Hannover führten Hans-Joachim Knobloch und Oliver Oettinger am 14.03.2023 auf einem eintägigen Workshop in die Grundlagen der zertifikatsbasierten Anmeldung am Active Directory und Angriffe mit „Goldenen Zertifikaten“ ein. Einen verdichteten Überblick zum Thema gab Hans-Joachim Knobloch am 15.03.2023 in seiner Keynote.

Secorvo Seminare

Tanken Sie fünf Tage geballtes Wissen und lassen Sie sich anschließend als Experte für IT-Sicherheit zertifizieren: In unserem T.I.S.P. Seminar vom **27.** bis **31.03.2023** haben wir noch letzte freie Plätze.

Von den Grundlagen bis zur Planung Ihrer eigenen PKI: Alle wichtigen Aspekte von Public Key Infrastrukturen lernen Sie im PKI-Seminar vom **24.** bis **27.04.2023** kennen. In Workshops setzen Sie die Erkenntnisse aus den Vorträgen direkt um.

Von Praktikern für Praktiker: Mit unserem 3-Tages-Seminar „BSI Vorfall-Experte – Aufbauschulung“ vom **09.** bis **11.05.2023** sind Sie bestens gerüstet für die Zertifizierung zum Vorfall-Experten gemäß BSI-Curriculum.

Wir freuen uns auf Ihre Anmeldung.

Phish me, if you can

Ein weltweit agierendes Kollektiv anarchischer Hacker, getrieben von anarchistischen Freiheitsidealen, hat sich zum Ziel gesetzt, die vorherrschenden Gesellschaftsstrukturen zu destabilisieren und in totales Chaos zu stürzen. Ihr erstes Ziel: die Energiewirtschaft.

Beim Jahreseröffnungsevent der KA-IT-Si am **16.03.2023** berichtet Jan Tomasch, Information Security Awareness Manager der EnBW, in seinem Vortrag „Security Awareness Kampagne mit Gamification“, wie die Mitarbeitenden der EnBW als Cyber-Interventionsteam ihre Verteidigungslinie aufbauen, um den Hackern das Handwerk zu legen.

Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Net(t)-working“. Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen – und empfehlen eine zügige Anmeldung, da die Teilnehmerzahl auf 150 beschränkt ist.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2023	
14.-16.03.	secIT 2023 (Heise Medien, Hannover)
16.03.	KA-IT-Si Event Phish me, if you can (KA-IT-Si, Karlsruhe)
21.-24.03.	DFRWS EU 2023 (DFRWS, hybrid)
27.-31.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
April 2023	
23.-27.04.	Eurocrypt 2023 (IACR, Lyon/FR)
24.-27.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-27.04.	Datenschutztage 2023 (WEKA, virtuell)
25.-26.04.	Security Forum 2023 (Hagenberger Kreis, Hagenberg/AT)
Mai 2023	
09.-10.05.	BvD Verbandstag 2023 (BvD, Berlin)
09.-11.05.	BSI Vorfall-Experte - Aufbauschulung (Secorvo, Karlsruhe)
09.-12.05.	Blackhat Asia 2023 (Blackhat, Singapur/ASE)
09.-12.05.	European Identity and Cloud Conference 2023 (KuppingerCole, Berlin, hybrid)
10.-11.05.	19. Deutscher IT-Sicherheitskongress (BSI, virtuell)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Stefan Gora, Kai Jendrian, 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

secorvo
security consulting

Secorvo Security News

März 2023

Von Bäumen und Wäldern

Es gab eine Zeit in der IT-Sicherheit, da galten einfache, klare Regeln. So erforderte eine gute Authentifikation ‚Wissen' und ‚Besitz' und wurden Daten, die von außen durch die Firewall gelangten, grundsätzlich als ‚potentiell gefährlichen Inhalts' eingestuft.

Das war einmal. Nicht, dass diese Prinzipien in Frage stünden. Wohl aber kippt immer öfter die praktische Umsetzung. Drei Beispiele: Für den bequemen Zugriff vom Mobilgerät auf E-Mails oder die Unternehmens-Cloud verlässt man sich zunehmend auf die Authentifikation des Nutzers am Gerät – die nicht selten auf schwachen Wischcodes oder leicht zu täuschenden Fingerabdruck-Scannern beruht. „Moderne" Zahlungssysteme lassen sich gänzlich ohne Transaktions-Authentifikation nutzen – um keine Kunden an andere Anbieter zu verlieren, geht das inzwischen sogar mit der EC-Karte (bis 50 € und fünfmal in Folge) und über Apple oder Google Pay. Und damit wir unseren Terminkalender nicht mehr pflegen müssen, werden per E-Mail zugesandte Einladungen ungefragt von Outlook eingetragen.

Der Preis, den wir für diese Bequemlichkeiten zahlen, ist hoch. So werden schwache Authentifikationen durch immer ausgefeiltere Datenerhebungen und Profilbildungen kompensiert (entsprechen Höhe und Empfänger der Zahlung den Gewohnheiten? kommt sie von demselben Endgerät – und aus dem richtigen Land?) – mit den unvermeidlichen Begleiterscheinungen gelegentlicher Sperrungen durch „false positives" und einer Verhaltensanalyse, die selbst George Orwells Vorstellungsvermögen überstiegen hätte. Zugleich eröffnet die dadurch anwachsende Komplexität der IT immer wieder unerwartete Angriffsflächen – vom „Denial of Service" auf das Konto bis zur Outlook-Attacke via Termineinladung (siehe „Termin-Hack").

Dagegen helfen würde mehr Einfachheit: ein „Stopp" bei vermeidbarer Komplexität, sodass neben den Bäumen der Wald wieder in den Blick käme. Aber das wäre wahrscheinlich – kompliziert.

Inhalt

secorvo
security consulting

Security News

Termin-Hack

Am 14.03.2023 hat Microsoft eine kritische Lücke (CVE-2023-23397) in allen Outlook-Versionen gepatched, über die ein Angreifer mit einer präparierten E-Mail ohne Zutun des Empfängers den NetNTLMv2-Hash des Nutzers abgreifen konnte. Die Schwachstelle existiert offenbar schon eine Weile – und wurde nachweislich schon seit April 2022 ausgenutzt. Am 20.03.2023 wurde ein Proof of Concept auf Github veröffentlicht. Man sollte übrigens Microsofts Empfehlung folgen und den Port TCP 445/SMB (ausgehend) an der Firewall sperren – die Lücke ist offenbar noch ausnutzbar.

Die Details der Schwachstelle sind delikat. Wer einen Outlook-Kalendereintrag erzeugt, kann diesem Termin eine selbst gewählte Sound-Datei für den Erinnerungsalarm zuordnen. Wird der Termin an einen (externen) Teilnehmer geschickt, öffnet dessen Outlook zum Zeitpunkt des Alarms diese Sound-Datei. Verlinkt der Angreifer hier auf einen externen Server, dann versucht der Outlook-Client des Empfängers, sich mit dessen Credentials dort anzumelden…

Die Schwachstelle ist das Ergebnis einer Software-Entwicklungsstrategie, die automatisiertes „Eindringen" in eine fremde Infrastruktur zur Regel macht: Outlook trägt jede Terminänderung ohne Freigabe des Empfängers beim Eintreffen der E-Mail automatisch in dessen Kalender ein. Verwunderlich ist daher nicht die Schwachstelle, sondern die Tatsache, dass Spammer und Phisher diesen Mechanismus nicht schon längst nutzen – denn was macht ein Empfänger wohl mit einem Link in einem Termin, den er nicht zuordnen kann?

Produkthaftung für Software

Die National Cybersecurity Strategy der US-Regierung vom 01.03.2023 listet auf 35 Seiten, strukturiert in fünf „Säulen" (Schutz kritischer Infrastrukturen, Bekämpfung von Angreifern, Stärkung der Widerstandskräfte des Marktes, Investitionen in Widerstandsfähigkeit und Internationale Zusammenarbeit), zahlreiche Maßnahmen und Vorgaben zum Schutz digitaler Infrastrukturen. (Allein die kompakte Darstellung ist beispielgebend – die Cybersicherheitsstrategie der Bundesregierung vom 08.09.2021 benötigte 142 Seiten, davon allein vier für das Inhaltsverzeichnis.) Folgenreich könnte die Zuweisung der Verantwortlichkeit von Software-Unternehmen für Sicherheitsmängel sein: "*Companies that make software must have the freedom to innovate, but they must also be held liable when they fail to live up to the duty of care they owe consumers, businesses, or critical infrastructure providers.*" Daraus lässt sich eine Haftung bei Pflichtverletzungen ableiten: Wer gegen Best Practices verstößt oder typische Fehler wiederholt, muss für daraus entstehende Schäden gerade stehen.

In Deutschland hält sich bisher die Auffassung, dass Software – juristisch – kein Produkt ist: Der Käufer erwirbt lediglich ein Nutzungsrecht. Ein Schritt zu mehr Herstellerverantwortung war die Einführung einer Aktualisierungspflicht zum 01.01.2022 (in § 475b und § 327f BGB). Mit dem EU Cyber Resilience Act vom 15.09.2022 will die EU-Kommission nun die Anforderungen an die Sicherheit von Software und den Umgang mit Schwachstellen stärker regulieren. Im Entwurf der neuen Produkthaftungsrichtlinie gilt Software als Produkt. Damit unterläge Software der Produkthaftung – eine gute Nachricht für Unternehmen, die sich schon heute um Software-Sicherheit kümmern.

Die Forderungen an die Hersteller im Anhang des Richtlinienentwurfs sind äußerst konkret: „*Products with digital elements shall be delivered without any known exploitable vulnerabilities, (…) with a secure by default configuration, (…) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data').*"

Don't roll your own crypto

Die Implementierung von Krypto-Algorithmen ist fehleranfällig (SSN 12/2022). So darf beispielsweise die Zufallszahl, die der ECDSA für die Signatur einer Nachricht benötigt, nicht erneut verwendet werden. Daher wird diese Zahl auch „Nonce" (= number used only once) genannt. Eine am 06.03.2023 veröffentlichte Untersuchung von Kudelski Security zeigt eine weitere Angriffsmöglichkeit: Wird für ECDSA ein schlechter Pseudozufallszahlengenerator verwendet, dessen Ausgabewerte in einem polynomiellen (oder sogar linearen) Zusammenhang stehen, kann unter speziellen, aber plausiblen Umständen der private Schlüssel rekonstruiert werden. Als die Autoren ihr Verfahren an den Signaturen in der Bitcoin Blockchain ausprobierten, konnten sie den privaten Schlüssel von 762 Wallets (im Wert von rund 9,4 Mio. US$) rekonstruieren – dank fehlerhafter ECDSA-Implementierungen, die Nonces wiederverwenden. Daher sollte – wo immer möglich – auf Standard-Krpyto-Bibliotheken und -Protokolle zurückgegriffen werden.

TrustPid freigegeben

Mit TrustPid sollen Mobilgeräte-Nutzer zukünftig nicht mehr durch Cookies oder Browser Fingerprinting, sondern durch ihre Internet-Provider getrackt werden (SSN 06/2022). Die Einwilligung der Nutzer

wird über die Webseite verwaltet. Nach erfolgreicher Durchführung des Machbarkeitstests soll TrustPID nun europaweit eingesetzt werden; dafür hat die EU-Kommission am 10.02.2023 die wettbewerbsrechtliche Freigabe erteilt. Als technische Plattform für digitale Werbung in Europa haben die europäischen Mobilfunkanbieter Orange, Telefónica, Vodafone und Telekom ein Gemeinschaftsunternehmen mit Sitz in Belgien gegründet.

Trotz seiner Unzuständigkeit hat sich Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, zu TrustPid geäußert: Zwar erfolge der Einsatz auf der Grundlage einer Einwilligung der Nutzer, dennoch sei die besondere Vertrauensstellung, die Telekommunikationsanbietern zukommt, „nur schwer mit einem Tracking ihrer Nutzerinnen und Nutzer vereinbar". Außerdem müssten potenzielle Gefahren wie die Zusammenführung von pseudonymen Kennungen mit Login-Daten bei Webdiensten, die eine Re-Identifikation und die Verknüpfung von Tracking-Daten ermöglichen, verhindert werden. Fazit: Besser deaktivieren.

90-Tage-Zertifikate

Am 03.03.2023 hat das Chromium-Projekt von Google erneut eine drastische Verringerung der Gültigkeiten von Browser-Zertifikaten vorgeschlagen (und angekündigt, dies ggf. direkt im Chrome-Root-Programm zu verankern): Root-Zertifikate sollen maximal sieben, CA-Zertifikate bis zu drei Jahre und öffentliche TLS-Sever-Zertifikate nur noch 90 Tage gültig sein (bei Let's Encrypt ist das schon lange Praxis). Mit diesem Schritt sollen CAs dazu gebracht werden, etwa alle fünf Jahre ihre Infrastruktur auf den aktuellen Stand der Technik zu bringen – und die Server-Betreiber, automatisierte Protokolle wie ACME zur Zertifikatsaktualisierung zu verwenden. Sollte sich der Vorschlag durchsetzen, wäre das der Anfang vom Ende des Geschäftsmodells der kommerziellen Zertifikatsanbieter. Zugleich könnte er die Entwicklung von ACME-Clients für Plattformen jenseits der verbreiteten Betriebssysteme und Webserver (wie Hypervisor, Appliances oder IoT-Schnittstellen) beschleunigen – und so die überfällige Automatisierung der Zertifikatsaktualisierung zum Standard machen.

Kontrolle ist besser

Für großes Erstaunen, nicht nur bei der Landesbeauftragten für den Datenschutz Niedersachsen, Barbara Thiel, hat die Entscheidung des VG Hannover vom 09.02.2023 zur ununterbrochenen Überwachung von Mitarbeitern mit Handscannern bei Amazon gesorgt (10 A 6199/20). Obwohl beim EuGH (Rechtssache C-34/21) gerade die Frage der DSGVO-Konformität des § 26 BDSG zur Entscheidung ansteht, ist das VG Hannover überzeugt, dass das berechtigte Interesse des Unternehmens hier die Interessen der Arbeitnehmer überwiegt. Die von Amazon geltend gemachten Zwecke zur Steuerung der Logistik und der Mitarbeiterqualifizierung sowie zur Schaffung objektiver Bewertungsgrundlagen für Feedbackgespräche seien (ge)wichtiger als der permanente Überwachungsdruck auf die Arbeitnehmer. Diese wüssten um die Überwachung und müssten angesichts der großen Anzahl offener Stellen auch keine Angst vor Arbeitsplatzverlust haben, wenn sie sich dieser Überwachung nicht aussetzen wollten. Zwar seien einige Punkte wie etwa die Speicherdauer grenzwertig, aber letztlich könne man sich der Argumentation von Amazon anschließen.

Unternehmen, die Überwachungsmaßnahmen planen, sollten ihre Motivation plausibel darlegen und dokumentieren – und sich in Niedersachen ansiedeln. Allerdings prüft die LfDI Niedersachsen gerade den Gang in die nächste Instanz.

Secorvo News

Secorvo Seminare

Machen Sie den ersten Schritt zum BSI Vorfall-Experten mit unserem Seminar „BSI Vorfall-Experte – Aufbauschulung" vom **09. bis 11.05.2023.** Oder krönen Sie Ihre Qualifikation mit dem T.I.S.P.-Zertifikat: Beim vorbereitenden T.I.S.P.-Seminar vom **19. bis 23.06.2023** sind noch Plätze frei.

Das Seminarprogramm und weitere Informationen finden Sie auf unserer Website. Wir freuen uns auf Ihre Anmeldung.

AD = Anno Domini?

Wie realistisch ist es für Angreifer, mit frei verfügbaren und öffentlichen Informationen Domain-Administrator auf einem fremden System zu werden? Beim KA-IT-Si-Event am **04.05.2023** in der *Church* (CyberForum e.V.) zeigen die Ethical Hacker von aramido in ihrem Vortrag „In 30 min. zum Domain-Admin" anhand von realen Bedrohungen, wie ein Angreifer auf interne Systeme zugreifen und anschließend die gesamte Infrastruktur übernehmen kann, indem er Domain-Admin-Privilegien erlangt. Dabei wird auch auf mögliche Abwehrmaßnahmen und Best Practices für die IT-Sicherheit eingegangen.

Anschließend gibt es natürlich wieder den fachlichen und persönlichen Austausch beim „Buffet-Networking". Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2023	
23.-27.04.	Eurocrypt 2023 (IACR, Lyon/FR)
25.-27.04.	Datenschutztage 2023 (WEKA, virtuell)
25.-26.04.	Security Forum 2023 (Hagenberger Kreis, Hagenberg/AT)
Mai 2023	
04.05.	KA-IT-Si-Event: "AD = Anno Domini?" (KA-IT-Si, Karlsruhe)
09.-10.05.	BvD Verbandstag 2023 (BvD, Berlin)
09.-11.05.	BSI Vorfall-Experte - Aufbauschulung (Secorvo, Karlsruhe)
09.-12.05.	Blackhat Asia 2023 (Blackhat, Singapur/ASE)
09.-12.05.	European Identity and Cloud Conference 2023 (KuppingerCole, hybrid)
10.-14.05.	ISSE 2023 (IEEE, Timisoara/ROU)
10.-11.05.	19. Deutscher IT-Sicherheitskongress (BSI, virtuell)
22.-24.05.	Omnisecure 2023 (in TIME berlin, Berlin)
23.-24.05.	24. Datenschutzkongress (EUROFORUM, Berlin)
23.-24.05.	IMF 2023 (Fraunhofer-Institut IAO, München)

Fundsache

Am 23.03.2023 hat das BSI eine neue Technische Richtlinie (TR 03145-5) mit Anforderungen an den sicheren Betrieb von Public Key Infrastrukturen für technische Sicherheitseinrichtungen veröffentlicht (26 Seiten).

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, 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

secorvo
security consulting

Secorvo Security News

April 2023

Lernen durch Schmerzen

In jüngster Zeit mussten sich Gerichte vermehrt mit Schadensersatzklagen im Zusammenhang mit Datenschutzverstößen befassen. Immer wieder war dabei die Frage zu beantworten: Reicht es für einen Schmerzensgeldanspruch, dass sich ein Datenschutz-Risiko verwirklicht hat? Und falls ja, welches Schmerzensgeld ist angemessen?

Gemäß Art. 82 Abs. 1 DSGVO lässt sich die erste Frage schnell mit „Ja“ beantworten: Haftung und Verantwortung sind Wesenselemente des europäischen Datenschutzrechts. Allerdings messen die Gerichte mit zweierlei Maß: Bei Daten-Scraping (also dem Abgreifen personenbezogener Daten, die bspw. über ein Social-Media-Profil zugänglich sind) wird ein Schadensersatzanspruch in der Regel abgelehnt (so z.B. vom LG Gießen am 03.11.2022), selbst wenn die Betroffenen dabei ein „schlechtes Gefühl“ beschleicht. Anders sieht es bei einem „richtigen“ Datenschutzvorfall aus: Dann besteht ein Anspruch unabhängig davon, ob die Betroffenen durch das verwirklichte Risiko tatsächlich einen Schaden erlitten haben oder nicht – es reiche aus, dass die Betroffenen ein wenig Bauchgrummeln verspüren (so das OLG Hamm am 20.01.2023). Denn wenn nur genügend Betroffene ihre Ansprüche geltend machen würden, sei das in der Summe für den Verantwortlichen schmerzhaft, und Abschreckung müsse schließlich sein.

Übersehen wird dabei allerdings, dass für einen Schadensersatzanspruch auch ein materieller oder immaterieller Schaden entstanden sein muss – ein „Strafschmerzensgeld“ ist dem deutschen Recht nicht bekannt. Und das aus gutem Grund: Für die Sanktionierung von Datenschutzvorfällen und -verstößen sind die Datenschutz-Aufsichtsbehörden zuständig – und sollen das auch bleiben. Der Spagat zwischen einem wirksamen Grundrechtsschutz und der vorsätzlichen missbräuchlichen Ausnutzung lässt sich nur durch eine einheitliche Rechtsprechung bewältigen.

Inhalt

secorvo
security consulting

Security News

Grundschutz in der Cloud

Am 03.04.2023 hat Microsoft drei Leitfäden zur Umsetzung von IT-Grundschutz bei der Nutzung der Cloud-Lösungen Azure, Office 365 und Dynamics 365 veröffentlicht. In den Workbooks wird zu den Anforderungen aus dem Baustein OPS.2.2 des Grundschutz-Kompendiums zur Cloud-Nutzung erläutert, welche Microsoft-Funktionen und Konfigurationen deren Umsetzung unterstützen. Die Workbooks enthalten Referenzen auf weiterführende Microsoft-Informationen, und in einem weiteren Kapitel wird ausgeführt, was zur Erfüllung des „Mindeststandards des BSI zur Nutzung externer Cloud-Dienste“ (NCD.2) zu tun ist.

Angesichts der zahlreichen von Microsoft zur Verfügung gestellten Funktionen und Optionen sind die Leitfäden eine wertvolle Hilfestellung für alle am IT-Grundschutz ausgerichteten IT-Infrastrukturen, die die Microsoft-Cloud nutzen. Der Bericht der europäischen Datenschutz-Aufsichtsbehörde (edpb) vom 17.01.2023 über die Prüfung der Nutzung von Cloud-Diensten im öffentlichen Bereich dürfte Microsoft motiviert haben, die Nutzer bei der Umsetzung der technischen und organisatorischen Schutzmaßnahmen besser zu unterstützen.

Bauchschmerzen

Das OLG Hamm entschied am 20.01.2023, dass für einen Schadensersatzanspruch ein „schlechtes Gefühl“ der von einer Datenpanne betroffenen Person ausreicht. Nur wenn der Verantwortliche beweisen kann, dass er in keinerlei Hinsicht für die Panne verantwortlich ist, ist seine Haftung nach Art. 82 Abs. 3 DSGVO ausgeschlossen. Dafür müssen sämtliche notwendigen technischen und organisatorischen Maßnahmen ergriffen, umgesetzt und ausreichend dokumentiert sein.

Dies gilt übrigens auch für die Frage, ob eine nicht umfänglich erteilte Auskunft einen Schadensersatzanspruch auslösen kann (siehe Urteile des LAG Niedersachsen und des LArbG Nürnberg). Wer nicht zwischen den Mahlsteinen der Justiz zerrieben werden will, erteilt die Auskunft so, wie es Art. 12 DSGVO vorsieht. Dafür unerlässlich ist ein Datenschutzmanagement mit etablierten und dokumentierten Regelungen und Prozessen.

Software Security Game

Am 21.03.2023 hat GitHub als Teil seiner Ausbildungsangebote ein Spiel veröffentlicht, mit dem sich die Kenntnisse zur Sicherheit von Software trainieren lassen. Dieses Secure Code Game richtet sich an Entwickler, die Schwachstellen in Software besser erkennen und vermeiden wollen. Der Fokus liegt auf der Programmiersprache Python, doch sind die vermittelten Konzepte größtenteils sprachunabhängig. Das Spiel kann lokal geclont oder in GitHub Codespaces genutzt werden.

Jahr des DSB

Der Europäische Datenschutzausschuss (EDSA) hat am 15.03.2023 für das Jahr 2023 eine koordinierte Prüfung der Situation der Datenschutzbeauftragten (DSB) angekündigt. Geprüft werden soll, ob die DSB gemäß den Vorgaben der Art. 37-39 DSGVO organisatorisch eingebunden und mit ausreichenden Ressourcen ausgestattet sind. Dazu werden zunächst Fragebögen an die DSB verschickt (deren Auswertung später zur Verfügung gestellt werden soll), ggf. gefolgt von förmlichen Untersuchungen der nationalen Aufsichtsbehörden.

Mut zum Besseren

„Das Bessere ist der Feind des Guten“ wusste schon Voltaire. Hätte es damals schon IT gegeben, wären ihm allerdings Zweifel gekommen – denn da hält man gerne an Bewährtem fest, solange z. B. Kryptoverfahren nicht komplett gebrochen sind. Das war schon bei der Hashfunktion SHA-1 so, bis das CA/Browser-Forum 15 Jahre später den Einsatz des Nachfolgers SHA-2 erzwang.

Für die Linux-Festplattenverschlüsselung LUKS hat der Linux-Entwickler Matthew Garrett am 17.04.2023 empfohlen, von älteren Versionen mit der Schlüsselableitung per PBKDF2 (Ursprung 1993) auf das vor 9 Jahren eingeführte LUKS2 mit Argon2id zu wechseln. Zwar muss man dem dieser Empfehlung zu Grunde liegenden Gerücht über einen erfolgreichen Angriff auf PBKDF2 mit Skepsis begegnen. Aber Argon2 wurde gegen Angriffstypen gehärtet, die beim Design von PBKDF2 noch gar nicht „auf dem Schirm“ waren. Daher sollte man den Mut zum Besseren haben – der Wechsel wird sicherlich weniger schmerzen als vielleicht befürchtet.

Der Preis ist heiß

Neben den klassischen Cookie-Bannern gibt es – insbesondere auf Webseiten mit „redaktionellen Inhalten“ – Cookie-Walls, bei denen die Nutzer entscheiden müssen, ob sie mit Daten (Zustimmung zu Tracking und Werbung) oder mit Geld bezahlen wollen (Pur-Abo). Die DSK hat am 22.03.2023 entschieden, dass solche Abo-Modelle zulässig sind, wenn beide Varianten (Tracking und Geldzahlung) gleichwertig sind. Dafür müssen „die Angebote zumindest dem Grunde nach die gleiche Leistung umfassen“. Leider klärt die DSK nicht, welches Entgelt angemessen ist und verweist nur auf die Marktüblichkeit. Das ist bedauerlich, da ein unan-

gemessenes Entgelt die Freiwilligkeit der Einwilligung in Frage stellen kann.

Patchpolizei Exchange

Im Exchange-Team-Blog kündigte Microsoft am 23.03.2023 an, dass Exchange-Server in der Cloud zukünftig sukzessive keine Nachrichten mehr von ungepatchten on-premise-Exchange-Servern annehmen werden. Betreiber verwundbarer Exchange-Server sollen erst informiert, dann der Empfang gedrosselt und, sofern innerhalb von 90 Tagen keine Abhilfe geschaffen wird, die Verbindung abgebrochen werden. Betroffene E-Mail-Absender werden darüber informiert.

Keine Frage: Für die „Internet-Hygiene“ und die Sicherheit der Allgemeinheit ist es eine gute Sache, wenn Patch-Muffel unter Druck gesetzt werden. Aber maßt sich Microsoft hier nicht eine bestenfalls hoheitliche Aufgabe an? Und was passiert mit nicht gepatchten Postfix-Mailservern? Oder veralteten Webservern? Sollte in solchen Fällen zukünftig auch ein E-Mail-Empfang als erzieherische Maßnahme verweigert werden? Aber bei wem liegt die Verantwortung, wenn einem Nutzer, der den Patch-Stand des Servers seines Providers nicht beeinflussen kann, durch die Nichtzustellung einer Nachricht ein Schaden entsteht? Zwar wird man Microsoft nicht vorwerfen können, dass dabei Nachrichten unterdrückt werden, um einem Dritten einen Nachteil zuzufügen (§ 274 Abs. 1 StGB). Allerdings könnten die verweigerten E-Mails einwandfrei sein, nur eben der versendende „Gammel“-Server nicht: In diesem Fall läge nicht zwingend eine Bedrohung für Exchange-Online vor. Daher empfehlen wir eine genauere Betrachtung der insbesondere rechtlichen Implikationen einer solchen Zwangsmaßnahme.

Datenschutzmanagement

Ein Verarbeitungsverzeichnis muss regelmäßig gepflegt werden; darauf weist der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) in einer Kurzinformation vom 01.04.2023 hin.

Die Umsetzungstipps sind nicht nur für öffentliche Stellen wertvoll. Dennoch greift diese Sicht zu kurz: Nicht nur das Verzeichnis der Verarbeitungstätigkeiten, sondern alle wesentlichen Datenschutz-Dokumente sollten regelmäßig, mindestens jährlich auf Vollständigkeit, Aktualität, Eignung und Korrektheit überprüft werden. Dazu sind, wie beim Informationssicherheitsmanagement, die notwendigen Abläufe (Prozesse) festzulegen und umzusetzen. Genau das sind Wesenselemente eines Datenschutzmanagementsystems – es wird Zeit, dass die Aufsichtsbehörden diese Gesamtsicht in den Blick nehmen.

Gesetzgeber gefordert

Mit seinem Urteil vom 30.03.2023 hat der Europäische Gerichtshof (EuGH) festgestellt, dass die Regelung in § 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes den Anforderungen der DSGVO nicht genügt. Damit dürfen diese und gleichlautende Regelungen zum Beschäftigtendatenschutz (also auch § 26 BDSG) nicht mehr angewendet werden. Wer seine Datenverarbeitungen auf diese Rechtsgrundlage stützt, sollte schnellstmöglich nach einer Alternative suchen. Die Rechtmäßigkeit der Verarbeitung richtet sich nunmehr ganz allgemein nach Art. 6 Abs. 1 DSGVO, solange die Gesetzgeber des Bundes und der Länder nicht durch entsprechende (neue) Regelungen dafür sorgen, dass ein Beschäftigtendatenschutz in Deutschland endlich vernünftig eingeführt und umgesetzt wird (was die DSK schon seit Längerem fordert).

Secorvo News

Seminare

Bereiten Sie sich mit unserem T.I.S.P.-Seminar vom **19. bis 23.06.2023** auf Ihre Zertifizierung vor: In 18 Lernmodulen vertiefen Sie Ihr Wissen in Informationssicherheit und Datenschutz. Bei Buchung bis zum 14.05.2023 profitieren Sie von unserem Frühbucherrabatt. Wir empfehlen eine schnelle Anmeldung – es sind nicht mehr viele Plätze frei.

Wo ist meine schwache Stelle?

Schwachstellen sind die Kletterhaken der Angreifer – wer Software entwickelt, muss sie meiden wie der Teufel das Weihwasser. Wie man mit Hilfe von Vulnerability Management Systemen Schwachstellen sucht und bewertet, wird das Thema des nächsten KA-IT-Si-Events am **22.06.2023** um 18 Uhr in den wunderbaren Räumen der WIBU-Systems (IT Security Club) sein. Wir freuen uns auf Ihre Anmeldung!

Tag der IT-Sicherheit

Nach zwei ausgefallenen (2020, 2022) und einer reinen Online-Veranstaltung (2021) wird der 13. Tag der IT-Sicherheit in diesem Jahr endlich wieder im bewährten Format in der IHK Karlsruhe stattfinden. Zusammen mit KASTEL, dem CyberForum und der IHK laden wir sie herzlich ein, am **20.07.2023** ab 14 Uhr mit Experten, IT-Sicherheits- und Datenschutzbeauftragten über aktuelle Herausforderungen wie Quantencomputer, KI und Patch-Management zu diskutieren. Auch hier empfehlen wir eine frühe Anmeldung – die Zahl der Plätze ist begrenzt (und die Nachfrage groß).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2023	
04.05.	KA-IT-Si-Event: "AD = Anno Domini?" (KA-IT-Si, Karlsruhe)
09.-10.05.	BvD Verbandstag 2023 (BvD, Berlin)
09.-12.05.	Blackhat Asia 2023 (Blackhat, Singapur/ASE)
09.-12.05.	European Identity and Cloud Conference 2023 (KuppingerCole, hybrid)
10.-14.05.	ISSE 2023 (IEEE, Timisoara/ROU)
10.-11.05.	19. Deutscher IT-Sicherheitskongress (BSI, virtuell)
22.-24.05.	Omnisecure 2023 (in TIME berlin, Berlin)
23.-24.05.	24. Datenschutzkongress (EUROFORUM, Berlin)
23.-24.05.	IMF 2023 (Fraunhofer-Institut IAO, München)
Juni 2023	
01.-02.06.	Annual Privacy Forum 2023 (ENISA et al., Lyon/FR)
12.-13.06.	DuD 2023 (COMPUTAS, Berlin)
14.-15.06.	Entwicklertag 2023 (VKSI, GI, ObjektForum, Karlsruhe)
19.-23.06.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
21.-22.06.	31. ID:SMART Workshop (Fraunhofer SIT, Darmstadt)
22.06.	Wo, bitte, ist meine schwache Stelle? (KA-IT-Si, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende (Editorial), 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

secorvo
security consulting

Secorvo Security News

Mai 2023

Tröpfchen

Ohne Einwilligung, gesetzliche Grundlage oder einen Vertrag ist die Verarbeitung personenbezogener Daten verboten. Das gilt auch für Daten, die nach Vertragsende oder Ablauf einer Aufbewahrungspflicht noch in Systemen schlummern.

Diese Daten sind der Kern des (Datenschutz-) Problems. Sie erlauben eine Rekonstruktion vieler unserer Lebensbereiche: Reisen (Flug- und Bahnkarten, GPS-Daten), Nutzung (Apps, Browser, Online-Shops) und Kommunikation (Telefonie, E-Mail, Messenger). Inzwischen protokollieren auch Geräte (Autos, Saugroboter, Sportuhren, ...) unser Leben. Wer diese Daten kennt, kennt die Menschen: ihre Kaufentscheidungen, ihr Sozialverhalten und ihre Freizeitbeschäftigungen, ihre Gesundheit, ihr Fahrverhalten und ihre Vorlieben. Und damit wachsen auch die Begehrlichkeiten – sowohl kommerzielle als auch staatliche.

Welche Größenordnungen letztere schon heute annehmen zeigt eine Antwort der Bundesregierung auf eine Anfrage im Bundestag vom 27.04.2023 zu Fluggastdatenabfragen: 424 Mio. Datensätze von 121 Mio. Passagieren wurden von den Fluggesellschaften 2022 an das Bundeskriminalamt (BKA) geliefert. Damit wurden rund 19.800 zur Fahndung ausgeschriebene Passagiere identifiziert und es kam zu knapp 1.400 Festnahmen – 0,001% der von den BKA-Abfragen betroffenen Personen. In 99,999% der Fälle wurden vom BKA also Daten von Unschuldigen erhoben und verarbeitet. Klammern wir die Kosten für den Aufbau (54 Mio. €) und den Betrieb (14,5 Mio. €, also 10.500 € je Festnahme) des Fluggastdatensystems einmal aus: Kann man das noch „verhältnismäßig“ nennen?

Dabei hat das BKA die Auto- und Scooterverleiher noch gar nicht entdeckt. Viele speichern bislang praktisch unkontrolliert GPS-Daten – meist ohne Löschfristen. Erst am 28.03.2023 hatte die französische Aufsichtsbehörde CNIL ein Bußgeld gegen Cityscoot verhängt (125.000 €). Ein Tröpfchen auf einem glühenden Stein.

Inhalt

secorvo
security consulting

Security News

Eine Kopie ist (k)eine Kopie

Am 04.05.2023 stellte der EuGH zum datenschutzrechtlichen Auskunftsanspruch nach Art. 15 DSGVO klar, dass es nicht ausreicht, den Betroffenen Auskunft in Form allgemeiner Beschreibungen der Daten bzw. Datenkategorien zu geben. Das Recht auf Kopie bedeutet, dass „der betroffenen Person eine originalgetreue und verständliche Reproduktion aller dieser Daten" zu übermitteln ist. Ist dies nicht möglich, müssen die verarbeiteten Daten so zur Verfügung gestellt werden, dass „der betroffenen Person die wirksame Ausübung der ihr durch diese Verordnung verliehenen Rechte" ermöglicht, dabei aber auch die Rechte und Freiheiten anderer berücksichtigt werden. Damit werden insbesondere Geschäftsgeheimnisse und die Rechte Dritter geschützt. Dem Anspruch auf eine originalgetreue Kopie dürfen die Verantwortlichen also nicht uneingeschränkt nachkommen, sondern müssen eine Abwägung mit Rechten und berechtigten Interessen Dritter vornehmen.

Recovery Attack

Zusätzliche Sicherheitsmechanismen können auch zusätzliche Risiken bergen, wie Apples Recovery Key beweist. Der bereits 2014 eingeführte Mechanismus schützt die Apple-ID: Hat man das Kennwort zu seiner Apple-ID vergessen oder wurde es bei einem Angriffsversuch gesperrt, kann es mit einem vorher erzeugten, 28-stelligen zufälligen Recovery Key zurückgesetzt werden. Den Key sollte man außerhalb des Geräts speichern oder ausgedruckt in einen Tresor legen. Seit iOS 14 (2020) unterstützt Apple nach Aktivierung des Recovery Keys kein anderes Rücksetzungsverfahren mehr. Damit kann der Mechanismus nach hinten losgehen: Gewinnt ein Angreifer kurzzeitig physischen Zugriff auf das iPhone, kann er einen Recovery Key wählen oder einen bestehenden durch einen neuen ersetzen. Damit kann sich der Angreifer später jederzeit Zugriff auf die Apple-ID und damit das iCloud-Backup aller zugehörigen Geräte verschaffen – und den Geräteinhaber „aussperren".

Vertrauenskett(ch)en

Wer eine Vertrauenskette aufbaut, steht vor dem gleichen Dilemma wie Baron Münchhausen, der sich samt Pferd am eigenen Zopf aus dem Sumpf zog – im echten Leben gelingt das nur mit einer standfesten Verankerung. In der angelsächsischen Version der Legende zieht der Protagonist sich an den eigenen Stiefelriemen heraus – er „boot strap"-t.

Ist im Betriebssystem Secure-Boot aktiviert, prüft es, ob die UEFI-Firmware des Computers korrekte Daten zur Integritätsprüfung übergibt. Wie UEFI die herleitet, ist eine andere Frage. Um den Vertrauensanker dazu möglichst stabil zu gestalten, bietet Intel (in teureren CPUs) das Boot-Guard Verfahren an, dessen Details leider nicht offengelegt sind. Die Grundzüge sind wie folgt: Ein Computerhersteller kann über „Fuses" den Hashwert eines eigenen Public-Keys in die verbaute CPU brennen. Mit dessen Hilfe prüft der Microcode in der CPU die Integrität des ersten UEFI-Codeblocks, noch ehe ein Befehl aus der Firmware des Computers aufgerufen wird.

Dumm nur, wenn, wie Anfang Mai MSI und zuvor schon Lenovo passiert, der Private-Key dazu entschlüpft. Noch schlimmer, wenn der Mechanismus gar nicht aktiviert ist und eine UEFI-Malware den eigenen Key in die CPU-Fuses brennen könnte, um sich auch dort schon einzunisten – und somit Firmware-Updates zum Entfernen der UEFI-Malware selbst dem Hersteller nur noch durch Austausch der CPU möglich wären.

Insgesamt fehlt es der Secure-Boot-Vertrauenskette an Transparenz und Aufsicht. Im Web-PKI-Ökosystem ist – trotz Verbesserungspotenzials auch dort – die Vertrauenskette um Größenordnungen besser etabliert. Das CA/Browser-Forum ist die Steuerungsinstanz, die Requirements transparent veröffentlicht und ein recht striktes Aufsichts-Regime mit jährlichen Audits, Certificate Transparency usw. etabliert hat. Secure-Boot sollte da bald nachziehen, damit dessen Vertrauenskette nicht dauerhaft auf tönernen Füßen steht – und dessen Nutzer sich in falscher Sicherheit wähnen, wenn Secure-Boot aktiviert ist.

Top Secret

Am 24.11.2022 veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Stellungnahme zum datenschutzkonformen Einsatz von Microsoft 365 (SSN 11/2022) und stellte dabei Anforderungen an den Auftragsverarbeiter, die sich so nicht in der DSGVO wiederfinden. Daraufhin hat Microsoft zum 01.01.2023 das EU Data Boundary eingeführt (SSN 12/2022), wonach personenbezogene Daten im beschriebenen Rahmen innerhalb der EU gespeichert und verarbeitet werden sollen. An der Position der DSK hat sich jedoch nichts geändert.

Mittlerweile haben die Länder ein Rechtsgutachten zum Datenschutz konformen Einsatz von MS 365 anfertigen lassen. Ein Antrag von Frag den Staat auf Überlassung des Gutachtens wurde am 14.02.2023 abgelehnt. Begründung: Die Herausgabe dürfe nicht dazu führen, dass sich Dritte durch darin enthaltene Informationen wirtschaftliche Vorteile zu

Lasten öffentlicher Haushalte verschaffen (§ 14 Nr. 7 Landestransparenzgesetz Rheinland-Pfalz). Darüber hinaus würde eine Herausgabe das Verfahren zum Einkauf cloudbasierter Software und deren Vertragsmodalitäten – und damit die Verhandlungsposition gegenüber Microsoft – *„erheblich beeinträchtigen“* (§ 6 lit. b IFG NRW). Eine Anfrage von golem wurde ebenfalls abgelehnt.

Dabei liegt doch ein datenschutzkonformer Einsatz von Microsoft 365 mit geeigneten technischen und organisatorischen Mahnahmen im Interesse aller Beteiligten. Da fragt man sich doch, wie ein offenes und transparentes Vorgehen die Verhandlungsposition der Länder wohl schwächen könnte...

Kausalitätsprinzip

Am 04.05.2023 hat der EuGH die Voraussetzungen für das Vorliegen eines immateriellen Schadens nach Art. 82 DSGVO konkretisiert. Demnach setzt der Schadensersatzanspruch für immaterielle Schäden nicht voraus, dass der Schaden eine gewisse Erheblichkeit erreichen muss. Auch führt ein bloßer Verstoß gegen die Regelungen der DSGVO nicht automatisch zu einem Schadensersatzanspruch. Vielmehr bedarf es (1) eines Verstoßes gegen die DSGVO, (2) eines materiellen oder immateriellen Schadens, der aus diesem Verstoß resultiert, und (3) eines Kausalzusammenhangs zwischen Schaden und Verstoß. Dies entspricht dem deutschen Schuldrecht, welches ebenfalls einen kausalen Schaden als Voraussetzung für den Schadensersatz verlangt (§ 280 Abs. 1 BGB).

Zwar steigt durch das Urteil des EuGH das Risiko für Unternehmen auf Schadensersatzansprüche durch Betroffene, allerdings wird sich in der Praxis der Nachweis eines immateriellen Schaden schwierig gestalten.

Geburtstagswünsche

Mit Inkrafttreten der DSGVO am 25.05.2018 wurde innerhalb des Europäischen Wirtschaftsraums ein „einheitliches Datenschutzrecht“ geschaffen und das Recht auf informationelle Selbstbestimmung der Betroffenen gestärkt.

Allerdings mangelt es noch immer an einer konsequenten Durchsetzung und Kontrolle durch die Aufsichtsbehörden. Zwar erhielten die deutschen Aufsichtsbehörden im letzten Jahr ein Gesamtbudget von ca. 114 Millionen Euro, das deutlich über dem Budget anderer Mitgliedstaaten liegt. Doch verursacht der Föderalismus unterschiedliche Interpretationen und Durchsetzungsansätze bei den 17 deutschen Aufsichtsbehörden (inklusive der Sonderzuständigkeiten für Medien und Kirchen). Beschwerden konnten im letzten Jahr nicht zufriedenstellend bearbeitet werden. So kam es entweder nur zu geringen oder gar keinen Bußgeldern. Viele Beschwerden wurden insbesondere durch die Schaffung einer „Erheblichkeitsschwelle“ abgewiesen. Auch mangelt es an Transparenz, da – anders als in anderen Mitgliedstaaten – die Entscheidungen der Aufsichtsbehörden nicht konsequent veröffentlicht werden. Der Fokus liegt auf Informations- und Beratungstätigkeit und nicht auf konkreten Entscheidungen, wie sie beispielsweise zum Einsatz von Microsoft 365 überfällig wären.

Auch bei anderen europäischen Aufsichtsbehörden wird ein Großteil der Beschwerden nicht bearbeitet. Darüber hinaus zeigt der Bericht der ICCL deutlich, dass die irische Aufsichtsbehörde noch immer die Rolle eines Verhinderers bei der Durchsetzung des Datenschutzes gegen große IT-Unternehmen spielt. So wurden in der Vergangenheit rund 88 % der Entscheidungen der irischen Datenschutzbehörde durch den Europäischen Datenschutzausschuss außer Kraft gesetzt. Zum Geburtstag wünschen wir der DSGVO klarere Entscheidungen, einheitlichere Auslegungen des Datenschutzrechts und in der Höhe abgestimmte Bußgelder.

Secorvo News

Secorvo Seminare

Auf unserem Spätsommer-T.I.S.P.-Seminar vom **18. bis 22.09.2023** sind noch Plätze frei. Wir freuen uns auf Ihre Anmeldung.

Wo, bitte, ist meine schwache Stelle?

Schwachstellen sind die Kletterhaken der Angreifer – wer Software entwickelt, muss sie meiden wie der Teufel das Weihwasser. Wie man mit Hilfe von Vulnerability Management Systemen Schwachstellen sucht und bewertet, erfahren Sie am **22.06.2023** um **18 Uhr** auf dem kommenden Event der KA-IT-Si von den Experten der WIBU-Systems. Genießen Sie beim anschließenden „Buffet-Networking“ den Sommer auf der Dachterrasse. Schnell anmelden – die Zahl der Plätze ist begrenzt.

Back to normal

Endlich wieder im bewährten Format: Der 13. Tag der IT-Sicherheit findet am **20.07.2023** ab **14 Uhr** im Saal Baden der IHK Karlsruhe statt.

Es erwarten Sie Fachvorträge u. a. zur Bedrohung durch Quantencomputer, den Herausforderungen durch KI und zum Patchmanagement – sowie ein intensives Buffet-Networking. Hier geht's zu Programm und Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2023	
12.-13.06.	DuD 2023 (COMPUTAS, Berlin)
14.-15.06.	Entwicklertag 2023 (VKSI, GI, ObjektForum, Karlsruhe)
19.-23.06.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
22.06.	Wo, bitte, ist meine schwache Stelle? (KA-IT-Si, Karlsruhe)
Juli 2023	
03.-07.07.	8th IEEE European Symposium on Security and Privacy (IEEE, Delft/NL)
09.-12.07.	DFRWS USA 2023 (DFRWS, hybrid)
10.-15.07.	PETS 2023 (Université de Lausanne, hybrid)>
20.07.	13. Tag der IT-Sicherheit (KA-IT-Si, IHK, CyberForum, KASTEL Karlsruhe)

Fundsache

Die aktualisierte Handreichung zum "Stand der Technik" des TeleTrusT vom 09.05.2023 führt technische und organisatorische Maßnahmen auf, die gemäß definiertem Bewertungsschema von Unternehmen und Institutionen umgesetzt werden sollten. Die Handreichung wird kontinuierlich weiterentwickelt, ergänzt und stellt in kompakter Form die jeweilige Maßnahme vor und welche Schutzziele sie unterstützt. Aus unserer Sicht absolut lesenswert.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, 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

secorvo
security consulting

Secorvo Security News

Juni 2023

Die IT frisst ihre Kinder

Es war wohl der IBM PC, der vor über 40 Jahren den Siegeszug der Informationstechnik auslöste. Das Versprechen: Computer machen unser Leben leichter. Und tatsächlich: Wer zuvor Schreibmaschine und Stift für die Korrespondenz benutzt hatte, konnte seinen Durchsatz mit Tastatur und E-Mail leicht verzehnfachen.

Als rund 20 Jahre später Internet-Portale Bankgeschäfte, Einkäufe, Musikgenuss, Videoverleih und Behördengänge von zuhause ermöglichten, steigerte auch das unsere Lebensqualität. Die Ersetzung des transportresistenten PC durch Laptops und Smartphones, auf denen Kommunikation, Portale, Unterhaltung und Nachrichten per Fingertipp verfügbar sind, krönte diese Entwicklung und festigte die Überzeugung, dass IT unser Leben verbessert. Doch stimmt das noch?

Selbst wenn man verödende Innenstädte, erhöhtes Verkehrsaufkommen durch individuelle Warentransporte, die Verlagerung von „Tippdiensten" (Stichwort Grundsteuer) auf die Bevölkerung und den Energieverbrauch von IT-Geräten (inzwischen fast 30% des Strombedarfs) als unvermeidliche Nebeneffekte hinnimmt, macht uns die Digitalisierung zunehmend das Leben schwer. Wer sich durch eine Telefon-Hotline „durchgeklickt", seine Steuererklärung mit digitalen Rechnungen gemacht, einen Smartphone-Modellwechsel durchgezogen, versucht hat, an einer Kasse mit leerem Handy-Akku zu bezahlen oder sich gerade wieder beim Online-Banking per Transaktion neu authentifizieren muss, obwohl er erst am Vortag eine Überweisung getätigt hat, kann davon ein Lied singen.

Dabei ist ein großer Teil der Komplexität hausgemacht. Das gilt nicht zuletzt für Schutzmechanismen – in sehr vielen Fällen sind Authentifikationen überflüssig, in anderen Fällen ließen sie sich durch Nutzung der 2021 eingeführten eID-Funktion des Personalausweises vereinfachen. Und: Im Biergarten kann man nach wie vor sicher und anonym mit Bargeld bezahlen. Solange man noch einen Geldautomaten findet.

Inhalt

secorvo
security consulting

Security News

Cloud Supply Chain Security

Ein Satz wie „Der Angriff erfolgte ausschließlich auf den Dienstleister" (Kommentar der Barmer Ersatzkasse vom 17.06.2023 nach einem Hackerangriff auf den Dienstleister des Bonussystems) ist für Kunden keine Beruhigung. Vor allem: Ein Unternehmen wird die Verantwortung für die Datenverarbeitung durch die Verlagerung in die Cloud nicht los – häufig aber den Überblick.

Am 01.06.2023 veröffentlichte TeleTrusT einen Leitfaden zum Thema Cloud Supply Chain Security, der kompakt zusammenfasst, worauf es beim Einsatz von Cloud-Lösungen in der Supply Chain ankommt. Durch Maßnahmen wie „SBOM" (*Software Bill of Materials*) erfahren Auftraggeber, welche konkreten Frameworks und Software-Komponenten in den gebuchten Cloud-Diensten zum Einsatz kommen. Damit kann für die genutzten Cloud-Dienste im Incident Handling ein temporäres Abschalten bei der Identifikation ungepatchter Software-Komponenten vorgesehen werden.

Harmonie

Am 24.05.2023 hat der europäische Datenschutzausschuss (EDPB) die fast 50-seitigen Richtlinien zur einheitlichen Bemessung von Bußgeldern bei Verstößen gegen die DSGVO nach einjähriger öffentlicher Kommentierungsmöglichkeit (SSN 5/2022) verabschiedet. Das Vorgehen umfasst fünf Schritte von der Identifizierung bis zur finalen Bewertung. Besonders relevant für die Bußgeldhöhe ist die Festlegung des Ausgangspunktes. Dazu werden die Schwere (bezogen auf den Einzelfall), die Art und die Dauer des Verstoßes sowie die maximale Bußgeldhöhe herangezogen, die vom Umsatz des Unternehmens bestimmt wird. Erscheint der Verstoß schwerer als gleichartige Verstöße, soll das Bußgeld höher ausfallen. Bewertet wird auch das Verhalten des Verantwortlichen in Vergangenheit und Gegenwart; je nachdem erhöht oder vermindert sich das Bußgeld.

Die Richtlinien schaffen durch viele Beispielfälle mehr Transparenz bei der Bemessung von Bußgeldern. Sie liefern allerdings keine mathematische Formel, nach der Verantwortliche das Bußgeld berechnen könnten. Der Ermessenspielraum der einzelnen Aufsichtsbehörden bleibt trotz aller Vereinheitlichung erhalten – und das ist auch gut so.

Don´t roll your own crypto

Sichere Verschlüsselung ist schwierig umzusetzen. Schwachstellen können über fehlerhaft entworfene Protokolle (SSN 12/2022) oder auch schwache Komponenten, wie beispielsweise Zufallszahlen-generatoren (SSN 03/2023) entstehen.

Am 13.06.2023 veröffentlichten Forscher der Universität des Negev in Israel einen Seitenkanalangriff, der in der Lage ist, einen geheimen Schlüssel von einem Smartphone oder aus einer Smartcard auszulesen. Dafür wurde eine Variante der „Poweranalysis" verwendet, bei der der Stromverbrauch des Prozessors während einer Krypto-Operation zeitlich hoch aufgelöst aufgezeichnet und daraus der geheime Schlüssel abgeleitet wird.

Die Besonderheit bei dem neuen Angriff: Der Stromverbrauch des Prozessors wurde aus dem Flackern der Power-LED des Smartcard-Lesers bestimmt. Dafür war keine spezielle Kamera nötig: Der Angriff wurden mit einem handelsüblichen iPhone 13 durchgeführt. Das Geheimnis: Beim technisch bedingten „Rolling-Shutter" wird das Bild zeilenweise ausgelesen – die Zeilen des Bildes entstehen daher nicht zeitgleich. Füllt das Licht der Power-LED das gesamte Bild, so liefert jede Zeile eines Bildes Informationen über einen anderen Zeitpunkt. Wird durch den „Rolling-Shutter" das einzelne Bild beispielsweise in 1000 Schritten ausgelesen, so kann aus einem Video mit 60 Bildern pro Sekunde eine Messreihe mit 60.000 Messpunkten pro Sekunde abgeleitet werden. Diese Auflösung ist für eine „Poweranalysis" ausreichend. Allerdings benötigt der Angriff gut eine Stunde Videomaterial mit kontinuierlichen Krypto-Operationen, was einen realen Angriff mit dieser Methode stark erschwert. Der Angriff zeigt aber wieder einmal, dass (wie McGraw und Vega schon vor über 20 Jahren aufzeigten) bei der Implementierung von Kryptoverfahren viel schief gehen kann – auch an unerwarteten Stellen.

Verpfiffen

Der deutsche Gesetzgeber hat mit Verspätung zum 31.05.2023 das deutsche Hinweisgeberschutzgesetz beschlossen. Es tritt am 02.07.2023 in Kraft und beinhaltet für Unternehmen ab 50 Mitarbeitern die Pflicht, eine interne Meldestelle einzurichten. Unternehmen ab 250 Mitarbeiter müssen die Meldestelle mit Inkrafttreten errichtet haben; für kleinere Unternehmen gilt eine Umsetzungsfrist bis zum 17.12.2023.

In ihrer Orientierungshilfe zu Whistleblowing-Hotlines vom 14.11.2018 haben die Datenschutzaufsichtsbehörden darauf hingewiesen, dass die Meldungen von Hinweisgebern auch für die durch den Hinweis belasteten Personen ein hohes Risiko für deren Rechte und Freiheiten darstellen. Deshalb verlangen sie zu Recht die Durchführung einer

Datenschutz-Folgenabschätzung vor der Einführung von technischen Systemen zur Umsetzung der Meldestellenpflicht. Auch müssen die Mitarbeiter über etwaige Datenverarbeitungen informiert werden.

Wer dies vermeiden möchte, kann die Meldestelle bei einer Anwaltskanzlei einrichten – das spart nicht nur die Kosten für ein hoffentlich selten eingesetztes System, sondern auch dessen Pflege und Wartung.

Brute-Force-Biometrie-Attacke

Am 18.05.2023 veröffentlichten zwei chinesische Forscher einen BrutePrint getauften neuen Angriff auf die Fingerabdruck-Erkennung diverser Smartphone-Modelle. Anders als die meisten derartigen Angriffe versucht BrutePrint jedoch nicht, den Fingerabdruck zu fälschen: Die Forscher hängen nach Öffnen des Gehäuses ein eigenes Gerät in die SPI-Bus-Verbindung vom Fingerabdrucksensor zum Smartphone – ähnlich einem Hardware-Keylogger, der in die Tastaturleitung eingeschleift wird. Darüber kann der Angreifer übertragene Fingerabdruck-Samples mitlesen oder als Man-in-the-Middle eigene einspielen und durchprobieren. Daher auch der Name des Angriffs: *Brute*-Force-Finger-*Print*. Unter den getesteten Smartphones waren nur die (noch mit Touch-ID ausgestatteten) iPhones weitgehend resistent gegen den Angriff, da Apple als einziger Hersteller die SPI-Bus-Verbindung kryptographisch sichert.

Zwar haben alle Geräte einen Fehlbedienungszähler, der nach mehreren falschen Fingerpints eine Pause erzwingen soll, um Angreifer auszubremsen. Aber sogar bei iPhones war es möglich, den Vorgang über den SPI-Bus abzubrechen, bevor der Fehlbedienungszähler erhöht wird. Bei vielen Geräten war außerdem während der erzwungenen Pause zwar keine Anmeldung möglich, aber eingespielte Fingerabrücke wurden dennoch weiterhin ungebremst geprüft. Ein Lehrbeispiel dafür, wie man biometrische Sensoren nicht integrieren sollte.

Trau keinem Trust-Center

Zur einfachen Beantragung und automatisierten Erneuerung von TLS-Serverzertifikaten wird das ACME-Protokoll (zu Recht) immer populärer. Dabei verbindet sich ein ACME-Client (wie Certbot oder acme.sh) mit dem Trust-Center, das die Zertifikate ausstellt. Allerdings sollte sich das Vertrauen in das Trust-Center nur auf die ausgestellten Zertifikate und Sperrinformation beziehen, wie der am 08.06.2023 bekannt gewordene Vorfall bei einem chinesischen Trust-Center zeigt: Der Betreiber hatte eine unbekannte Remote-Code-Injection-Schwachstelle in acme.sh ausgenutzt, um während des Zertifikats-Enrollments zusätzliche Kommandos auf dem beantragenden Server auszuführen.

Zwar wurde schon am 09.06.2023 eine korrigierte Version von acme.sh veröffentlicht, aber da amce.sh manchmal auch in die Firmware von Appliances, Firewalls o. ä. integriert ist, kann es eine Weile dauern, bis nur noch gefixte Versionen im Einsatz sind. Eine Vorsichtsmaßnahme wäre, auf betroffenen Appliances ACME temporär zu deaktivieren und in den sauren Apfel des manuellen Enrollments zu beißen. Dann muss sich auch der Betreiber der chinesischen CA etwas Neues ausdenken…

Secorvo News

Aus dem Secorvo-Team

Mit Jochen Schlichting hat seit Juni ein weiteres Mitglied unseres Beratungsteams als „ISO/IEC 27001:2022 Lead Auditor“ die Lizenz zum Prüfen. Und seit Anfang Juli unterstützt uns unser neuer Kollege Paul Blenderman mit seiner über 20-jährigen Erfahrung mit IT-Sicherheit in Produktionsumgebungen. Willkommen im Secorvo-Team!

Seminare nach der Sommerpause

Bevor Sie Ihre Urlaubskoffer packen, werfen Sie doch noch einen Blick in unser Seminarangebot für das 2. Halbjahr. Wir starten mit unserem T.I.S.P.-Seminar vom **18. bis 22.09.2023** in den Herbst – noch gibt es freie Plätze.

Das Seminar IT-Security-Insights (**26.–27.09.2023**) aktualisiert Ihren Wissenstand zur Informationssicherheit. Wer sich mit Public-Key Infrastrukturen auskennen möchte, ist bei unserem PKI-Seminar (**09.–12.10.2023**) genau richtig. Und mit der Teilnahme am BSI-Seminar (**17.–19.10.2023**) bereiten Sie sich auf die Zertifizierung zum BSI-Vorfall-Experten vor. Wir freuen uns auf Ihre Anmeldung.

13. Tag der IT-Sicherheit

Endlich wieder im bewährten Format: Der 13. Tag der IT-Sicherheit findet am **20.07.2023 ab 14 Uhr** im Saal Baden der IHK Karlsruhe statt. Es erwarten Sie Fachvorträge zur Bedrohung durch Quantencomputer, den Herausforderungen durch die gestiegene Leistungsfähigkeit von KIs und zum Patchmanagement – sowie ein intensives Buffet-Networking. Hier geht's zum vollständigen Programm und zur Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2023	
10.-15.07.	PETS 2023 (Université de Lausanne, Lausanne/CH)
20.07.	13. Tag der IT-Sicherheit (KA-IT-Si, IHK, CyberForum, KASTEL, Karlsruhe)
August 2023	
05.-10.08.	Blackhat USA 2023 (Blackhat, Las Vegas/US)
06.-08.08.	SOUPS 2023 (usenix, Anaheim/US)
09.-11.08.	32nd USENIX Security Symposium (usenix, Anaheim/US)
10.-13.08.	DEF CON 31 (DEFCON, Las Vegas/US)
19.-24.08.	Crypto 2023 (Santa Barbara/US)
September 2023	
11.-13.09.	heise devSec 2023 (dpunt.verlag, heise, Karlsruhe)
18.-22.09.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-27.09.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
27.-29.09.	Informatik 2023 (GI, Hamburg)

Fundsache

Das Bayerische Landesamt für Datenschutzaufsicht hat sich der vom EDSA angekündigten Prüfaktion zu Stellung und Aufgaben von Datenschutzbeauftragten angeschlossen. Die Fragen zur Prüfung kann man u. a. bei IITR Datenschutz GmbH herunterladen.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, 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

secorvo
security consulting

Secorvo Security News

Juli 2023

Die Quanten kommen

Im Jahr 1994 schockierte Peter Shor die Krypto-Community mit der Publikation eines Algorithmus', mit dem die Faktorisierung ganzer Zahlen und die Bestimmung diskreter Logarithmen auf einem Quantencomputer mit einen Aufwand von O(log n) möglich ist – also in polynomieller Zeit. Damit erschütterte er die Grundlagen der modernen (asymmetrischen) Kryptographie, kurz: den Kern aller heutigen Schutzmechanismen in vernetzten IT-Systemen. Seitdem beten die Kryptologen, dass Quantencomputer in der erforderlichen Größe (10-100 Mio. QBits für 2048-bit-Schlüssel) so schnell nicht kommen – und suchen derweil fieberhaft alternative, gegen Quantencomputer resistente Algorithmen. Die 2016 vom US-amerikanischen NIST gestartete Standardisierungs-Initiative für Post-Quantum Public Key-Algorithmen hat inzwischen schon zahlreiche gebrochene Verfahren aussortiert – mit anderen mathematischen Problemen, die sich für asymmetrische Verfahren eignen könnten, kennen wir uns eben bei weitem nicht so gut aus wie mit der Faktorisierung ganzer Zahlen und dem diskreten Logarithmus.

Sollten die Kryptologen das Wettrennen gegen die Milliardeninvestitionen in Quantencomputer nicht gewinnen, werden wir wohl in archaische IT-Verhältnisse zurückfallen, denn ohne asymmetrische Kryptografie lassen sich Cloud-Computing, Internet-Banking oder Online-Shops praktisch nicht absichern.

Vielleicht haben die Kryptologen noch etwas Zeit. Denn Quantencomputer heutiger Konstruktion sind nicht so einfach herzustellen: Sie müssen bis nahe an den absoluten Nullpunkt gekühlt werden und verbrauchen daher gigantische Energiemengen. Auch die Bereitstellung einer großen Zahl an QBits ist bisher nicht einfach – und da kann man mit größeren Schlüssellängen ein wenig gegensteuern.

Irgendwann aber wird es solche Quantencomputer geben. Ich habe gewettet, dass das noch mindestens 30 Jahre dauert. Mit mehr als einer Kiste Bier wollte ich dabei allerdings nicht ins Risiko gehen.

Inhalt

secorvo
security consulting

Security News

Dritter Anlauf

Nach dem Scheitern von Safe Harbour und Privacy Shield verabschiedete die Europäische Kommission am 10.07.2023 mit dem Data Privacy Framework (DPF) den dritten Angemessenheitsbeschluss für die USA. Personenbezogene Daten dürfen damit wieder ohne zusätzliche Maßnahmen in die USA übertragen werden, sofern die Empfänger DPF-zertifiziert sind. Das U.S. Department of Commerce pflegt die öffentliche Liste aller zertifizierten Organisationen – die sich blitzschnell mit rund 2.500 Einträgen füllte, da das DPF eine reine Selbst-Zertifizierung ist.

Gemäß den Urteilen Schrems I und Schrems II des EuGH ist die US-Überwachung nach FISA 702 und EO 12.333 nicht verhältnismäßig und damit rechtswidrig. In der EO 14.086 (einer leicht angepassten Version der EO 12.333) wurde eine Verhältnismäßigkeitsprüfung ergänzt, die aber faktisch wenig Relevanz haben dürfte: Beschwerden können an den Civil Liberties Protection Officer (CLPO) gerichtet werden, der die Beschwerde jedoch nur prüfen und interne Weisungen erteilen kann. Das Ergebnis der Prüfung kann von einem Data Protection Review Court überprüft werden. Dem Betroffenen wird jedoch nicht mitgeteilt, ob er tatsächlich von einer Überwachungsmaßnahme betroffen war und welche Wirkung seine (anerkannte) Beschwerde hatte.

Nachdem der EUGH bereits die ersten beiden Angemessenheitsbeschlüsse für nichtig erklärt und Max Schrems angekündigt hat, auch den aktuellen Beschluss gerichtlich prüfen zu lassen, sollte man besser nicht auf eine lange Lebenszeit des DLP wetten.

Blindgänger aus Crypto War

Unter dem Namen TETRA:BURST hat die niederländische IT-Sicherheitsfirma Midnight Blue am 24.07.2023 fünf Schwachstellen veröffentlicht, die sie im Auftrag der NLnet-Stiftung mit Hilfe eines Motorola-Fahrzeugfunkgeräts im TETRA-Standard gefunden hat. Dieser 1995 entwickelte ETSI-Standard wird in über 120 Ländern in den Funknetzen von Polizei und Feuerwehr genutzt.

Die meisten Verwundbarkeiten hängen direkt oder indirekt mit der verwendeten proprietären, geheim gehaltenen 80-bit-Stromchiffre zusammen, für die kein öffentliches Peer Review erfolgte. Aufgrund der damaligen Exportbeschränkungen wurde (wie auch bspw. bei Lotus Notes) sogar eine Schwachstelle eingebaut: Damals entwickelte Export-Geräte verwenden effektiv nur 32 Bit lange Schlüssel, die die Forscher mit einem Laptop in wenigen Minuten knacken konnten. Die Details der Schwachstellen (CVE-2022-24400 bis -24404) sollen am 09.08.2023 publiziert werden.

Eine von der ETSI angekündigte Überarbeitung des Standards und die Updates der Hersteller werden die kompromittierten Kryptoverfahren jedoch kaum komplett ersetzen, da die (ungepatchte) Gebrauchsdauer von einmal beschafften Funkgeräten weit über der eines Durchschnitts-PCs oder Smartphones liegt.

Signierte Malware-Kernel-Treiber

Sophos X-Ops publizierte am 11.07.2023 zeitgleich mit einem Microsoft Advisory (ADV230001), dass sie über 100 mit Malware versetzte Windows-Kernel-Treiber entdeckt haben, die bis April 2021 zurückreichen und von Microsoft und anderen Code-Signing-Autoritäten digital signiert worden waren.

Die entdeckten Treiber waren entweder Varianten bekannter Windows-Rootkits oder „Protection Disabler", die Schutzmechanismen des Betriebssystems deaktivieren. Microsoft hat die Treiber in ihre Sperrliste aufgenommen und Sophos hat die Hashwerte und weitere Details zu den betroffenen Treibern in Github publiziert.

BSI Standard 200-4 – Finale Version

Seit dem 14.06.2023 ist der BSI Standard 200-4 „Business Continuity Management" 1.0 verfügbar, der den BSI Standard 100-4 „Notfallmanagement" abgelöst hat. Dies markiert das Ende eines sehr intensiven Peer-Reviewprozesses von Community Drafts (CD 1.0 01/2021, CD 2.0 09/2022) bis zum international gültigen Standard ISO/IEC 22301:2019 „Security and resilience – Business continuity management systems – Requirements".

Der 200-4 geht inhaltlich deutlich über den ISO/IEC 22301 hinaus und bietet eine Mischung aus Anforderungen, Umsetzungsvorschlägen und selbsterklärenden Texten. Sehr praktisch ist der Anforderungskatalog zum Standard 200-4 in Excel, der ein detailliertes Mapping auf die Anforderungen des ISO-Standards enthält, deren Erfüllung so nach Implementierung eines BCM-Systems (BCMS) nach 200-4 leichter nachgewiesen werden kann.

Da bereits der Vorgängerstandard 100-4 im Umfeld von MaRisk und KRITIS als Anforderungskatalog genutzt wurde, ist davon auszugehen, dass auch der 200-4 eine größere Rolle in der Finanzbranche spielen wird. Dabei eignet er sich für jedes Unternehmen, dass ein BCMS in deutscher Sprache aufbauen möchte.

Besonders wertvoll sind die sehr umfangreichen und ziemlich ausgereiften Hilfsmittel zum 200-4

wie Vorlagen und ein Kennzahlensystem. Einziger Wermutstropfen: Die thematische Struktur folgt nicht genau dem zertifizierbaren ISO 22301:2019.

Mobilfunk-Bewegungsdaten

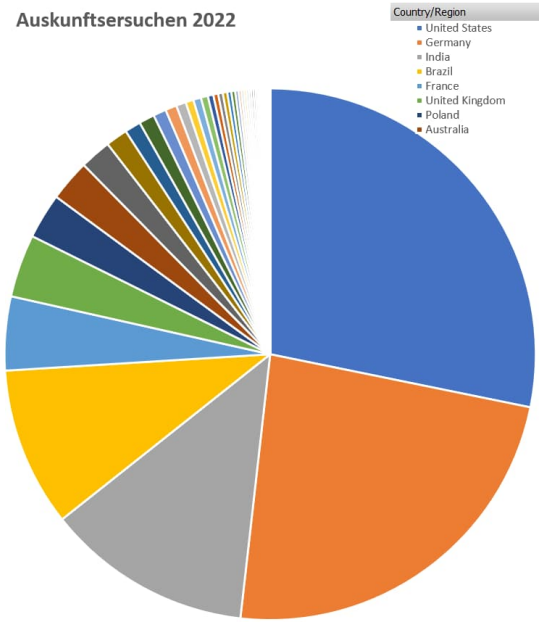
Die Mobilfunknetzbetreiber in Deutschland sammeln, analysieren und verkaufen die Bewegungen ihrer Kunden in anonymisierter Form zu Marketingzwecken an Drittunternehmen. Das ist nicht neu – wir berichteten darüber schon vor fast 15 Jahren (SSN 12/2008).

Durch das Schrumpfen der durchschnittlichen Größe einer Funkzelle in LTE-Netzen werden diese Daten immer genauer – in Städten geben sie ein ziemlich präzises Bewegungsprofil eines Mobilfunkteilnehmers, aus dem sich Wohnort, Arbeitsplatz, Einkaufsverhalten und Freizeitaktivitäten ablesen lassen.

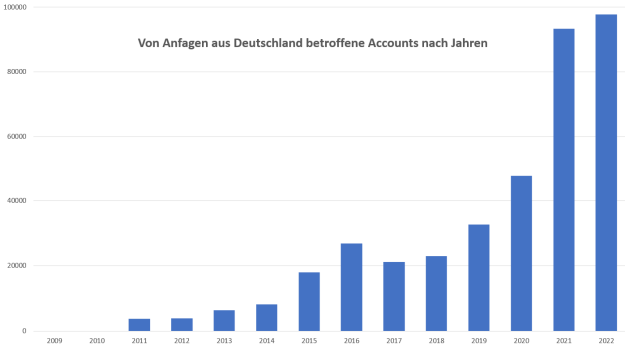
Zwar wirbt Telefónica mit einem dreistufigen Anonymisierungsverfahren; konkrete Informationen über dessen Funktionsweise möchten aber weder sie noch andere Netzbetreiber wie die Telekom herausgeben. Immerhin: Man kann der Verarbeitung der Bewegungsdaten widersprechen. Als Kunde von Telefónica (O2, Blau, Fonic, Simyo u. w.) muss man dafür eine (kostenlose) SMS mit dem Text „Abmelden“ an die Nummer 66866 senden. Telekom-Kunden (Congstar, Klarmobil u. w.) können über ein Opt-Out-Portal widersprechen.

Im Überwachungsstaat

Seit 2009 dokumentiert Google in seinem Transparenzbericht die weltweiten Auskunftsanfragen von behördlichen Stellen. Sieht man sich die Statistiken ein wenig genauer an, kommt man zu ernüchternden Einsichten: Es sind keineswegs die „Schurkenstaaten“, die Google mit Anfragen überhäufen: Auf die USA folgt mit weitem Abstand vor allen anderen 91 Ländern – Deutschland.



Auch steigt die Zahl der von deutschen Anfragen insgesamt betroffenen Accounts seit vielen Jahren. Willkommen im Überwachungsstaat.



Secorvo News

Überarbeitetes T.I.S.P.-Curriculum

Seit dem 01.07.2023 gilt für den TeleTrusT Information Security Professional ein umfangreich überarbeitetes Curriculum. Alle Inhalte wurden von den Anbietern auf den Prüfstand gestellt, aktualisiert, ergänzt oder gekürzt. Hinzu kamen zwei neue Module zu „Virtualisierung“ und „Cloud-Security“. Damit wurden die Inhalte des T.I.S.P.-Seminars zum dritten Mal an aktuelle Entwicklungen der Informationssicherheit angepasst.

In einem Beitrag in der iX 9/2023 stellt Stefan Gora das neue Curriculum des T.I.S.P. ausführlich vor.

Secorvo Seminare

Noch keine Weiterbildung in diesem Jahr besucht? Dann werfen Sie doch mal einen Blick auf unsere Fachseminare im Herbst – Infos und Anmeldung unter https://www.secorvo.de/seminare.

Authenticate. Generate. Repeat.

Das nächste KA-IT-Si-Event am **14.09.2023** (18 Uhr) in der IHK Karlsruhe 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 Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2023	
10.-13.08.	DEF CON 31 (DEFCON, Las Vegas/US)
19.-24.08.	Crypto 2023 (Santa Barbara/US)
September 2023	
11.-13.09.	heise devSec 2023 (dpunt.verlag, heise, Karlsruhe)
14.09.	Authenticate. Generate. Repeat. (KA-IT-Si, Karlsruhe)
18.-22.09.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-27.09.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
28.09.	IT-Sicherheitsrechtstag 2023 (Swiss Cyber Storm Association, Bern/CH)
Oktober 2023	
9.-12.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
10.-12.10.	it-sa 2023 (NürnbergMesse GmbH), Nürnberg
17.-19.10.	BSI Vorfall-Experte – Aufbauschulung (Secorvo, Karlsruhe)

Fundsache

Eine gute Hilfestellung bei der Prüfung von Auftragsverarbeitungsverträgen bietet die Checkliste des „Datenschutz-Gurus“ Rechtsanwalt Stephan Hansen-Oest.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, 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

secorvo
security consulting

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 Schnellstrasse 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.

Inhalt

secorvo
security consulting

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), 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

secorvo
security consulting

Secorvo Security News

September 2023

Morgengrauen

Seit dem Inkrafttreten der Datenschutz-Grundverordnung hat sich die Spannung zwischen Grundrechtschützern und (nicht allein staatlichen) Kontrollinteressen spürbar verschärft. Während einerseits engagierte Datenschützer wie Max Schrems von vielen klaren EuGH-Entscheidungen zu Gunsten des Persönlichkeitsschutzes Recht bekamen, fielen zugleich immer mehr Lebensbereiche der raumgreifenden digitalen Erfassung unseres Verhaltens zum Opfer: Kameras und GPS-Sensoren in Fahrzeugen, Nutzungsprofile in Cloud-Apps und Präferenzanalysen von Musik- und Video-Streaming-Diensten liefern inzwischen nicht nur ein lückenloses Bild unserer Tagesabläufe, sondern können sogar – meist auf der rechtlichen Grundlage von einmal erteilten und längst vergessenen Einwilligungen – unser zukünftiges Verhalten zuverlässig vorhersagen (siehe z. B. Churn Prediction).

Die wegweisenden EuGH-Entscheidungen zu Datentransfers, Tracking, Schadenersatzansprüchen und anderen wichtigen Datenschutz-Fragen kommen allerdings häufig spät und scheinen immer wieder der Realität hinterherzuhinken, während die Digitalisierung unseres Lebens sich ungebremst auszubreiten scheint. Aber manchmal kommt es eben doch anders als man denkt – und das gibt immer wieder Anlass zu Hoffnung. Denn Grundsatzentscheidungen hoher Gerichte können im Handstreich nicht nur ganze Klassen von Datenverarbeitungen für rechtswidrig erklären, sondern auch elementare Begehrlichkeiten und Haltungen. Daher ist das Urteil des Bundesverwaltungsgerichts vom 07.09.2023, mit dem die Vorratsdatenspeicherung endgültig für unzulässig erklärt wurde, in seiner Bedeutung kaum zu überschätzen. Das Signal ist eindeutig: Die Nutzung und Speicherung personenbezogener Daten für andere als die eigentlichen Zwecke der Erhebung ist unzulässig – und ist der Zweck erfüllt, sind die Daten zu löschen. Das gilt für Strafverfolgungsbehörden genauso wie für Unternehmen.

Inhalt

secorvo
security consulting

Security News

Gefährliche Zeitkorrekturen

2016 erweiterte Microsoft den Windows Time Service um die fragwürdige Fähigkeit, die korrekte Uhrzeit aus dafür nicht gedachten Feldern im TLS-Handshake auszulesen und eine abweichende Systemuhrzeit rigoros daran anzugleichen. Gedacht, um Probleme auf kleinen Endgeräten ohne batteriegestützte Hardwareuhr zu lösen, wurde das Feature jedoch so implementiert, dass es auch auf Servern greift. Und da sorgt es immer wieder für dramatische Probleme, wenn es etwa das Datum um 55 Tage in die Zukunft verlegt.

Microsoft verlässt sich für die Implementierung darauf, dass im Handshake die Unix-Zeit verwendet wird. Das steht aber schon seit 2013 in Frage und ist bspw. in OpenSSL deaktiviert. Dennoch hält Microsoft bis heute an dem Feature fest, hat aber immerhin dokumentiert, wie man es abschalten kann. Nicht nur wir, sondern auch einer von Microsofts Escalation Engineers empfiehlt, das auf Domain Controllern sowie auf allen Servern zu tun.

Passwörter in der Cloud

Passwortmanager helfen nicht nur, sich zahlreiche unterschiedliche Passörter zu merken, sondern auch, schlechte und bereits verwendete zu vermeiden. Cloudbasierte Lösungen wie 1Password oder LastPass sind derzeit weit verbreitet. Im November 2022 gelang es Hackern, Passwort-Datenbanken bei LastPass von den Cloudservern abzuziehen. Am 22.12.2022 gestand LastPass ein, den Schlüssel für einzelne Datenbanken mit viel zu wenig PBKDF2-Interationen aus dem Master-Passwort berechnet zu haben. Und am 28.08.2023 wurde bekannt, dass ein paar der Datenbanken mit Brute-Force-Angriffen entschlüsselt werden konnten. Den Einfluss der PBKDF2-Iterationen erläuterte daraufhin Wladimir Palant in seinem Blog: Sehr alte Datenbanken mit nur einer Iteration können in etwa 17 Stunden entschlüsselt werden; erst bei 100.000 Iterationen steigt der Aufwand auf rund 100.000 GPU-Jahre.

Softwareentwicklern, die nicht in dieselbe Falle tappen wollen, empfehlen wir die Teilnahme an einem T.P.S.S.E.-Seminar...

Dreimal Pieps und der Zug steht

Am 11.01.2008 berichtete The Telegraph, wie ein Jugendlicher im polnischen Łódź mit einer TV-Fernbedienung U-Bahn-Weichen umgestellt und so mindestens eine Entgleisung verursacht hatte (SSN 01/2008). Sicherer ist die Technik auch 15 Jahre später nicht: Am 26.08.2023 meldete die BBC, dass (mutmaßlich mit Russland verbundene) Hacker bei etwa zwanzig polnischen Zügen eine Notbremsung ausgelöst hatten, indem sie per Funk drei kurze Signaltöne sandten. Erst im kommenden Jahr soll die unsichere analoge UKW-Funktechnik in Polen durch GSM-R ersetzt werden.

Ein Beispiel für Risiken, die aus der oft sehr langen Betriebszeit solcher analogen Systeme erwachsen – vermutlich findet sich ähnlich archaische Technik auch noch anderswo auf der Welt in sicherheitsrelevanten Umgebungen.

Quod licet Iovi...

Inzwischen gibt es zahlreiche gesetzliche Regelungen und Rechtsprechung zur optischen und inhaltlichen Gestaltung von Cookie-Bannern (siehe zuletzt SSN 8/2023). Probleme mit der rechtskonformen Anpassung der Banner sowie dem Einwilligungsmanagement hat jedoch offenbar die öffentliche Verwaltung: Hier stolpert man immer wieder über unzulässige Lösungen. Ursache dafür mag sein, dass öffentliche Stellen im Unterschied zu Unternehmen bei Datenschutzverstößen keine Bußgelder fürchten müssen (SSN 6/2022). Unzulässiges Tracking und rechtswidrige Cookie-Banner sind aber ein rechtswidriger Grundrechtseingriff und daher inakzeptabel.

Um diesem Missstand einen Riegel vorzuschieben, richten wir gerade einen „Banner-Pranger“ ein. Dort sollen ausgewählt schöne Beispiele wie die Cookie-Banner der Regierungspräsidien Baden-Württemberg, der baden-württembergischen Gerichte oder der rekordverdächtige Abwahl-Banner des Guinness Buchs der Rekorde öffentlich gemacht werden. Wir freuen uns auf Ihre Einreichungen und Vorschläge (redaktion-security-news@secorvo.de)!

Wenn aus Apps Trojaner werden

Hin und wieder werden SmartPhone-Apps mit guter Reputation von ihren Entwicklern an Dritte verkauft, die die Anwendung um Funktionen ergänzen, die nicht im Interesse der Nutzer sind. So berichtete ESET Research am 23.05.2023, dass die Android-App iRecorder vermutlich schon im August 2022 über ein Update zu einem Spionagetrojaner erweitert wurde. Ähnliches passierte kürzlich auch einer Mac-Anwendung: Die eigentlich überflüssig gewordene App NightOwl, die noch auf vielen Macs installiert ist, wurde vom Käufer über ein automatisches Update einem Botnet hinzugefügt. Sofern die Zusatzfunktion weitere Berechtigungen benötigt, werden die immerhin über das Betriebssystem zur Freigabe angefragt. Ein solches Pop-Up-Fenster nach einem Update sollte daher alarmieren und nicht zur reflexartigen Freigabe verleiten.

Recht sicher, nicht rechtssicher

Mit dem am 10.07.2023 veröffentlichten EU-US Data Privacy Framework (DPF) hat die EU-Kommission einen neuen Angemessenheitsbeschluss gefasst. Die Datenschutzkonferenz der deutschen Aufsichtsbehörden (DSK) hat nun Anwendungshinweise zum DPF veröffentlicht, in denen sie die wesentlichen Hintergründe und Inhalte erläutert, u. a. die neu geschaffenen Rechtsschutzmöglichkeiten für betroffene Personen sowie die Schaffung von geeigneten Garantien, sofern der Auftragsverarbeiter nicht DPF-zertifiziert ist.

Vom Votum der DSK weicht der Thüringer LfDI mit einer eigenen Stellungnahme ab: Er hat insbesondere bei zertifizierten Unternehmen Bedenken, da diese lediglich eine Selbstzertifizierung durchführen, die ausschließlich im Beschwerdefall geprüft werden werde. Auch bestünde weiterhin die Gefahr einer rechtswidrigen Datenverarbeitung durch US-Behörden bei Strafverfolgung und in Fällen der „nationalen Sicherheit". Zudem schließt er sich den von Max Schrems geäußerten Kritikpunkten an.

Trotz der Anerkennung durch die EU-Kommission sollten Übermittlungen personenbezogener Daten in die USA auch weiterhin sehr zurückhaltend erfolgen, denn wir teilen die Einschätzung des Thüringer LfDI, dass „die Wahrscheinlichkeit, dass der Europäische Gerichtshof den Adäquanzbeschluss aufheben wird, (...) recht hoch" ist. Anfang September reichte der französische Parlamentarier Philippe Latombe als Privatperson Klage beim EuGH ein, und Max Schrems hat angekündigt, vor nationalen Gerichten gegen Unternehmen zu klagen, die sich bei der Übermittlung von personenbezogenen Daten in die USA auf das DPF berufen.

Secorvo News

Silbernes Jubiläum

Vor 25 Jahren, am 01.09.1998, erblickte Secorvo das Licht der Welt – und zählt damit zu den ältesten IT-Security-Dienstleistern in Deutschland.

Mit weit über 2.000 erfolgreichen Projekten für fast 1.000 deutsche und internationale Unternehmen, rund 450 Fachveröffentlichungen und vielen hundert Fachveranstaltungen mit insgesamt rund 35.000 Teilnehmern sowie 1.000 Seiten „Secorvo Security News" blicken wir ein wenig stolz auf dieses Vierteljahrhundert zurück – und freuen uns, in dieser Zeit wirksam zu Informationssicherheit und Datenschutz in Deutschland beigetragen zu haben.

Wir danken unseren Kunden für das in uns gesetzte Vertrauen und allen ehemaligen und derzeitigen Mitarbeiterinnen und Mitarbeitern für ihren engagierten und kompetenten Einsatz – und freuen uns auf ein weiteres Vierteljahrhundert, in dem wir diese Welt noch ein kleines Stück besser machen.

Secorvo Seminare

Sichern Sie sich noch einen der letzten freien Plätze auf unserem T.I.S.P.-Seminar vom **13.–17.11. 2023.** Profitieren Sie vom Wissenstransfer in über 20 Modulen des aktuellen Curriculums und lassen Sie sich im Anschluss zertifizieren. Die **vierte Auflage** unseres T.I.S.P.-Begleitbuchs wird Anfang 2024 erhältlich sein.

Wer Software-Entwicklung sicher gestalten will, dem bieten wir mit unserem neu konzipierten T.P.S.S.E.-Seminar **vom 27. bis 30.11.2023** jede Menge Inhalte mit Praxisbezug und interaktiven Workshops – und im Anschluss auch hier die Möglichkeit, sich zertifizieren zu lassen.

Planen Sie schon Ihre Weiterbildung für nächstes Jahr? Dann werfen Sie doch einen Blick in unseren Seminarkalender 2024. Wir freuen uns auf Ihre Anmeldung!

RaaS – Ransomware as a Service

Was McDonald's mit Ransomware gemeinsam hat und wie mit dem Geschäftsmodell „Ransomware-as-a-Service" auch technisch weniger versierte Akteure mit leistungsstarken Angriffstools zu erfolgreichen Cyberkriminellen werden können, stellt Martin Dukek vom Kompetenzzentrum IT-Sicherheit beim nächsten KA-IT-Si-Event im House of Living Labs (FZI) vor.

Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum intensiven Buffet-Networking. Wir freuen uns auf Sie am **12.10.2023** um 18 Uhr! (Zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Oktober 2023	
10.-12.10.	it-sa 2023 (NürnbergMesse GmbH, Nürnberg)
12.10.	RaaS – Ransomware as a Service (KA-IT-Si, Karlsruhe)
24.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
November 2023	
7.-8.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
7.-9.11.	IDACON 2023 (WEKA-Akademie, München)
13.-17.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-30.11.	ACM CCS 2023 (ACM/SIGSAC, Kopenhagen/DK)
27.-30.11.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Fundsache

Durch das EuGH-Urteil vom 30.03.2023 steht § 26 BDSG auf tönernen Füßen. Die FAQs des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg zeigen alternative Rechtsgrundlagen zur Verarbeitung von Beschäftigtendaten.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, 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

secorvo
security consulting

Secorvo Security News

Oktober 2023

Herrschaftswissen

Der Philosoph *Max Scheler* (1874-1928) definierte in seiner Anthropologie Herrschaftswissen als das Wissen, das der Stabilisierung einer Herrschaft und deren Machtbestrebungen dient.

Im Kern ist darunter jeder Wissensvorsprung zu verstehen, der in diesem Sinne vorteilhaft für den Wissenden ist. Jede Herrschaft ist bestrebt, sich mit solchen exklusiven Wissensvorsprüngen zu stabilisieren – je prekärer die Legitimation, je geringer der Rückhalt bei den Beherrschten und je größer die äußere Bedrohung, desto stärker dieses Bestreben. Spionage, nach außen und nach innen, ist daher die logische Folge jeder Herrschaft – vor allem einer prekären.

Da Herrschaftswissen in der Hand der Herrschenden eine mächtige Waffe sein kann, versuchen Demokratien, Herrschaftswissen überall dort zu begrenzen, wo es der Exekutive Macht über den eigentlichen Souverän – das Volk – gibt. Aus dieser Perspektive lässt sich Datenschutz verstehen als eine systematische Begrenzung des Herrschaftswissens über Menschen: Die Forderung einer Rechtsgrundlage für die Verarbeitung, die strikte Zweckbindung und strenge Löschfristen sollen verhindern, dass solches Herrschaftswissen überhaupt erst entsteht.

Auch im sozialen Miteinander soll Datenschutz die Allokation von Herrschaftswissen zumindest erschweren, denn ein Airtag, der einem Stalker den Aufenthaltsort seines Opfers verrät, ist ein ähnlich starkes Machtinstrument wie eine Spionage-Drohne oder ein versteckter GPS-Sender. Daher sollte dem Verbot der anlasslosen Vorratsdatenspeicherung (BVerwG 6 C 6.22/7.22) nun auch bald ein Verbot der Nutzung von Informationstechnik zur heimlichen Feststellung des aktuellen Aufenthaltsorts von Personen folgen.

Auf kurze Löschfristen sollte man auch bei jeder App achten, die personenbezogene Daten speichert. In die falschen Hände geraten können auch sie – und damit zu Herrschaftswissen mutieren.

Inhalt

secorvo
security consulting

Security News

Konfigurationsfehler

Am 05.10.2023 stellten CISA und NSA eine gemeinsame Übersicht der Top Ten Cybersecurity Misconfigurations. Einige der aufgelisteten Konfigurationsfehler scheinen auf den ersten Blick ein alter Hut zu sein: In der Praxis ermöglichen aber offensichtlich eben diese alten Hüte immer wieder Einbrüche in IT-Infrastrukturen. Das Dokument enthält detaillierte Ursachenanalysen und Gegenmaßnahmen für die identifizierten Top Ten. Dabei wird immer wieder auf die hilfreichen Werkzeuge Mitre ATT&CK und Mitre D3FEND verwiesen.

Die Hartnäckigkeit der Schwachstellenmuster im Betrieb ähnelt der der Weaknesses in der Software-Entwicklung. Vielleicht sollten sie ähnlich exponiert und populär kommuniziert werden, wie es Mitre mit den CWE vormacht.

Schwachstellenschwemme

Die National Vulnerability Database des NIST weist für Oktober 2023 erneut über 2000 neu veröffentlichte Schwachstellen aus. Mindestens zehn dieser Verwundbarkeiten werden bereits aktiv ausgenutzt. Betroffen sind u. a. der Netscaler (Citrix) und Confluence (Atlassian). Besonders kritisch ist die mit dem Maximalscore 10.0 bewertete Cisco-IOS-XE-Lücke, da die Admin-Schnittstelle von Tausenden von Switches und Routern über das Internet erreichbar ist (siehe NET.3.1.A4, BSI-Grundschutz) und die Geräte daher ein leichtes Opfer sind. Dabei wären viele Lücken vermeidbar, etwa beim Cisco Emergency Responder, der mit einem Standard-Admin-Passwort ausgeliefert wurde.

Secure by Design – Joint Effort

Am 25.10.2023 hat die US-amerikanische CISA vor dem Hintergrund einer nicht nachlassenden Anzahl von Security-Schwachstellen in Produkten nachdrücklich auf die Handreichung Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software hingewiesen. Darin haben viele internationale Sicherheitsbehörden grundlegende Bausteine für sichere Software-Produkte übersichtlich zusammengestellt. Die Hinweise wurden im April 2023 vom BSI vorgestellt.

Wir empfehlen nachdrücklich, die darin vorgestellten Prinzipien ernst zu nehmen – auch vor dem Hintergrund der Anforderungen, die voraussichtlich mit dem Cyber-Resilience-Act an die Sicherheit von Software gestellt werden.

Das Thema Secure by Design Software ist auch ein Baustein im T.P.S.S.E.-Seminar, das sich umfassend mit Sicherheit in der Software-Entwicklung beschäftigt – die Bekämpfung von Schwachstellen also von der Wurzel aus angeht.

Meinungsmache

Am 04.09.2023 veröffentlichte die Mozilla Foundation eine „Studie", nach der moderne Autos ein „Datenschutz-Albtraum" seien. Mehrere Medien zitierten die Veröffentlichung, darunter der heise-Newsticker. Befasst man sich jedoch eingehender mit dem Text (vulgo: liest man ihn…), kommt man schnell zu dem Ergebnis, dass von einer systematischen Analyse keine Rede sein kann – die „Forschungsergebnisse" sind Resultat einer Durchsicht der Datenschutzerklärungen von 25 Herstellern und einer offenbar vorurteilsbeladenen und kompetenzbefreiten Sicht der Autoren. Zitat: „Automarken stellen mit Ihren persönlichen Daten oft alles Erdenkliche an, was noch irgendwie im rechtlichen Rahmen zulässig ist." Oder: „Am meisten Sorgen macht uns, dass wir nicht einmal wissen, ob überhaupt eine der geprüften Marken alle persönlichen, im Auto gespeicherten Daten verschlüsselt." Die anhängenden Vitae der Autoren lassen ebenfalls kein Expertenwissen im Datenschutz erkennen – die Autoren sehen sich selbst als „investigative Storyteller".

Undifferenzierte und inkompetente Positionspapiere dieser Art stiften mehr Schaden als Nutzen, machen sie es doch leicht, die Kritik als Scharlatanerie abzutun. Denn in einigen Punkten ist fundierte Kritik durchaus berechtigt – und tatsächlich sollten die Datenschutzerklärungen vieler Hersteller durchaus aussagekräftiger sein.

Auskunftsrecht

Das Recht eines jeden Menschen auf Auskunft über Verarbeitungen seiner personenbezogenen Daten ist in Art. 8 der EU-Grundrechtscharta verankert. In der Folge wurde 2013 das Recht auf Einsichtnahme in die eigene Patientenakte als § 630g ins Bürgerliche Gesetzbuch aufgenommen. Seitdem wurde allerdings immer wieder über die Frage gestritten, ob ein Patient die Kosten des Kopierens der Akte tragen muss.

Am 26.10.2023 hat nun der EuGH diese Frage abschließend höchstrichterlich beantwortet – mit einem klaren „Nein". Die Kosten der (ersten) Kopie einer Patientenakte sind vom Arzt bzw. der Klinik zu tragen (C-307/22). Das ist ein Sieg der Transparenz – der aber auch zu einer erheblichen Belastung medizinischer Einrichtungen werden kann, wenn viele Patienten eine Kopie anfordern.

Die Entscheidung des EuGH könnte daher die Digitalisierung im Gesundheitswesen beschleunigen, denn eine elektronische Gesundheitsakte würde nicht nur die Archivierung, sondern auch die Beauskunftung erheblich vereinfachen.

HSM-Restrisiko

Es ist immer eine gute Idee, wichtige Schlüssel in einem Hardware Security Modul (HSM) zu halten – beispielsweise solche, mit denen Zertifikate oder Authentication-Token signiert werden. Das alleine garantiert aber noch keine vollständige Sicherheit. Zu berücksichtigen ist auch, wer über die Schlüssel im HSM verfügen darf: Bei mindestens einem (verbreiteten) HSM-Modell darf das jeder Benutzer auf dem Windows-Server, an den das HSM angeschlossen ist.

Hans-Joachim Knobloch (Secorvo) erläutert diesen Schwachpunkt in seinem Blog-Artikel vom 06.10. 2023 und zeigt, wie man sich darüber ein Goldenes Zertifikat von einer Microsoft-CA erschleichen könnte – falls der CA-Server nicht so gehärtet ist, dass sich nur berechtigte Administratoren anmelden können. In der Tradition der einschlägigen Angriffsvektoren ESC1 bis ESC11 hat er diesen „ESC12“ getauft.

Website Evidence Collector

Bereits am 22.10.2019 wurde der Website Evidence Collector des Europäischen Datenschutzbeauftragten von der International Conference of Data Protection and Privacy Commissioners (ICDPPC) mit dem Global Privacy and Data Protection Award für Innovation ausgezeichnet. Das Tool für die automatische Überprüfung der Erhebung und des Schutzes personenbezogener Daten auf Websites kann Belege für die Verarbeitung personenbezogener Daten (wie Cookies) oder Anfragen an Dritte erzeugen.

Es lädt ohne weitere Benutzerinteraktion nacheinander alle im Besuch einer URL enthaltenen Webseiten. Dabei werden unter anderem Screenshots der Seiten angefertigt und Listen der http-Links, der besuchten Webseiten, der im lokalen HTML5-Speicher gehaltenen Informationen, aller Cookies, des http-Verkehrs sowie alle über Web Sockets ausgetauschten Nachrichten erzeugt.

Das unter der EU Public Licence (EUPL 1.2) veröffentlichte Tool ist auf GitHub für Linux, macOS und Windows zum Herunterladen verfügbar. Es ermöglicht eine schnelle und einfache Prüfung von Webseiten: Bleibt zu hoffen, dass es nicht für automatisierte Abmahnwellen missbraucht wird.

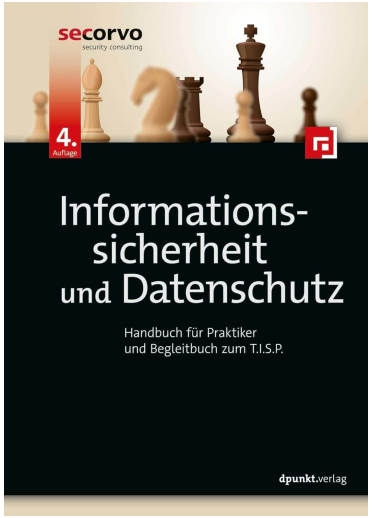
Secorvo News

Secorvo Seminare

Last but not least: Mit unserem neu konzipierten T.P.S.S.E.-Seminar beschließen wir vom **27. bis 30.11.2023** das Seminarjahr 2023: Vier Tage interaktive Workshops und jede Menge Inhalte mit Praxisbezug rund um die sichere Software-Entwicklung.

Die nächste Chance für Ihre T.I.S.P.-Zertifizierung bieten wir Ihnen auf unserem T.I.S.P.-Seminar vom **11. bis 15.03.2024**: Wissenstransfer aus über 20 Modulen des jüngst aktualisierten Curriculums. Dazu erscheint Anfang 2024 die **vierte Auflage** unseres T.I.S.P.-Begleitbuchs im dpunkt-Verlag.

Bevor wir Sie in die Adventszeit entlassen, werfen Sie doch noch einen Blick in unseren Seminarkalender 2024. Wir freuen uns auf Ihre Anmeldung!



Passe partout

Je mehr kryptografische Zertifikate als Authentifikationsmechanismus genutzt werden, desto kritischer sind Konfigurations- oder Implementierungsfehler, die es Angreifern ermöglichen, gefälschte Zertifikate als „Dietrich“ zu benutzen. Das hat erst kürzlich der Diebstahl eines „Generalschlüssels“ zur Microsoft Cloud gezeigt (siehe SSN 8/2023).

Beim Jahresabschlussevent 2023 der KA-IT-Si am **23.11.2023** werden Hans-Joachim Knobloch und Oliver Oettinger (Secorvo) aktuelle Angriffe auf das Active Directory mit solchen „Goldenen Zertifikaten“ demonstrieren und zeigen, wie man sich davor schützen kann. Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum Networking am Buffet.

Wir freuen uns auf Sie im Haus der Wirtschaft der IHK Karlsruhe – und empfehlen (wie immer) eine schnelle Anmeldung...

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2023	
23.11.	Passe partout (KA-IT-Si, Karlsruhe)
26.-30.11.	ACM CCS 2023 (ACM/SIGSAC, Kopenhagen/DK)
27.-30.11.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Dezember 2023	
04.-07.12.	Black Hat Europe 2023 (Blackhat, London/UK)
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 (DFN-CERT, Hamburg)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, 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

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

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