secorvo
security consulting

Secorvo Security News

Mai 2026

Wie wirklich ist die Wirklichkeit?

Vor 50 Jahren erschien der Klassiker der Kommunikationstheorie des Psychotherapeuten *Paul Watzlawick* (1921-2007). Seine Kernthese, dass das „Bild der Wirklichkeit“ in unserem Kopf das Ergebnis individueller Konstruktionsprozesse ist – und deshalb meist von den Wirklichkeitsbildern anderer Menschen abweicht – hat bis heute nicht an Bedeutung verloren.

Im Gegenteil: Noch immer erscheint uns zwischenmenschliche und mediale Kommunikation meist als zumindest im Kern „objektive“ Informationsvermittlung – obwohl unsere eigene Erfahrung immer wieder bestätigt, dass das, was wir mitteilen möchten, selten genau so beim Empfänger ankommt, wie wir es gemeint haben. Dennoch neigen wir dazu, zu glauben, das läge allein daran, dass unsere Gesprächspartner uns nicht richtig zuhören.

Dabei ergänzen Körpersprache, Ausstrahlung, Kleidung, Rollen – aber auch unsere eigenen (Vor-)Urteile, Annahmen, Erfahrungen und Assoziationen – den Informationsanteil von Kommunikation nicht nur, sondern sie verändern ihn auch: Was wir für wahr halten, wird von zahlreichen Faktoren beeinflusst, die uns oft nicht bewusst sind. Bei gutem Wetter und guter Laune wirken dieselben Nachrichten positiver als bei Regen und gedrückter Stimmung; Äußerungen von Menschen, die uns äußerlich besser gefallen und uns freundlich gegenübertreten, erscheinen uns glaubwürdiger, Fremdartiges und Ungewohntes – Wortwahl, Sprachstil, Gesten, Kleidung – macht uns eher misstrauisch. Trotzdem sind wir oft überzeugt, die (einzig) „richtigen“ Einsichten gewonnen und Schlüsse gezogen zu haben.

Daher lässt sich der Verbreitung KI-erzeugter Deep Fakes womöglich doch etwas Positives abgewinnen: Sie erinnern uns, dass viele unserer Urteile auf Plausibilität gründen. Vielleicht lernen wir dadurch, unsere eigenen Wahrnehmungen häufiger kritisch zu überprüfen, bevor wir aus ihnen Überzeugungen und Gewissheiten ableiten.

Inhalt

secorvo
security consulting

Security News

Haftung der Geschäftsleitung

Das BSI hat am 17.04.2026 die Vorgaben für NIS-2-Geschäftsleitungsschulungen angepasst. Einige sehr konkrete Anforderungen wurden gelockert (z. B. regelmäßige Schulungen statt fester Zyklen), für die keine ausreichende gesetzliche Grundlage bestand.

Die grundsätzlichen Pflichten bleiben jedoch bestehen und setzen einen Trend in der EU-Gesetzgebung fort: Immer mehr Pflichten der Geschäftsführung sind nicht (mehr) delegierbar, wie DORA, NIS2, Hinweisgeberschutzgesetz und Lieferkettensorgfaltspflichtengesetz zeigen. Meldepflichten bei IT-Vorfällen, Risikomanagement in der Lieferkette oder Cybersicherheit müssen Geschäftsleitungen persönlich überwachen. Die Haftung bleibt bei ihnen – auch wenn sie die Aufgaben an Dritte übertragen.

Klartext

Am 04.05.2026 berichtete der Sicherheitsforscher Tom Jøran Sønstebyseter Rønning auf X, dass Microsoft Edge alle gespeicherten Passwörter als Klartext im Arbeitsspeicher hält – sogar, wenn man sie aktuell nicht verwendet. Microsofts Reaktion: Das sei kein Fehler, sondern eine Designentscheidung. Vor dem Hintergrund der ausgelösten Diskussionen lenkte das Unternehmen jedoch ein und entschärfte das Verhalten von Edge in Version 148. Forscher von avantguard zeigten allerdings am 22.05.2026, dass sich immer noch Passwörter aus dem Speicher auslesen lassen – sowohl bei Edge als auch bei Chrome.

Aber ist das tatsächlich eine Gefährdung? Ein Angreifer, der den Speicher eines Geräts auslesen kann, kann auch Tastatureingaben mitschneiden – davor schützt kein Passwortmanager. Microsoft schloss die Meldung mit einem Verweis auf sein Bedrohungsmodell, in dem Angreifer mit Codeausführung im Nutzerkontext folgerichtig ausgeklammert sind.

Der wichtigste Nutzen eines Passwortmanagers ist ein anderer: Er ermöglicht für jeden Dienst ein eigenes, starkes Passwort: Dadurch gefährdet ein Passwortverlust nicht sofort alle Konten. Zudem schützt er vor Phishing, denn Browser oder Browser-Erweiterungen tragen Zugangsdaten nur auf der korrekten Seite ein und verweigern den Dienst auf einer gefälschten. Die Klartext-Schwäche sollte man daher nicht überbewerten. Wer sie vermeiden möchte, sollte auf moderne Authentifikationsverfahren wie Passkeys setzen.

Schein statt Sign (I)

Das Landgericht (LG) Karlsruhe wies am 20.05.2026 die Klage eines Ehepaares zurück, das um den Kaufpreis für 42 Goldbarren (109.185 €) betrogen worden war. Nach Darstellung der Parteien wurde die Rechnung per E-Mail an die Käufer geschickt und auf dem Transportweg von einem unbekannten Dritten vertauscht – genau war der Hergang nicht aufzuklären.

Nach Ansicht der Kläger hätte die Verkäuferin die E-Mail mit Ende-zu-Ende-Verschlüsselung schützen müssen und sei deshalb verpflichtet, die Goldbarren zu liefern. Das LG sieht hingegen die Kläger in der Pflicht, eine Risikoabwägung vorzunehmen. Vor der Verhandlung habe das Ehepaar nie auf höhere Sicherheit gedrungen und kommunizierte weiterhin unverschlüsselt mit der Beklagten. Es übermittelte auch nie einen Verschlüsselungsschlüssel, daher habe die Verkäuferin keine Möglichkeit gehabt, die E-Mail zu verschlüsseln.

Kleiner Faktencheck: Tatsächlich wäre der Betrug auch mit einer Ende-zu-Ende-Verschlüsselung nicht zu verhindern gewesen (wie sie in einem ähnlichen Fall das OLG Schleswig-Holstein im Urteil vom 18.12.2024 gefordert hat), denn auch eine gefälschte Rechnung hätte mit dem öffentlichen Schlüssel des Ehepaares verschlüsselt werden können. Gegen Integritätsverletzungen schützen nur digitale Signaturen, und für die benötigt der Versender nur seinen eigenen Schlüssel – das hat sich unter Richtern offenbar noch nicht herumgesprochen.

Schein statt Sign (II)

Am 19.05.2026 berichtete Microsoft über die Zerschlagung von Fox Tempest, einer Cyberkriminellen-Gruppe, die „Malware-Signing-as-a-Service" anbot: Über die Plattform signspace.cloud konnten andere Kriminelle ihre Schadsoftware mit gültigen Microsoft-Zertifikaten digital signieren lassen. Dadurch wirkten die signierten Dateien wie legitime Software und konnten Sicherheitskontrollen umgehen. Für die Identitätsprüfung von Microsofts Dienst Artifact Signing fälschte oder stahl Fox Tempest Identitäten und imitierte echte Organisationen.

Hunderte betrügerische Microsoft-Konten stammten von Fox Tempest; zu den „Kunden" zählten die Hinterleute bekannter Ransomware (Rhysida, Akira) und Gruppen wie Vanilla Tempest oder Storm-0501. Microsoft sperrte im Mai 2026 mehr als 1.000 falsche Codesignatur-Zertifikate.

Der Fall zeigt die Achillesferse digitaler Signaturen: Moderne, KI-gestützte oder biometrische Identitätsprüfungen können mit Deepfakes und künstlich erzeugten Identitäten getäuscht werden. Doch ohne fälschungssichere Identitätsnachweise gibt es auch keine fälschungssicheren Signaturen – und damit keine überprüfbare Integrität.

secorvo
security consulting

Vertrauensgrenzen

Beim Trusted Publishing von npm erhält ein Build-System wie GitHub Actions über OpenID Connect ein kurzlebiges, signiertes JSON-Web-Token, das npm beim Veröffentlichen eines Pakets mit einer zuvor registrierten Kombination aus Aussteller und Identität des Workflows vergleicht. Damit überprüft npm die Herkunft des Build-Prozesses.

Diese Vertrauenskette wurde beim Bitwarden-CLI-Angriff unterlaufen. Wie Bitwarden am 23.04.2026 berichtete, manipulierten Angreifer den Quellcode im Repository; der Build-Prozess erhielt weiterhin gültige Trusted Publishing Token und das Paket wurde veröffentlicht. Denn Trusted Publishing prüft (naturgemäß) nicht die Integrität des übergebenen Codes. Automatisierte Vertrauensmechanismen sollten daher nicht ohne zusätzliche Kontrollen eingesetzt und durch reproduzierbare Builds, strenge Workflow-Regeln und verpflichtende Code-Reviews ergänzt werden.

Geschwächtes Schwachstellenmanagement

Die National Vulnerability Database (NVD) des NIST ist 2025 um knapp 42.000 neue CVEs angewachsen, 45% mehr als jemals zuvor. Am 15.04.2026 kündigte das NIST daher an, die Einträge zu begrenzen: Vollständige CPE-Applicability-Statements, CWE und CVSS-Vektoren wird es zukünftig nur noch für CISA-KEV-Einträge, staatlich genutzte und kritische Software geben; der Rest bleibt „Not Scheduled". Trotzdem wächst der Backlog weiter.

Diese Kapitulation vor dem CVE-Volumen ist eine Datenkrise mit Ansage: In Werkzeugen, die direkt gegen NVD-Applicability-Statements prüfen – wie SBOM-Abgleiche, direktes CPE-Matching ohne Fallback oder Eigenbau-Workflows – fehlen nun die Treffer für „Not Scheduled"-CVEs. Das sind falsch-negative Ergebnisse, die nach Entwarnung aussehen, aber keine sind. Authentifizierte Scanner wie Nessus, Qualys oder OpenVAS trifft das weniger, weil sie eine eigene Detection-Logik mitbringen.

Außerdem gibt das NIST seine Rolle als unabhängiger Zweitbewerter auf und reicht künftig die Scores der jeweiligen CNAs durch. Doch Hersteller bewerten eigene Lücken erfahrungsgemäß zurückhaltender. VulnCheck misst für solche sekundären Quellen Fehlerraten um 15% - bei Primärquellen liegen sie nur bei 1%. Auch die EUVD erbt diese Defizite, denn sie bezieht ihre Kerndaten aus dem CVE-Programm und der NVD – wer NVD oder EUVD weiter stillschweigend als Single Source of Truth verwendet, bekommt nun ein Qualitätsproblem.

Wer Schwachstellenmanagement betreibt (siehe SSN 06/2025), sollte seine Datenversorgung diversifizieren: CISA Vulnrichment für CWE und CVSS (CPE liefert es seit Dezember 2024 nicht mehr), EPSS zur risikobasierten Priorisierung – und für strukturiertes CPE-Matching VulnCheck NVD++ oder Vulners. Für SBOM-Pipelines ist OSV.dev mit GitHub Security Advisories präziser, weil die PURL-Identifier direkt aus dem Paketmanager kommen; für Infrastruktur-Scanner gegen Appliances und Betriebssysteme hilft das nicht. Die EUVD bleibt nützlich für Exploitation-Status, Patch-Hinweise und CSAF-Advisories.

Schwachstellenmanagement wird also auf absehbare Zeit Flickwerk bleiben – ausgerechnet jetzt, da NIS-2 und der Cyber Resilience Act die Lieferkette ins Zentrum der regulatorischen Aufmerksamkeit rücken.

Secorvo News

Weiterbildung

In unserer vierstündigen NIS-2-Schulung nach BSIG vermitteln wir am **15.10.2026** Geschäftsleitungen die erforderlichen Kenntnisse zur Erkennung und Bewertung von Informationssicherheitsrisiken.

Die fünftägige T.I.S.P.-Schulung (**28.09.–02.10.** und **16.–20.11.2026**) bereitet Sie auf die Online-Prüfung vor – mit 20jähriger Erfahrung und hunderten erfolgreichen Zertifizierungen. Referenten sind die Autoren des T.I.S.P.-Begleitbuchs „Informationssicherheit und Datenschutz" (4,9 ✶ bei Amazon).

Die vertiefenden Seminare ISMS verstehen und planen (**12.–13.10.2026**) und PKI – Grundlagen, Vertiefung, Realisierung (**23.–26.11.2026**) vermitteln Ihnen Praxiswissen für den Aufbau und Betrieb eines wirksamen Sicherheitsmanagements und von Public-Key-Infrastrukturen.

Planen Sie jetzt Ihre Weiterbildung für das 2. Halbjahr und sichern Sie sich den Frühbucherrabatt. Alle Seminarangebote und die Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

16. Tag der IT-Sicherheit

Welche Lehren zieht man aus dem ersten und bisher einzigen Cyberkatastrophenfall in Deutschland? Wie gelingt ein wirksames ISMS? Wie erreicht man sichere Software mit Hilfe eines Dependency Tracks? Antworten auf diese Fragen gibt es auf dem Tag der IT-Sicherheit am **23.07.2026** in den Räumen der IHK Karlsruhe – ein Networking-Event der Karlsruher IT-Sicherheitsinitiative, des CyberForum, der IHK Karlsruhe und KASTEL.

Hier geht's zur Anmeldung – wir freuen uns auf Sie.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz.

Juni 2026	
15.-16.06.	DuD 2026 (COMPUTAS, Berlin)
18.-19.06.	AREA41 Conference 2026 (AREA41, Zürich/CH)
22.-25.06.	ACNS 2026 (New York/US)
22.-26.06.	OWASP Global AppSec EU 2026 (OWASP Foundation, Wien/AT)
Juli 2026	
06.-10.07.	11th IEEE European Symposium on Security and Privacy (IEEE Computer Society, Lissabon/PT)
20.-25.07.	PETS 2026 (University of Calgary, Calgary/CA)
23.07.	16. Tag der IT-Sicherheit (CyberForum, IHK, KA-IT-Si, Karlsruhe)
27.-30.07.	DFRWS USA 2026 Conference (DFRWS, Arlington/US)
August 2026	
01.-06.08.	Black Hat USA 2026 (Black Hat, Las Vegas/US)
03.-05.08.	IEEE Internation Conference on Cyber Security and Resilience (IEEE CSR 2026) (IEEE, LogosRI, Lissabon/PT)
06.-09.08.	Defcon 34 (DEF CON Communications, Inc., Las Vegas/US)
12.-14.08.	35th USENIX Security Symposium (usenix, Baltimore/US)
17.-20.08.	Crypto 2026 (IACR, Santa Barbara/US)

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