Secorvo Security News

November 2025

Gel(i)ebte Freiheit

Risikomanagement ist in vielen Unternehmen ein ungeliebtes Kind: Entweder fristet es ein trauriges Schicksal als Teil des Compliance-Buzzword-Bingo oder es quält Riskmanager und Unternehmensleitungen Jahr für Jahr bei dem Versuch, das nicht Messbare irgendwie zu objektivieren.

Mit etwas Distanz betrachtet wirkt das eigenwillig. Denn „Management" ist Tag für Tag nichts anderes als der Umgang mit Risiken: Marktrisiken, Inflationsrisiken, Innovationsrisiken, Personalrisiken, Wettbewerbsrisiken, Sicherheitsrisiken: Jede Management-Entscheidung ist eine Entscheidung über eine ungewisse Zukunft, die sich im Rückblick als falsch erweisen kann. Das ist – riskant. Will man dieses Risiko senken, das Ungewisse also etwas „beherrschbarer" machen, hilft manchmal Erfahrung, manchmal „eine gute Nase" (sprich: Glück) – und fast immer die Begrenzung des möglichen Schadens (nicht alle „eggs in one basket") sowie die Erhöhung der „Eintrittsbarrieren" für den Fehlerfall.

Dreierlei ist jedoch gewiss: Ein Ausschluss aller Risiken ist unmöglich, die Minimierung der Auswirkungen von Fehlentscheidungen zu teuer und eine umfassende Risikovermeidung ein Selbstmord in Raten. Management bleibt ein Balanceakt – anders wäre es nur, wenn wir die Zukunft verlässlich voraussagen könnten. Doch dann könnte das jeder, und die Freiheit wäre, ganz nebenbei, auch dahin: Eine vorhersagbare Zukunft lässt sich nicht mehr beeinflussen.

Warum feiern wir nicht unsere Entscheidungsfreiheit und erfreuen uns daran, dass wir Risiken managen dürfen? Nachdenken über die Konsequenzen von Entscheidungen ist dann nichts als die Übernahme von Verantwortung – und zielt auf die Vermeidung unnötiger und unvertretbarer Risiken. Genau das sollte ein gutes Risikomanagement leisten: Maßnahmen gegen vermeidbare und inakzeptable Risiken ergreifen. Vielleicht hilft ja die NIS-2-Richtlinie, das Risikomanagement aus der staubigen Schmuddelecke wieder ins (rechte) Licht zu rücken.

Security News

Künstliche Objektivität

Am 23.10.2025 warnten die IT-Sicherheitsexperten Gadi Evron und Bruce Schneier vor der Möglichkeit, von KI-Helfern erzeugte Gesprächsprotokolle zu manipulieren. Ähnlich der Suchmaschinenoptimierung lassen sich auch KI-Zusammenfassungen durch gezielte Formulierungen im Gespräch beeinflussen. Bei dem von ihnen „AI summarization optimization" getauften Vorgehen sorgen Phrasen wie „Unsere wichtigste Erkenntnis ist…" für eine Priorisierung von Themen – die

vermeintliche Objektivität der KI-Zusammenfassung entpuppt sich dabei als Irrglaube.

In ihrem Beitrag verweisen sie auf mehrere Studien, die zeigen, wie solche Manipulationen gelingen. Sie raten Nutzern von KI-Protokollanten, solche Einflussnahmen durch Gesprächsteilnehmer zu unterbinden. Organisationen sollten hierfür klare Regeln festlegen. Auch technische Gegenmaßnahmen können helfen, wie die Prüfung auf auffällige Formulierungen oder das Filtern von Prompt Injections.

Unzureichend verschlüsselt

Im September wurden sämtliche in der Cloud gespeicherten Konfigurationssicherungen von SonicWall-Firewalls gestohlen. Einzelheiten hat SonicWall in der zuletzt am 28.10.2025 aktualisierten Mitteilung an ihre Kunden offengelegt.

Danach verschlüsselte das Sicherungsverfahren lediglich die in der Konfiguration enthaltenen Passwörter und Schlüssel – mit AES-256, bei älteren Systemen mit 3DES. Alle übrigen Daten waren im Klartext gespeichert. Sie liefern wertvolle Einblicke in die interne Netzwerkstruktur der SonicWall-Kunden.

Sicherheitshalber wurden die Kunden aufgefordert, die Zugangsdaten ihrer Firewalls zu ersetzen.

Grundsätzlich ist gegen eine Sicherung in der Cloud wenig einzuwenden – vorausgesetzt, das gesamte Backup wird verschlüsselt und der Schlüssel wird außerhalb der Cloud aufbewahrt.

Und immer wieder Cookies

Am 04.11.2025 veröffentlichte die Bundesbeauftragte für den Datenschutz die Ergebnisse einer forsa-Umfrage zu Cookie-Einwilligungen. Die Erkenntnisse überraschen nur teilweise: Zwar ist 83% die Kontrolle über die eigenen Daten wichtig oder sehr wichtig; dennoch assoziieren 37% eher Negatives mit dem Begriff Datenschutz. Auch wenn 56% nicht genau wissen, was Cookies sind, lehnen 77% nach eigenen Angaben in Cookie-Bannern nach Möglichkeit alles ab. 75% vertrauen nicht einmal darauf, dass sich Anbieter an ihre Einstellungen halten.

Angesichts der nach wie vor weiten Verbreitung von Bannern ohne „Alles ablehnen"-Knopf ist der Handlungsbedarf offensichtlich: Ohne schärfere Sanktionen gegen gesetzeswidrige Banner dürfte auch die Akzeptanz des Datenschutzes Schaden nehmen.

Mehr Pflichten, mehr Haftung

Am 13.11.2025 verabschiedete der Deutsche Bundestag das Umsetzungsgesetz zur NIS-2-Richtlinine; kurz darauf stimmte der Bundesrat zu. Damit wird das BSI-Gesetz an die Vorgaben der NIS 2-Richtlinie angepasst – mit weit reichenden Konsequenzen für Unternehmen und ihre Verantwortlichen (§ 30 BSIG).

Bisher unterlagen bereits die KRITIS-Bereiche strengen Audit- und Nachweispflichten, die nun in § 39 BSIG verankert sind. Doch das Gesetz geht weiter: Künftig kann das BSI auch für bisher nicht erfasste Branchen Nachweis- und Auditpflichten anordnen, sobald es ein entsprechendes Risiko in einer (besonders) wichtigen

Einrichtung erkennt. Damit steigt die Zahl der potentiell betroffenen Unternehmen deutlich, die dieser „Auditgefahr“ ausgesetzt sind.

Eine zentrale Anforderung ist die neue Schulungspflicht für Geschäftsleiter: Wer nicht nachweisen kann, dass er sich zu „Kenntnissen und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken“ der Informationssicherheit fortbildet und Risikomanagementmaßnahmen überwacht, setzt sich der Gefahr persönlicher Haftung aus (§ 38 BSIG).

Um dieser Haftung vorzubeugen bietet Secorvo 2026 „NIS-2-Kaminabende“ an, auf denen wir nicht nur die erforderlichen Kenntnisse im Risk-Management vermitteln, sondern zugleich ein C-Level-Forum für den Erfahrungsaustausch bieten (Terminanfragen bitte an info@secorvo.de).

Nord-Süd-Gefälle

Am 15.11.2025 veröffentlichte der Hessische Landesbeauftragte für Datenschutz seinen Bericht zur datenschutzkonformen Nutzung vom MS365. Während Schleswig-Holstein – auch aufgrund der Einschätzungen des ULD – mit seiner Open-Source-Strategie die Abhängigkeit von Microsoft verringert, schlagen Hessen und Bayern den entgegengesetzten Kurs ein: Sie bauen auf eine vertrauensvolle Zusammenarbeit mit dem US-Giganten und auf das schon vom Land Niedersachsen verhandelte Data Protection Addendum (DPA) für öffentliche Stellen.

Kritisch mag stimmen, dass die Zusagen von Microsoft bisher nicht technisch überprüft wurden. Wer MS365 einsetzt, sollte prüfen, inwieweit die Vorgaben aus Hessen umgesetzt sind. Darüber hinaus ist zu hoffen, dass das DPA für öffentliche Stellen bald auch anderen Kunden angeboten wird.

Fake Coding Interviews

Seit Anfang 2024 beobachten Sicherheitsexperten eine Welle von Social-Engineering-Angriffen, die sich gegen Software-Entwickler und IT-Freelancer richten. Am 15.10.2025 beschrieb David Dodda in seinem Blog einen solchen Angriff aus der Perspektive des Opfers.

Dabei täuschen die Täter die Bewerber mit professionell erstellten Firmenprofilen und seriöser Kommunikation. Als Teil des Bewerbungsprozesseses verlangen sie einen vermeintlichen Programmiertest, der als Code-Repository in Bitbucket oder GitHub bereitgestellt wird. Der Code enthält getarnte bösartige Skripte, die bei Ausführung eine Backdoor auf dem System des Bewerbers installieren. Sie verschafft den Hackern Fernzugriff. Das vermutliche Ziel: Anmeldedaten zu Cloud-Diensten und Produktionssystemen von Unternehmen.

Entwickler sollten Code ungesicherten Ursprungs ausschließlich in einer Sandbox oder einer virtuellen Maschine ausführen. Das sollte nicht nur in der eigenen Entwicklungsabteilung Pflicht sein, sondern auch mit Freelancern vereinbart werden.

Schutz vor dem Mittelsmann

Webseiten ohne HTTPS-Unterstützung sind zur Ausnahme geworden. Projekte wie whynohttps.com, die unsichere HTTP-Seiten auflisten, haben daher ihre Bedeutung weitgehend verloren. Zum Schutz vor Man-in-the-Middle-Angriffen sollten unverschlüsselte HTTP-Verbindungen konsequent unterbunden werden.

Mit HTTP Strict Transport Security (RFC 6797) kann ein Server einem anfragenden Browser vorschreiben, eine Webseite künftig ausschließlich über HTTPS aufzurufen. Alternativ können HTTP-Aufrufe automatisch auf HTTPS umgeleitet werden. Beide Verfahren schützen jedoch nicht den ersten Verbindungsaufbau. Daher kündigte Google am 28.10.2025 an, dass Chrome ab Oktober 2026 die Zustimmung des Anwenders einholen wird, bevor es eine öffentliche Website ohne HTTPS lädt.

Administratoren können (und sollten) die Chrome-Einstellung „Immer sichere Verbindungen verwenden" bereits jetzt per Gruppenrichtlinie aktivieren. Erforderliche Ausnahmen lassen sich darin vermerken. Ähnliche Einstellungen bieten Edge und Firefox.

Secorvo News

Risikomanagement für Verantwortliche

§ 38 BSIG verpflichtet Geschäftsleitungen (besonders) wichtiger Einrichtungen, Risikomanagementmaßnahmen umzusetzen und zu überwachen – und sich regelmäßig zu Kenntnissen und Fähigkeiten zur Erkennung und Bewertung von Risiken und Risikomanagementpraktiken der Informationssicherheit weiterzubilden.

Wir machen aus der Not eine Tugend: Auf unseren NIS-2-Kaminabenden führen wir Sie konzentriert und erfahren in diese Praktiken ein – und bieten Ihnen zugleich ein C-Level-Forum für den Austausch mit anderen Verantwortlichen. Die Termine finden Sie ab Mitte Januar 2026 auf unserer Webseite – wir informieren Sie auch gerne per E-Mail.

Seminare 2026

Auf unseren Seminaren vermitteln wir auch 2026 aktuelle Einblicke und bieten praxisorientierte Vertiefungen zu Themen der Informationssicherheit. Mit den Seminaren T.I.S.P., T.P.S.S.E. und Vorfallsexperte bereiten wir Sie auf den Erwerb anerkannter berufsqualifizierender Zertifizierungen vor.

Im kommenden Jahr bieten wir neben dem „Klassiker" zu Konzeption und Aufbau von Public-Key Infrastrukturen mit dem ISMS-Intensivseminar einen praxisorientierten und pragmatischen Einstieg in den Aufbau eines wirksamen Sicherheitsmanagements.

Threat Modeling

Entdeckt man potentielle Sicherheitslücken bereits beim Design eines Systems oder einer Software, lässt sich viel Ungemach vermeiden. Das gelingt durch eine systematische Modellierung möglicher Bedrohungen, denen das System im Betrieb ausgesetzt sein wird –

Threat Modeling ist daher ein Kernelement von Security by Design.

In der Ausgabe 1/2026 der iX führen Oliver Oettinger und Kai Jendrian in die Grundlagen und Möglichkeiten des Threat Modeling ein – von den Grundprinzipien bis zur Tool gestützten Modellierung komplexer Bedrohungsmodelle.

Schöne Weihnachten!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Dezember 2025	
08.-12.12.	Asiacrypt 2025 (IACR, Melbourne/AU)
11.12.	KA-IT-Si-Event "Hokus, Pokus, KIdibus" (KA-IT-Si, Karlsruhe)
Januar 2026	
19.-21.01.	Omnisecure 2026 (in TIME, Berlin)
27.-28.01.	33. DFN Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg)
Februar 2026	
02.-06.02.	IT-Defense 2026 (cirosec, Würzburg)
18.-19.02.	ID:SMART Workshop 2026 (CAST, Darmstadt)
März 2026	
02.-06.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
09.-12.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-19.03.	secIT 2026 (Heise Medien, Hannover)
23.-24.03.	ISMS verstehen und planen (Secorvo, Karlsruhe)

Fundsache

Das Bayerische Landesamt für Datenschutzaufsicht bietet auf insgesamt 24 Seiten eine 10-Punkte-Checkliste mit technischen und organisatorischen Sicherheitsmaßnahmen für mehr Datensicherheit. Die

durchgehend praktischen Umsetzungsvorschläge umfassen auch Anforderungen der ISO/IEC 27001.

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, Julian Wahl

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.