

Secorvo Security News

Januar 2026



Denkfehler

Stolz sind wir auf unser Gehirn, das täglich 400-500 Kalorien (20% unseres Energiebedarfs) verbraucht – im Ruhezustand. Fangen wir an richtig nachzudenken, verdoppelt sich sein Energiehunger. Doch die Ergebnisse sind oft dürftig – denn uns unterlaufen systematische Fehler, die Psychologen wie [Daniel Kahneman](#) in den vergangenen 50 Jahren entdeckt haben. Sie führen zu Fehlentscheidungen – nicht nur manchmal, sondern ständig.

Ein Beispiel aus dem Alltag. Ein CISO führt eine (aufwändige) Phishing-Kampagne durch. Am Jahresende lobt ihn der Vorstand: Anders als bei einem Mitbewerber kam es zu keinem Sicherheitsvorfall. Das Lob sei dem CISO gegönnt – allerdings darf bezweifelt werden, dass er es damit verdient hat. Denn der Vorstand hat Korrelation (Phishing-Kampagne und kein Vorfall) mit Kausalität verwechselt: Gab es denn nachweislich einen durch „Nicht-Klicken“ verhinderten Angriff? War das Unternehmen vielleicht nur zufällig nicht das Ziel eines solchen? Oder hat das konsequente Patch-Management geholfen – denn irgendjemand klickt immer, Kampagne hin oder her? Oder war nur die Software nicht im Einsatz, deren Schwachstellen die Phishing-Angriffe auszunutzen versuchten?

Der Vorstand entscheidet, nun regelmäßig Phishing-Trainings durchzuführen – das machen ja andere Unternehmen auch (ein klassischer Social-Proof-Fehler). Damit vernichtet er Arbeitszeit und verknappt das Budget für womöglich sinnvollere Schutzmaßnahmen: Der potentielle Schaden eines Ransomware-Angriffs ist so beeindruckend groß, dass er dessen Eintrittswahrscheinlichkeit missachtet – die, wenn der CISO einen guten Job gemacht hat, sehr klein sein kann. Maßnahmen zur Angriffserkennung oder Schadensbegrenzung verringern das Risiko vielleicht weit mehr – auch das anderer Angriffsarten.

Kennen wir die Denkfallen, die unser Gehirn uns stellt, können wir unsere Entscheidungen verbessern. Auch in der IT-Sicherheit.

(Mehr dazu am 26.02.2026 auf dem [Jahresauftakt-Event der KA-IT-Si.](#))

Security News

BodySnatcher

Am 13.01.2026 veröffentlichte der Sicherheitsforscher Aaron Costello (AppOmni) den [detaillierten Bericht](#) zu einer kritischen Schwachstelle, über die er am 23.10.2025 die betroffene KI-Plattform [ServiceNow](#) informiert hatte ([CVE-2025-12420](#)). Mit einem CVSS-Score von 9.3 sei dies die „schwerste KI-getriebene Schwachstelle, die bisher entdeckt wurde“.

Die [Schwachstelle](#) steckte in der Virtual-Agent-API, Basis für alle Chatbot-Funktionen einschließlich der KI-gestützten Now-Assist-Agenten. Diese Agenten nutzten für die Authentifikation von Drittanbietern den String „servicenowexternalagent“; zur User-Identifikation genügte die E-Mail-Adresse: Weder Passwort noch MFA waren erforderlich. Ein Angreifer konnte so beliebige Benutzerkonten übernehmen und die KI-Agenten für sich arbeiten lassen. Costello demonstrierte, wie er einen KI-Agenten ein neues Admin-Konto anlegen ließ; so erhielt er Vollzugriff auf die Plattform.

ServiceNow hat die Lücke am 30.10.2025 geschlossen; Hinweise auf eine Ausnutzung der Schwachstelle gibt es bisher nicht. Vielleicht hätte ein Blick in die [OWASP TOP 10 for Agentic Applications](#) geholfen, den Fehler zu vermeiden: „Identity & Privilege Abuse“ steht darin auf Platz drei (ASI03). Oder ein Besuch unseres [Seminars zur sicheren Software-Entwicklung](#) (T.P.S.S.E.).

Bei aller KI-Begeisterung: Auch für AI-Agenten gilt „*It's important to implement a review process prior to deploying them to production environments*“, wie Costello zu Recht [schreibt](#).

Blue Screen of Death

In den [SSN 3/2025](#) berichteten wir über „ClickFix“-Angriffe, bei denen Anwender aufgefordert werden, mit der Tastenkombination „Windows+R“, „Strg+V“ und „Enter“ einen via JavaScript in die Zwischenablage kopierten Befehl auszuführen, der dann Schadsoftware lädt.

Am 16.12.2025 [meldete](#) der Sicherheitsforscher „JAMESWT“ eine Variante, bei der ein Windows-Systemabsturz vorgetäuscht wird: Der „Blue Screen of Death“ enthält die Anweisungen zum Herunterladen der Schadsoftware ([Demo](#)). Kreativ ist auch die am 16.01.2026 im Huntress-Blog beschriebene Variante „CrashFix“, die sogar einen Absturz des Edge-Browsers herbeiführt.

Angesichts der Wirksamkeit dieser Angriffsmethode bei Anwendern ohne IT-Kenntnisse sollte, [wie schon empfohlen](#), die Tastenkombination „Run/Ausführen“ [per Gruppenrichtlinie](#) deaktiviert werden. Noch wirksamer ist es, den Zugriff auf PowerShell mit Mitteln wie [AppLocker und WDAC](#) zu unterbinden.

Rule Breaker

Nach einem fehlerhaften Software-Update hat die [irische Passbehörde](#) zwischen dem 23.12.2025 und dem 06.01.2026 Pässe ausgestellt, in denen der Zusatz „IRL“ fehlt – sie sind nach den internationalen Luftfahrt-Standards der ICAO ungültig. Laut „[The Irish Times](#)“ sind rund 13.000 Ausweise betroffen.

Die irische Behörde hat alle Grenzstellen weltweit informiert – und diese Pässe, bis auf weiteres, für „gültig“ erklärt. Gleichzeitig wurden alle Betroffenen aufgefordert, die fehlerhaften Ausweise an die Adresse „Passport Return, Customer Care, Passport Service“ zurückzusenden.

Ein klassischer Fall von ‚[Move fast and break things](#)‘: Keine Hinweise zu einem sicheren Versand, eine

Adresse, die verrät, dass sich im Umschlag ein Pass befindet – und eine nachträgliche Gültig-Erklärung für nach internationalen Regeln ungültige Ausweisdokumente. Unfassbar.

Cheating the cheater

Das US-amerikanische Cybersicherheitsunternehmen Resecurity [berichtete](#) am 24.12.2025 über den Erfolg eines Honeytrap-Kontos mit synthetischen Daten, die so aus im Dark Web geleakten Informationen erzeugt worden waren, dass deren Struktur der offiziellen Stripe API des Unternehmens entsprach.

Ein Angreifer legte beim Auslesen der vermeintlich wertvollen Daten seine echte IP-Adresse offen, und eine bekannte Cybercrime-Gruppe hielt den Honeypot für ein kompromittiertes System und behauptete öffentlich, Resecurity gehackt zu haben.

Gut gestaltete Honeypots können Angreifer von den operativen Systemen ablenken; sie vereinfachen die Detektion und ermöglichen so eine frühe Reaktion. Sie sind daher ein wertvolles Element in jeder Intrusion-Detection-Strategie.

PQC Award

Die Migration zur Post-Quanten-Kryptografie drängt ([SSN 06/2025](#)). Geeignete Verfahren wurden vom US-amerikanischen NIST bereits [standardisiert](#), darunter [ML-KEM](#) zur Verschlüsselung, das u. a. in der Hybrid-Variante „X25519MLKEM768“ schon [rund die Hälfte des Datenverkehrs bei Cloudflare](#) schützt.

Wie viele der [vorgeschlagenen Verfahren](#) verwendet ML-KEM eine Technik, die am 04.12.2025 auf der Kryptografie-Konferenz [TCC 2025](#) mit dem „[Test-of-Time-Award](#)“ ausgezeichnet wurde. Sie ermöglicht es, ein schwach sicheres Verschlüsselungsverfahren in ein Verfahren zu transformieren, das starke Sicherheit gegen aktive Angriffe bietet.

Die Autoren Dennis Hofheinz (ETH Zürich, damals Karlsruher Institut für Technologie, KIT), Kathrin Hövelmanns (TU Eindhoven) und Eike Kiltz (Ruhr-Uni Bochum) passten dafür eine Transformation für den Post-Quanten-Einsatz an (publiziert auf der [TCC 2017](#)).

Secorvo News

Secorvo live

Auf der diesjährigen [Heise-Konferenz secIT](#) (17.-19.03.2026) werden Kai Jendrian und Oliver Oettinger aus dem [Secorvo-Consulting-Team](#) unter dem Titel „Das Risiko-Dilemma: Wenn gängige Methoden an ihre Grenzen stoßen“ ein paar heilige Kühe des Risikomanagements schlachten – und einige praxiserprobte Methoden vorstellen.

Von Experten für Experten

[05.03.2026 | NIS-2 – Risikomanagement am Kamin](#) gestaltet die Pflichtschulung für Geschäftsleitungen als Kaminabend mit Erfahrungsaustausch. Sie erwerben die nach § 38 BSI geforderten Kenntnisse zum Risikomanagement und profitieren von den Erfahrungen anderer Führungskräfte und unserer Risikoman-

gement-Experten – gemeinsames Dinner in der [Villa Hammerschmiede](#) in Söllingen (bei Karlsruhe) inklusive ([Anmeldung](#)).



[23.+24.03.2026 | ISMS verstehen und planen](#) unterstützt Sie bei der Konzeption Ihres Informationsmanagementsystems oder der Vorbereitung auf eine Zertifizierung: In zwei Tagen entwickeln Sie Ihre individuelle ISMS-Roadmap – von der Gap-Analyse bis zum Audit. Praxisnah, interaktiv und ohne spezielle ISMS-Vorkenntnisse. Weitere Termine und die Möglichkeit zur Online-Anmeldung finden Sie unter <https://www.secorvo.de/seminare>.

Wenn Du denkst, Du denkst...

Warum kümmern sich Unternehmen oft erst um Informationssicherheit, wenn etwas passiert ist? Und warum gelingt es nicht immer, die Notwendigkeit von Informationssicherheit – und die dazu erforderlichen Maßnahmen – Kollegen, Mitarbeitern und manchmal auch der Unternehmensleitung zu vermitteln?

Die Ursachen hierfür sind tief in uns verankert: Das menschliche Gehirn arbeitet mit Heuristiken, bei denen uns ständig systematische Fehler unterlaufen. Der Nobelpreisträger David Kahneman hat sie „kognitive Verzerrungen“ genannt; Rolf Dobelli spricht von Ablenkungen vom „klaren Denken“.

Ein tieferes Verständnis dieser typischen „Denkfehler“ ermöglicht uns nicht nur bessere Entscheidungen zu treffen, sondern hilft auch die Erfordernisse der IT-Sicherheit wirksamer zu vermitteln.

Beim **Jahresauftakt-Event 2026** der [Karlsruher IT-Sicherheitsinitiative](#) stellt Dirk Fox (Secorvo) typische kognitive Verzerrungen vor und demonstriert, wie ihre Berücksichtigung zu höherer Informationssicherheit, wirksamerer Kommunikation und mehr Awareness im Unternehmen führen kann. Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“.

Wir freuen uns auf Sie am **26.02.2026** um 18:00 Uhr im Haus der Wirtschaft der IHK Karlsruhe. Bei Interesse empfehlen wir eine schnelle [Anmeldung](#).



Veranstaltungshinweise

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

Februar 2026	
18.-19.02.	ID:SMART Workshop 2026 (CAST, Darmstadt)
26.02.	KA-IT-Si-Event „Wenn Du denkst, Du denkst...“ (KA-IT-Si, Karlsruhe)
März 2026	
05.03.	NIS-2 - Kaminabend zum Risiko-management (Secorvo, Karlsruhe)
17.-19.03.	secIT 2026 (Heise Medien, Hannover)
23.-24.03.	ISMS verstehen und planen (Secorvo, Karlsruhe)
23.-26.03.	RSA Conference 2026 (RSA Conference, San Francisco/US)
23.-27.03.	FSE 2026 (IACR, Singapur/ASE)
24.-27.03.	DFRWS EU 2026 (DFRWS, Linnköping/SE hybrid)
April 2026	
14.-16.04.	Datenschutztag 2026 (WEKA-Akademie, Frankfurt)
14.-16.04.	POCrypto 2026 (IACR, Saint-Malo/FR)
21.-22.04.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)

Fundsache

Die [Fantom App](#) der [CNIL](#) erklärt einfach und verständlich, wie man seine Privatsphäre in sozialen Medien aktiv schützt, persönliche Daten kontrolliert und unerwünschte Freigaben vermeidet. Eine deutsche Version wäre absolut wünschenswert.

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.