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.

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