

# Secorvo Security News

Februar 2026



## Endlich Zahlen

Ransomware-Angriffe haben Hackergruppen zu Millionären gemacht – und bei einigen Unternehmen, wie z. B. PILZ, ruinöse Schäden durch Betriebsausfälle verursacht. Sie sind daher zu Recht gefürchtet.

Aber wie wahrscheinlich ist es, Opfer eines Ransomware-Angriffs zu werden? Bisher gab es dazu keine verlässlichen Zahlen. Bei Risikobewertungen urteilen Menschen in solchen Fällen nachweislich nach dem Schadensausmaß – und überschätzen die Gefahr häufig deutlich. Gilt das auch für Ransomware?

Seit dem Inkrafttreten des Digital Operational Resilience Act (DORA) am 17.01.2025 müssen 3.600 Unternehmen des Finanzsektors schwerwiegende IKT-Vorfälle an die Finanzdienstleistungsaufsicht (BaFin) melden. Am 28.01.2026 stellte Mark Branson, Präsident der BaFin, die Studie „Risiken im Fokus 2026“ vor – mit Zahlen, aus denen sich die Ransomware-Angriffswahrscheinlichkeit abschätzen lässt.

In den ersten drei Quartalen 2025 wurden der BaFin 525 Vorfälle gemeldet, davon 10% Sicherheitsvorfälle. Hochgerechnet sind das ca. 70 Sicherheitsvorfälle pro Jahr; 30% davon traten bei Dienstleistern auf. 13,3% der restlichen Sicherheitsvorfälle, nämlich 7, waren Ransomware-Angriffe. Deren Eintrittswahrscheinlichkeit liegt damit für Finanzunternehmen bei etwa 0,18% pro Jahr. Da viele Schutzmaßnahmen das Schadensausmaß begrenzen, verursachten nur wenige größere Schäden. Finanzunternehmen zählen zu den für Angreifer besonders attraktiven Zielen, daher ist diese Eintrittswahrscheinlichkeit vermutlich eine obere Grenze. Sie ist keineswegs vernachlässigbar, aber mit 99,82%iger Wahrscheinlichkeit ist Ihr Unternehmen 2026 nicht betroffen. Viel eher sollten Sie mit schwerwiegenden IKT-Ausfällen rechnen – sie haben eine hundert Mal so hohe Eintrittswahrscheinlichkeit: 17,8%.

Behalten Sie vor allem die im Blick – und konzentrieren Sie sich hinsichtlich Ransomware auf Schadensbegrenzungsmaßnahmen.

## Security News

### Zwölf auf einen Streich

Am 27.01.2026 veröffentlichte das OpenSSL-Projekt ein [Security Advisory](#) mit zwölf neuen Schwachstellen – allesamt [entdeckt](#) vom autonomen KI-System der Firma AISLE. Das Unternehmen hatte seinen Analyzer bereits im [August 2025](#) auf OpenSSL angesetzt und arbeitete die Ergebnisse anschließend in enger Zusammenarbeit mit dem Projekt auf.

Die schwerwiegendste Lücke ist [CVE-2025-15467](#): ein Stack-Buffer-Overflow beim Parsen von CMS-Nach-

richten. [CVE-2025-11187](#) betrifft fehlerhafte PBMAC1-Validierung in PKCS#12-Dateien. Die zehn weiteren, weniger kritischen Lücken verteilen sich über QUIC, TLS 1.3, OCB-Mode und PKCS7-Komponenten; bei einigen lieferte AISLE gleich den Patch mit.

OpenSSL gehört zu den am intensivsten manuell geprüften Open-Source-Bibliotheken der Welt. Trotzdem blieben diese Schwachstellen jahrelang unentdeckt. Anders als die halluzinierten Schwachstellenmeldungen, die Open-Source-Autoren wie curl-Entwickler Daniel Stenberg täglich [beschäftigen](#) ([SSN 06/2025](#)), steht AISLE hier für die konstruktive Seite: koordinierte Offenlegung statt automatisierter Spam-Reports, KI als Lupe statt Autopilot.

Wer OpenSSL einsetzt, sollte unverzüglich auf eine gepatchte Version aktualisieren. Patches sind seit dem 27.01.2026 für alle aktiven OpenSSL-Versionen verfügbar.

## Ich weiß, wo du gestern warst

Am 22.01.2026 veröffentlichte Le Monde einen [Artikel](#) (Bezahlschranke) von Martin Untersinger über das Geschäft mit Geodaten, die aus eingeblendeter Werbung in Smartphone-Apps gewonnen werden. Das Geschäft nennt sich Advertising-based Intelligence (A-DINT). Mittlerweile ist daraus ein Markt mit mindestens 15 Anbietern entstanden. Die Firmen sammeln Geodaten aus gewöhnlichen Apps und versprechen Sicherheitsbehörden, einzelne Geräte nahezu weltweit verfolgen zu können – teils rückwirkend über Jahre und laufend aktualisiert.

[Laut Forbes](#) zahlt etwa die US-Behörde ICE Millionenbeträge für solche Daten; auch Finanzinstitute zählen zum Kundenkreis.

Mehrere Anbieter werben sogar offen damit, einzelne Nutzer identifizieren zu können, indem sie die pseudonymen Werbe-IDs mit anderen Datenquellen verknüpfen, auch mit gehackten Datensätzen. Dass das funktioniert, hat [Netzpolitik.org](#) bereits am 04.11.2025 in einer Studie nachgewiesen.

Auch wenn viele der Daten ungenau sind, bleiben die Werkzeuge attraktiv, da sie Muster, Bewegungsprofile und Trends sichtbar machen. Rechtlich bewegen sich die Anbieter in einer Grauzone; einige sollen manipulierte Werbeanzeigen einsetzen, um Spyware auf Geräten zu platzieren.

Wer die Bewegungsprofile von Führungskräften vertraulich halten will, sollte (z. B. mit einem MDM) die Installation von Apps und die Nutzung von Standortdaten einschränken – und Werbeblocker einrichten.

## Fast Stalking

Der Google-Dienst GFPS für das schnelle Pairing von Bluetooth-Geräten bietet eine „Ein-Klick-Verbindung“, wenn er ein BLE-Gerät in unmittelbarer Nähe entdeckt. Dazu muss am Gerät der Kopplungs-Modus aktiviert sein.

Die [Forschungsgruppe COSIC](#) (Computer Security and Industrial Cryptography) an der Universität Leuven (NL) veröffentlichte am 15.01.2026 ein [Video](#), in dem gezeigt wird, wie damit [einige BLE-Devices](#) über-

nommen werden können: Sie reagieren durch einen Implementierungsfehler auch auf GFPS, wenn der Kopplungsmodus nicht aktiviert ist. Damit können nicht nur über kleinere Distanzen Gespräche belauscht, sondern auch die Geräteinhaber verfolgt werden, wenn das gekoppelte Device vom Angreifer in [Googles „Find Hub“-Netzwerk](#) aufgenommen wird. Für diesen „[WhisperPair](#)“ genannten Angriff ([CVE-2025-36911](#)) erhielten die Forscher von Google ein Bug Bounty in Höhe von 15.000 USD.

Beunruhigend ist weniger der Implementierungsfehler, der bisher nur in einer geringen Zahl von BLE-Devices entdeckt wurde, sondern die von diesem Bug unabhängige Erkenntnis, dass man seine Bluetooth-Devices besser nicht zur Nutzung an fremden Geräten verleihen sollte: Wenn deren Hersteller eine App mit Ortungsfunktion anbietet oder Find Hub unterstützt, ist die Spur des Devices nachverfolgbar.

## Wer liest, gewinnt

Wer sagt, dass Datenschutzerklärungen langweilig sein müssen?

Der US-Mobilfunkanbieter Cape versteckte laut [Blogbeitrag](#) vom 30.01.2026 bereits 2025 ein „Easter Egg“ in seinen Datenschutzhinweisen: eine kostenlose Reise in die Schweiz. Eine Kundin entdeckte das Angebot nach zwei Wochen und gewann Hin- und Rückflug, drei Nächte in einem Chalet und 1.500 USD Verpflegungsgeld.

Die am 27.01.2026 veröffentlichten Ergebnisse einer [Umfrage des eco-Verbands](#) zeigen: Nicht einmal 10% der Befragten lesen Datenschutzerklärungen vollständig. Für 66% sind sie zu lang, für 34% zu kompliziert oder schwer verständlich.

Cape beweist, dass es auch anders geht: Statt juristischer Floskeln bietet das Unternehmen klare, kurze Informationen. Datenschutz muss verständlich sein – sonst ist er wertlos. Vielleicht lohnt beim nächsten Mal ein genauerer Blick in die Datenschutzerklärung. Wer weiß, was man dort findet?

## Trojanisches Update

Der [Angriff auf die Notepad++-Infrastruktur](#) zwischen Juni und Dezember 2025 zeigt, wie verwundbar auch etablierte Software sein kann. Dabei wurde [nicht die Anwendung selbst](#) kompromittiert, sondern der Hosting-Provider, über den Angreifer manipulierte Inhalte einschleusten. Ein kompromittierter Server, fehlende Signaturprüfungen im Updater und die gezielte [Umleitung einzelner Systeme](#) ermöglichten monatelange unbemerkte Manipulationen.

Der Vorfall unterstreicht, wie wichtig robuste Sicherheitsmechanismen in Update-Prozessen sind. Automatische Updates sollten grundsätzlich so gestaltet sein, dass nur eindeutig vertrauenswürdige Dateien installiert werden. Dazu gehört eine Prüfung der Code-Signatur inklusive des vollständigen Zertifikats des Installers. Notepad++ zeigt mit seinem [Fix](#) vom 01.12.2025, wie so etwas in der Praxis aussieht: Der Updater akzeptiert nur noch Installer, die zum hinterlegten Zertifikat gehören, und bricht den Vorgang anderenfalls sofort ab.

Der Fall zeigt aber auch, dass selbst vertrauenswürdige Quellen nicht immun gegen Angriffe sind – auch deren Infrastruktur kann Schwachstellen aufweisen, die ein Angreifer ausnutzen kann.

## Ablagerisiko

Am 15.01.2026 hat der Bayerische Landesbeauftragte für Datenschutz eine [aktuelle Kurzinformation](#) zur sicheren Ablage von Daten veröffentlicht.

In vielen Behörden und Unternehmen werden Fileserver-Shares für den internen Datenaustausch genutzt. Das ist praktisch, kann aber zum Datenschutz-Risiko werden, wenn die Ablage weder zugriffsbeschränkt erfolgt noch protokolliert wird – und meist auch noch nicht zügig wieder gelöscht wird. Dabei kommt es immer wieder zur unberechtigten Offenlegung personenbezogener Daten – und das sind meldepflichtige Datenschutzvorfälle.

Für den Austausch von Personaldaten dürfen ausschließlich zugriffsbeschränkte File-Shares verwendet werden. Eine gute Wahl für die Übermittlung vertraulicher Daten kann auch ein über den Browser erreichbarer Share-Server mit Zugangsschutz und verschlüsselter Ablage sein – oder der Versand als E-Mail-Anhang, denn der wird intern verschlüsselt. Die Empfängerliste sollte man vor dem Absenden jedoch noch einmal genau prüfen. Vorsicht auch beim Dateinamen – der sollte keine personenbezogenen Angaben enthalten.

## Secorvo News

### Secorvo Seminare

[21.-22.04.2026 | IT Security Insights](#) gibt einen Überblick über aktuelle Themen der IT-Sicherheit und des Datenschutzes – ein Update für alle CISOs, Informationssicherheitsmanager und IT-Sicherheitsbeauftragten.

[19.-21.05.2026 | Vorfallexperte](#) bereitet Sie nach dem Curriculum des BSI auf die Zertifizierung zum Vorfall-Experten vor. Für alle, die im Bereich Informationssicherheit, IT-Sicherheit, Datenschutz, Notfallplanung oder der Aufrechterhaltung des Geschäftsbetriebs Verantwortung tragen.

[15.-19.06.2026 | T.I.S.P.](#) vermittelt Ihnen praxisnahes Grundlagenwissen zu Informationssicherheit, Datenschutz und IT-Grundschutz – mit offizieller Zertifizierung durch TeleTrust und DEKRA. Ideal für erfahrene IT-Sicherheitsverantwortliche, die ihre Qualifikation sichtbar machen möchten.

[22.-25.06.2026 | PKI](#) ist unser erfolgreiches Grundlagen- und Vertiefungsseminar zu Public Key Infrastrukturen – von der Konzeption über den Aufbau zum Betrieb, mit praktischen Übungen.

Versäumen Sie nicht den Frühbucherrabatt. [Hier](#) geht's zur Anmeldung.

## Rogue, thou hast liv'd too long

Im Jahr 2025 wurden über 45.000 neue Schwachstellen entdeckt, ein Teil davon durch unabhängige Sicherheitsforscher. Wie sollen Unternehmen auf die

Meldung von Schwachstellen reagieren – soll der Forschende verklagt werden oder ein Bug Bounty erhalten? Und wie soll die Schwachstelle behoben und dazu kommuniziert werden?

Beim [nächsten Event](#) der KA-IT-Si am 16.04.2026 stellen Dr. Matthias Schmidt und Armin Harbrecht (aramido) anhand eines auf wahren Begebenheiten beruhenden Falls Wege zum Umgang mit Schwachstellenmeldungen vor.

Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Hier geht's zur [Anmeldung](#) – wir freuen uns auf Sie.

## Veranstaltungshinweise

Auszug aus [Veranstaltungsübersicht IT-Sicherheit und Datenschutz](#).

| März 2026  |  |
|------------|--|
| 17.-19.03. | <a href="#">GI Sicherheit 2026</a> (GI/HAW, Hamburg)                                   |
| 17.-19.03. | <a href="#">secIT 2026</a> (Heise Medien, Hannover)                                    |
| 23.-26.03. | <a href="#">RSA Conference 2026</a> (RSA Conference, San Francisco/US)                 |
| 23.-27.03. | <a href="#">FSE 2026</a> (IACR, Singapur/ASE)  |
| 24.-27.03. | <a href="#">DFRWS EU 2026</a> (DFRWS, Linköping/SE hybrid)                             |
| April 2026 |  |
| 14.-16.04. | <a href="#">Datenschutztag 2026</a> (WEKA-Akademie, Frankfurt)                         |
| 14.-16.04. | <a href="#">PQCrypto 2026</a> (IACR, Saint-Malo/FR))                                   |
| 16.04.     | <a href="#">KA-IT-Si-Event „Rogue, thou hast liv'd too long“</a> (KA-IT-Si, Karlsruhe) |
| 21.-22.04. | <a href="#">IT Security Insights - T.I.S.P. Update</a> (Secorvo, Karlsruhe)            |
| 21.-24.04. | <a href="#">Black Hat Asia 2026</a> (Blackhat, Singapur/AS)                            |
| 28.-29.04. | <a href="#">Cybersecurity Summit 2026</a> (Trailblazer Summits Group, Hamburg)         |

## Fundsache

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat den europaweit ersten offiziell anerkannten Consent-Management-Dienst [Consenter](#) zugelassen. Ein bisschen befremdet allerdings, dass er Cookies ohne Einwilligung setzt...

## Impressum

[Secorvo Security News](#) – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Paul Blenderman, Kai Jendrian, Dr. Alexander Koch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Michael Schrempp, Liza Trace.

Herausgeber (V. i. S. d. P.): Dirk Fox,  
Secorvo Security Consulting GmbH  
Bahnhofplatz 8  
76137 Karlsruhe  
Tel. +49 721 255171-0  
Fax +49 721 255171-100

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

Wir freuen uns über Ihr Feedback an [redaktion-security-news@secorvo.de](mailto:redaktion-security-news@secorvo.de)

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.