Secorvo Security News

November 2022

Festgebissen

Was die Animosität ausgelöst hat, wird sich kaum mehr feststellen lassen. Sicher ist: Die deutschen Aufsichtsbehörden haben sich auf Microsoft eingeschossen, wie die aktuelle Entscheidung der Datenschutzkonferenz (DSK) zu MS 365 vom 24.11.2022 belegt. Wie berechtigt die Kritik auch einmal gewesen sein mag: Sie bewirkte schon vor 20 Jahren einen Strategiewechsel bei Microsoft. Nicht nur, dass Microsoft sich bereits 2007 (!) beim ULD mit dem „Update Service 6.0" und „WSUS 2.0" für ein Datenschutz-Gütesiegel qualifizierte. Microsoft war auch der erste amerikanische Software-Riese, der 2014 mit auf das EU-Recht abgestimmten Verträgen für Office 365 auf Servern in Irland warb – lange bevor Cisco, Amazon oder Google auch nur das Problem verstanden hatten. Secorvo war seitdem bei vielen Unternehmen an der Abstimmung von MS 365-Verträgen gutachterlich oder mit einer DSFA beteiligt, und ich erinnere mich gut an meine eigene Überraschung über die hohe Qualität und Transparenz der Unterlagen von Microsoft. Seitdem hat Microsoft wiederholt nachgelegt, z. B. mit der Reaktion auf das Schrems-II-Urteil (New steps to defend your data und Initiative Tech fit 4 Europe) oder der Ankündigung einer „EU Data Boundary" für die MS-Cloud am 06.05.2021. Auch zum CLOUD Act hat Microsoft Position bezogen und bemüht sich um möglichste Transparenz, z. B. durch Veröffentlichung aller Law Enforcement Requests.

Man mag argwöhnen, dass das substanzloses Marketing-Geklapper ist. Aber ist das plausibel? Anders als die US-Internet-Giganten lebt Microsoft nicht von Nutzerdaten. Im Gegenteil: Ein einziger begründeter Verdacht, dass Microsoft trotz seiner Zusicherungen Kundendaten missbraucht, würde den gesamten europäischen Markt zusammenbrechen lassen. Dem Datenschutz wäre mehr gedient, wenn die DSK sich endlich die erklärten Feinde des Datenschutzes vornehmen würde, anstatt das erkennbare Bemühen Microsofts mit fadenscheinigen Einwänden zu entmutigen.

Security News

Abgelaufen

Eine Möglichkeit, die Übermittlung personenbezogener Daten in Drittländer (also Ländern außerhalb des europäischen Wirtschaftsraums) ohne ein anerkannt gleichwertiges Datenschutzniveau rechtskonform zu gestalten ist der Abschluss eines Vertrags nach den von der EU Kommission vorgegebenen Standardvertragsklauseln. Die „alten" Standardvertragsklauseln aus dem Jahr 2001 wurden als Folge des Schrems-II-Urteil des EuGH mit Durchführungsbeschluss 2021/914 vom 04.06.2021 abgelöst (siehe SSN 6/2021). Bis zum 27.12.2022 müssen alle bestehenden Verträge auf die neuen Standardvertragsklauseln für internationalen

Datentransfer umgestellt werden. Altverträge werden nach dem zweiten Weihnachtstag automatisch unwirksam – und damit die betroffene Datenübermittlung rechtswidrig.

Abgesichert

Die wachsende Bedeutung des Schutzes von Software Supply Chains wurde erst kürzlich durch die Veröffentlichung des Enduring Security Frameworks der NSA vom 24.08.2022 deutlich. Dabei spielen Code-Signaturen zum Schutz der Authentizität und Integrität von Software eine zentrale Rolle. Doch bis vor kurzem galten für Code-Signing noch Bedingungen, die denen der „Prä-LetsEncrypt-Ära" für Web-Zertifikate entsprachen: kompliziert, aufwändig, teuer. Besonders Open-Source-Entwickler scheuten den Aufwand zur Schlüsselverwaltung und Beschaffung von Zertifikaten. Das könnte sich nun ändern: Das am 17.11.2022 von Newman, Meyers und Torres-Arias veröffentlichte Open-Source-Projekt „Sigstore" – inspiriert durch Let's Encrypt – könnte die Hürden für Code-Signaturen deutlich senken. Dahinter steckt eine Sammlung von Werkzeugen, mit deren Hilfe Code(fragmente) extrem einfach signiert und zur Prüfung in Transparency Logs veröffentlicht werden können. Unter der etwas irreführenden Bezeichnung „keyless signing" arbeitet Sigstore mit Einmalschlüsseln, für die nach einer Bestätigung der Identität des Entwicklers über OpenID-Connect ein kurzlebiges Zertifikat ausgestellt wird. Mit diesem kann ein Codefragment signiert, im Log veröffentlicht und von jedermann auf Gültigkeit überprüft werden. Sigstore übernimmt das Schlüsselmanagement für den Entwickler. Dieser muss sich lediglich um den Schutz seiner OpenID kümmern.

Abgemeldet

Der Messenger-Dienst WhatsApp bedient sich bekanntlich (SSN 4/2016) am Adressbuch des Smartphones und lädt auch die Namen und Telefonnummern von Personen hoch, die weder bei WhatsApp noch bei Instagram oder Facebook ein Benutzerkonto haben. Zu diesen Personen erstellt Meta ein sogenanntes Schattenprofil.

Bisher waren die Möglichkeiten begrenzt, das zu verhindern. Verwehrt man WhatsApp den Adressbuchzugriff, wird bei jeder Nachricht nur noch die Telefonnummer des Absenders angezeigt – eine erhebliche Komforteinbuße.

Zwar steht Betroffenen nach der DSGVO ein Recht auf Löschung zu, jedoch werden die Daten nach einer Löschung beim nächsten Adressbuchabgleich erneut an Meta übermittelt. Und der Versand von Unterlassungserklärungen an alle eigenen Telefonbuchkontakte ist keine besonders freundschaftserhaltende Option.

Am 31.10.2022 berichtete Shona Ghosh bei Businessinsider, dass Meta offenbar seit Mai 2022 „Nicht-Kunden" eine Möglichkeit bietet, im globalen Meta-Adressbuch nach der eigenen Telefonnummer oder E-Mail-Adresse zu suchen – und sie auf Wunsch löschen und in eine „Blacklist" aufnehmen zu lassen. Der Link ist in den „Informationen für Personen, die keine Meta-Produkte nutzen" versteckt – im Absatz „Klicke

hier, wenn du eine Frage zu den Rechten hast, die dir möglicherweise zustehen." Irreführender geht es kaum.

Abgemahnt

Die systematischen und automatisierten Abmahnungen von Webseitenbetreibern wegen der Einbindung von Google Fonts (SSN 8/2022) reißen nicht ab. Neuerdings enthalten einige Abmahnschreiben neben Schmerzensgeldanspruch und Gebührenrechnung auch noch ein Auskunftsersuchen.

Zwar sind Zweifel angebracht, dass die Erheblichkeitsschwelle für die Geltendmachung eines Schadensersatzanspruchs überschritten ist (vgl. OLG Frankfurt/Main, Urteil v. 30.06.2022, 16 U 229/20). Einem Auskunftsersuchen hingegen ist unabhängig davon nachzukommen. Allerdings muss der Betroffene dafür seine Identität nachweisen. Stellt sich jedoch heraus, dass die Berufung auf die Betroffenenrechte missbräuchlich erfolgt, besteht auch keine Auskunftspflicht.

Abgelehnt

Am 24.11.2022 veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Zusammenfassung des Berichts zum datenschutzkonformen Einsatz von Microsoft 365 und stellt fest, „dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, (...) nicht geführt werden kann." Kernpunkt der Kritik ist weiterhin die Datenverarbeitung von Microsoft für legitime Geschäftszwecke und die angebliche Unmöglichkeit, der Rechenschaftspflicht als Auftragsverarbeiter beim Einsatz von Microsoft 365 wegen intransparenter Datenverarbeitungen durch Microsoft nachzukommen.

Hier verliert die DSK völlig aus dem Blick, welche Anforderungen vernünftigerweise an eine Auftragsverarbeitung zu stellen sind. Dass ein Unternehmen zur Erfüllung der Rechenschaftspflicht seines Auftraggebers sämtliche Datenverarbeitungen und damit auch gegebenenfalls Geschäftsgeheimnisse offenlegen soll, ist nicht nachvollziehbar. Unberücksichtigt bleibt auch, dass Microsoft eine bestimmte Menge an Diagnose- und Telemetriedaten verarbeiten muss, um die angebotenen Dienste überhaupt vertragsgemäß erbringen zu können. Warum die DSK zudem nicht die angekündigten Neuerungen in Sachen EU Data Boundary abgewartet hat, ist nicht zu verstehen.

Microsoft hat in einer Stellungnahme bereits auf die Verlautbarung reagiert und die Kritik (erwartungsgemäß) zurückgewiesen. Für Verantwortliche aus dem öffentlichen Sektor bringt das DSK-Papier viel Arbeit mit sich, wenn sie Microsoft 365 dennoch datenschutzkonform einsetzen möchten – möglich bleibt das jedoch, aller Kritik zum Trotze.

Abgestraft

Im Jahr 2018 hatten 40 (!) US-amerikanische Bundesstaaten Google wegen der heimlichen Sammlung von Standortdaten verklagt. Auslöser war ein Bericht von Keith Collins vom 21.11.2017, in dem er aufdeckte,

dass Android seit Anfang 2017 auch bei abgeschalteten Location Services und sogar ohne eingelegte SIM-Karte Standortinformationen in Gestalt der Cell ID der Mobilfunkzellen in Reichweite sammelt und an Google übermittelt, sobald das Smartphone wieder online ist.

Nach vier Jahren wurde Google nun am 14.11.2022 zur Zahlung einer Geldstrafe von 391,5 Mio. US$ verurteilt – ein historisches Urteil, nicht nur wegen der Höhe der Strafe, sondern weil es zeigt, dass sich auch in den USA langsam eine Sensibilität für die Schutzwürdigkeit der Privatsphäre entwickelt.

Secorvo News

E-Mail-Tracking

Das Nachverfolgen (Tracking) von Webseitenbesuchen und die Erstellung von Besucherprofilen stehen schon lange im Fokus des Datenschutzes und müssen von Anbietern via Cookie-Banner transparent gemacht werden. Tracking und Profiling bei E-Mails sind hingegen bisher der Aufmerksamkeit von Aufsichtsbehörden entgangen – obwohl sie bei E-Mail-Newslettern inzwischen üblich sind. Meist erfolgt das heimlich – und verstößt somit gegen geltendes Datenschutzrecht.

Am 03.11.2022 gaben Christian Blaicher und Milan Burgdorf beim KA-IT-Si-Event „Gotcha. E-Mail-Tracking und -Profiling" einige vertiefte technische und rechtliche Einblicke in das Thema. Dabei ging es einerseits darum, wie Unternehmen E-Mail Tracking und Profiling innerhalb der Grenzen der DSGVO und des TTDSG rechtskonform gestalten können. Andererseits wurde erläutert, wie sich Empfänger solcher E-Mails sowohl rechtlich als auch technisch davor schützen können. Die Referenten haben das Wichtigste in einem Handout zusammengefasst.

Sollten Sie den Vortrag verpasst haben: Christian Blaicher wird zu dem Thema auf der DFN-Konferenz „Sicherheit in vernetzten Systemen" am 09.02.2023 um 14 Uhr in Hamburg vortragen.

Seminarprogramm 2023

Seit Ende November ist der Secorvo-Seminarkalender 2023 online – just in time für Ihre frühzeitige Weiterbildungsplanung im kommenden Jahr.

Lernen wird überbewertet

Vor rund einem Jahr sorgte die Schwachstelle log4j für erhebliche Aufregung. Der Auslöser ist mittlerweile beseitigt, und viele der betroffenen Softwareprodukte wurden von den Herstellern gepatcht. Doch die tiefere Ursache des Problems besteht weiterhin. Denn die Schwachstelle war gar kein Fehler, sondern eine gewünschte Funktionalität, die über viele Jahre in der Bibliothek enthalten war.

Das eigentliche Problem bestand darin, dass eine komplexe und leistungsfähige Bibliothek für sehr einfache Aufgaben eingesetzt und an der Schnittstelle nutzergenerierte Inhalte ohne Input-Validierung übergeben wurden. Verursacher war also nicht log4j, sondern die Tatsache, dass die Bibliothek verwendet wurde, ohne

zuvor zu prüfen, ob die Funktionalität überhaupt gebraucht wird.

Security-by-Design geht anders, wie Johann Grathwohl (CONITAS) auf dem kommenden KA-IT-Si-Event am **08.12.2022** in seinem Vortrag „Log4j und was wir (nicht) daraus gelernt haben" zeigen wird. Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Dezember 2022	
05.-08.12.	Black Hat Europe 2022 (Blackhat, London/UK)
08.12.	Lernen wird überbewertet (KA-IT-Si, virtuell)
Januar 2023	
20.-22.01.	ShmooCon 2023 (The Shmoo Group, Washington/US)
Februar 2023	
08.-10.02.	30. DFN-Konferenz „Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg)
13.-16.02.	OWASP 2023 Global AppSec (OWASP Foundation, Dublin/IRL)
März 2023	
14.-16.03.	secIT 2023 (Heise Medien, Hannover)
21.-22.03.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
27.-31.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Am 11.11.2022 veröffentlichte die ENISA die TOP 10 aufkommenden Cybersicherheitsbedrohungen bis 2030. Neben aktuell diskutierten Bedrohungen wie gefährdeten Lieferketten oder Desinformationskampagnen werden darin auch der Missbrauch intelligenter Geräte oder künstlicher Intelligenz und Lösungen für die erwarteten Herausforderungen in der Cybersicherheit beschrieben.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Milan Burgdorf, 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