Secorvo Security News

Februar 2025

Datenschutz tötet doch!

Der Datenschutz hat sein erstes Todesopfer gefordert – zum Glück kein menschliches, sondern ein technisches: das gute alte Fax.

Vor fünf Jahren wurde in Österreich das Gesundheitstelematikgesetz verabschiedet, das das Ende des Faxes im Gesundheitssystem zum 01.01.2025 besiegelte. Die Umsetzung kam, wie könnte es anders sein, für alle Beteiligten völlig überraschend. Daher gelang es auch nicht, sich rechtzeitig auf ein einheitliches sicheres Kommunikationssystem zur Ablösung des Faxes zu einigen. Den verschiedenen Parteien im Gesundheitssystem stehen nun viele verschiedene Möglichkeiten zur Kommunikation zur Verfügung, sodass es jeweils zunächst einer Abstimmung bedarf, ob über das Gesundheitspartnerportal, via FTAPI, DaMe oder gar per Ende-zu-Ende-verschlüsselter E-Mail kommuniziert werden kann und soll.

Auch in Deutschland wird immer wieder ein Faxverbot für personenbezogene Daten diskutiert und von einzelnen Aufsichtsbehörden forciert. Dienste wie KiM (Kommunikation in der Medizin) haben sich jedoch bisher nicht durchgesetzt. Dabei wäre das tatsächlich wichtig, denn eine Fax-Übertragung ist nicht nur nach heutigen Maßstäben technisch unsicher, sondern auch fehleranfällig: Eine falsche Ziffer, und der kritische und hochsensible Laborbefund landet beim Bauunternehmer statt in der Klinik.

Zunächst kommt es daher darauf an, sich auf ein sicheres, unkompliziertes und in der Praxis funktionierendes Verfahren zur Übermittlung vor allem medizinischer Daten zu einigen. Denn wenn – wie jetzt in Österreich – Befunde, Röntgenbilder etc. nur noch in Papierform oder auf USB-Sticks per Post oder Kurier verschickt werden dürfen, dann ist möglicherweise doch nicht auszuschließen, dass Professorin Buyx Recht hat und durch ein datenschutzkonformes Verbot von Faxen Menschenleben gefährdet werden.

Security News

Nur ein einziger Buchstabe

Am 14.01.2025 berichtete Philippe Caturegli vom IT-Sicherheitsunternehmen Seralys von einem winzigen Fehler mit großer Wirkung. Mastercard hatte im DNS für ihre Domäne „az.mastercard.com“ fünf Nameserver eingetragen. Einer davon endete irrtümlich nicht auf „akam.net“ (die Domäne des DNS-Anbieters Akamai), sondern auf „akam.ne“. Doch „.ne“ ist die TLD von Niger. Durch Registrieren von „akam.ne“ hätte etwa jede fünfte Anfrage bei Mastercard manipuliert und angegriffen werden können. Dieser Fehler blieb mehr als vier Jahre unentdeckt.

Caturegli registrierte die Domäne und analysierte die bei seinem Server eintreffenden DNS-Anfragen. Dabei stellte er fest, dass auch andere Akamai-Kunden denselben Fehler gemacht hatten. Brian Krebs ergänzte am 22.01.2025, ein Russe habe die Domäne zwischen 2016 und 2018 besessen und in der Zeit Anfragen an einen gemieteten Server in Deutschland weitergeleitet. Ein heikler und möglicherweise gar nicht so seltener Fehler – Mastercard ist vermutlich nicht das einzige Unternehmen, dem ein Buchstabe in der DNS-Konfiguration fehlt.

Korrektheit und Konsistenz der DNS-Konfiguration sind entscheidende Sicherheitsattribute. Dabei können Verfahren wie „Configuration as Code" und eine regelmäßige Überprüfung helfen.

Maschinenrechte

Das Open Worldwide Application Security Project (OWASP) veröffentlichte am 10.12.2024 eine Liste der zehn kritischsten Fehler im Umgang mit Non-Human Identities (NHIs), also beispielsweise Service Accounts und API-Keys. Sie regeln die Berechtigungen in automatisierten IT-Infrastrukturen. Werden diese unsachgemäß verwaltet, können schwere Sicherheitslücken entstehen: Verwaiste Accounts und offengelegte Zugangsdaten können ein Einfallstor für Angreifer sein. Auch veraltete Authentifizierungsmethoden und übermäßige Berechtigungen erleichtern Angreifern die Arbeit.

Die OWASP-Liste zeigt nicht nur die häufigsten Fehler, sondern auch, wie sie vermieden werden können. Daher kann sie – wie die bekannten „OWASP Top 10" – als Leitfaden für Softwareentwickler genutzt werden. Aber auch für eine Überprüfung der eigenen IT-Infrastruktur eignet sich die Liste. Vorfälle wie der Midnight Blizzard-Angriff bei Microsoft am 12.01.2024 und der Einbruch in das Okta-Support-System am 28.09.2023 verdeutlichen, welche Risiken von kompromittierten NHIs ausgehen.

Geheimdienstbewerber

Am 12.01.2025 wies der Unternehmer und Aktivist Bert Hubert öffentlich darauf hin, dass Bewerbungen für den niederländischen Geheimdienst Google bekanntgegeben werden: nicht absichtlich, sondern weil das staatliche Bewerbungsportal werkenvoornederland.nl unbedacht Google Analytics verwendet. Der Cookie-Banner bietet keine Möglichkeit, diese Datenweitergabe zu unterbinden. Dabei schreibt der Geheimdienst AIVD selbst: „Wir bitten Sie, nicht mit anderen über Ihre Bewerbung bei der AIVD zu sprechen. Es könnte Ihrer Bewerbung und Ihrer möglichen Karriere beim AIVD schaden und Ihre Sicherheit gefährden." Huberts Hinweis führte zu einer bisher unbeantworteten Anfrage des Abgeordneten Derk Boswijk an die Innenministerin.

Auch auf karriere.bund.de kann man sich für Stellen beim Verfassungsschutz und beim Bundesnachrichtendienst bewerben. Laut Datenschutzerklärung nutzt die Webseite die polnische Google-Analytics-Alternative Piwik PRO, wobei IP-Adressen gekürzt werden. Doch genügt das? Piwik und sein

Schwesterprojekt Matomo könnten auch auf bundeseigenen Servern betrieben werden.

Immer wieder kommt es zur Preisgabe hoch sensibler Daten durch die unbedachte Verwendung von Standard-Technologie, wie 2020 die Standortdaten von Kasernen durch Fitnesstracker (SSN 11/2020).

Vertrauen durch Transparenz

Seit dem 04.02.2025 vertraut Firefox in Version 135 nur noch TLS-Zertifikaten, die in Certificate Transparency (CT) Logs erfasst sind. Dabei verpflichten sich Trust Center, alle ausgestellten TLS-Zertifikate in Protokollen zu veröffentlichen. Darüber können Zertifikate von verdächtigen Domains, wie sie beispielsweise bei Phishing-Angriffen genutzt werden, schneller gefunden und gesperrt werden. Dieses Verfahren wurde unter anderem als Reaktion auf Vorfälle bei DigiNotar und TrustWave entwickelt.

Firefox stuft nun Zertifikate, die nicht in CT-Logs erfasst sind, als unsicher ein. Chrome und Safari verfahren bereits seit 2018 so. Öffentliche Trustcenter sind damit gezwungen, CT zu nutzen. In den Browsern Firefox und Chrome lässt sich einstellen, CT für vorgegebene Hostnamen zu ignorieren.

Die neue Zertifikatstransparenz nutzen bereits Dienste wie Red Sift, die vor dem Ablaufen der Gültigkeit von Zertifikaten warnen. Crt.sh ermöglicht die Suche nach Zertifikaten, und das CT-Log-Dashboard von Cloudflare visualisiert die Daten der CT-Logs.

Digitalisierung in der Praxis

In einer Entscheidung vom 18.12.2024 stellte das Schleswig-Holsteinische OLG unter Bezugnahme auf die DSGVO fest, dass eine reine Transportverschlüsselung beim Versand geschäftlicher E-Mails zwischen Unternehmer und Kunden zumindest dann nicht ausreicht, wenn für den Schuldner ein hohes finanzielles Risiko aus einer Fälschung einer angehängten Rechnung erwächst. In diesem Fall biete die Transportverschlüsselung keinen „geeigneten“ Schutz im Sinne der DSGVO.

Offen lässt das Gericht, ab welchem Betrag eine Rechnung als besonders sensibles Datum gilt. Zudem ist es zwar wünschenswert, dass sich Ende-zu-Ende-Verschlüsselung mit Verfahren wie S/MIME durchsetzt, doch spielt sie in der Praxis keine nennenswerte Rolle.

Eine wirksame Lösung wären digital signierte und damit fälschungssichere PDF-Rechnungen – doch die werden gerade von der X-Rechnung abgelöst. Will der Rechnungsempfänger das Prozessrisiko vermeiden, bleibt ihm wohl nur die Überprüfung der angegebenen Bankverbindung, bevor er einen hohen Betrag überweist – oder die Rückkehr zur Papierrechnung. Solange das noch zulässig ist.

Your boss is watching you

Am 19.12.2024 hat der Europäische Gerichtshof (EuGH) zur Verarbeitung von Arbeitnehmerdaten aufgrund einer Kollektivvereinbarung geurteilt. In Deutschland sind das insbesondere Betriebsvereinbarungen zwischen Arbeitgeber und Betriebsrat; sie sind

vor allem dann erforderlich, wenn der Arbeitgeber technische Maßnahmen einführt, die sich zur Arbeitnehmerüberwachung eignen.

Die rechtlichen Anforderungen an eine solche Verarbeitung sind hoch: Es müssen sowohl die mitbestimmungsrechtlichen Fragen als auch, wie der EuGH nun höchstrichterlich feststellte, die Datenschutzgrundsätze Rechtmäßigkeit, Zweckbindung, Erforderlichkeit und Transparenz beachtet werden. Betriebsvereinbarungen nach § 26 BDSG setzen also nicht die Anforderungen der DSGVO außer Kraft.

In einer im August 2024 veröffentlichten Fallstudie stellte das unabhängige Wiener Forschungszentrum Cracked Labs fest, dass nicht nur die Nutzung von dafür gedachten Werkzeugen wie Microsofts Viva Insights eine Arbeitnehmerüberwachung darstellt. Auch der Einsatz von Cybersicherheitsanwendungen wie SIEMs oder solchen des Insider Risk Managements (Forcepoint, Sentinel, Purview) diene der Arbeitnehmerüberwachung. Er ist sowohl mitbestimmungspflichtig als auch eine Datenverarbeitung, die die Bestimmungen der DSGVO einhalten muss.

Kein „Schrems III“?

Das Privacy and Civil Liberties Oversight Board (PCLOB) ist die Beschwerdestelle für Europäer bei Datenverarbeitungen im Rahmen des EU-US Data Privacy Framework. Am 27.01.2025 nun hat das PCLOB bestätigt, dass die drei Mitglieder Franklin, Felten und LeBlanc von US-Präsident Trump entlassen wurden. Ohne ein funktionsfähiges PCLOB steht damit das Data Privacy Framework – ganz ohne Zutun von Max Schrems – auf der Kippe.

Wer vermeiden möchte, dass seine auf dem Data Privacy Framework basierende Verarbeitung plötzlich ohne Rechtsgrundlage dasteht, sollte auf die nach dem Ende des EU-US Privacy Shields geschaffenen Werkzeuge für Datenübermittlungen in unsichere Drittstaaten zurückgreifen.

Secorvo News

Secorvo Seminare

Wissens-Booster: Nutzen Sie das Seminar IT-Security Insights – T.I.S.P.-Update am **29. und 30.04. 2025**, um sich in der IT-Sicherheit auf den aktuellen Stand zu bringen.

Im Ernstfall die Nerven und den Überblick bewahren? Als Vorfall-Experte (BSI) sind Sie für den Worst Case gewappnet. Vom **06. bis 08.05.2025** bereiten wir Sie auf die Zertifizierung vor.

Alle Seminare bei Secorvo sind als Weiterbildungen für die T.I.S.P.-Rezertifizierung anerkannt. Programm und Online-Anmeldung unter www.secorvo.de/seminare.

Krypto-Blackout

Die Entwicklung der Quantencomputer bedroht alle heute eingesetzten kryptografischen Verfahren und schreitet offenbar schneller voran, als noch vor wenigen Jahren erwartet. Die Migration auf quantenresistente Public-Key-Verfahren wird daher in den

kommenden Jahren zur Herausforderung – und möglicherweise zu einem Wettlauf gegen die Zeit.

Beim **KA-IT-Si-Event** am **03.04.2025** im House of Living Labs (FZI) zeigt Hans-Joachim Knobloch (Secorvo), welche praktischen Herausforderungen sich beim Umstieg auf die neuen, so genannten ‚Post-Quantum'-Kryptoverfahren stellen.

Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2025	
10.-14.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
17.-21.03.	31st Fast Software Encryption Conference (IACR, Rom/IT)
18.-20.03.	secIT 2025 (heise Medien, Hannover)
April 2025	
01.-04.04.	DFRWS EU 2025 (DFRWS, Brno/CZ hybrid)
01.-04.04.	Black Hat Asia 2025 (Black Hat, Singapur/ASE)
03.04.	Event „Krypto-Blackout" (KA-IT-Si, Karlsruhe)
08.-10.04.	PQCrypto 2025 (IACR, Taipeh/TW)
28.04.-01.05.	RSA Conference 2025 (RSA, San Francisco/US)
29.-30.04.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
Mai 2025	
04.-08.05.	Eurocrypt 2025 (IACR, Madrid/ES)
06.-08.05.	Vorfall-Experte (BSI) (Secorvo, Karlsruhe)
06.-09.05.	European Identity & Cloud Conference 2025 (KuppingerCole, Berlin)

Fundsache

Am 10.02.2025 hat TeleTrusT einen Forderungskatalog zur Umsetzung des Konzepts „Cyber-Nation" veröffentlicht. Die beiden letzten Forderungen des Katalogs sollten Grundpfeiler der Informationssicherheit in jedem Unternehmen sein.

Impressum

Secorvo Security News – ISSN 1613-4311

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

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de (Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de