

Secorvo Security News

März 2026



Vom Sams lernen

Wer kennt nicht Paul Maars wundervolles Buch „Eine Woche voller Samstage“? Ein Kinderbuch voller Weisheiten. Eine ist die Sache mit dem Büroschlüssel, die Herrn Taschenbier einen freien Tag beschert. Sein Chef, Herr Oberstein, hat diesen nämlich zur Sicherheit versteckt: in ein Taschentuch gewickelt, dann in einem Stiefel im Kleiderschrank eingeschlossen, den Schrankschlüssel in eine Zigarrenkiste gelegt und die Kiste in der Schreibtischschublade verschlossen. Dann hat er vergessen, wohin er den Schubladenschlüssel geräumt hat.

Während man noch über die Tollpatschigkeit von Herrn Oberstein lächelt, loggt man sich vielleicht gerade in seinem Online-Banking-Account ein, um kurz den Kontostand zu prüfen. Oder besser: Man will sich einloggen. Doch die letzte Zwei-Faktor-Authentifikation ist gerade 91 Tage her und muss wiederholt werden. Welches Verfahren war das? Braucht man dafür den TAN-Generator, bei dem vor zwei Tagen die Batterie aufgegeben hat? Oder die Banking-App – oh je, hat man auch daran gedacht, sie auf das neue Handy umzuziehen?

Schon ein wenig genervt (es sollte doch ganz schnell gehen) vertippt man sich dann dreimal bei der PIN – Account gesperrt. Kein Problem: Es gibt ja noch ein Telefon. Hatte man für solche Fälle nicht vor ein paar Jahren ein Telefonpasswort festgelegt? Und an einem sicheren Ort hinterlegt? Mist. Geht sicher auch ohne. Ja, sagt einem der freundliche Bankberater – durch Vorlage des Personalausweises in der nächsten Filiale. Knapp 250 km entfernt. Vielleicht hätte man nach dem letzten Umzug doch die Hausbank wechseln sollen?

Wir leben in einer Welt der Obersteins: Für jeden Zugang ein anderes Passwort, eine andere 2FA-Methode und ein anderer Rücksetzungsprozess. Und mit ein wenig Pech hat man sich ausgeschlossen. Einfacher und benutzerfreundlicher wäre ein einheitliches Verfahren, z. B. die Online-Ausweisfunktion des Personalausweises. Die fände sich am selben Ort wie Obersteins Schubladenschlüssel: in der Hosentasche.



Inhalt

Vom Sams lernen

Security News

Zauberlehrling

Old School Hack

Kein Bug. Ein Feature.

Gültig nur mit Unterschrift

Heiß gekocht, kalt gegessen

Abgelaufen

Secorvo News

Secorvo Seminare

Rogue, thou hast liv'd too long

Veranstaltungshinweise

Fundsache

Security News

Zauberlehrling

Am 23.02.2026 veröffentlichten 38 Forschende unter der Leitung von Natalie Shapira auf arXiv die Studie „[Agents of Chaos](#)“. Zwei Wochen lang hatten sie autonome KI-Agenten in einer realen Laborumgebung betrieben – ausgestattet mit persistentem Speicher, E-Mail-Zugängen, Discord, Dateisystem und Shell-Zugriff. Zwanzig Forschende arbeiteten währenddessen sowohl unter normalen als auch unter adversarialen Bedingungen (also mit gezielten Manipulationsversuchen) mit den Agenten. Als Modelle kamen Claude Opus 4.6 und Kimi K2.5 zum Einsatz – modernste KI-Technik.

Ergebnis: In elf dokumentierten Fällen führten die Agenten Aufgaben ohne Berechtigung aus, legten sensible Informationen offen, lösten Denial-of-Service-Zustände aus, täuschten Identitäten vor, verbrauchten unkontrolliert Ressourcen und übernahmen Systeme teilweise. Mehrfach widersprachen die gemeldeten Aufgabenabschlüsse dem tatsächlichen Systemzustand.

Die Studie wirft die Frage auf, wer für den Schaden haftet, den ein autonomer Agent anrichtet. Unternehmen, die autonome KI-Agenten planen oder bereits einsetzen, sollten die Studie lesen – und Agenten nur mit den minimal erforderlichen Rechten ausstatten, alle Aktionen protokollieren und Eskalationspfade für unvorhergesehene Handlungen definieren. Least Privilege gilt für Agenten genauso wie für menschliche Nutzer – nur stellen Agenten keine Rückfragen.

Old School Hack

Am 16.03.2026 beschrieben Forscher von SRLabs in einem [Blogbeitrag](#), wie sie einen nicht namentlich genannten Enterprise-KI-Assistenten vollständig kompromittierten – nicht über das KI-Modell, sondern über die zugehörige Webanwendung. Der Türöffner: „DEBUG = True“ in der Produktivumgebung.

Djangos eigene [Dokumentation](#) macht es unmissverständlich: „Never deploy a site into production with DEBUG turned on.“ Im Debug-Modus liefert das Framework bei jedem Fehler vollständige Stack Traces und sämtliche Umgebungsvariablen, darunter ADMIN_USERNAME und ADMIN_USER_PWD im Klartext. Die Forscher fanden die Backend-URL in den JavaScript-Quelldateien. Ein einzelner nicht authentifzierter GET-Request genügte, um die Debug-Seite auszulösen und damit Admin-Credentials im Klartext zu erhalten. Das Panel kannte weder Rate-Limiting noch MFA – und enthielt OAuth-Tokens von Microsoft Entra ID, mit denen die Forscher Millionen Mitarbeiterprofile über die Microsoft Graph API abfragen konnten.

Das OWASP [Django Security Cheat Sheet](#) und das [Secrets Management Cheat Sheet](#) beschreiben beide Schwachstellenklassen seit Jahren. Django liefert mit manage.py check --deploy sogar ein eingebautes Werkzeug, das DEBUG = True in Produktion explizit meldet. Wer einen KI-Assistenten einführt, sollte diesen Check zur Pflicht machen – und Secrets nicht in Umgebungsvariablen, sondern in dedizierten Secret-Management-Systemen verwalten.

Kein Bug. Ein Feature.

Am 02.03.2026 beschrieb [Microsoft](#), wie Angreifer den OAuth-Mechanismus durch einen Designfehler ausnutzen können, ohne dafür eine Sicherheitslücke

zu benötigen. Dazu registriert ein Angreifer eine reguläre OAuth-App und hinterlegt eine Phishing-Domain als Redirect-URL. Dem Opfer schickt er eine vertrauenswürdig wirkende E-Mail mit einem offiziellen Microsoft-Link. Doch manipulierte Parameter sorgen für einen Fehler im OAuth-Flow, wodurch der Empfänger automatisch an die Redirect-URL weitergeleitet wird. Dort können seine Anmeldedaten abgegriffen oder Schadsoftware wie Ransomware nachgeladen werden.

Da der Link in der E-Mail tatsächlich von Microsoft stammt, greifen klassische Awareness-Tipps wie das Prüfen von Links hier nicht. Erst nach dem provozierten Fehler erfolgt die Weiterleitung auf die schädliche Domain, sodass man den Angriff kaum visuell erkennen kann. Wirksam sind allein technische Maßnahmen: Eine [Beschränkung der Entra-ID](#) auf eigene oder explizit zugelassene OAuth-Apps kann verhindern, dass externe Anwendungen überhaupt OAuth-Flows starten dürfen. Restriktive [Consent Policies](#) und [Conditional-Access-Regeln](#) können helfen, riskante oder unbekannte App-Zugriffe zu blockieren. Dadurch lässt sich ein Missbrauch des OAuth-Mechanismus zumindest deutlich erschweren.

Gültig nur mit Unterschrift

Am 20.02.2026 löste Roel van Bueren, Spezialist für Softwareverteilung, auf LinkedIn eine [Diskussion](#) über das populäre Open-Source-Projekt [7-Zip](#) aus: Weder Installer noch Binaries sind digital signiert; Windows warnt die Anwender (zu Recht) vor der Installation. Das ist nicht einmal ein theoretisches Risiko, denn erst im Februar wurde die gefälschte Downloadseite [7zip.com](#) [abgeschaltet](#).

Microsoft bietet mit [Artifact Signing](#) und ihrem [Store](#) eigene Lösungen an, die aber viele Entwickler

freier Software als proprietär ablehnen. Code-Signing-Zertifikate aber kosten bei [üblichen Anbietern](#) jährlich über 200 US\$. Das CA/Browser-Forum, das Richtlinien für den Umgang mit öffentlichen Zertifikaten herausgibt, legt zudem in seinen [Anforderungen](#) fest, dass der Signaturschlüssel in sicherer Hardware, etwa einer Smartcard, gespeichert wird. Aber das Entwickeln von Open-Source-Software ist meist eine brotlose Kunst.

Immerhin sind viele Open-Source-Anwendungen für Windows, etwa Notepad++, Audacity, VLC und KeePass digital signiert. Doch 7-Zip ist kein Einzelfall: Auch [FileZilla](#) ist bislang nicht signiert. Unternehmen und Institutionen, die diese Anwendungen kostenlos nutzen, sollten die Entwickler im eigenen Interesse unterstützen, um ihnen das Signieren finanziell zu ermöglichen.

Heiß gekocht, kalt gegessen

Am 08.01.2021 [verhängte](#) das LfD Niedersachsen ein Bußgeld in Höhe von 10,4 Mio. € gegen notebooksbilliger.de. Der Onlinehändler legte Widerspruch ein und das Landgericht Hannover [reduzierte das Bußgeld](#) 2024 auf 0,7 Mio. €. Wenig erstaunlich ging das Verfahren daraufhin in die nächste Instanz: Das OLG Celle setzte das Bußgeld auf 0,9 Mio. € fest – 8,5% des ursprünglichen Betrags.

Wie sinnvoll ist die Verhängung hoher Bußgelder, wenn sie anschließend von den Gerichten regelmäßig zurechtgestutzt werden? Die Ursache ist in den schwammigen gesetzlichen Regelungen zur Bemessung der Bußgeldhöhe zu finden. Zunächst gab es lediglich Vereinbarungen der Aufsichtsbehörden zum Vorgehen bei der Bußgeldbemessung.

Das hat sich inzwischen maßgeblich geändert. In den [EDSA-Leitlinien](#) zur Bußgeldbemessung wurden am

12.05.2022 ([SSN 5/2022](#)) Leitplanken festgelegt: Sie beschreiben ein 5-stufiges Modell zur Berechnung von Bußgeldern, das u. a. die Schwere des Verstoßes, die Umsatzgröße des Unternehmens und erschwerende oder abschwächende Umstände berücksichtigt. An diesem Berechnungsmodell sollten sich auch die Gerichte orientieren, denn wiederholte Zehntelungen verhängter Bußgelder könnten Unternehmen verleiten, diese schlichtweg einzupreisen.

Abgelaufen

Am 06.03.2026 ist die Frist zur [Registrierung](#) für von NIS2 betroffenen Unternehmen abgelaufen. Gemäß den Angaben auf der Webseite des BSI als zuständiger Aufsichtsbehörde müssten sich [29.500 Unternehmen registrieren](#). Bisher sind es gerade einmal 11.000. Wenn sich die Fachleute des BSI nicht verschätzt haben, riskieren 18.500 Unternehmen damit wissentlich oder unwissentlich ein Bußgeld.

Die Prüfung, ob ein Unternehmen unter die Regelungen des BSI-Gesetzes fallen, kann mit juristischer Unterstützung erfolgen. Bei der Umsetzung der Anforderungen der neuen Regelungen unterstützt Secorvo gerne fachlich.

Secorvo News

Secorvo Seminare

Für Kurzsentschlossene gibt es noch freie Plätze im Seminar [21.-22.04.2026 | IT Security Insights](#). Sie erhalten 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 und Datenschutz – mit offizieller Zertifizierung durch TeleTrust und DEKRA. Ideal für erfahrene IT-Sicherheitsverantwortliche, die ihre Qualifikation sichtbar machen möchten.

Programme und die Möglichkeit zur Online-Anmeldung finden Sie [hier](#).

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](#).

April 2026	
14.-16.04.	Datenschutztag 2026 (WEKA-Akademie, Frankfurt)
14.-16.04.	PQCrypto 2026 (IACR, Saint-Malo/FR)
16.04.	KA-IT-Si-Event „Rogue, thou hast liv'd too long“ (KA-IT-Si, Karlsruhe)
21.-22.04.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
21.-24.04.	Black Hat Asia 2026 (Blackhat, Singapur/AS)
28.-29.04.	Cybersecurity Summit 2026 (Trailblazer Summits Group, Hamburg)
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)

Fundsache

„Shock! Shock!“ So beginnt Donald Knuth seinen am 28.02.2026 veröffentlichten [Aufsatz](#) „Claude's Cycles“: Innerhalb einer Stunde und in 31 systematischen Erkundungsschritten löste Claude Opus 4.6 ein offenes graphentheoretisches Problem, an dem der Stanford-Informatiker selbst wochenlang gearbeitet hatte. Lesenswert auch für alle, die sich fragen, was KI-gestützte mathematische Deduktion für die Zukunft der Kryptografie bedeuten könnte.

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.

