Secorvo Security News

Januar 2025

„Bisher noch nie gehackt“

Die elektronische Patientenakte (ePA) ist im Grunde eine gute Sache: weniger Papier, überall verfügbar. Verständlich, dass Bundesgesundheitsminister Karl Lauterbach sie endlich für alle einführen will. Die Akte enthält jedoch äußerst vertrauliche Daten. Ein besonders sicheres Konzept und eine sorgfältige technische Umsetzung sind daher unerlässlich. In seiner Rede im Bundestag zum Gesundheitsdatennutzungsgesetz versicherte Lauterbach, das aktuelle System verwende Technik, die „bisher noch nie gehackt werden“ konnte.

Die Gematik, die das System betreibt, hatte 2024 das Fraunhofer SIT mit einer Sicherheitsanalyse beauftragt. Wer den Bericht (und nicht nur die Zusammenfassung) liest, findet darin reichlich begründete Kritik. Herausstich, dass es keine Sicherheitsanforderungen an die von Praxen, Apotheken und Krankenhäusern verwendeten sogenannten Primärsysteme gibt. Die Gematik befand hingegen am 10.10.2024, dass das Gutachten die Sicherheit des ePA-Systems bestätige. Zu einem anderen Ergebnis kamen Martin Tschirsich und Bianca Kastl auf dem 38. Chaos Computer Congress. In ihrem Vortrag zeigten sie, dass es diverse, teils einfach ausnutzbare Schwachstellen gibt. So wird beim Zugriff auf die Akte auf die kryptografische Prüfung der Kartennummer verzichtet, sodass jeder Leistungserbringer (oder wer sich erfolgreich als solcher ausgibt) Zugriff auf sämtliche 70 Mio. Akten hat. Die Gematik reagierte darauf am 27.12.2024 mit dem Hinweis, dass die gezeigten Angriffe illegal und technisch komplex seien – kündigte jedoch (offensichtlich notwendige) Nachbesserungen vor dem bundesweiten Rollout an.

Jeder Versicherte kann der Nutzung der ePA widersprechen – auch vorläufig. Wie das geht, erklärt beispielsweise der BayLfD. Sollte die Gematik die Sicherheitsprobleme beheben, lässt sich die Entscheidung jederzeit rückgängig machen.

Security News

LOTL-Ransomware

Ransomware-Angriffe ohne Schadcode funktionieren auch in der Cloud. Das Halcyon Research Team berichtete am 13.01.2025, dass Hacker über ausgespähte Administratorkonten beispielsweise in AWS S3 dafür die Funktion SSE nutzen, die die Cloud-Datenspeicher verschlüsselt – mit der Option -C, die eigene Schlüssel verwendet. Diese erhält das betroffene Unternehmen nach der Lösegeldzahlung. Um den Druck zu erhöhen wird über die Funktion Object Lifecycle eine automatische Löschung nach einer festen Anzahl Tage eingestellt. Die Methode ähnelt dem ShrinkLocker, der

Windows' BitLocker verwendet, um lokale Systeme zu verschlüsseln. Auch Angreifer beherzigen offenbar „Don't roll your own Crypto". Amazon empfiehlt am 15.01.2025 vier Schutzmaßnahmen: Deaktivieren von SSE-C (sic!), Authentifizierung mit Amazons Security Token Service, Erstellung von Sicherheitskopien und Nutzung der Überwachungsfunktionen.

Langwellenhacking

Beim 38. Chaos Computer Congress stellten Luca Melette und Fabian Bräunlein vom Berliner IT-Sicherheitsunternehmen Positive Security am 28.12. 2024 die Ergebnisse ihrer Untersuchungen zur Funkrundsteuertechnik vor. Sie wird von Energieversorgern genutzt, um z. B. große Stromverbraucher und erneuerbare Stromerzeuger ein- und auszuschalten. Dazu nutzt es leistungsfähige Langwellensender ähnlich dem Zeitzeichensender DCF77. Die Technik wurde Anfang der 90er Jahre entwickelt und versendet unsignierte Nachrichten. Die Forscher zeigten, wie sie mit einfachster Technik Ampeln ein- und Photovoltaik-Anlagen abschalten konnten. Mit starken Sendern ließe sich das Stromnetz destabilisieren, da etwa 1,5 Millionen Empfänger betroffen sind, die rund 16 % der Stromproduktion und fast 30 % des Verbrauchs steuern.

Der Vortrag erinnert an den Angriff über analoge UKW-Funktechnik, mit dem Hacker 2023 bei polnischen Zügen eine Notbremsung auslösten (SSN 9/2023). Wie schon damals vermutet gibt es noch immer „Legacy-Systeme" mit unsicherer Technik in sicherheitsrelevanten Umgebungen.

Nicht ob, sondern wann

Seit über 30 Jahren wird über Quantencomputer diskutiert, die Verschlüsselungsverfahren wie RSA und ECDSA brechen könnten. Auch wenn Skeptiker bezweifeln, ob solch ein Quantencomputer jemals relevant wird, spielt diese Frage für die Planung des Umstiegs auf die seit dem vergangenen Jahr standardisierten Post-Quanten-Kryptoverfahren (PQC) keine entscheidende Rolle mehr – denn Aufsichtsbehörden und Fachgremien fordern den Umstieg auf PQC in ihren Compliance-Anforderungen und Best-Practice-Empfehlungen.

Nach Moscas Ungleichung entsteht Handlungsdruck, wenn die Summe aus dem Zeitbedarf für die Migration und dem Zeitraum, in dem herkömmlich verschlüsselte oder signierte Daten sicher bleiben müssen, die geschätzte Zeit bis zur Verfügbarkeit eines geeigneten Quantencomputers erreicht.

Das BSI ging 2023 noch davon aus, dass dieser Zeitraum 20 Jahre beträgt. In seinem am 02.01.2025 veröffentlichten Update zum Stand 2024 wurde die Schätzung auf 16 Jahre verkürzt, also bis 2040. In den USA fordert die NSA für "National Security Systems", mit dem Umstieg z. B. beim TLS-Schlüsselaustausch bereits jetzt zu beginnen, bei Public-Key-Infrastrukturen (PKIs) spätestens 2030. Verantwortliche für Schlüsselmanagementsysteme, PKIs und ähnliche kryptografische Infrastrukturen sollten daher bald über eine Migration zu PQC nachdenken und mit den Vorbereitungen beginnen.

Wer den Schaden hat...

Am 18.11.2024 entschied der Bundesgerichtshof, dass Betroffene Anspruch auf Schadensersatz haben, wenn sie infolge eines DSGVO-Verstoßes kurzzeitig die Kontrolle über ihre personenbezogenen Daten verlieren. Auf eine missbräuchliche Verwendung der Daten oder sonstige negative Folgen komme es nicht an. Einen anderen Standpunkt vertritt das Bundesarbeitsgericht (BAG), das am 20.06.2024 einen Schadensersatzanspruch wegen einer nicht vollständig erteilten Auskunft ablehnte. Die Verletzung des Auskunftsanspruchs begründe keinen immateriellen Schaden; das hypothetische Risiko einer missbräuchlichen Verwendung reiche nicht aus. Zwei höchstrichterliche Entscheidungen entgegengesetzten Inhalts – das Thema wird die Gerichte weiter beschäftigen.

Sehr geehrte/r ???

Am 09.01.2025 hat der europäische Gerichtshof in einem praxisrelevanten Urteil entschieden, dass die französische SCNF in ihrem Online-Fahrkarten-Shop die Anrede nicht verpflichtend abfragen darf. Zwar sei es höflich, bei der Ansprache der Kunden eine korrekte Anrede zu verwenden, aber keineswegs erforderlich - folglich handele es sich um eine freiwillige Angabe. Unternehmen sollten daher ihre Kontaktformulare auf Webseiten oder in Apps daraufhin überprüfen, ob die Angabe der Anrede tatsächlich dem Betroffenen überlassen bleibt.

Am Verteilnetz vorbei

Kevin Beaumont dokumentierte im Dezember 2024 in seinem Blog detailliert die DDOS-Angriffe der pro-russischen Gruppe NoName057(16) auf britische Websites. Die Angreifer, die auch in Deutschland aktiv waren, umgingen die vor die Webseiten geschalteten Content Delivery Networks (CDN) und griffen direkt die Ursprungsserver an, die oft leicht zu finden sind – davor schützt auch nicht die Wahl eines schwer zu erratenden Servernamens, wie beispielsweise von Akamai empfohlen. Wirksamen Schutz bietet nur eine Firewall, die den Zugriff auf den Ursprungsserver ausschließlich Servern des CDN erlaubt. Akamai bietet mit Site Shield und Origin IP ACL eine solche Lösung an, wie Laban Sköllermark am 13.12.2023 ausführlich erläutert hat.

Nur noch mit SID

Am 11.02.2024 wird es soweit sein: Der von Microsoft ursprünglich für Februar 2023 angekündigte und mehrfach verschobene Patch für AD-Domain-Controller zum besseren Schutz gegen Goldene Zertifikate wird ausgerollt. Anschließend werden Domain-Controller eine zertifikatsbasierte Anmeldung am AD (wie etwa Smartcard-Logon oder TLS-ClientAuthentifikation) nur noch akzeptieren, wenn in einer Erweiterung des Zertifikats der nicht änderbare Security Identifier (SID) des betreffenden AD-Kontos aufgeführt ist. Die AD Certificate Services („Microsoft PKI“) selbst wurden schon vor Jahren entsprechend angepasst, aber für die SCEP- und PKCS-Konnektoren, über die Intune Zertifikate für gemanagte Geräte und Benutzer abruft, hat Microsoft erst kurz vor Toresschluss Updates bereit-

gestellt. Wer Zertifikate über ein Device Management System ausrollt, sollte daher sicherstellen, dass diese – falls erforderlich – den SID enthalten.

Kurze Schlüssel

Im April 2024 veröffentlichte Andreas Wulf das Ergebnis einer Prüfung der E-Mail-Authentifizierung von einer Million Domänen und fast 500.000 DKIM-Signaturen. Dabei entdeckte er Domänen, die noch RSA-Schlüssel mit einer Länge von nur 512 Bit verwenden – und namhafte E-Mail-Provider, die so kurze Schlüssel noch akzeptieren. In einem Blogartikel vom 08.01.2025 zeigt er, dass man – wie zu erwarten – solche Schlüssel auf handelsüblicher Hardware in weniger als vier Tagen knacken kann. Allerdings betrifft dies lediglich 0,05% der von ihm analysierten Schlüssel (rund 250 Domänen). Weitere 0,31% verwenden ebenfalls nicht mehr empfohlene 768-Bit-Schlüssel. Um diese zu knacken würde seine einfache Hardware allerdings bereits Jahrzehnte benötigen.

Fast die Hälfte aller untersuchten Domänen verwenden noch 1024-Bit-Schlüssel. Dafür gibt es keinen nachvollziehbaren Grund: Das BSI empfiehlt RSA-Schlüssel mit mindestens 3000 Bit; und RFC 8301 von 2018 schreibt vor, dass E-Mail-Server auch Signaturen mit 4096-Bit-DKIM-Schlüssel prüfen können. Auch unsere Erfahrungen damit sind positiv: Bei E-Mails an etwa eintausend Domänen pro Monat hat noch kein einziger E-Mail-Server 4096-Bit-DKIM-Signaturen abgelehnt.

Secorvo News

Der lange Weg zur quantenresistenten PKI

Auf der 32. DFN-Konferenz "Sicherheit in vernetzten Systemen" am 11. und 12.02.2025 berichten Hans-Joachim Knobloch und Noah Freising über den Stand der Nutzbarkeit von PQC-Verfahren im Bereich PKI, unterschiedliche Ansätze, wie die Migration vonstattengehen könnte und empfehlenswerte Schritte zur Vorbereitung. Ein Vorabdruck des Beitrags ist im Linux-Magazin erschienen.

Weiterbildung und Zertifizierung

Vom **10. bis 14.03.2025** bereiten wir Sie auf die Zertifizierung zum T.I.S.P. vor – unterstützt von unserem bewährten Begleitbuch, das Sie nach Ihrer Anmeldung vorab erhalten. Am **24. bis 27.03.2025** führen wir Sie in die Grundlagen der sicheren Softwareentwicklung ein (T.P.S.S.E.). Wie Sie PKI-Lösungen erfolgreich einführen und nutzen können, zeigt Ihnen unser Kollege Hans-Joachim Knobloch vom **07. bis 10.04.2025**. Alle Seminare sind als Weiterbildungen für die T.I.S.P.-Re-Zertifizierung anerkannt (zur Anmeldung).

Wer zahlt die Zeche?

Risiken kann man ignorieren, reduzieren – oder transferieren. Mit der Zunahme erfolgreicher Cyberangriffe steigt daher auch die Nachfrage nach Cyber-Versicherungen. Aber wie das so ist im Leben: Erst im Ernstfall zeigt sich, was eine Vereinbarung wert ist. Nicht jeder Vorfall ist auch ein Versicherungsfall – angesichts wachsender Vorfallszahlen und sinkender Margen im

Cyber-Versicherungsgeschäft wird daraus schnell ein Streitfall.

Was Versicherungsnehmer schon bei Vertragsabschluss beachten sollten erläutert Dr. Christian Förster (Bartsch Rechtsanwälte) beim Jahresauftakt-Event 2025 der Karlsruher IT-Sicherheitsinitiative an Beispielen aus der Praxis am **27.02.2025** um 18:00 Uhr im Saal Baden (IHK Haus der Wirtschaft). Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (schnelle Anmeldung empfohlen).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2025	
11.-12.02.	32. DFN-Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg)
12.-14.02.	IT-Defense 2025 (cirosec, Stuttgart)
19.-20.02.	ID:SMART Workshop 2025 (CAST e. V., Darmstadt)
27.02.	KA-IT-Si-Event „Wer zahlt die Zeche?“ (KA-IT-Si, Karlsruhe)
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)
24.-27.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
April 2025	
01.-04.04.	DFRWS EU 2025 (DFRWS, Brno/CZW hybrid)
01.-04.04.	Black Hat Asia 2025 (Black Hat, Singapur/ASE)
07.-10.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

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

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100

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

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