

Secorvo Security News

April 2026



Überraschung...

Keine drei Jahre liegt die Veröffentlichung des [Cloud-Reports 2023](#) des Bitkom zurück. Darin gaben 64% der rund 500 befragten Unternehmen an, mit dem Umstieg auf Cloud-Dienste in erster Linie Kosten reduzieren zu wollen.

Im [Cloud-Report 2025](#) klangen die Befragten ernüchtert: 67% meinten, ohne Cloud-Dienste würde das Unternehmen stillstehen, 64% sahen sich gezwungen, Cloud-Dienste zu nutzen und 53% fühlten sich den Cloud-Anbietern ausgeliefert.

Das war vorhersehbar. Seit Jahren ersetzen Softwarehersteller nach dem Vorbild von Microsoft ihre On-Premise-Lösungen durch Cloud-Angebote und stellen auf monatsbezogene, nutzerbasierte Lizenzmodelle um. In der Cloud muss sich der Anbieter nicht mit zueinander inkompatiblen Betriebssystemen herumärgern; er kann mit Lock-In-Mechanismen wie dem Verweben von Diensten (E-Mail und Kalender, Ticketsystem und Wiki) oder der Verwendung proprietärer Datenformate den Wechsel für die Unternehmen zum riskanten Abenteuer machen und dann durch Drehen an der Preisschraube die maximale Zahlungsbereitschaft der Kunden ausloten. Zugleich schwinden Kompetenz und Ausstattung der Unternehmen für den IT-Eigenbetrieb – was die Abhängigkeit weiter verstärkt. Das Resultat kann man den Bilanzen der IT-Giganten entnehmen: Über 35% Gewinnmarge bei Microsoft 2025 – der Produktivitätszuwachs durch den IT-Einsatz wird zunehmend von (vor allem nicht-europäischen) IT-Cloud-Anbietern abgeschöpft.

Damit sind wir von „digitaler Souveränität“ heute weiter entfernt denn je. Und erpressbar – sowohl beim Preis als auch beim „politischen Wohlergehen“. Mit fortschreitender Digitalisierung wird der unternehmerische Gestaltungsspielraum bei IT-Entscheidungen zu einem wichtigen Element der Wettbewerbsfähigkeit. Daher sollte jedes Unternehmen als Teil des Risikomanagements und bei wichtigen IT-Entscheidungen seinen „Souveränitätsindex“ bestimmen.

Security News

Risk by Default

Seit dem 17.04.2026 ist in Microsoft Copilot das [Flex-Routing](#) für EU-/EFTA-Kunden per default aktiviert: Es leitet bei Bedarf die KI-Verarbeitung an Rechenzentren außerhalb der EU-Datengrenze weiter, etwa in die USA oder Kanada. Zwar werden die Daten verschlüsselt übertragen und nur in der EU gespeichert, doch werden sie zumindest temporär im nicht-europäischen Ausland verarbeitet.

Um Compliance-Risiken zu vermeiden sollten Administratoren die Einstellung prüfen und anpassen, denn

ohne manuelle Deaktivierung im Microsoft 365 Admin Center oder im Power Platform Admin Center drohen ungewollte Datenübertragungen. Die Standardeinstellung ist daher keine sichere Wahl.

Vergifteter Scanner

Am 19.03.2026 [kompromittierte](#) die Gruppe TeamPCP den verbreiteten Open-Source-Vulnerability-Scanner [Trivy](#) von [Aqua Security](#) und verwandelte ihn in eine Waffe gegen seine eigenen Nutzer. Der Einstieg [gelang](#) über eine [GitHub-Actions-Fehlkonfiguration](#): Der Workflow `apidiff.yaml` nutzte `pull_request_target` und führte damit externen PR-Code mit vollen Repository-Rechten aus – ein als „[Pwn Request](#)“ bekanntes Muster, das [poutine](#) von Boost Security bereits am 29.11.2025 [gemeldet](#) hatte: ein vermeidbares Problem also.

Per KI-Bot ([hackerbot-claw](#)) leiteten die Angreifer am 19.03.2026 mit dem gestohlenen Organisations-Token 76 von 77 Version-Tags in `aquasecurity/trivy-action` auf eigenen Schadcode um. Wer eine betroffene Version verwendete, führte seitdem Code von TeamPCP aus, der alle Zugangsdaten aus dem RAM auslas. Die gestohlenen Identitäten lösten eine [wochenlange Kaskade](#) aus: [Checkmarx](#), [LiteLLM](#), [Axios](#) und [Bitwarden](#) CLI wurden danach ebenfalls kompromittiert.

GitHub Actions sollten ausschließlich per vollständigem Commit-SHA eingebunden werden statt über einen Tag – `uses: aquasecurity/trivy-action@<SHA>`. Der Trigger `pull_request_target` darf keinen Code aus dem PR-Branch ausführen. Beide Maßnahmen beschreibt GitHub im [Security-Hardening-Guide](#) als obligatorisch. Für kritische Pipelines empfiehlt sich [SLSA v1.2 Build L3](#).

Wer manipulierte `trivy-action`-Tags oder betroffene Software eingesetzt hat, muss sämtliche Secrets sofort wechseln. Konkrete Hilfestellungen bieten [Step-Security](#) und [Microsoft Security](#). Wo Pakete bereits [Sigstore/cosign](#)-Signaturen oder SLSA-Provenance-Attestierungen bereitstellen, sollten diese vor dem Einsatz geprüft werden. Für die Mehrheit der Pakete fehlen solche Nachweise noch. Die Trivy-Krise zeigt, warum kryptografische Herkunftsbelege für alle Ökosysteme überfällig sind.

Don't trust every manual

Das IT-Sicherheitsunternehmen SpecterOps publizierte am 24.03.2026 in einem [Blog-Post](#), dass die offiziellen Handbücher von 16 großen Softwareherstellern Administratoren dazu anleiten, sicherheitskritische Fehlkonfigurationen in den Active Directory Certificate Services (AD CS) vorzunehmen, die bereits am 17.06.2021 in einer [Studie](#) beschrieben worden waren. Das Ergebnis sind Angriffspfade, die schwerer wiegen können als klassische CVE-Sicherheitslücken.

Der Autor Martin Sohn Christensen informierte die betroffenen Hersteller; daraufhin korrigierten einige innerhalb eines Monats ihre Anleitungen, darunter CyberArk und ManageEngine. Andere, wie Cisco, Oracle und ServiceNow, hatten die Hinweise zum Zeitpunkt der Veröffentlichung noch nicht korrigiert; Omnisca [reagierte](#) erst am 15.04.2026. Zudem informierten

nicht alle ihre Kunden über die Fehler. Merke: Bei der Konfiguration von PKIs sollte man sich nicht blind auf Handbücher verlassen – sondern wissen, was man tut.

Schlüssel vergessen

Hanno Böck, Betreiber des Projekts [badkeys](#), das die Qualität kryptografischer Schlüssel prüft, [berichtete](#) am 15.04.2026 über einen 384-bit-RSA-DKIM-Schlüssel der Domäne t-systems.nl – möglicherweise hatte jemand die Mindestschlüssellängen für RSA mit denen für ECC verwechselt. Weil T-Systems die Zahlung einer Bug Bounty für den Hinweis ablehnte, veröffentlichte badkeys den leicht berechenbaren privaten Schlüssel.

Auf den ersten Blick scheint der Fehler harmlos, denn die [T-Systems Nederland B.V.](#) nutzt seit Jahren die E-Mail-Domäne t-systems.com. Den Schlüssel verwendeten sie höchstwahrscheinlich nicht mehr und hatte ihn nur nicht gelöscht. Doch ganz so harmlos ist es nicht: Ein Phishing-Angriff könnte „authentische“ E-Mails im Namen der weiterhin offiziellen Domäne versenden. Auch öffentliche DNS-Einträge bedürfen daher einer regelmäßigen Pflege.

Axios compromised

Am 01.04.2026 [meldete](#) Microsoft einen gezielten Supply-Chain-Angriff auf das populäre npm-Paket axios. Zwischen dem 30. und dem 31.03.2026 wurden für etwa drei Stunden manipulierte axios-Versionen veröffentlicht. Die Angreifer gelangten über einen via Social-Engineering-Kampagne eingeschleusten RAT (Remote Access Trojan) auf den Rechner des Maintainers; anschließend nutzten sie ein gestohlenen Token, um dessen npm-Account zu kompromittieren. Ein verschleiertes Post-Install-Skript identifizierte das Betriebssystem und stellte eine Verbindung zu einem C2-Server her, um einen plattformübergreifenden RAT nachzuladen – ein [Angriff](#), der Windows, macOS und Linux gleichermaßen treffen konnte. Der Trojaner sammelte Systeminformationen, richtete sich persistent ein und ersetzte anschließend die package.json durch eine [unauffällige Version](#); das erschwerte die forensische Analyse.

Der Vorfall ist ein beispielhafter Supply-Chain-Angriff: Axios hat eine enorme Verbreitung und der Trojaner war gut getarnt. Das größte Risiko birgt nicht der Code, sondern das Vertrauen in die Lieferkette. Maintainer sollten Hardware-2FA und kurzlebige Token verwenden; sinnvoll ist außerdem die Überwachung veränderter Abhängigkeiten.

Missbrauchsverdacht

Nach dem [Urteil des EuGH](#) vom 19.03.2026 kann selbst ein erstes Auskunftersuchen nach Art. 15 DSGVO als exzessiv und missbräuchlich gelten, wenn es allein dazu dient, Schadensersatz zu provozieren. Entscheidend ist die Intention, nicht die Anzahl der Anträge. Verantwortliche dürfen solche Anträge zurückweisen, müssen aber die Missbrauchsabsicht konkret nachweisen.

Ein Schadensersatzanspruch scheitert, wenn der Betroffene den Schaden selbst verursacht hat. Der EuGH betont: Die DSGVO schützt Grundrechte, nicht deren

Instrumentalisierung. Wenn Sie bei einem Auskunftsersuchen Anhaltspunkte dafür haben, dass das Ziel nicht die Auskunft, sondern Schadensersatz ist, dann lohnt eine genaue Prüfung, bei der Secorvo gerne unterstützt.

Speicher weg, Dienste weg

Am 13.04.2026 meldete der IT-Dienstleister [ITEBO](#), dass ein zentrales Speichersystem ausgefallen war. Betroffen waren insbesondere die DNS-Server. Die Vertriebsmitarbeiterinnen Jeanett Conquest und Katharina Hässler beschrieben daraufhin ziemlich genau, was schiefgegangen ist: Transparenz schafft Vertrauen. Leider entfernte das Unternehmen die Seite, nachdem die Störung behoben war; in der [WayBack-Machine](#) ist sie zum Glück noch zu finden.

Auch ein redundantes zentrales Speichersystem kann ausfallen. Für kritische Dienste wie DNS fordert [RFC 1034](#) daher seit 1987 mehrere Nameserver, [RFC 2182](#) (1997) verlangt sogar geografische Verteilung auf getrennten Netzsegmenten und bei unterschiedlichen Upstream-Providern. DNS benötigt kaum Speicherplatz und repliziert seine Datenbank automatisch – es gibt daher keinen Grund, DNS-Server von einem gemeinsamen SAN abhängig zu machen. Wer das trotzdem tut, verletzt einen drei Jahrzehnte alten Standard.

Secorvo News

Secorvo Seminare

Freie Plätze für Kurzentschlossene: [19.-21.05.2026 | Vorfall-Experte](#). Wir bereiten Sie auf die Zertifizierung zum Vorfall-Experten nach dem Curriculum des BSI vor. Für alle, die im Bereich Informationssicherheit, IT-Sicherheit, Datenschutz, Notfallplanung oder der Aufrechterhaltung des Geschäftsbetriebs Verantwortung tragen.

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

Für alle Beteiligten im Software Entwicklungsprozess wie Requirements Engineers, Software Architekten, Entwickler und Projektmanager: [29.06.-02.07.2026 | T.P.S.S.E.](#) Wir zeigen Ihnen, wie Sie durch die systematische Integration des Themas „Sicherheit“ in den Software Development Lifecycle Sicherheitslücken proaktiv vermeiden können.

Seminarprogramm und Online-Anmeldung finden Sie unter <https://www.secorvo.de/seminare>.

Kevin – Allein im Netz?

2024 wurden dem BKA 131.000 Cybercrime-Fälle mit Tätern in Deutschland bekannt, darunter 950 Ransomware-Angriffe. Mit 32% lag die Aufklärungsquote deutlich unter der Quote von 58% der polizeilichen Kriminalstatistik. BKA und Landeskriminalämter haben in den vergangenen Jahren zahlreiche Maßnahmen ergriffen, um diese wachsende Bedrohung zu bekäm-

pfen. Dazu zählt die Aufklärung besonders komplexer Verfahren in Cybercrime-Zentren der Bundesländer.

Die Leiterin des Cybercrime-Zentrums (CCZ) Baden-Württemberg, Tomke Beddies, wird auf dem [kommenden KA-IT-Si Event](#) am 11.06.2026 beim CyberForum vorstellen, welche Fälle im CCZ bearbeitet werden, und einen Einblick in Bekämpfungsstrategien des CCZ geben.

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](#).

Mai 2026	
10.-14.05.	Eurocrypt 2026 (IACR, Rom/IT)
19.-21.05.	Vorfall-Experte (BSI) (Secorvo, Karlsruhe)
19.-21.05.	27. Datenschutzkongress (EUROFORUM, Berlin)
19.-22.05.	European Identity & Cloud Conference 2026 (KuppingerCole, Berlin/hybrid)
25.-28.05.	PKC 2026 (IACR, Palm Beach/US)
Juni 2026	
08.-10.06.	Entwicklertag 2026 (andrena, GI, ObjektForum, Karlsruhe)
11.06.	Kevin – Allein im Netz? (KA-IT-Si, CyberForum, Karlsruhe)
15.-19.06.	T.I.S.P. - TeleTrust Information Security Professional (Secorvo, Karlsruhe)
15.-16.06.	DuD 2026 (COMPUTAS, Berlin)
18.-19.06.	AREA41 Conference 2026 (AREA41, Zürich/CH)
22.-25.06.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
22.-25.06.	ACNS 2026 (New York/US)
22.-26.06.	OWASP 2026 Global AppSec (OWASP Foundation, Wien/AT)
29.06-02.07.	T.P.S.S.E. - TeleTrust Professional for Secure Software Engineering (Secorvo, Karlsruhe)

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 (Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an 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.