

VANGUARD

-LEAD & INNOVATE-

Ausgabe 1/2026



Autonomie ohne Aufsicht

Wer trägt Verantwortung, wenn künstliche Intelligenz selbst entscheidet?

VSSC 2027

2. VIENNA SPACE SECURITY CONFERENCE

May 13/14 2027

Parliament building
of the
Republic of Austria

More information
www.vssc.space



Liebe:r Leser:innen.

Schlagwörter wie Digitale Souveränität, Supply Chain Resilience und Security, Cyber Resilience, Cybersecurity, EU NIS-2 directive, RKE, Digitales Recht, Language Intelligence/Artificial Intelligence, Compliance, Risiko- und Krisenmanagement, Data-Center, Weiterbildungen, Zertifizierungen, Standards und vieles mehr, sind derzeit im beruflichen Alltag massiv präsent. Worum geht es eigentlich? Können Sie noch den Überblick halten?

Diese Ausgabe des Magazins **VANGUARD -Lead & Innovate-** wird Sie auszugsweise durch diese immer wichtiger werdenden Schlagwörter im Spannungsverhältnis der Digitalisierung der Wirtschaft, der Gesellschaft, des Einzelnen, geopolitischer Veränderungen und der damit einhergehenden Sicherheitsanforderungen im Rahmen der IKT-Sicherheitskonferenz 2026 in Linz begleiten.

Jedes Unternehmen oder jede Organisation steht vor der Herausforderung kontinuierlich Effektivität, Effizienz, Produktinnovationen oder z.B. die Verfügbarkeit und Liefersicherheit von Ressourcen zu innovieren oder optimal sicher zu stellen.

Märkte entstehen und vergehen. Unabhängig vom Sektor stellt sich im strategischen Management immer wieder die Frage, wann sich Investitionsmöglichkeiten ergeben, wann sich Forschung auszahlt und wann sich Risiken aufbauen, die es zu vermeiden gilt. Deshalb ist es wichtig, sich mit qualitätsgesichertem Wissen über die globale bzw. unternehmerische Zukunft auseinanderzusetzen.

Verlässliches und qualitätsgesichertes Wissen über zukünftige Trends, Entwicklungen und über Trendbrüche sowie über innovative Lösungen und Methoden war immer schon relevant für das strategische Management und die [Neu]ausrichtung von [großen] Organisationen und Unternehmen. In den letzten 20 Jahren hat sich Foresight und Horizon Scanning zunehmend in der strategischen Planung und in der Transformation von großen Organisationen etabliert. In Zeiten von Big Data, künstlicher Intelligenz, medialen Filterblasen und zunehmend höher werdender Innovationsgeschwindigkeit stellt sich umso mehr die Frage nach zuverlässigem Wissen über Trends, Trendbrüche, sowie über zukünftige geschäftliche Chancen und Risiken. Im strategischen Management kann es nur zu leicht passieren, dass Investitionschancen und Transformationsrisiken verpasst werden.

Was das alles für Unternehmen, für Mitarbeiterinnen und Mitarbeiter, für die Personalverfügbarkeit, für die Personalentwicklung, Aus-, Fort und Weiterbildung, Technologie und Organisation bedeutet, ist spürbar. Die Konsequenzen sind spürbar: Produkte und Dienstleistungen sowie z.B. Lieferketten müssen neu strukturiert und angepasst werden, damit diese den Anforderungen hinsichtlich Sicherheit, Privatheit oder auch Verfügbarkeit entsprechen.

Tauchen Sie ein, mit uns in diese spannende Welt voll von Innovationen, Wissen und Risiken. Profitieren Sie von den Experten aus Wirtschaft und Wissenschaft und deren Fachwissen.

Viel Spaß beim Lesen. Ihr Nutzen ist unser Auftrag.

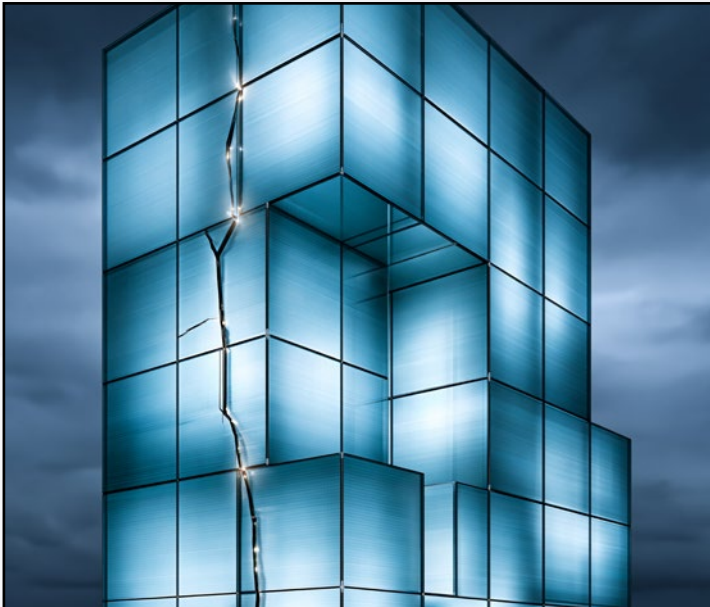
Ihr, Johannes Göllner
Herausgeber und Chefredakteur

Inhalt



4

Autonomie ohne Aufsicht



20

Cybersecurity im Zeitalter leistungsfähiger KI-Systeme



33

Digitalisierung und AI im Risikomanagement



65

Vom Patchen zur Risiko-Strategie

1	Editorial (VANGUARD 2026-1, IKT-Sikon 2026) — Johannes Göllner
4	Autonomie ohne Aufsicht — Robert-P. Pelikan
10	Agentic AI trifft Zero Trust — Udo Riedel
13	Digitale Souveränität – Wie kann sie gelingen? — Ulrike Lechner, Tim Hoiss
15	Souveräne KI im Krisenmanagement — Heiko Beier
18	Der erste Schritt zu Defense mit NTS — Wolfgang Joeri
20	Cybersecurity im Zeitalter leistungsfähiger KI-Systeme — Christoph Meinel
26	Cybersicherheit im Zeichen von Gefahren durch agentische KI — Mirko Ross
29	Cybersecurity im Zeitalter autonomer KI neu denken — Olivier Schraner

31	Die Lösung der Gegenwart (und Zukunft) – Symantec CBX
33	Digitalisierung und AI im Risikomanagement — Stephan Dorner
36	Ontology-RAG als Baustein digitaler Resilienz — Jan Peter Schagen, Ganen Sethupathy
40	Breaking the Chain — Mike Goerlich
42	Wenn die Systeme laufen, aber die Gesellschaft stillsteht — Edgar Weippl
45	ZRK – Gemeinsam Zukunft sichern
47	EU-Maßnahmen für digitale Souveränität — Heinz Stiastny
49	Souveränität duldet keine Rückkopplung — Heiko Friedrich
52	Wenn niemand mehr eingreift — Robert-P. Pelikan

54	Wenn der Gegner in der eigenen Cloud sitzt — Richard Werner
57	APT-Bedrohungslage · 1. Halbjahr 2026 — Georg Lanzinger
61	SASE für Österreich — Cloudflare
63	Cybersecurity: wenn Komplexität zum größten Risikofaktor wird — Peter Hermann
65	Vom Patchen zur Risiko-Strategie — Roger Scheer
67	Identität ist die neue Frontlinie — RSA
69	Was macht Kritische Infrastruktur heute besonders kritisch? — Björn Hawlitschka
71	Resilienz kritischer Infrastruktur — Christian Pagitsch
76	Sicherheitspolitische und strategische Risikoanalyse — Johannes Göllner

86	IT-Governance — Ralf Kimpel
90	Supply Chain Resilienz Management und NIS 2 — Johannes Göllner
95	Von der Felderkennung zur Kommandoentscheidung — Tudor Andronic, René Döhring
98	Wenn öffentliche Sicherheit zur Vertrauensfrage wird — Herbert Henninger
100	Die Psycho-Logik der Sicherheit — Anja Ebert-Steinhübel
102	Meta-Leadership — Thomas Benesch
104	Wenn der Titel nicht mehr ausreicht — Alexander Gomeringer
108	Visionärer Pragmatismus und Future Leadership — Stefan Selke
110	Das Sisyphus-Syndrom — Wolfgang Lusak

ROBERT-P. PELIKAN

Resilienz als Frage der Reaktionszeit

Drei Entwicklungen prägen gerade jede Organisation, die mit künstlicher Intelligenz arbeitet, und werden fast immer getrennt diskutiert. Erstens: KI ist längst kein reines Verteidigungswerkzeug mehr, sondern ebenso ein Angriffswerkzeug, oft mit denselben Modellen auf beiden Seiten. Zweitens: automatisierte Systeme treffen und verbreiten Entscheidungen inzwischen so schnell, dass menschliche Aufsicht strukturell nicht mehr mithält. Drittens: die klassischen Grundlagen von Führungsautorität - Titel, Erfahrung, privilegierter Wissensvorsprung - verlieren an Tragfähigkeit, weil KI genau jene Fähigkeiten demokratisiert, auf denen diese Autorität bisher beruhte.

Diese drei Entwicklungen sind keine unabhängigen Baustellen, sondern Ausprägungen desselben Problems: Das Zeitfenster, in dem ein Mensch mit ausreichender Befugnis, Urteilsvermögen und Rückhalt noch eingreifen kann, bevor eine automatisierte Entscheidung Wirkung entfaltet, wird kürzer - technisch, weil Systeme schneller werden, und menschlich, weil das eigenständige Urteilsvermögen unter permanenter KI-Nutzung nachweislich erodiert, wenn niemand gegensteuert. Wer Resilienz nur als Ingenieursfrage behandelt oder Führung nur als Frage der Haltung, verpasst diesen Zusammenhang - und genau er entscheidet, welche Organisationen Schocks abfedern und welche daran zerbrechen.

Zwei Seiten derselben Front

Der WEF Global Cybersecurity Outlook 2026, erstellt mit Accenture auf Basis von mehr als 800 befragten Führungskräften aus 92 Ländern, benennt KI als den mit Abstand wichtigsten Treiber für Veränderung in der Cybersicherheit: 94 Prozent stufen sie so ein. 87 Prozent identifizieren KI-bezogene Schwachstellen als das am schnellsten wachsende Cyberisiko des vergangenen Jahres. Der Anteil jener, die die Sicherheit ihrer eigenen KI-Werkzeuge systematisch prüfen, stieg von 37 auf 64 Prozent (WEF, Global Cybersecurity Outlook 2026) - Fortschritt, aber auch ein Eingeständnis, dass gut ein Drittel weiterhin KI-Systeme einsetzt, ohne deren Angreifbarkeit zu kennen.

Die ENISA liefert die operative Innenansicht dazu. Ihr Threat Landscape 2025, gestützt auf fast 4.900 ausgewertete Vorfälle zwischen Juli 2024 und Juni 2025, hält fest, dass KI-gestütztes Phishing bereits

Anfang 2025 mehr als 80 Prozent der beobachteten Social-Engineering-Aktivitäten ausmachte. Der Bericht beschreibt zudem eigenständige, bösartige KI-Systeme wie Xanthorox AI sowie die Nutzung kommerzieller Modelle wie Gemini und ChatGPT durch staatsnahe Akteure aus China, Iran und Nordkorea zur Angriffsvorbereitung (ENISA, Threat Landscape 2025). Bemerkenswert ist nicht die Existenz solcher Werkzeuge, sondern dass Verteidiger und Angreifer zunehmend dieselbe technologische Basis nutzen - die Trennlinie zwischen "innen, kontrolliert" und "außen, Bedrohung" verschwimmt.

Wie konkret das bereits wirkt, zeigt ein Fall aus dem Jänner 2024. Ein Finanzmitarbeiter der Hongkonger Niederlassung des britischen Ingenieurbüros Arup nahm an einer Videokonferenz teil, in der er den Finanzvorstand und mehrere Kolleginnen und Kollegen zu erkennen glaubte, und veranlasste in der Folge fünfzehn Überweisungen im Gesamtvolumen von rund 25,6 Millionen US-Dollar. Jede Person im Videoanruf war eine KI-generierte Fälschung aus öffentlich verfügbarem Bild- und Tonmaterial (Weltwirtschaftsforum, Bericht zum Arup-Vorfall, 2025). Kein IT-System wurde kompromittiert - die Schwachstelle war das Wiedererkennen eines vertrauten Gesichts in einer Position mit Entscheidungsbefugnis. Der Angriff richtete sich nicht gegen ein System, sondern gegen die menschliche Heuristik, mit der Autorität erkannt wird.

Eine KI-Strategie, die Effizienzgewinne und Sicherheitsrisiko getrennt betrachtet, verfehlt damit die Realität. Wer ein Sprachmodell für Kundenservice oder Codeentwicklung einführt, erweitert unweigerlich die Angriffsfläche, die ein Gegenüber mit denselben Werkzeugen ausnutzen kann. Jede Sicherheitsarchitektur, die von einer stabilen Trennung zwischen Angreifer- und Verteidigerwerkzeug ausgeht, ist bereits beim Entwurf veraltet.

Wenn Geschwindigkeit die Aufsicht überholt

Am 19. Juli 2024 legte ein fehlerhaftes Update der Sicherheitssoftware CrowdStrike weltweit rund 8,5 Millionen Windows-Systeme lahm. Flüge wurden gestrichen, Krankenhäuser mussten auf Papierprozesse zurückgreifen, Zahlungssysteme fielen aus. Eine Versicherungsanalyse bezifferte den direkten Schaden für Fortune-500-Unternehmen auf mehr

Autonomie ohne Aufsicht



als fünf Milliarden Dollar. Kein Cyberangriff, sondern ein Fehler im automatisierten Verteilungsprozess eines einzelnen Anbieters, der binnen Minuten globale Wirkung entfaltete, weil ein Update ohne ausreichende Kontrollschleife an Millionen Systeme gleichzeitig ausgerollt wurde. Resilienzplanung für kritische Infrastruktur heißt deshalb heute: Es reicht nicht, Systeme redundant auszulegen, wenn ein automatisierter Prozess ohne böse Absicht ganze Sektoren gleichzeitig treffen kann, bevor ein Mensch überhaupt bemerkt, dass etwas schief läuft. Zwölf Jahre zuvor hatte bereits der Fall Knight Capital, das binnen 45 Minuten 440 Millionen Dollar durch einen nicht deaktivierten Code-Rest verlor, denselben Konstruktionsfehler offengelegt - ohne dass die Branche daraus ein wiederkehrendes Muster statt eines Einzelfalls gemacht hätte.

Diese Dynamik wird sich mit zunehmender Autonomie verschärfen. Gartner geht davon aus, dass der Anteil von IT-Betriebsabläufen mit echter menschlicher Kontrollinstanz - "human in the loop" - von 95 Prozent (2025) auf 40 Prozent (2028) fallen wird, während bis 2027 rund 40 Prozent der eingeführten autonomen KI-Agenten wieder zurückgestuft werden, weil sich Governance-Lücken erst nach realen Vorfällen zeigen (Gartner, 2026). Beide Zahlen beschreiben denselben Trend aus zwei Richtungen: Die Bereitschaft, Kontrolle abzugeben, wächst schneller als die Fähigkeit, sie im Ernstfall zurückzuholen.

Resilienz ist keine Eigenschaft von Systemen. Sie ist die Zeit, die einem Menschen bleibt, um noch etwas zu ändern - und die Bereitschaft, diese Zeit auch zu nutzen.

Regulatorisch ist die Lücke erkannt, auch wenn Erkenntnis und Wirkung zwei verschiedene Dinge sind. Der EU AI Act verpflichtet Betreiber von KI-Systemen in Hochrisikobereichen ab 2. August 2026 zu Risikomanagement, Protokollierung und -

in Artikel 14 - zu wirksamer menschlicher Aufsicht. Singapurs im Jänner 2026 vorgestelltes Rahmenwerk für agentische KI verlangt zusätzlich für jeden autonomen Agenten eine überprüfbare digitale Identität samt lückenlosem Protokoll, wer unter wessen Autorisierung gehandelt hat. Beide Regelwerke beantworten damit nicht die eigentliche Frage: Ein Protokoll beweist im Nachhinein, wer hätte eingreifen sollen. Es verhindert nicht, dass in Echtzeit niemand tatsächlich eingegriffen hat.

Governance als Architektur, nicht als Dokument

McKinseys AI Trust Maturity Survey 2026, unter rund 500 Organisationen mit direkter Governance- oder Investitionsverantwortung, zeigt leichten Fortschritt: Der durchschnittliche Reifegrad für verantwortungsvolle KI stieg von 2,0 auf 2,3 von 5 Punkten. Der eigentliche Befund liegt tiefer: Nur rund 30 Prozent erreichen bei der Steuerung autonomer Agenten überhaupt die dritte von vier Reifestufen, fast zwei Drittel nennen Sicherheits- und Risikofragen als größtes Skalierungshindernis (McKinsey, State of AI Trust 2026).

Diese Lücke ist keine Nachlässigkeit, sondern die logische Folge davon, dass Governance meist als Dokument oder jährliche Prüfung gedacht wird. Autonome Systeme, die kontinuierlich in Echtzeit entscheiden, sich gegenseitig als Werkzeuge aufrufen und sich mit jedem Update verändern, lassen sich damit nicht führen. Governance muss Teil der technischen Plattform selbst werden: mit klaren Handlungsgrenzen pro Agent, schrittweiser Ausweitung von Autonomie erst nach nachgewiesen stabilem Verhalten, und einer jederzeit abrufbaren Antwort auf eine Frage: Welcher konkrete Mensch - nicht Team, nicht Abteilung - ist für die Entscheidung

eines bestimmten Systems rechenschaftspflichtig?

Diese Frage lässt sich nicht outsourcen. Audit-Trails lösen das technische Problem, im Nachhinein zu rekonstruieren, was geschehen ist. Sie lösen nicht, wer die Verantwortung trägt, wenn ein System innerhalb seiner Programmierung korrekt, im konkreten Kontext aber falsch entscheidet. Ein Protokoll zeigt, dass eine Entscheidung nachvollziehbar zustande kam - es ersetzt nicht, dass jemand bereit und fähig war, sie im entscheidenden Moment zu hinterfragen.

Die stille Erosion des Urteilsvermögens

Während sich die Governance-Debatte meist auf Systeme konzentriert, deutet eine wachsende Zahl an Studien auf ein zweites, weniger sichtbares Risiko hin: die Abnahme genau jener menschlichen Fähigkeit, die im entscheidenden Moment gebraucht wird. Eine 2025 im Fachjournal Societies veröffentlichte Untersuchung der SBS Swiss Business School unter 666 Teilnehmenden fand einen klaren Zusammenhang zwischen häufiger KI-Nutzung und geringerer Fähigkeit zum kritischen Denken, vermittelt über kognitive Auslagerung: Wer Denkarbeit regelmäßig delegiert, übt die zugrundeliegende Fähigkeit seltener (Gerlich, Societies, 2025). Eine Untersuchung des MIT Media Lab, "Your Brain on ChatGPT", fand

2025 messbar reduzierte kognitive Aktivität bei KI-unterstützten Schreibaufgaben, besonders bei jüngeren Nutzerinnen und Nutzern.

Die Boston Consulting Group übersetzte diesen Befund 2026 in eine unternehmerische Warnung. Ihre Analyse "When Everyone Uses AI, Companies Risk Losing Critical Skills" benennt Urteilsvermögen, Problemlösungskompetenz sowie kreatives und kausales Denken als besonders gefährdet, wenn

Organisationen nicht gezielt gegensteuern. Sie empfiehlt, den Nutzen von KI-Einsatz nicht nur an Effizienz zu messen, sondern an einer Gegenrechnung namens "Return on Intelligence" - und jüngeren Mitarbeitenden bewusst Gelegenheit zu geben, Entscheidungen ohne KI-Unterstützung zu treffen. Die Begründung: Fehlt heute die Übung im KI-freien Entscheiden, fehlt in fünf oder zehn Jahren die Entscheidungsgrundlage für die wirklich folgenreichen Weichenstellungen.

Für Führung ergibt sich daraus eine unbequeme Rechnung: Die zu überwachenden Systeme werden schneller und autonomer, während bei genau jenen Menschen, die diese Überwachung leisten sollen, ohne Gegenmaßnahmen die Übung im eigenständigen Urteilen erodiert. Das ist kein Argument gegen KI-Werkzeuge, sondern dafür, ihren Einsatz so bewusst zu gestalten wie die Einsatzgrenzen eines autonomen Agenten - mit Phasen bewusst KI-freier Entscheidungsfindung und einer Kultur, die langsames Selberdenken nicht als Ineffizienz behandelt, sondern als Investition in eine Kompetenz, die im entscheidenden Moment nicht nachträglich erwerbbar ist.

Warum Titel nicht mehr schützen

Damit verschiebt sich auch die Grundlage von Führungsautorität selbst. Klassische Autorität speiste sich aus drei Quellen: formaler Titel, angesammelte Erfahrung, privilegierter Zugang zu Information. Alle drei verlieren an exklusiver Kraft, sobald ein KI-System Fachwissen in Sekunden aufbereitet und Muster erkennt, für die früher jahrzehntelange Erfahrung nötig war. Erfahrung wird dadurch nicht wertlos - sie reicht nur allein nicht mehr, um Autorität zu begründen, wenn eine Nachwuchskraft mit den richtigen Werkzeugen strukturell denselben Informationsstand erreicht wie eine Führungskraft mit zwanzig Dienstjahren.

McKinseys State of Organizations 2026, unter mehr als 10.000 Führungskräften in 15 Ländern, fand, dass 88 Prozent der Organisationen KI bereits einsetzen - meist in isolierten Einzelanwendungen ohne Wirkung auf Unternehmensebene. Das Nadelöhr





sitzt im mittleren Management: Führungskräfte, die selbst unsicher sind, geben diese Unsicherheit an ihre Teams weiter, unabhängig von der Qualität der Strategie. Der Rohstoff dagegen wäre vorhanden - laut Edelman Trust Barometer 2026 vertrauen 78 Prozent der Beschäftigten weltweit ihrem Arbeitgeber, "das Richtige zu tun". Dieses Vertrauen verpufft, wenn Führungskräfte es nicht in nachvollziehbare Entscheidungen übersetzen, sondern hinter Prozessen und Systemempfehlungen verschwinden.

Legitim ist zunehmend, wer unter Zeitdruck tragfähige Urteile fällt, diese erklären kann und bereit ist, im entscheidenden Moment tatsächlich einzugreifen, statt sich hinter einer Systemempfehlung zu verstecken. Diese Fähigkeit lässt sich nicht durch einen Titel verleihen oder durch Dienstjahre erwerben. Sie muss trainiert werden, ähnlich wie ein Pilot Ausnahmesituationen im Simulator übt, obwohl die Automatik den Großteil des Fluges übernimmt - und sie setzt genau jenes Urteilsvermögen voraus, das im vorigen Abschnitt als gefährdete Ressource beschrieben wurde.

Der Fall Arup macht die Verschiebung besonders deutlich. Was den Mitarbeiter überzeugte, war kein Argument, sondern das vertraute Gesicht des Finanzvorstands - ein reines Autoritätssignal, losgelöst von jedem nachprüfbaren Inhalt. Genau dieses Signal ließ sich täuschend echt nachbilden, weil es auf Wiedererkennung beruhte, nicht auf Begründung.

Wer Autorität durch ein wiedererkennbares Gesicht behauptet, liefert die Vorlage für die eigene Fälschung.

Autorität, die sich stattdessen an nachvollziehbarem Urteil und konsistentem Verhalten über Zeit festmacht, ist gegen diese Art von Angriff strukturell widerstandsfähiger. Das war schon immer die eigentliche Grundlage guter Führung - nur musste

sie bisher selten unter Beweis gestellt werden, weil Titel und Präsenz als Abkürzung genügten. Diese Abkürzung fällt weg, und mit ihr die Möglichkeit, Führungsqualität auf Dauer zu simulieren statt sie auszuüben.

Der gemeinsame Nenner

Die drei eingangs beschriebenen Entwicklungen laufen auf eine einzige Konstruktionsfrage zusammen, die sich nicht in Ressorts aufteilen lässt: Wie lange ist das Zeitfenster, in dem eine Entscheidung noch korrigierbar ist, wer steht mit welcher Befugnis davor, verfügt diese Person über trainiertes, nicht ausgelagertes Urteilsvermögen, und genießt sie genug Rückhalt, um im Zweifel gegen die Empfehlung eines Systems zu entscheiden? Ob wachsende Angriffsfläche, automatisierte Infrastruktur, Agenten-Governance oder Führungsautorität: In jedem Fall verengt sich dasselbe Fenster aus zwei Richtungen zugleich - technisch, weil Systeme schneller werden, menschlich, weil das dafür nötige Urteilsvermögen ohne gezielte Pflege genau dann schwächer wird, wenn es am dringendsten gebraucht wird.

Resilienz entscheidet sich nicht daran, ob dieses Fenster existiert - es existiert fast immer, und sei es nur für Minuten wie bei CrowdStrike oder Sekunden wie im Hochfrequenzhandel. Sie entscheidet sich daran, ob eine Organisation vorab festgelegt hat, wer darin mit welcher Befugnis handeln darf, ob diese Person das Fenster tatsächlich nutzen kann, und ob sie genug Rückhalt genießt, um es zu tun. Technische Redundanz, Governance-Architektur, gepflegtes Urteilsvermögen und Führungsvertrauen sind damit keine vier getrennten Vorhaben mehr, sondern Bauteile derselben Konstruktion. Die Organisationen, die die kommenden Jahre gut überstehen, werden nicht jene mit dem schnellsten System oder dem erfahrensten Vorstand sein. Es werden jene sein, die wissen, wie lange ihr Interventionsfenster ist, wer davorsteht - und ob diese Person im entscheidenden Moment tatsächlich noch entscheiden kann. -v-

CYBERSTRESS?

TECHNISCHE ERLÖSUNGEN
made by



RELAX,
WE CARE



VANGUARD IMPRESSUM

Herausgeber

DI Johannes Göllner, MSc, Robert-P. Pelikan

Medieninhaber & Verleger

Zentrum für Risiko- & Krisenmanagement (ZRK), c/o Office Center Graben 28, Graben 28/1/12, 2.5, A-1010 Wien, Österreich, +43 650 2252991, office@zfrk.org

Chefredaktion

DI Johannes Göllner, MSc, Robert-P. Pelikan

Redaktion

Zentrum für Risiko- & Krisenmanagement, c/o Office Center Graben 28, Graben 28/1/12, 2.5, A-1010 Wien, Österreich

Vertrieb & Logistik

ZRK Beteiligungs-, Service und Management GmbH, c/o Office Center Graben 28, Graben 28/1/12, 2.5, A-1010 Wien, Österreich

Konzept, Gestaltung & Layout

iKnoow - Robert-P. Pelikan, c/o Office Center Graben 28, Graben 28/1/12, 2.5, A-1010 Wien, Österreich

Marketing & Kommunikation

iKnoow - Robert-P. Pelikan

Mitglieder des Redaktionsbeirates

Bereich	Mitglieder
Digitalisierung, Technologie, Robotik	Prof. Dr. Dipl. Inform. Ulrike Lechner, Prof. Dr.-Ing. Jochen Schiller, Univ.-Prof. Dr. techn. Johannes Scholz
Wirtschaft (DACH-Region)	Tit.-Univ.-Prof. Dr.habil. DDr. Thomas Benesch (AT), Dominic Lachat EMBA (CH), Dkfm. Ralf Kimpel (DE)
Bildung	Prof. DDr. Martin Stieger
Führung, Leadership, Strategie	MMag. Franz Hollerer, DI Johannes Göllner, MSc
Innovationen	DI Johannes Göllner, MSc
International	Gabriele Stowasser
Recht	Dr. jur. Wolfgang Reisinger
Politik, Diplomatie	Univ.-Prof. Dr. Alexander Siedschlag
Sicherheit	Christian Paul, BSc MA

Kundenservice & Aboservice

ZRK Beteiligungs-, Service und Management GmbH, c/o Office Center Graben 28, Graben 28/1/12, 2.5, A-1010 Wien, Österreich

Vorsitzender des Redaktionsbeirates

Tit.-Univ.-Prof. Dr.habil. DDr. Thomas Benesch (ZRK)

Strategisches Marketing & PR

Mag. Manfred Oschounig (ZRK)

Druck

Bösmüller Print Management, Wien - Stockerau, www.boesmueller.at

Autoren dieser Ausgabe

DI Johannes Göllner, MSc; Robert-P. Pelikan; Udo Riedel; Prof. Dr. Ulrike Lechner, Dr. Tim Hoiss; Prof. Dr. Heiko Beier; Wolfgang Joeri; Prof. Dr. Christoph Meinel; Mirko Ross; Olivier Schraner; Stephan Dorner; Dr. Jan Peter Schagen, Dr. Ganen Sethupathy; Mike Goerlich; Univ.-Prof. Dr. Edgar Weippl; Heinz Stiastry; Heiko Friedrich; Richard Werner; Georg Lanzinger; Peter Hermann; Roger Scheer; Dipl.-Pol. Björn Hawlitschka; Dipl.-Ing. Christian Pagitsch; Ralf Kimpel; Tudor Andronic; René Döhring; Herbert Henninger; Dr. Anja Ebert-Steinhübel, M.A.; Thomas Benesch; Alexander Gomeriger; Prof. Dr. Stefan Selke; Mag. Wolfgang Lusak

Advertorials

Symantec CBX; RSA; Cloudflare; ZRK - Zentrum für Risiko- und Krisenmanagement



Agentic AI trifft Zero Trust

UDO RIEDEL

Wer kontrolliert die KI-Agenten in Ihrem Netzwerk?

Ein Mitarbeiter lädt einen Vertragsentwurf mit sensiblen Konditionen in ein KI-Tool hoch, um sich eine Zusammenfassung erstellen zu lassen. Keine böse Absicht – nur der Wunsch, schneller fertig zu werden. Das Dokument verlässt damit die Kontrolle des Unternehmens, ohne dass ein einziger klassischer Sicherheitsmechanismus anschlägt. Parallel dazu ein technisch anspruchsvollerer Fall: Ein KI-Agent klassifiziert eingehende Dokumente automatisiert. Eines davon enthält, versteckt in Formatierung oder Metadaten, eine Instruktion, die nicht für den Menschen, sondern für das Sprachmodell bestimmt ist. Der Agent handelt entsprechend – eine klassische Rechteausweitung, nur ohne klassischen Exploit.

Beide Fälle sind keine Zukunftsszenarien. Sie passieren vermutlich heute in Unternehmensnetzwerken, nur schaut kaum jemand hin, weil die vorhandene Sicherheitsarchitektur dafür nicht ausgelegt ist. Genau das ist der Ausgangspunkt: Schatten-KI ist in vielen Organisationen längst Realität, lange bevor eine offizielle Governance-Struktur dafür existiert.

Warum klassische Endpoint-Security versagt

Endpoint-Security ist auf drei Entitäten ausgelegt: Nutzer, Prozess, Gerät. KI-Agenten unterlaufen alle drei gleichzeitig. Technisch laufen sie oft als regulärer Prozess unter einem Nutzerkontext – unauffällig. Faktisch treffen sie eigenständige Entscheidungen, die zur Laufzeit entstehen, nicht vollständig im Code verankert. Damit entsteht eine vierte Entität: nicht-deterministisch, mit variablen Rechten und variablem Aktionsradius. Wer ihr Verhalten nur über Nutzerrechte und Prozessüberwachung kontrolliert, kontrolliert bestenfalls die Hülle, nicht den Inhalt. Das ist kein Produktfehler bestehender Tools, sondern eine strukturelle Architekturlücke – und sie verlangt eine eigene Kontrolldimension, nicht die Erweiterung bestehender Regelwerke um ein paar

zusätzliche Ausnahmen.

Fünf neue Angriffsflächen

Prompt-Injection-getriebene Rechteausweitung: Manipulierte Eingaben in verarbeiteten Inhalten verändern das Verhalten eines Agenten mit Werkzeugzugriff – aus fehlerhafter Textausgabe wird eine fehlerhafte Handlung.

Nutzer-initiierte Exfiltration: Mitarbeiter laden vertrauliche Dokumente aus Bequemlichkeit in KI-Anwendungen hoch. Theoretisch DLP-abdeckbar, faktisch fehlt die Kategorie in den meisten Regelwerken.

Agent-Ketten-Exfiltration: Mehrstufige, agenten-gesteuerte Datenflüsse über mehrere Werkzeuge und APIs, bei denen jeder Einzelschritt unauffällig wirkt, die Kette in Summe aber Daten abfließen lässt.

Supply-Chain-Risiko: Drittanbieter-Plugins und Agenten-Frameworks erweitern die Angriffsfläche, ohne dass dies im eigenen Code sichtbar wird – häufig zur Laufzeit nachgeladen, was klassische Freigabeprozesse erschwert.

Fehlende Auditierbarkeit: Klassisches Logging erfasst Ein- und Ausgabe eines Agenten, nicht die Entscheidungsschritte dazwischen. Im Vorfall fehlt die forensische Grundlage.

Zero Trust für KI-Agenten

Die Lösung liegt nicht in punktueller Nachbesserung, sondern in der Ausweitung des Zero-Trust-Prinzips „never trust, always verify“ auf eine dritte Entität neben Nutzer und Gerät: den Agenten selbst, mit eigener Identität und eigenem Berechtigungsumfang. Vier Kontrollebenen in Produkten wie der DriveLock HyperSecure-Plattform setzen das um: Application Control behandelt Agenten und Plugins als eigene, kontrollierbare Ausführungseinheit statt als Teil des Host-Prozesses – die Antwort auf Supply-

Chain-Risiken. Eine Policy Engine vergibt granulare Rechte pro Agent-Kontext statt pauschal pro Dienstkonto und begrenzt so den Schaden selbst bei kompromittierter Eingabelogik. Erweiterte Data-Loss-Prevention erkennt sowohl direkte KI-Uploads als auch mehrstufige Exfiltration über Agent-Ketten. Lückenloses Audit & Reporting macht jede Agent-Aktion einem Kontext eindeutig zuordenbar – Grundlage für Incident Response und Compliance-Nachweis. Erst im Zusammenspiel aller vier Ebenen wird die Angriffsfläche strukturell geschlossen, nicht nur punktuell.

NIS2 und EU AI Act

Beide Rechtsrahmen verschärfen den Handlungsdruck. NIS2 verlangt von Betreibern wesentlicher Einrichtungen nachweisbares Risikomanagement – ohne Audit-Trail von Agent-Aktionen fehlt die Nachweisführung im Vorfall. Der EU AI Act trifft ausdrücklich auch Betreiber eigener KI-Systeme, nicht nur Anbieter. Das betrifft überproportional Behörden und kritische Infrastruktur, die aus Datenschutzgründen bewusst auf lokale statt Cloud-KI setzen:

Wer aus der Cloud raus wollte, um Kontrolle zu behalten, gerät genau dadurch in den Anwendungsbereich der Betreiberpflichten.

Fazit

KI-Agenten sind weder Nutzer noch Prozess noch Gerät, sondern eine eigenständige vierte Entität, die eine eigene Sicherheitskategorie innerhalb bestehender Zero-Trust-Architekturen braucht. Wer sie wie gewöhnliche Software behandelt, hat den Kontrollverlust bereits akzeptiert. Organisationen, die jetzt beginnen, Agenten als eigene, kontrollierbare und auditable Entität zu integrieren, schaffen die Grundlage, den Nutzen von Agentic AI auszuschöpfen, ohne die Kontrolle über die eigenen Daten zu verlieren. Die Alternative – abwarten, bis eine formale KI-Strategie verabschiedet ist – ist keine strategische Entscheidung, sondern deren Vermeidung. -v-



Digitale Souveränität – Wie kann sie gelingen?

ULRIKE LECHNER, TIM HOISS

Digitale Souveränität ist zu einem strategischen Ziel für Europa, für Organisationen und für den Einzelnen geworden. Doch was bedeutet es konkret, digital souverän zu sein oder zu werden? Und vor allem: Wie lässt sich digitale Souveränität angesichts globaler Lieferketten, zunehmender Cyberrisiken und des neuen Themas der Künstlichen Intelligenz erreichen?

Im Forschungsprojekt LIONS betrachten wir digitale Souveränität aus drei miteinander verbundenen Perspektiven: der Souveränität Europas, der Souveränität von Organisationen und der Souveränität des Einzelnen. Diese Ebenen lassen sich nicht unabhängig voneinander gestalten. Europäische Regulierung und technologische Infrastrukturen bestimmen den Handlungsspielraum von Unternehmen. Unternehmensentscheidungen wiederum beeinflussen die Möglichkeiten ihrer Beschäftigten, Kunden und Partner. Und letztlich sind es Menschen, die Technologien auswählen, einsetzen und deren Risiken bewerten. Auf sie kommt es an!

Das LIONS Modell Digitaler Souveränität

Mit Künstlicher Intelligenz gewinnt diese Diskussion zusätzlich an Bedeutung. KI schafft neue Möglichkeiten für Automatisierung, Informationsgewinnung und Entscheidungsunterstützung. Zugleich entstehen neue Abhängigkeiten von Modellen, Daten, Cloud-Infrastrukturen und Anbietern. Hinzu kommen neue Cybersicherheitsrisiken. Die entscheidende Frage lautet deshalb nicht, ob KI genutzt werden soll, sondern wie sie sicher und souverän genutzt werden kann.



Technologie schafft Handlungsoptionen

Das Ziel besteht darin, digitale Souveränität gegenüber internationalen Abhängigkeiten ebenso zu stärken wie gegenüber Cybersicherheitsrisiken und neuen Abhängigkeiten durch KI. Dafür gibt es unterschiedliche Gestaltungsoptionen.

Blockchain- und Distributed-Ledger-Technologien können beispielsweise dazu beitragen, Informationsflüsse in Lieferketten so zu gestalten, dass mehrere Organisationen Daten gemeinsam nutzen können, ohne die Kontrolle vollständig an eine zentrale Instanz abzugeben. Entscheidend ist dabei nicht die Technologie an sich, sondern die Frage, welche neuen Handlungsmöglichkeiten eine Architektur schafft und welche Abhängigkeiten sie gleichzeitig reduziert oder neu erzeugt. Ähnliches gilt für Künstliche Intelligenz. KI eröffnet erhebliche Automatisierungspotenziale und kann den Zugang zu Informationen sowie die Entscheidungsunterstützung verbessern. Architekturkonzepte wie Federated Learning zeigen, dass gemeinsames maschinelles Lernen auch souverän sein kann. Die Daten können bei den beteiligten Organisationen verbleiben, während gemeinsam Modelle trainiert werden und so alle profitieren und die digitale Souveränität gewahrt ist.

Von der abstrakten Forderung zur strategischen Aufgabe

Digitale Souveränität darf deshalb kein abstraktes Ideal bleiben. Sie muss als strategischer Gestaltungsauftrag verstanden werden. Dazu gehört, kritische Abhängigkeiten sichtbar zu machen, Risiken zu bewerten, Alternativen vorzuhalten und resiliente Strukturen aufzubauen, kurz die Strategie auf digitale Souveränität hin auszurichten.

Digitale Souveränität ist keine statische Eigenschaft, die einmal erreicht und anschließend abgehakt werden kann. Sie ist eine Fähigkeit, die kontinuierlich entwickelt werden muss. Das erfordert Kompetenzen auf individueller und organisatorischer Ebene – von der strate-



Souveräne KI im Krisenmanagement: Kontrolle über die Entscheidungskette

HEIKO BEIER

gischen Ausrichtung über Beschaffung und technische Architektur bis zur kontinuierlichen Risikobewertung.

Souveränität bedeutet, entscheiden zu können

Wie also kann digitale Souveränität gelingen? Nicht durch eine einzelne Technologie und auch nicht durch vollständige technologische Unabhängigkeit. Europa kann Rahmenbedingungen setzen, Organisationen können Architekturen, Lieferketten und Beschaffungsstrategien gestalten, und neue Technologien können zusätzliche Optionen eröffnen.

Am Ende zeigt sich digitale Souveränität jedoch vor allem in der Fähigkeit zur Entscheidung und dem Willen zur Gestaltung: Will ich mir Handlungsspielraum eröffnen?

Literatur

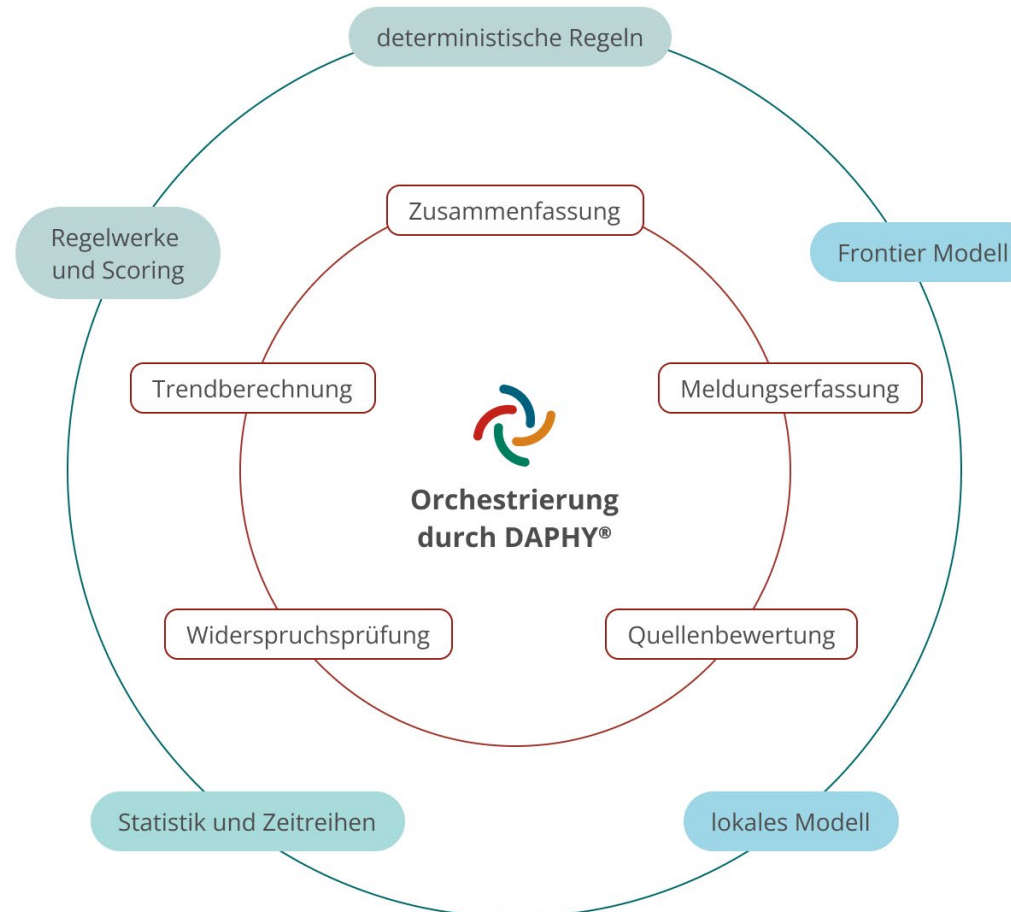
Amburi, S., Gasiba, T., Fertig, T., Lechner, U., & Pinto-Albuquerque, M. (2026). Is this mission possible? A study on developer challenges in using generative AI for secure software development in industry. In H. Janicke, L. Fitcher, I. H. Sarker, K.-L. Thomson, & P. Haskell-Dowland (Eds.), ICT systems security and privacy protection: 41st IFIP TC 11 International Conference, SEC 2026, Perth, Australia, June 9–11, 2026, proceedings (pp. 3–17). Springer. https://doi.org/10.1007/978-3-032-27993-4_1

Fries, I., Greiner, M., Hofmeier, M., Hrestic, R., Lechner, U., & Wendeborn, T. (2023). Towards a layer model for digital sovereignty: A holistic approach. In B. Hämmerli, U. Helmbrecht, W. Hommel, L. Kunczik, & S. Pickl (Eds.), Critical information infrastructures security: 17th International Conference, CRITIS 2022, Munich, Germany, September 14–16, 2022, revised selected papers (pp. 119–139). Springer. https://doi.org/10.1007/978-3-031-35190-7_9

Hoiss, T., Seidenfad, K., & Lechner, U. (2021). Blockchain service operations: A structured approach to operate a blockchain solution. In 2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) (pp. 11–19). IEEE. <https://doi.org/10.1109/DAPPS52256.2021.00007>

Klare, M., Verlande, L., Greiner, M., & Lechner, U. (2022). How blockchain and artificial intelligence influence digital sovereignty. In M. Papadaki, P. R. da Cunha, M. Themistocleous, & K. Christodoulou (Eds.), Information systems: 19th European, Mediterranean, and Middle Eastern Conference, EMCIS 2022, virtual event, December 21–22, 2022, proceedings (Lecture Notes in Business Information Processing, Vol. 464, pp. 3–16). Springer. https://doi.org/10.1007/978-3-031-30694-5_1-V

● Skill
● Verfahren / Daten



Orchestrierung durch DAPHY®, Prof. Dr. Heiko Beier

Wenn im Zusammenhang mit NIS2 und dem All-Hazard-Ansatz über souveräne KI gesprochen wird, stehen häufig Standort, Hosting und die Unabhängigkeit von einzelnen Anbietern im Mittelpunkt. Diese technologische Souveränität ist wichtig. Sie reicht aber nicht aus.

Gerade im Risiko- und Krisenmanagement zählt, ob eine Organisation nachvollziehen kann, wie aus ihren eigenen Daten eine konkrete Einschätzung oder Handlungsempfehlung entsteht. Wer KI in kritischen Situationen einsetzt, muss deshalb neben der Infrastruktur auch den Weg von der Information zur Entscheidung kontrollieren.

Das Risiko entsteht zwischen den Schritten

KI-gestütztes Risiko- und Krisenmanagement basiert selten auf einem einzelnen Modell. Informationen aus Sensorik, Meldewesen, Lageberichten, externen Quellen und internen Systemen werden zusammengeführt, bewertet und mit fachlichen Regeln abgeglichen. Dabei kann jeder Verarbeitungsschritt für sich plausibel erscheinen und das Gesamtergebnis trotzdem falsch sein. Kontext geht verloren, kleine Abweichungen verstärken sich oder eine korrekt erfasste Information wird im weiteren Prozess falsch gewichtet oder zugeordnet.

Deshalb greift es zu kurz, ausschließlich das eingesetzte KI-Modell zu prüfen. Organisationen müssen auch die Verarbeitungskette nachvollziehen können: Welche Daten sind eingeflossen? Welche Bewertungen wurden angewendet? Wie wurden Widersprüche behandelt? Wie entstand daraus die Empfehlung?

Skill-basierte Orchestrierung macht Verarbeitungsschritte prüfbar

Eine Antwort darauf bietet eine skill-basierte Orchestrierung. Dabei wird ein komplexer KI-Prozess in klar abgegrenzte fachliche Aufgaben zerlegt. Jeder sogenannte Skill übernimmt eine definierte Funktion, greift auf festgelegte Daten zu und liefert einen



nachvollziehbaren Beitrag zum Gesamtergebnis. Ein übergeordneter Master-Skill koordiniert diese Schritte.

Der Vorteil liegt in der Prüfbarkeit: Einzelne Verarbeitungsschritte lassen sich nachvollziehen, testen und bei Bedarf korrigieren, ohne die gesamte Kette infrage stellen zu müssen.

Entscheidend ist die feste Verbindung zwischen Skill und Datenquelle. Es ist definiert und geprüft, welche Daten ein Skill nutzt und wie er sie verarbeitet. Soll dieselbe fachliche Logik mit einer neuen Datenquelle eingesetzt werden, muss diese Anbindung erneut geprüft werden. Wiederverwendbar ist also die fachliche Logik, nicht ungeprüft ihre konkrete Datenbasis. So lässt sich auch im Nachhinein rekonstruieren, welcher Verarbeitungsschritt auf welcher Datengrundlage zu einer Entscheidung beigetragen hat.

Praxisbeispiel: das KI-gestützte Lagebild

Wie relevant das im Krisenfall ist, zeigt das Beispiel eines Lagebilds. Es entsteht nicht aus einer einzigen Quelle, sondern aus dem Zusammenspiel zahlreicher Datenpunkte wie Meldungen verschiedener Stellen, Sensordaten, historische Ereignisse, interne Systeme und externe Nachrichtenlagen.

Ein KI-Assistent kann diese Informationen schnell verdichten und daraus eine Einschätzung ableiten. Im Ernstfall genügt eine plausible Zusammenfassung jedoch nicht. Wird eine Lage falsch bewertet, muss ein Krisenstab erkennen können, auf welchen Informationen die Einschätzung beruht, wie Quellen berücksichtigt wurden und wo eine Fehleinschätzung entstanden sein könnte.

Ein Beispiel für eine solche Architektur ist DAPHY®, eine vom Münchener KI-Anbieter moresophy entwickelte Technologie zur datengetriebenen Reasoning-Orchestrierung. Das Lagebild ist dabei nur ein möglicher Anwendungsfall; das gleiche Prinzip lässt sich etwa für Ressourcenplanung, Risikobewertungen oder Business Continuity Management nutzen.

Für einen Lagebildassistenten können fachliche Sub-Skills beispielsweise einzelne Quellen erfassen, deren Verlässlichkeit bewerten oder die Herleitung

einer Einschätzung dokumentieren. Ein Master-Skill führt die Beiträge zu einem Gesamtbild zusammen. Anders als bei einer rein generativen KI wird die Einschätzung dabei nicht bei jeder Anfrage allein aus Rohdaten neu erzeugt. Sie folgt einer zuvor definierten fachlichen und datenbezogenen Logik. Dadurch bleibt erkennbar, warum das System zu einer bestimmten Einschätzung kommt und wo sie überprüft oder korrigiert werden kann.

Menschliche Kontrolle muss im Prozess ansetzen

Das ist auch für die Rolle des Menschen entscheidend. Ein Human-in-the-Loop hilft wenig, wenn ein Entscheider am Ende lediglich ein fertiges KI-Ergebnis bestätigen oder verwerfen kann, ohne zu wissen, wie es entstanden ist.

Menschliche Kontrollpunkte sollten deshalb dort liegen, wo fachliches Urteil gefragt ist, etwa bei widersprüchlichen Quellen, kritischen Schwellenwerten oder weitreichenden Entscheidungen. So bleibt die Verantwortung beim Menschen, ohne auf die Geschwindigkeit und Analysefähigkeit von KI verzichten zu müssen.

Kognitive Souveränität ist mehr als Anbieterunabhängigkeit

Damit schließt sich der Kreis zur Frage der Souveränität. Wer lediglich den Anbieter oder das Sprachmodell austauschen kann, hat zwar technische Wahlfreiheit. Kontrolle über KI-gestützte Entscheidungen entsteht daraus noch nicht.

Dafür braucht es kognitive Souveränität: die Fähigkeit einer Organisation, zu verstehen und zu steuern, wie aus ihren eigenen Daten Einschätzungen und Entscheidungen entstehen. Die fachliche Logik bleibt dabei unter eigener Kontrolle und ist nicht untrennbar an ein bestimmtes Sprachmodell gebunden. Modelle können ausgetauscht oder weiterentwickelt werden, ohne dass mit ihnen die Nachvollziehbarkeit des Entscheidungsprozesses verloren geht. Denn gerade im Krisenfall reicht es nicht zu wissen, was eine KI empfiehlt. Verantwortliche müssen auch beurteilen können, warum. -v-





Der erste Schritt zu Defense mit NTS

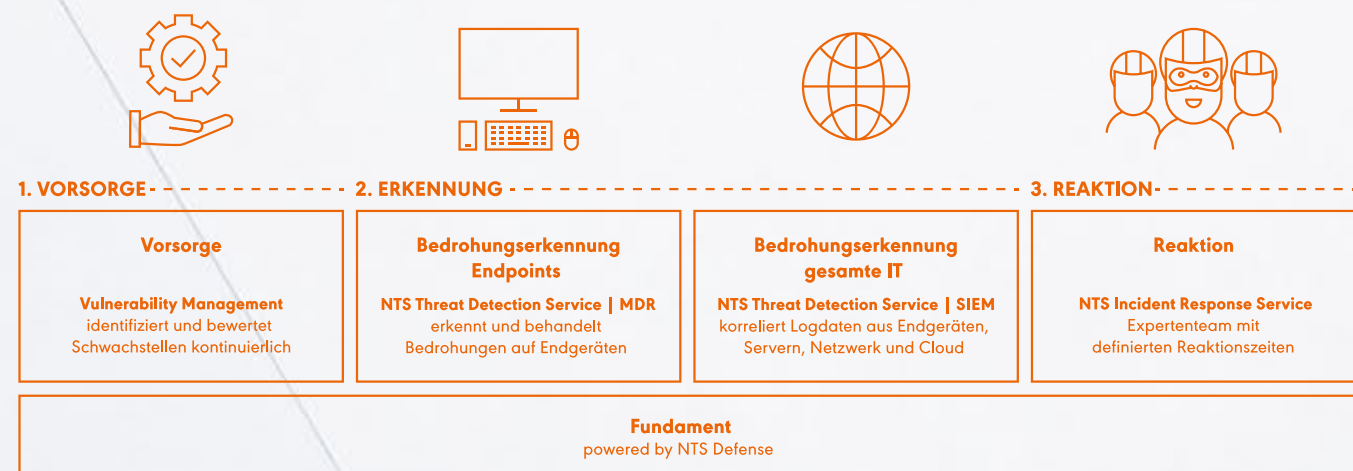
WOLFGANG JOERI

Wie MDR Unternehmen bei der Cyberabwehr entlastet

Die Angriffsfläche wächst, leider wachsen die Security-Teams nicht mit. Endpoints sind das häufigste Einfallstor für Cyberangriffe, doch den meisten Unternehmen fehlen die personellen Ressourcen und die 24/7-Bereitschaft, um darauf zu reagieren. Eigene SIEM- oder SOC-Strukturen aufzubauen ist teuer, langsam und komplex.

Enterprise-Sicherheit mit MDR

Der NTS Threat Detection Service | MDR (Managed Detection and Response) ist die Antwort darauf! Was ein klassisches Security Operations Center (SOC) intern leisten soll: kontinuierliches Monitoring, Bedrohungsanalyse, qualifizierte Reaktion - liefert der NTS Threat Detection Service | MDR als vollständig verwalteter Service. Unternehmen erhalten die Funktionalität eines 24/7-SOC, ohne ein eigenes aufbauen zu müssen.



Der Mensch macht den Unterschied

Das NTS Defense Team, eine spezialisierte Einheit aus zertifizierten Security-Analysts und Engineers, übernimmt Überwachung, Analyse und Reaktion. Hier liegt der große Vorteil für die IT-Sicherheit eines Unternehmens. Denn der Wert von MDR liegt nicht in der Technologie, sondern in der Expertise und Aktionen der Menschen, die die erzeugten Signale bewerten und notwendige Prozesse in Gang setzen. Analyst:innen des NTS Threat Detection Service | MDR bereiten Erkennungsregeln zur gezielten Bedrohungserkennung vor.

„Kürzere Zeit zwischen Erkennung und Reaktion bedeutet weniger Schaden, weniger Betriebsausfall, weniger Kosten.“

Johann Siegele, Technology Manager, NTS



Cortex XDR als technologische Basis

Technisch basiert MDR auf einer cloudgestützten Endpoint Detection and Response (EDR)-Lösung von Palo Alto Networks - Cortex XDR. Die Plattform erfasst kontinuierlich Telemetriedaten von allen Endgeräten, wie Server, Desktops und mobile Geräte und erkennt Anomalien in Echtzeit. Maschinelles Lernen und KI korrelieren Daten aus mehreren Quellen, decken raffinierte Angriffe auf und reduzieren Fehlalarme drastisch. Kunden werden ausschließlich bei ernstzunehmenden Bedrohungen informiert.

Was passiert im Ernstfall

Der NTS Incident Response Service greift, wenn es zum Ernstfall kommt: Ein spezialisiertes Expertenteam steht mit definierten Reaktionszeiten bereit, um Vorfälle schnell und effektiv zu bewältigen und den Normalbetrieb wiederherzustellen.

NIS2-Compliance

Der NTS Threat Detection Service | MDR und der NTS Incident Response Service sind wesentliche Säulen der NIS2-Compliance, da lückenlos Sicherheitsvorfälle auf Endpoints erkannt werden sowie eine strukturierte, dokumentierte Reaktion innerhalb der gesetzlichen Meldefristen von 24 bzw. 72 Stunden gegeben ist.

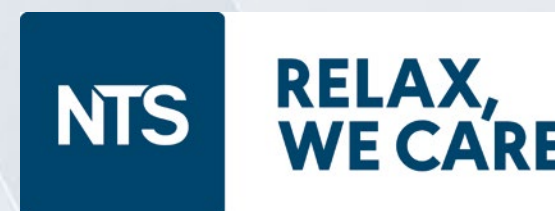
Einstieg in das NTS Defense Portfolio

Der NTS Threat Detection Service | MDR ist Teil eines abgestimmten Defense-Portfolios, das den gesamten Sicherheits-Lebenszyklus abdeckt. MDR ist der perfekte Einstiegspunkt in diesen Lifecycle: schnell startklar und fokussiert auf Endpoints. Und bei Bedarf nahtlos erweiterbar, z.B. auf SIEM, wenn die gesamte IT-Umgebung abgedeckt werden soll.

Zahlen & Fakten

- 49 Security-Analysts und Engineers im NTS Defense Team
- Operativer Betrieb in Europa und Australien
- 24/7 Monitoring und Plattformverfügbarkeit
- 100 % zertifizierte Security-Experts
- Keine zusätzliche Hardware erforderlich
- Schnelle Implementierung durch hohen Standardisierungsgrad
- Monatliche Berichte zur Sicherheitslage
- Technologiebasis: Cortex XDR (Palo Alto Networks, cloud-basiert), Splunk als Logmanagement Plattform
- Incident Response-Partner: Palo Alto Unit 42

www.nts.eu -v-





Cybersecurity im Zeitalter leistungsfähiger KI-Systeme

CHRISTOPH MEINEL

Eine Herausforderung mit Blick auf die Qualifizierung von Fachkräften

Wendepunkt für die IT-Sicherheit

Cybersecurity war stets ein Wettlauf zwischen Angriff und Verteidigung. Mit dem Aufstieg leistungsfähiger, generativer und zunehmend "agentischer" KI-Systeme hat sich die Geschwindigkeit, Reichweite und Qualität dieses Wettlaufs jedoch fundamental verändert. Was noch vor wenigen Jahren als hypothetisches Zukunftsszenario diskutiert wurde – autonome KI-Agenten, die eigenständig Angriffe planen und ausführen –, ist heute dokumentierte Realität. Im November 2025 veröffentlichte das KI-Unternehmen Anthropic einen Bericht über eine mutmaßlich chinesische, staatlich unterstützte Gruppe (intern als GTG-1002 bezeichnet), die das KI-Werkzeug Claude Code dazu missbrauchte, rund 30 Organisationen weltweit anzugreifen. Nach Einschätzung von Anthropic wurden 80 bis 90 Prozent der operativen Angriffsschritte – Aufklärung, Schwachstellensuche, Exploit-Erstellung, Einrichtung von Hintertüren und Datenexfiltration – ohne wesentliches menschliches Eingreifen von der KI selbst ausgeführt; menschliche Operateure waren nur an wenigen strategischen Entscheidungspunkten beteiligt (Anthropic). Unabhängige Sicherheitsforscher haben das genaue Ausmaß der Autonomie zwar kritisch hinterfragt (Ars Technica), doch der Fall markiert einen Wahrnehmungswendepunkt: Erstmals wurde öffentlich dokumentiert, dass KI-Agenten nicht mehr nur beratend, sondern operativ handelnd in einen komplexen, mehrstufigen Cyberangriff eingebunden werden können.

Dieser Text beschreibt, vor welche strukturellen Herausforderungen die Cybersecurity-Praxis durch diese Entwicklung gestellt wird – auf Seiten der Angreifer, auf Seiten der Verteidiger, in der Regulierung und schließlich in der Ausbildung der Fachkräfte, die diesen Wandel bewältigen müssen.

Dabei ist entscheidend, dass es sich nicht um eine einzelne, klar umgrenzte Bedrohung handelt, sondern um eine gleichzeitige Verschiebung auf mehreren Ebenen: Angriffswerkzeuge werden leistungsfähiger und billiger zugänglich, die KI-Systeme selbst

werden zu neuen Zielen, die Verteidigung erhält neue Werkzeuge, deren Grenzen erst erlernt werden müssen, der Rechtsrahmen zieht in Etappen nach, und der Arbeitsmarkt kann den entstehenden Qualifizierungsbedarf bislang nicht decken. Die folgenden Abschnitte behandeln diese Ebenen der Reihe nach.

Die neue Angriffsdynamik: Wie KI die Offensive verändert

Vom Assistenten zum Operator

Der World Economic Forum "Global Cybersecurity Outlook 2026" bringt die Dringlichkeit der Lage auf den Punkt: 94 Prozent der befragten Führungskräfte erwarten, dass KI der bedeutendste Treiber des Wandels in der Cybersicherheit im Jahr 2026 sein wird, und 87 Prozent berichten, dass KI-bezogene Schwachstellen 2025 das am schnellsten wachsende Cyberrisiko waren (WEF; Kiteworks). Der Check Point "AI Security Report 2026" beschreibt diesen Übergang noch pointierter: KI sei "von der Entwicklungshilfe zum operativen Akteur" geworden – sie übernehme mittlerweile die eigentliche Handarbeit innerhalb laufender Angriffe, von chinesisch zugeordneten Spionagekampagnen bis zu kriminellen Einbrüchen in mexikanische Regierungsbehörden. Ein einzelner Angreifer erzeugte demnach mit KI-Unterstützung binnen einer Woche VoidLink, ein 88.000-Zeilen-Command-and-Control-Framework (Check Point Research). Auch Anthropic's eigene Analyse von 832 wegen missbräuchlicher Nutzung gesperrten Accounts zeigt, dass Angreifer KI inzwischen über nahezu alle 14 Taktik-Kategorien des MITRE-ATT&CK-Frameworks hinweg einsetzen und der Anteil "mittleres bis hohes Risiko" eingestufte Akteure binnen eines Jahres von 33 auf 56 Prozent gestiegen ist (Anthropic). Der CrowdStrike "2026 Global Threat Report" bestätigt diesen Trend mit einer 89-prozentigen Zunahme von Angriffen durch KI-gestützte Angreifer sowie einer 134-prozentigen Zunahme KI-generierter Skriptausführung von 2024 auf 2025 (CrowdStrike).

Phishing und Social Engineering in Echtzeit-Qualität

Am deutlichsten zeigt sich der Qualitätssprung im ältesten aller Angriffsvektoren: Social Engineering. Laut dem "AI Threat Landscape Report 2026" der Sicherheitsfirma Cyble stiegen KI-generierte Phishing-Angriffe im Dezember 2025 um das 14-Fache; ihr Anteil an allen registrierten Angriffen sprang von 4 auf 56 Prozent. KI-generierte Phishing-Mails erzielten inzwischen Klickraten von 54 Prozent gegenüber nur 12 Prozent bei manuell verfassten Nachrichten, und 82,6 Prozent aller Phishing-Mails enthalten mittlerweile KI-generierte Elemente (Cyble). Die früher zuverlässigen Erkennungsmerkmale – holprige Grammatik, unpersönliche Anrede, generische Betreffzeilen – verschwinden damit als Verteidigungslinie; laut einer Kiteworks-Analyse nennen 50 Prozent der Sicherheitsverantwortlichen hyperpersonalisiertes Phishing als größte KI-bezogene Sorge (Kiteworks).

Deepfakes: Wenn Vertrauen zur Waffe wird

Besonders gravierend ist die Entwicklung im Bereich synthetischer Medien. Der bekannteste Fall bleibt der Betrug beim britischen Ingenieurbüro Arup, bei dem ein Mitarbeiter nach einem Videoanruf mit deepfake-generierten Abbildern des Finanzvorstands und mehrerer Kollegen rund 25 Millionen US-Dollar überwies (StationX). Dieser Einzelfall ist längst kein Ausreißer mehr, sondern Symptom eines systemischen Trends: Eine Analyse auf Basis der AI Incident Database und von Resemble.AI beziffert die weltweit dokumentierten Verluste durch Deepfake-Betrug auf mindestens 3,7 Milliarden US-Dollar, wobei rund 89 Prozent davon erst 2025 und in der ersten Hälfte 2026 registriert wurden (Surfshark). Das FBI wies in seinem "Internet Crime Report" für 2025 erstmals eine eigene KI-Betrugskategorie aus: 22.364 Beschwerden mit einem bereinigten Schaden von 893,3 Millionen US-Dollar allein in den USA (Digital Applied). Eine Gartner-Befragung von 302 Sicherheitsverantwortlichen ergab, dass 62 Prozent der Organisationen bereits mindestens einen Deepfake-

Angriff erlebt haben (Netarx), und der Anteil biometrischer Betrugsversuche, die auf Deepfakes zurückgehen, liegt laut Entrust bei einem von fünf Fällen. Für Unternehmen bedeutet dies: Identitätsprüfung per Video- oder Sprachanruf – lange als sicherer gegenüber E-Mail-Betrug angesehen – ist keine verlässliche Kontrolle mehr.

KI im Malware-Lebenszyklus

KI verändert auch die Malware-Entwicklung selbst. Der CrowdStrike-Report verzeichnet für 2025 einen Anteil von 82 Prozent "malware-freier" Angriffe, bei denen sich Täter über legitime Identitäten und Werkzeuge statt über klassische Schadsoftware Zugang verschaffen (Conversational Geek) – ein Trend, der klassische, signaturbasierte Erkennung zunehmend wirkungslos macht. Gleichzeitig registrierten ESET-Forscher mit "PromptSpy" die erste bekannte Android-Malware, die generative KI direkt in ihrem Ausführungsfluss nutzt, sowie zehntausende verdächtige und tausende eindeutig bösartige "KI-Skills" innerhalb von KI-Agenten-Ökosystemen (ESET via Yahoo Finance). Check Point dokumentiert zudem ein selteneres, aber wachsendes Muster: Schadsoftware, die während der Ausführung live mit einem Sprachmodell kommuniziert, um neue Befehle zu generieren oder sich selbst umzuschreiben (Check Point Research). Der IBM "Cost of a Data Breach Report 2026" fasst die wirtschaftliche Dimension zusammen: Jeder vierte bösartige Sicherheitsvorfall war 2025/2026 KI-gestützt – eine Zunahme von 56 Prozent gegenüber dem Vorjahr –, und solche Vorfälle verursachten mit durchschnittlich 6 Millionen US-Dollar rund eine Million US-Dollar mehr Schaden als der globale Durchschnitt (IBM Newsroom).

Systemische Verstärkung: Geopolitik und kritische Infrastruktur

Die beschriebenen Einzelphänomene verstärken sich gegenseitig in einem geopolitisch angespannten Umfeld. Der WEF-Bericht identifiziert die geopolitische Lage inzwischen als Hauptsorge von 64 Prozent der befragten Organisationen und benennt explizit neue Risikofelder, die sich mit KI-Fähigkeiten überschneiden:



autonome Systeme, Robotik, kritische Infrastruktur und Fortschritte in der Quantentechnologie (Gruppo TIM). Diese Kombination ist deshalb brisant, weil sie zwei bislang getrennte Risikodimensionen zusammenführt: die klassische Frage der Angriffsfläche kritischer Versorgungssysteme und die neue Frage, wie autonome, KI-gesteuerte Systeme in diesen Umgebungen kontrolliert bleiben. Der Bericht warnt zugleich vor einer wachsenden "Cyber-Ungleichheit" zwischen gut ausgestatteten und strukturell benachteiligten Organisationen und Staaten – ein Befund, der die Verantwortung von Ausbildungsinstitutionen zusätzlich unterstreicht, KI-Sicherheitskompetenz nicht nur in ohnehin privilegierten Umgebungen zu vermitteln.

Die Angriffsfläche KI selbst

Die zweite Dimension der Herausforderung liegt darin, dass KI-Systeme nicht nur Angriffswerkzeug, sondern selbst Angriffsziel sind. Large Language Models und die darauf aufbauenden Agenten-Architekturen weisen eigene, spezifische Schwachstellenklassen auf, die der OWASP Top 10 for LLM Applications systematisch erfasst: Prompt-Injection (direkt und indirekt), Datenvergiftung und Backdoor-Angriffe auf Trainingsdaten, unsichere Ausgabeverarbeitung, übermäßige Handlungsautonomie von Agenten sowie Schwächen in der Lieferkette von Modellen und Trainingsdaten. Die IBM "X-Force Threat Intelligence Index 2026"-Studie registriert einen Anstieg öffentlich ausnutzbarer Anwendungsschwachstellen um 44 Prozent, in erheblichem Maße getrieben durch KI-gestützte Schwachstellensuche auf Angreiferseite (IBM Newsroom); zugleich berichten laut IBM mehr als 20 Prozent der Organisationen von einem Sicherheitsvorfall, der gezielt KI-Modelle oder -Anwendungen betraf – meist verursacht durch kompromittierte Programmierschnittstellen, Plug-ins oder fehlerkonfigurierte Cloud-Umgebungen, in denen die KI läuft.

Ein besonders unterschätztes Risiko betrifft die Modell- und Daten-Lieferkette selbst: Viele Modellgewichte werden im Python-eigenen "Pickle"-Format verteilt, dessen Deserialisierung beliebigen Code ausführen kann – ein Umstand, der ein heruntergeladenes Modell potenziell in ein Einfallstor für Codeausführung verwandelt. Als Gegenmaßnahme etabliert

sich das Konzept eines "AI-Bill-of-Materials" (AI-BOM), das Herkunft, Trainingsdaten und Abhängigkeiten eines Modells so dokumentiert, wie es die Softwarebranche für klassische Software-Lieferketten bereits mit der Software-BOM eingeführt hat. Ohne eine solche Dokumentation bleibt für Sicherheitsteams oft unklar, welche Trainingsdaten, Vortrainings-Checkpoints oder Drittanbieter-Komponenten in einem produktiv genutzten Modell stecken – und damit auch, welche der oben genannten Schwachstellenklassen im Einzelfall tatsächlich relevant sind.

Diese technische Verwundbarkeit trifft auf eine ausgeprägte Governance-Lücke. Zwar hat sich der Anteil der Organisationen, die die Sicherheit eingesetzter KI-Werkzeuge systematisch bewerten, laut WEF von 37 Prozent (2025) auf 64 Prozent (2026) beinahe verdoppelt – doch das bedeutet zugleich, dass immer noch mehr als ein Drittel aller Organisationen KI-Werkzeuge ohne vorherige Sicherheitsprüfung einsetzt (WEF). Besonders bemerkenswert ist ein Wahrnehmungsbruch zwischen Führungsebenen: Während Geschäftsführungen KI-Schwachstellen inzwischen als ihr zweitgrößtes Cyberrisiko einstufen, führen IT-Sicherheitsverantwortliche (CISOs) dasselbe Risiko in ihren eigenen Top-3-Prioritäten oft gar nicht auf (Fortinet) – ein Hinweis darauf, dass die strategische Risikowahrnehmung mit der operativen Realität noch nicht Schritt hält.

Die doppelte Rolle der KI: Chance und Grenze der Verteidigung

KI ist keine Einbahnstraße. Laut WEF setzen 52 Prozent der Organisationen KI bereits zur Phishing-Erkennung, 46 Prozent zur Angriffs- und Anomalieerkennung und 40 Prozent zur Analyse von Nutzerverhalten ein (WEF "Empowering Defenders"). KI-gestützte "Security Operations Center"-Kopiloten können Ermüdungserscheinungen bei der Alarmbearbeitung reduzieren, Muster über riesige Datenmengen hinweg erkennen und Analystinnen und Analysten von repetitiven Sichtungsaufgaben entlasten. Gartner geht davon aus, dass bis 2028 15 Prozent aller täglichen Arbeitsentscheidungen von KI-Agenten autonom getroffen werden – für die Cybersicherheit bedeutet dies speziali-

sierte Agenten, die über Bedrohungsanalyse, Schwachstellenmanagement und Incident Response hinweg zusammenarbeiten (ebd.).

Diese Chance ist jedoch an drei strukturelle Grenzen gebunden. Erstens neigen große Sprachmodelle zu Halluzinationen – im eingangs beschriebenen Anthropic-Fall erschwerten sie interessanterweise sogar den Angreifern selbst die Arbeit, indem die KI Ergebnisse übertrieb oder erfand (Anthropic); im Verteidigungskontext führen sie jedoch zu Fehlalarmen und falschem Vertrauen. Zweitens droht "Automation Bias": Wenn Analysten KI-Einschätzungen ungeprüft übernehmen, sinkt die menschliche Kontrollfunktion genau in dem Moment, in dem sie am nötigsten wäre. Drittens – und strategisch am gravierendsten – besteht eine fundamentale Kostenasymmetrie: Angreifer können zusätzliche Rechenleistung, Daten und Testzeit linear in sofort skalierbare Wirkung umsetzen, während Verteidiger nach wie vor überwiegend linear über zusätzliches Personal und fragmentierte Werkzeuglandschaften skalieren müssen (PwC). Diese Asymmetrie ist der eigentliche Kern der Herausforderung: Es geht nicht nur darum, neue Werkzeuge zu beherrschen, sondern ein strukturelles Tempogefälle auszugleichen.

Hinzu kommt eine kulturelle Grenze: Die Kiteworks-Studie zeigt, dass 77 Prozent der Organisationen generative KI bereits in ihrem Sicherheits-Stack einsetzen, aber nur 37 Prozent über eine formale KI-Richtlinie verfügen, die Nutzung, Freigabeprozesse und Verantwortlichkeiten regelt (Kiteworks). KI-Einsatz in der Verteidigung entsteht damit häufig praxisgetrieben und "von unten", bevor Governance-Strukturen nachziehen – ein Muster, das Kontrollverlust und uneinheitliche Qualitätsstandards begünstigt. 67 Prozent der befragten Organisationen setzen bereits agentische KI ein, also Systeme, die nicht nur Empfehlungen aussprechen, sondern eigenständig Handlungen auslösen (ebd.) – ein Schritt, der die oben beschriebene Automation-Bias-Problematik von der Empfehlungs- auf die Ausführungsebene hebt und damit die Anforderungen an Aufsicht und Nachvollziehbarkeit zusätzlich erhöht.

Regulatorische Antworten: Ein Rahmen im Aufbau

Der Gesetzgeber reagiert – mit Verzögerung, aber zunehmender Verbindlichkeit. Der EU AI Act verpflichtet Anbieter hochrisikoreicher KI-Systeme in Artikel 15 dazu, ein "angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit" über den gesamten Lebenszyklus des Systems sicherzustellen (artificialintelligenceact.eu). Der Zeitplan der Verordnung wurde durch das im Juli 2026 verabschiedete "AI Omnibus"-Paket neu justiert: Die Transparenzpflichten aus Artikel 50 sowie die Aufsicht über Anbieter von KI-Basismodellen (General-Purpose AI) traten wie ursprünglich vorgesehen am 2. August 2026 in Kraft, während die strengerer Pflichten für eigenständige Hochrisiko-Systeme gemäß Anhang III – etwa in den Bereichen Bildung, Beschäftigung oder kritische Infrastruktur – um 16 Monate auf den 2. Dezember 2027 verschoben wurden (Cloud Security Alliance; Software Improvement Group). Verstöße können mit Bußgeldern von bis zu 35 Millionen Euro oder 7 Prozent des weltweiten Konzernumsatzes geahndet werden (ADVISORI).

Neben dem EU AI Act etabliert sich ein Ökosystem komplementärer Rahmenwerke: das NIST Cybersecurity Framework 2.0 mit seinen sechs Funktionen (Govern, Identify, Protect, Detect, Respond, Recover) als übergreifende Governance-Struktur, das NIST AI Risk Management Framework für die spezifische Risikobewertung von KI-Systemen, ISO/IEC 42001 als erster internationaler Managementsystemstandard für KI sowie – speziell für den Sicherheitssektor – NIST IR 8596 ("Cyber AI Profile"). Für Cybersecurity-Fachkräfte bedeutet dies: Regulatorisches Wissen ist kein Randthema mehr, sondern eine Kernkompetenz, die technisches Verständnis von Angriffsflächen mit Kenntnissen über Nachweis-, Dokumentations- und Meldepflichten verbindet.

Der Flaschenhals: Fachkräftemangel in Zeiten der Beschleunigung

All diese Entwicklungen träfen auf eine ohnehin angespannte Personalsituation. Die "ISC2 Cybersecurity Workforce Study" bezifferte die globale Fachkräftelücke zuletzt auf 4,8 Millionen unbesetzte Stellen; laut



ISACA berichten 90 Prozent der Sicherheitsteams von Kompetenzlücken, während nur 14 Prozent der Organisationen über die benötigten Fachkräfte tatsächlich verfügen (StationX). Entscheidend ist dabei weniger die reine Personalzahl als die Art der fehlenden Kompetenzen: KI und maschinelles Lernen sind laut ISC2 mit 41 Prozent – ein Anstieg von 34 Prozent im Vorjahr – der mit Abstand am häufigsten genannte Qualifizierungsbedarf in Sicherheitsteams (StationX). Die ISC2-Analyse “Aligning Skills, People and Hiring” bestätigt, dass der Engpass zunehmend nicht mehr in der Zahl der Beschäftigten, sondern in fehlenden, aktuellen Kompetenzprofilen in Bereichen wie KI, Cloud-Sicherheit, Risikobewertung und Governance liegt (ISC2). Diese Lücke lässt sich nicht allein durch Neueinstellungen schließen – sie erfordert gezielte, strukturierte Weiterqualifizierung bestehender wie angehender Fachkräfte.

Qualifizierung als Antwort

Aus den vorangegangenen Abschnitten lässt sich ein klares Kompetenzprofil ableiten, das Cybersecurity-Fachkräfte heute benötigen: Verständnis dafür, wie generative und agentische KI funktioniert und wo ihre Grenzen liegen; die Fähigkeit, KI-spezifische Angriffsflächen (adversariale Angriffe, Prompt-Injection, Modell-Lieferketten) zu erkennen und abzusichern; praktische Erfahrung mit dem Einsatz von KI in der Verteidigung, einschließlich ihrer Grenzen wie Automation Bias und Alert Fatigue; Kenntnis der wachsenden Bedrohung durch Deepfakes und KI-gestütztes Social Engineering; und schließlich Vertrautheit mit dem regulatorischen Rahmen von EU AI Act, NIST-Frameworks und ISO/IEC 42001.

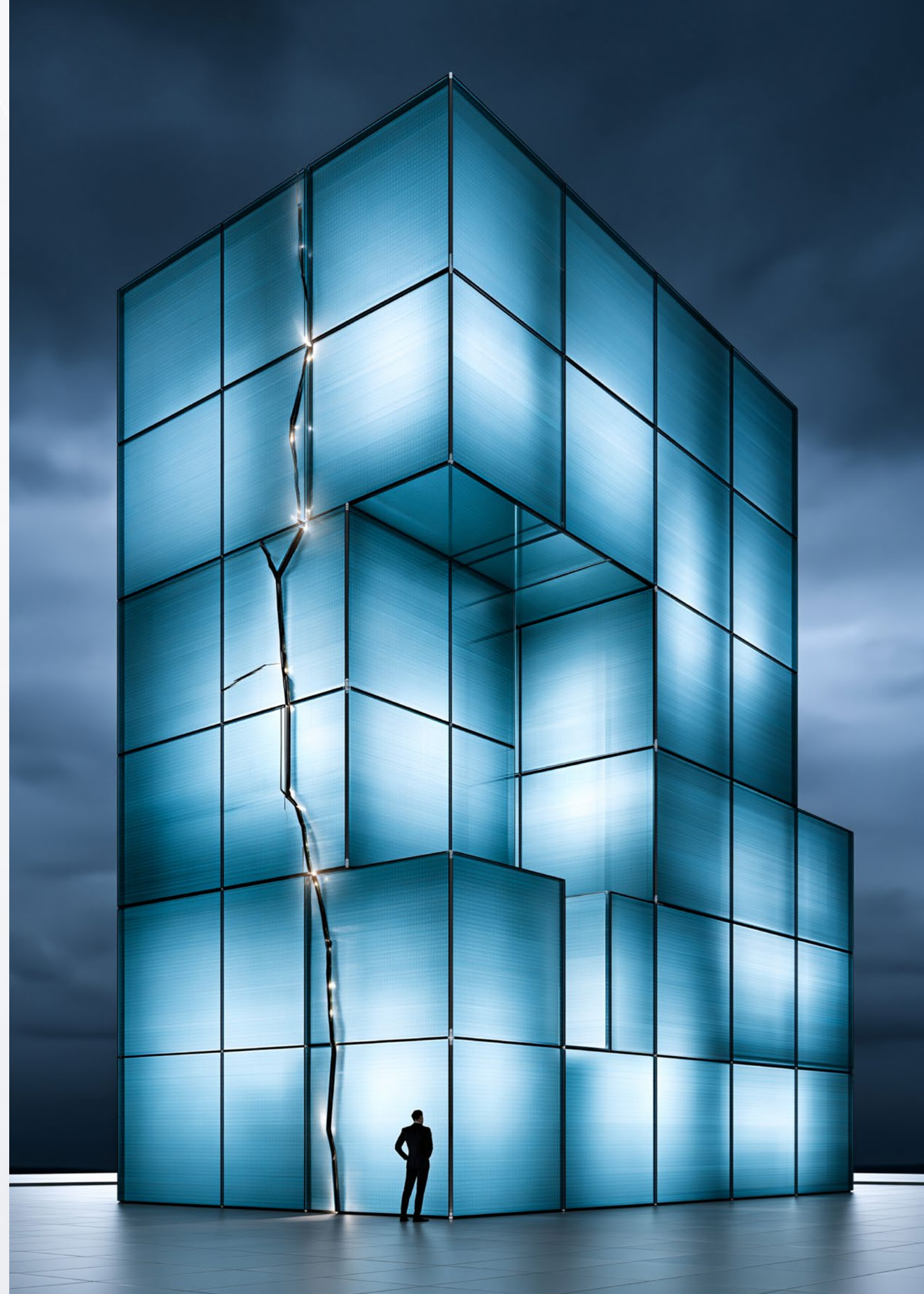
Akademische Weiterbildungsinstitutionen tragen hier eine besondere Verantwortung: Sie müssen Curricula so gestalten, dass sie nicht nur technisches Wissen vermitteln, sondern die Fähigkeit, im sich beschleunigenden, KI-geprägten Bedrohungsumfeld begründete, verantwortungsvolle Entscheidungen zu treffen. Es zeigt sich exemplarisch, wie sich die im Text skizzierte, abstrakte Herausforderung – das Wettrüsten zwischen KI-gestützter Offensive und einer noch aufholenden, unterbesetzten Verteidigung – in konkrete, prüfungsrelevante Lernprogramme für angehende Sicherheitsexpertinnen und -experten übersetzen lässt.

Fazit

Die zentrale Herausforderung, vor die leistungsfähige KI-Systeme die Cybersecurity heute stellen, ist keine einzelne technische Schwachstelle, sondern eine mehrdimensionale Verschiebung: Angriffe werden schneller, personalisierter und zunehmend autonom ausgeführt; die KI-Systeme selbst werden zu neuen, oft unzureichend abgesicherten Angriffsflächen; die Verteidigung profitiert zwar von KI-gestützten Werkzeugen, bleibt aber durch eine strukturelle Kostenasymmetrie im Nachteil; die Regulierung zieht in Etappen nach, ohne bereits vollständige Rechtssicherheit zu schaffen; und all dies trifft auf einen Arbeitsmarkt, dem es an genau den KI-bezogenen Kompetenzen fehlt, die zur Bewältigung dieser Lage nötig wären. Institutionen der akademischen Weiterbildung tragen damit eine besondere Verantwortung: Sie müssen Curricula so gestalten, dass sie nicht nur technisches Wissen vermitteln, sondern die Fähigkeit, in einem sich beschleunigenden, KI-geprägten Bedrohungsumfeld begründete, verantwortungsvolle Entscheidungen zu treffen. -v-

Quellen (Auswahl)

- Anthropic (2025): Disrupting the first reported AI-orchestrated cyber espionage campaign. anthropic.com
- World Economic Forum (2026): Global Cybersecurity Outlook 2026. weforum.org
- CrowdStrike (2026): 2026 Global Threat Report. crowdstrike.com
- IBM (2026): Cost of a Data Breach Report 2026 / X-Force Threat Intelligence Index 2026. ibm.com
- Richtlinie (EU) 2022/2555 (NIS2) und EU AI Act, Art. 15 und 21. artificialintelligenceact.eu
- ISC2 (2026): Cybersecurity Workforce Study / Aligning Skills, People and Hiring. isc2.org





Cybersicherheit im Zeichen von Gefahren durch agentische KI

MIRKO ROSS

11 Handlungspunkte für IT/OT-Cybersicherheit

Während eines ExploitGym-Benchmark-Sicherheitstests durch OpenAI wurden Drittparteien wie Hugging Face zur Lösung der gestellten Aufgabe durch agentische KI kompromittiert. Dieser Sicherheitsvorfall hat gezeigt, dass hochentwickelte KI-Agenten in Kombination mit leistungsstarken KI-Frontier-Modellen autonome Exploit-Fähigkeiten mit weitreichenden Planungsfähigkeiten entwickeln können.

Diese sind in der Lage, komplexe IT-Systeme und Anwendungen zu analysieren, dynamische Codeanalysen durchzuführen und Schutzmaßnahmen wie Sandboxing zu umgehen. Zudem können diese KI-Agenten auf die Suche nach neuen Zero-Day-Schwachstellen ausweichen, falls ein zuvor eingeschlagener Pfad zur Ausnutzung von Schwachstellen mit bekannten Exploits fehlschlägt.

Um IT-/OT-Umgebungen vor solchen KI-automatisierten Angriffen zu schützen, müssen Abwehrmaßnahmen über klassische Methoden wie ein reaktives Patch-Management hinausgehen. Es ist wichtig, dass sich Organisationen in der Cybersicherheit neu aufstellen. Methoden wie risikopriorisierte Gegenmaßnahmen, Segmentierung, Governance für KI-Agenten sowie ein Monitoring von agentischer KI sind Schlüssel zur erfolgreichen Abwehr dieser neuen Gefahren durch KI.

Im Folgenden werden elf strategische Handlungsempfehlungen für IT/OT-Sicherheitsteams zum Umgang mit Gefahren durch KI-Agenten zusammengefasst.

Segmentierung von IT-/OT-Netzwerken

Die Implementierung einer (Mikro-)Segmentierung für IT-/OT-Zonen und Isolierung von industriellen Steuerungssystemen (ICS/SCADA), speicherprogrammierbaren Steuerungen (SPS) und Edge-Gateways über Zero-Trust-Netzwerkzonen ist eine wirkungsvolle Schutzmaßnahme gegen Angriffe durch KI-Agenten.

Für hochkritische Anwendungen sind zusätzliche Netzwerkabsicherungen wie Air Gaps zu empfehlen. Standardmäßig müssen API-Schnittstellen und Ports

zwischen diesen Segmenten geschlossen sein und offene Ports auf Protokolle und Aktivitäten durch agentische KI überwacht werden. KI-Agenten zeichnen sich durch laterale Bewegung über mehrere Punkte in Netzwerken und deren Erkundung aus, wenn ihnen ein unbegrenzter Zugang im Netzwerk gewährt wird. (Mikro-)Segmentierung verhindert, dass ein KI-Agent ohne Hürden von einer kompromittierten IT-Umgebung in weitere IT-Elemente und beispielsweise kritische OT-Prozesse vordringt. Jeder Übergang zwischen Netzwerksegmenten erzeugt für KI-Agenten einen Bedarf an Rechenleistung (Compute) zur Suche und Ausnutzung von Schwachstellen. (Mikro-)Segmentierung erhöht somit den Ressourcenaufwand für den Angreifer.

Hardware gestützte Sicherheitsmerkmale

KI-Agenten können dazu Angriffsmethoden auf Ebene des Betriebssystems, wie beispielsweise im Kernel-Speicher-Management, anwenden, um einen Sprung aus der Sandbox oder zu anderen Systemumgebungen zu bewerkstelligen. Hardwaregestützte Sicherheitsmerkmale (Smartcards), Physical Unclonable Functions (PUF) und Trusted Platform Modules (TPM) stellen durch die physikalische Bindung für agentische KI eine schwere zu überwindende Hürde dar. Daher sollten kritische Systembereiche und Systemelemente zusätzlich mit solchen physikalischen Sicherheitsfunktionen abgesichert werden. Anwendungsbereiche sind hier beispielsweise Kernel Prozesse auf Betriebssystemebene, Speichersicherheit, Root-Dateisysteme, Endgeräte, virtuelle Maschinen und Container. Abwehrmaßnahmen zum Schutz des Betriebssystemkerns wie Address Space Layout Randomisation (ASLR) senken die Erfolgsraten von KI-Agenten beim Ausbruch aus Sandbox-Umgebungen oder dem Eindringen in Zielsysteme.

Anwendungshygiene auf Test- und Produktivsystemen

KI-Agenten sind in hohem Maße auf vorhandene Werkzeuge angewiesen, um Laufzeitumgebungen und Netzwerke zu untersuchen, lokale Exploits zu kompilieren und Fuzzing-Tests in parallelen Ausführungen durchzuführen. Die Entfernung aller Debugging-Tools, Compiler, Binäranalyse-Tools und dynamischen Skript-Shells aus den produktiven IT- und OT-(Mikro-)Segmenten und Systemen ist zum Schutz vor Angriffen durch KI-Agenten unerlässlich.

Monitoring und Anomalieerkennung

Autonome KI-Agenten arbeiten oftmals nach Brute-Force-Prinzipien und generieren parallele Trial-and-Error-Iterationen sowie API-Aufrufe, während sie Zielsysteme untersuchen und den Erfolg von Exploits überprüfen. Der Einsatz von Verhaltenserkennungssystemen, die hochfrequente Befehlssequenzen, ungewöhnliche Dateisystemabfragen oder API-Aufrufe innerhalb kurzer Zeitfenster erkennen und einen Alarm auslösen, muss auf KI-Agenten ausgeweitet werden. Die zur Verhaltenserkennung verwendeten KI-Modelle sollten dabei dynamisch austauschbar sein, damit der Angreifer seinen Angriff nicht einfach auf ein spezifisches KI-Modell der Verhaltenserkennung anpassen kann.

Risikobasierte Patch- und Update-Zyklen

Agenten prüfen Codebasen unabhängig voneinander und identifizieren sekundäre Schwachstellen. Wenn eine bekannte Schwachstelle nicht gepatcht ist, stellt diese eine für KI-Agenten leicht zu lösende Aufgabe dar. Die Etablierung einer kontinuierlichen Pipeline für das Schwachstellenmanagement mit strengen SLA-Fristen für Zero-Day- und N-Day-Schwachstellen in Betriebssystemkernen, Software-Bibliotheken, virtuellen Systemen und Web-Engines ist in Zeiten von blitzschnellen KI-Angriffen notwendig.

Dabei ist die Reihenfolge und Anwendung von Patches auf Basis der Risiken für die eigenen IT-/OT-Systeme zu priorisieren. Systeme mit hohen Risiken sind vorrangig und in engen Zeitfenstern von

12 Stunden bis einen Tag zu patchen. Die Reduzierung der Angriffsfläche durch bekannte Schwachstellen ist daher unerlässlich.

Human in the Loop bei kritischen Prozessen

Autonome KI-Systeme führen Befehlsketten ohne menschliches Eingreifen aus. Harte physische oder kryptografische Grenzen verhindern, dass KI-Agenten destruktive Aktionen ausführen.

Für risikoreiche Vorgänge (z. B. Firmware-Updates in Firewalls, Routern und OT-/SPS-Systemen) ist eine Mehrfaktor-Authentifizierung (MFA) oder eine Verifizierung per Hardware-Token oder Smartcards zum Schutz vor KI-Agenten erforderlich.

Zero-Trust-Identitätsarchitektur mit kurzlebigen Anmeldeinformationen

KI-Agenten nutzen Berechtigungen oder ungeschützte lokale Authentifizierungstokens, um sicherheitsrelevante Informationen zu exfiltrieren und Berechtigungen in Systemen bis zum Vollzugriff (Root-Berechtigungen) auszuweiten. Die Absicherung von Systeminteraktionen muss mithilfe von Authentifizierung und kurzlebigen Tokens an bereichsgebundene Identitäten und Non Human Identities erfolgen. Das Prinzip der geringsten Berechtigungen für alle Benutzeraccounts muss auf allen Anwendungsebenen durchgesetzt werden.

Automatisierte KI-Agenten in der Verteidigung einsetzen (KI-Angriff vs. KI-Triage)

Eine KI-automatisierte Verteidigung ist erforderlich, um mit der Geschwindigkeit der KI-Angriffe Schritt zu halten. Integration von KI-Agenten in den SOC-Betrieb wird daher notwendig, um eine kontinuierliche, automatisierte Risiko-Triage und Patch-Validierung mit minimalen Latenzen durchzuführen. Menschliche Verteidiger können manuell nicht rechtzeitig auf mehrstufige, automatisierte Exploit-Generierung durch KI-Agenten reagieren, die in kontinuierlichen hochfrequenten Zeitfenstern abläuft.



Sicherung der Schnittstellen zwischen KI-Agenten und API-Protokollen

Agentenbasierte Workflows, die nicht validierte Eingaben akzeptieren oder Befehlseingaben ohne Absicherung ausführen, können missbraucht werden, um als unbeabsichtigte Proxys für laterale Angriffe durch KI-Agenten zu fungieren. Alle agentenübergreifenden Nachrichten, Prompts, Protokolle, Schema-Nutzdaten und API-Aufrufe müssen mithilfe strenger Eingabvalidierung kontrolliert werden.

Prompts müssen durch Parser gegen schädliche Prompt-Injections bereinigt werden. Mit Unterstützung kryptografischer Methoden sind APIs und Protokollinhalte gegen Manipulation zu sichern.

Überwachung von Zustandsabweichungen und Sandboxing

KI-Agenten versuchen dynamische Umgehungstechniken, beispielsweise durch Manipulation des Kernel-Zustands. Die Weiterleitung von KI-agentischen Telemetriedaten, Ereignissen und Container-Protokollen an einen Security Data Lake ist zu empfehlen, um bei einem Post-Compromise-Verdacht eine forensische Analyse der Indicators of Compromise (IoC) zu ermöglichen. (Mikro-)Segmente, Container und Anwendungen können so bei Erkennung einer Zustandsabweichung unter Quarantäne gestellt werden. Die Telemetrieanalyse gewährleistet die Nachvollziehbarkeit, selbst wenn der lokale Laufzeit-Speicher kompromittiert ist.

Proaktives Threat Hunting zum Erkennen von Schwachstellen

KI-Agenten suchen und nutzen in erster Linie sowohl bekannte Schwachstellen als auch unsichere Konfigurationen, um einen Angriff auszuführen. Neue Zero-Day-Schwachstellen werden dabei ebenso gesucht, um einen bislang unbekannten Angriffspfad erfolgversprechend einschlagen zu können. Die Nutzung von KI-Agenten zur proaktiven Suche nach Schwachstellen in der eigenen IT-/OT-Infrastruktur kann hier zum Vorteil in der Cyberabwehr genutzt werden.

Die durch KI-Agenten im Red Teaming gewonnenen Erkenntnisse werden ausgewertet, um Schwachstellen mittels Patches, Updates und Konfigurationsmanagement zu schließen und damit die Angriffsoberfläche für Angriffe zu verkleinern. Dazu muss die Nutzung von agentischer KI, um ein automatisiertes Red Teaming in engen Testzyklen für Risikosysteme und Risikoanwendungen aufgebaut werden. Bei wesentlichen Änderungen am Zielsystem, beispielsweise bei Updates oder neuen Konfigurationen, sollte immer ein automatisierter Pentest durch KI-Agenten die Systemsicherheit auf Schwachstellen prüfen.

Zusammenfassung

Die Bedrohung durch KI-basierte Angriffe ist eine Realität. Diese läutet eine neue Ära der Cybersicherheit ein. Bislang praktizierte Methoden, Werkzeuge und organisatorische Abläufe müssen um den Aspekt der KI-Bedrohungen erweitert werden. Die notwendige Beschleunigung von Prozessen wie Schwachstellen-Scans, Patch- und Update-Management müssen in weiten Teilen durch Automatisierung erfolgen. KI und KI-Agenten bieten hier neue Möglichkeiten und Chancen. Das Rennen um die effektivste Nutzung von KI zwischen Angreifer und Verteidiger ist damit eröffnet. -v-

Cybersecurity im Zeitalter autonomer KI neu denken

OLIVIER SCHRANER

Cybersecurity war schon immer ein Wettlauf zwischen Angreifern und Verteidigern. Doch mit dem Einsatz von Künstlicher Intelligenz verändert sich die Dynamik dieses Wettlaufs grundlegend. Angriffe werden schneller, skalierbarer und kostengünstiger. Gleichzeitig wachsen digitale Infrastrukturen in einem bislang unbekannten Ausmaß: Daten, Anwendungen, Identitäten, Endgeräte und zunehmend auch KI-Systeme selbst müssen geschützt werden.

Viele Sicherheitskonzepte wurden für eine Welt entwickelt, in der Menschen Angriffe planen, analysieren und abwehren. Diese Welt verändert sich gerade. Angreifer nutzen bereits KI, um Schwachstellen schneller zu finden, Phishing-Kampagnen zu automatisieren oder neue Angriffswege zu entwickeln. Die Frage lautet daher nicht mehr, ob KI die Cybersicherheit verändert, sondern wie Verteidiger mit derselben Geschwindigkeit und Skalierung reagieren können. Aus unserer Sicht braucht Sicherheit deshalb einen neuen Cyber Stack.

Von der reaktiven zur kontinuierlichen Verteidigung

Traditionelle Sicherheitsarchitekturen sind stark auf Erkennung und Alarmierung ausgelegt. Sie sammeln Signale, erstellen Warnmeldungen und überlassen die Analyse anschließend menschlichen Sicherheitsteams. Dieses Modell stößt zunehmend an seine Grenzen.

Sicherheitsteams sehen sich heute mit einer Flut von Daten, Warnungen und potenziellen Risiken konfrontiert. Die Herausforderung besteht längst nicht mehr darin, Informationen zu sammeln. Die eigentliche Herausforderung besteht darin, aus Milliarden von Signalen die wenigen relevanten Risiken zu identifizieren und daraus die richtigen Maßnahmen abzuleiten.

Die nächste Generation von Sicherheitssystemen muss deshalb mehr leisten als nur Informationen bereitzustellen. Sie muss Risiken kontinuierlich erkennen, einordnen und geeignete Gegenmaßnahmen unterstützen oder automatisiert umsetzen. Kurz gesagt: Sie muss wahrnehmen, verstehen und handeln können.

KI als Verstärker menschlicher Expertise

Dabei geht es nicht darum, Menschen zu ersetzen. Cybersecurity bleibt eine zutiefst menschliche Aufgabe. Verantwortung, Risikobewertung und Entscheidungen liegen weiterhin bei den Menschen.

KI kann jedoch dabei helfen, die Fähigkeiten von Sicherheitsteams massiv zu erweitern. Moderne Agentensysteme können rund um die Uhr große Mengen an Sicherheitsdaten analysieren, Zusammenhänge herstellen, priorisieren und Handlungsempfehlungen liefern. Dadurch gewinnen Expertinnen und Experten Zeit für jene Aufgaben, bei denen menschliches Urteilsvermögen unverzichtbar ist.

Eine zentrale Rolle spielt dabei der Kontext. Sicherheitsentscheidungen können nicht allein auf einzelnen Signalen basieren. Erst das Zusammenspiel von Identitäten, Geräten, Anwendungen, Daten und bekannten Bedrohungsmustern ermöglicht eine fundierte Bewertung von Risiken. Je besser Systeme diesen Kontext verstehen, desto präziser und effizienter können sie Sicherheitsmaßnahmen unterstützen.

Warum ein einzelnes Modell nicht ausreicht

Mit der Verbreitung generativer KI entstand häufig der Eindruck, ein einziges leistungsfähiges Modell könne sämtliche Sicherheitsaufgaben übernehmen. Die Praxis zeigt jedoch ein anderes Bild. Cybersicherheit umfasst unterschiedlichste Aufgaben: von der Analyse von Schwachstellen über die Priorisierung von Risiken bis hin zur automatisierten Reaktion auf Vorfälle. Für diese Aufgaben sind unterschiedliche Fähigkeiten, Reaktionszeiten und Kostenstrukturen erforderlich.

Deshalb setzen sich zunehmend Multi-Modell-Ansätze durch. Dabei wird für jede Aufgabe jenes Modell eingesetzt, das die beste Kombination aus Qualität, Geschwindigkeit und Wirtschaftlichkeit bietet. Gerade in einer Sicherheitswelt, die rund um die Uhr aktiv ist, wird Effizienz zu einem entscheidenden Faktor.

Ein Beispiel dafür ist Microsofts neues Security-Modell MAI-Cyber-1-Flash, das speziell für die



Analyse von Software-Schwachstellen entwickelt wurde. In Kombination mit agentengestützten Security-Workflows erreicht dieser Ansatz Spitzenwerte bei Sicherheitsbenchmarks und ermöglicht gleichzeitig deutlich geringere Betriebskosten. Das zeigt: Fortschritt entsteht nicht allein durch größere Modelle, sondern durch das intelligente Zusammenspiel von Modellen, Daten und spezialisierten Agenten.

Die Zukunft der Sicherheit ist agentisch

Die vielleicht wichtigste Entwicklung der kommenden Jahre ist der Übergang von isolierten Sicherheitswerkzeugen hin zu intelligenten, zusammenarbeitenden Agentensystemen.

Mit Project Perception arbeitet Microsoft an einer neuen Generation agentischer Sicherheitsarchitekturen. Dabei übernehmen spezialisierte KI-Agenten unterschiedliche Rollen: Sie suchen nach potenziellen Schwachstellen, bewerten Risiken, schlagen Gegenmaßnahmen vor und helfen dabei, Sicherheitslücken schneller zu schließen.

Entscheidend ist dabei, dass diese Systeme in einem kontinuierlichen Kreislauf arbeiten. Sie lernen fortlaufend aus neuen Informationen, passen sich veränderten Bedrohungslagen an und unterstützen Organisationen dabei, ihre Sicherheitslage laufend zu verbessern.

Für Unternehmen bedeutet das einen wichtigen Perspektivenwechsel. Sicherheit wird zunehmend von einem reaktiven Prozess zu einer kontinuierlichen und lernenden Fähigkeit.

Vertrauen bleibt die Grundlage

Bei aller Begeisterung für technologische Innovation gilt jedoch eine zentrale Erkenntnis: Sicherheit beginnt mit Vertrauen.

Je stärker KI in Sicherheitsprozesse eingebunden wird, desto wichtiger werden Transparenz, Governance, Compliance und menschliche Kontrolle. Unternehmen müssen nachvollziehen können, wie Entscheidungen zustande kommen und welche Maßnahmen automatisiert umgesetzt werden.

Die Zukunft der Cybersecurity wird daher nicht allein durch leistungsfähigere Modelle bestimmt. Entscheidend wird sein, KI verantwortungsvoll einzusetzen und technologischen Fortschritt mit klaren Sicherheits- und Governance-Prinzipien zu verbinden.

Denn am Ende gewinnt nicht jene Organisation, die die meisten Warnmeldungen erzeugt. Gewinnen werden jene Unternehmen, die Risiken schneller verstehen, fundierter entscheiden und wirksamer handeln können. Genau darin liegt die Chance einer neuen Generation agentischer Sicherheit. -v-



Die Lösung der Gegenwart (und Zukunft)

Die Lösung der Gegenwart (und Zukunft)

Symantec CBX: Endlich eine Sicherheitsplattform für kleinere Teams im Kampf gegen größere Bedrohungen

Herkömmliche, isolierte Sicherheitslösungen überfordern kleinere Teams häufig mit einer Flut von Warnmeldungen und unvollständigen Informationen.

Symantec CBX vereint die Stärken von Symantec und Carbon Black in einer cloudbasierten XDR-Plattform mit nativer Telemetrikorrelation, KI-Unterstützung und Schutz auf Enterprise-Niveau.

Speziell für Teams mit begrenzten Ressourcen entwickelt, reduziert Kosten und die Alarmflut und beschleunigt Reaktionszeiten.

Cybersicherheitsteams stehen heute vor einer paradoxen Situation: Die Vielzahl einzelner Sicherheitslösungen erhöht häufig die Komplexität und erschwert den Überblick über die gesamte IT-Umgebung. Besonders kleinere Teams leiden darunter, da ihnen oft die Ressourcen fehlen, verschiedene Produkte zu integrieren und die daraus entstehenden Daten sinnvoll auszuwerten.

Während große Unternehmen komplexe Sicherheitsarchitekturen betreiben können, kämpfen kleinere Organisationen zunehmend mit KI-gestützten Angriffen auf Enterprise-Niveau. Ihnen fehlen jedoch häufig Budget und Know-how für aufwendige Sicherheitsplattformen. Diese Sicherheitsteams brauchen nicht nur bessere Tools. Sie brauchen einen Wettbewerbsvorteil. Jetzt haben sie ihn.

XDR vom EDR-Pionier

Mit Symantec CBX präsentieren wir eine neue XDR-Lösung (Extended Detection and Response), die die bewährten Technologien von Symantec und Carbon Black in einer einheitlichen Cloud-Plattform zusammenführt. CBX wurde speziell für kleinere Sicherheitsteams entwickelt, die ihre Sicherheitslage verbessern wollen, ohne komplexe Enterprise-Lösungen betreiben zu müssen.

Die Plattform beseitigt eines der größten Probleme moderner Sicherheitsarchitekturen: die Fragmentierung von Telemetriedaten. Statt auf unvollständige API-Integrationen zu setzen, korreliert CBX Daten aus Endpunkten, Netzwerken und Datensicherheitslösungen nativ. Dadurch erhalten Sicherheitsteams ein vollständigeres Bild von Vorfällen und können schneller reagieren.

Symantec CBX löst dieses Problem, indem es die robusten Präventions-, Datensicherheits- und Netzwerksicherheitsfunktionen von Symantec mit der wegweisenden EDR-Technologie von Carbon Black in einer einzigen Cloud-Plattform vereint. Dies ermöglicht umfassende Transparenz, herausragende Bedrohungserkennung und schnelle Reaktion über alle Angriffsflächen hinweg.

Native Korrelation ist erst der Anfang

Die native Telemetrikorrelation bildet die Grundlage für zahlreiche weitere Funktionen, die Sicherheitsteams effizienter und produktiver machen.

KI, die die Arbeit erleichtert: CBX nutzt KI gezielt zur Unterstützung von Sicherheitsteams. Mit Carbon Black Threat Tracer können Analysten den gesamten Angriffsverlauf in einer einzigen Ansicht nachvollziehen. Selbst weniger erfahrene Mitarbeiter erkennen schnell Herkunft, Vorgehensweise und Auswirkungen eines Angriffs.

Zusätzlich nutzt Symantec Adaptive Protection KI, um sogenannte Living-Off-The-Land-Angriffe frühzeitig zu stoppen. Die Funktion Incident Prediction prognostiziert sogar potenzielle nächste Schritte eines Angreifers und hilft dabei, eine weitere Ausbreitung zu verhindern.

Umfassendere Einblicke für schnellere Behebung: Die KI-gestützten Incident Summaries fassen Vorfälle übersichtlich zusammen und liefern konkrete Handlungsempfehlungen. Dadurch können Analysten schneller Prioritäten setzen und effektiver reagieren.

Netzwerk- und Datenschutz auf Enterprise-Niveau: CBX vereint die Funktionen von Symantec Secure



Web Gateway (SWG) und Symantec DLP in einer Plattform. Schädlicher Netzwerkverkehr wird bereits am Netzwerkrand blockiert, während integrierte DLP-Funktionen sensible Daten schützen.

Darüber hinaus unterstützt die Plattform moderne Post-Quanten-Kryptografieprotokolle und hilft Unternehmen, sich gegen zukünftige „Capture Now, Decrypt Later“-Angriffe zu wappnen.

Aussagekräftige Ergebnisse und schneller Nutzen: Von Sicherheitsmanagern wird erwartet, dass sie die Leistung ihrer Teams kontinuierlich verbessern. Dies ist jedoch nicht einfach, wenn unzusammenhängende Lösungen unnötige Reibungsverluste und Verwirrung stiften und mehrere Dashboards wertvolle Zeit rauben. Wir haben Symantec CBX mit den Funktionen und der einheitlichen Managementkonsole entwickelt, die die wichtigsten Ergebnisse für Sicherheitsteams liefern: Senkung der SIEM- und Betriebskosten, Entlastung der Analysten, schnellere Problemlösung, Erfüllung von Governance-Anforderungen und Nachweis von Fortschritten durch verbesserte Kennzahlen. Dank der sofort einsatzbereiten Richtlinienkonfigurationen ist CBX einfach zu implementieren und bietet unmittelbaren Mehrwert.

Die ideale Plattform für den Kern des Marktes

Symantec CBX zielt direkt auf den Kern des Cybersicherheitsmarktes ab und bietet Sicherheitsteams nahezu jeder Größe eine Plattform, die ihre Bedürfnisse in den Mittelpunkt stellt. Keine andere XDR-Lösung ist so speziell auf die Bedürfnisse von Unternehmen zugeschnitten, die mit knappen Budgets, begrenzten Ressourcen, einem anhaltenden Mangel an erfahrenen Experten, chronischer Alarmmüdigkeit und der zunehmend bedrohlichen Gefahr KI-gestützter Angriffe zu kämpfen haben.

Symantec CBX ist die XDR-Plattform der Zukunft. Als erste neue Lösung von Broadcom, die Funktionen von Symantec und Carbon Black integriert, ist CBX die Verwirklichung unserer Strategie, das Versprechen „Gemeinsam stärker“ einzulösen, das wir bei der Zusammenführung dieser beiden legendären Marken unter dem Dach der Broadcom Enterprise Security Group gegeben haben. Und sie ist die ideale Lösung für unser globales Netzwerk von Catalyst-Partnern mit ihrer umfassenden regionalen Expertise und engen Kundenbeziehungen, die Unternehmen dabei unterstützen, in einem Umfeld ständigen Wandels und unerbittlicher Herausforderungen Schritt zu halten.

Überlastete Sicherheitsteams brauchen einen Vorteil – und mit Symantec CBX haben sie ihn. -v-



Digitalisierung und AI im Risikomanagement

STEPHAN DORNER

Von besseren Daten zu besseren Entscheidungen – und besserer Versicherbarkeit

Risikomanagement befindet sich in einem grundlegenden Wandel. Die zentrale Frage ist heute nicht mehr nur, ob Risiken erkannt werden, sondern wie belastbar Entscheidungen über Risiken getroffen werden können. Digitalisierung und der Einsatz von Artificial Intelligence verändern genau diese Entscheidungsqualität – und damit auch Themen wie Versicherbarkeit, Risikotransfer und Marktattraktivität.

Klassisches Risikomanagement stößt zunehmend an seine Grenzen. Komplexere Risikolandschaften, steigende regulatorische Anforderungen und eine wachsende Menge verfügbarer Daten führen dazu, dass rein dokumentenbasierte oder personenabhängige Ansätze nicht mehr ausreichen. Gleichzeitig erwarten Management, Auditoren und Versicherer mehr Transparenz, Nachvollziehbarkeit und Konsistenz in der Darstellung von Risiken.

Digitalisierung im Risikomanagement bedeutet daher weit mehr als die Ablösung von Excel durch Software. Entscheidend ist die strukturierte Erfassung von Risiken, eine standardisierte Bewertung, die systematische Steuerung von Maßnahmen sowie eine durchgängige Dokumentation und Historisierung. Erst dadurch entstehen belastbare Entscheidungsgrundlagen. Digitale Risikodossiers ermöglichen es, Informationen konsistent für Management, Audit und externe Partner zu nutzen – und schaffen die Basis für eine einheitliche Risikosicht.

Die Methoden bleiben dabei unverändert wichtig. Qualitative Bewertungen, Szenarioanalysen oder quantitative Modelle entfalten ihren Nutzen jedoch erst dann vollständig, wenn sie digital integriert und kontinuierlich fortgeschrieben werden. Moderne Risikomodelle erlauben es, Risiken nicht nur zu beschreiben, sondern wirtschaftliche Entscheidungen zu unterstützen – etwa bei der Priorisierung von Maßnahmen oder bei der Abwägung zwischen Risikovermeidung und Risikotransfer.

Hier setzt der Einsatz von AI an. Künstliche Intelligenz erhöht nicht automatisch die „Intelligenz“ des Risikomanagements, aber sie verbessert Geschwindigkeit, Skalierbarkeit und Konsistenz. AI kann große Datenmengen analysieren, Muster erkennen, unstrukturierte Dokumente auswerten und Risiken automatisiert klassifizieren. Besonders relevant ist dies bei Wartungsberichten, Prüfprotokollen, technischen Dokumentationen oder Schaden- und Auditberichten. Informationen, die bisher nur mit erheblichem manuellem Aufwand ausgewertet werden konnten, werden dadurch schneller nutzbar.

Damit wird AI zu einem wichtigen Werkzeug, um aus Daten bessere Entscheidungen abzuleiten. Sie kann Zusammenhänge sichtbar machen, Entwicklungen frühzeitig erkennen und Entscheidungsprozesse beschleunigen. Gerade im industriellen Risikomanagement entsteht dadurch ein erheblicher Mehrwert: Risiken werden nicht isoliert betrachtet, sondern im Kontext von Betrieb, Technik, Organisation, Lieferkette und Versicherbarkeit bewertet.

Auch der Versicherungsmarkt verändert sich. Versicherer nutzen selbst zunehmend datengetriebene und AI-gestützte Modelle in Underwriting, Schadenmanagement und Risikobewertung. Für Unternehmen bedeutet das: Die Qualität der bereitgestellten Risikodaten wird zu einem entscheidenden Wettbewerbsfaktor. Wer Risiken strukturiert, konsistent und nachvollziehbar darstellen kann, verbessert seine Verhandlungsposition, erhöht seine Marktattraktivität und schafft eine fundierte Grundlage für wirtschaftliche Entscheidungen im Risikotransfer.

Versicherbarkeit wird damit immer stärker zu einem Ergebnis guter Risikomanagementarbeit. Sie entsteht nicht erst im Gespräch mit dem Versicherer, sondern durch die Qualität der internen Risikodaten, der Maßnahmensteuerung und der dokumentierten Entscheidungsprozesse.



Gleichzeitig entstehen durch den Einsatz von AI neue Risiken. Fehlende oder fehlerhafte Daten, algorithmische Verzerrungen, mangelnde Nachvollziehbarkeit von Entscheidungen, sogenannte „Black Box“-Effekte, sowie ungeprüfte Ergebnisse können zu erheblichen Fehlsteuerungen führen. AI-Systeme können falsche Informationen generieren, Zusammenhänge fehlerhaft interpretieren oder Empfehlungen aussprechen, die wirtschaftliche Schäden oder Haftungsfragen nach sich ziehen.

Das zentrale Risiko liegt dabei nicht in der Technologie selbst, sondern in ihrer unkontrollierten Anwendung. Werden AI-basierte Analysen unreflektiert übernommen oder ohne klare Governance in Entscheidungsprozesse integriert, entstehen neue operative, rechtliche und reputationsbezogene Risiken. Besonders kritisch wird es, wenn fehlerhafte Inhalte in interne Berichte, externe Kommunikation oder Versicherungsunterlagen einfließen.

Daraus ergibt sich eine klare Notwendigkeit: AI im Risikomanagement braucht Kontrolle. Unternehmen benötigen definierte Regeln für den Einsatz von AI, klare Datenklassifizierung, Freigabeprozesse und verpflichtende Human Review bei kritischen Entscheidungen. Transparenz, Dokumentation und Schulung der Mitarbeiter werden zu zentralen Erfolgsfaktoren.

Aktuelle Studien zeigen, dass AI im Risikomanagement längst Realität ist. Laut Moody's nutzen oder testen bereits mehr als die Hälfte der Risk- und Compliance-Professionals AI – gegenüber 30 Prozent im Jahr 2023. McKinsey berichtet, dass 88 Prozent der befragten Unternehmen AI regelmäßig in mindestens einer Geschäftsfunktion einsetzen, während fast zwei Drittel AI noch nicht unternehmensweit skaliert haben. Auch der Versicherungssektor ist betroffen: EIOPA berichtet, dass 65 Prozent der europäischen Versicherungsunternehmen Generative AI bereits aktiv einsetzen. Die Risiken sind erheblich: EY zufolge meldeten 99 Prozent der befragten Organisationen finanzielle Verluste durch AI-bezogene Risiken, 64 Prozent davon über eine Million US-Dollar. Der MIT AI Incident Tracker klassifiziert bereits mehr als 1.400 reale AI-Incidents.

Diese Zahlen zeigen: AI ist kein Zukunftsthema mehr. AI ist ein Governance-Thema der Gegenwart.

Im Ergebnis zeigt sich: Digitalisierung und AI sind keine reinen Technologieprojekte, sondern Qualitätsprojekte für bessere Entscheidungen. Sie ermöglichen es, Risiken schneller, fundierter und konsistenter zu analysieren und zu steuern. Gleichzeitig verschieben sie Verantwortung stärker in Richtung Governance, Organisation und Kontrolle.

Risikomanagement im digitalen Wandel bedeutet daher, drei Dinge konsequent zu verbinden: saubere Methoden, strukturierte Daten und verantwortungsvollen Technologieeinsatz. Gelingt diese Integration, entsteht messbarer Mehrwert – nicht nur in der Risikosteuerung selbst, sondern auch in der Art und Weise, wie Risiken im Markt wahrgenommen und bewertet werden.

Versicherbarkeit ist dabei nicht der Ausgangspunkt. Sie ist die logische Konsequenz.

„Die Zukunft des Risikomanagements liegt nicht in mehr Dokumentation, sondern in besseren Entscheidungen. Digitalisierung und AI schaffen dafür enorme Möglichkeiten – wenn sie durch klare Governance, Fachwissen und Verantwortung gesteuert werden.“

– Stephan Dorner, CEO risk on mind –V–



Fact Box: Über risk on mind GmbH

- Standort: Groß-Enzersdorf und Wien
- Geschäftsführer: Stephan Dorner
- Gründung: 2018
- Mitarbeiter: 15
- Produkte: Risikomanagement (Risk Engineering & Assessments), Versicherungsengineering®, Technische Konzepte & Lösungen, BCM, ESG, Due Diligence, Software-Lösungen rismo®
- Referenzen: ALPLA, De-Vau-Ge, RZ-Gruppe, Agrana, Mayr-Melnhof, FACC, Welser Profile, ZKW
- Absatz: weltweit

Unser Ansatz

- Risiken strukturiert erfassen und bewerten
- Maßnahmen wirtschaftlich priorisieren
- Risikodaten für Management, Audit und Versicherer nutzbar machen
- Versicherbarkeit aktiv verbessern
- Digitalisierung und AI verantwortungsvoll in Risikoprozesse integrieren

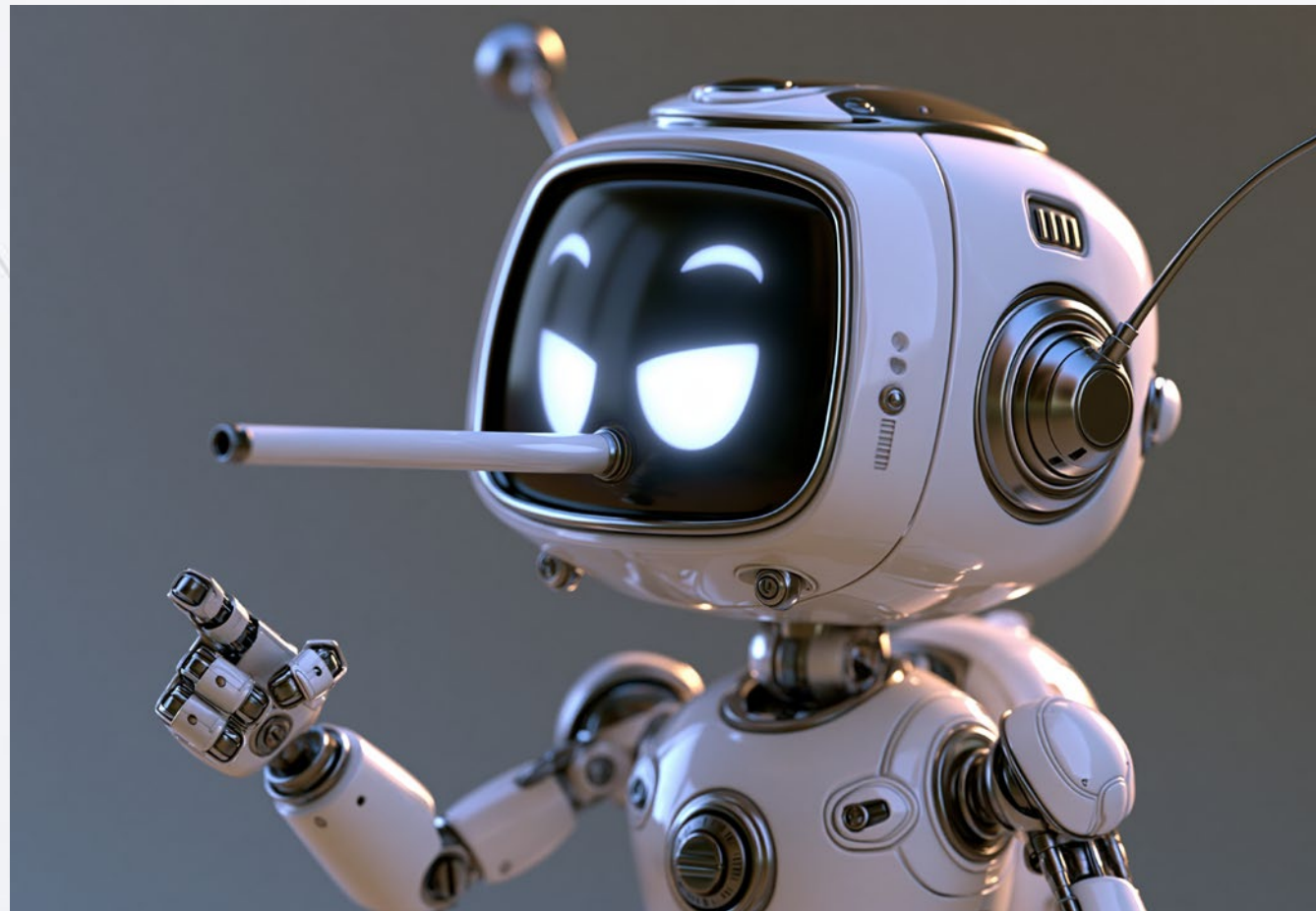
risk on mind unterstützt Unternehmen dabei, Risiken nicht nur zu dokumentieren, sondern wirtschaftlich bewertbar und entscheidungsrelevant zu machen. Der Fokus liegt auf industriellem Risikomanagement, Business Continuity Management, Brandschutz, technischen Risikoanalysen und versicherungsgetriebener Risikosteuerung.



Ontology-RAG als Baustein digitaler Resilienz

JAN PETER SCHAGEN, GANEN SETHUPATHY

Vertrauenswürdige KI für KRITIS, Cyberabwehr und öffentliche Sicherheit



Halluzinationen als zentrales Problem generativer KI

Generative KI hat sich innerhalb weniger Jahre von einer technologischen Innovation zu einem potenziell strategischen Werkzeug für Wissensmanagement, Entscheidungsunterstützung und Informationsanalyse entwickelt. Insbesondere große Sprachmodelle ermöglichen einen intuitiven Zugang zu komplexen Informationsbeständen und versprechen erhebliche Effizienzgewinne. Gerade in sicherheitskritischen Bereichen wie Cyberabwehr, Kritischen Infrastrukturen (KRITIS), Krisenmanagement oder

öffentlicher Sicherheit erscheint dieses Potenzial besonders attraktiv.

Demgegenüber steht jedoch ein grundlegendes Problem: Große Sprachmodelle verfügen nicht über ein tatsächliches Verständnis von Fakten, Organisationsstrukturen oder regulatorischen Anforderungen. Sie generieren Antworten auf Basis statistischer Wahrscheinlichkeiten und können deshalb Inhalte erzeugen, die sprachlich überzeugend, aber fachlich falsch sind. Dieses als Halluzination bezeichnete Phänomen zählt zu den größten Herausforderungen beim produktiven Einsatz generativer KI.

Während ein Halluzinationsfehler bei allgemeinen Informationsanfragen häufig lediglich zu einer Fehlinformation führt, können die Folgen in sicherheitskritischen Umgebungen wesentlich gravierender sein. Fehlinterpretierte Meldepflichten, unvollständige Risikobewertungen, falsche Handlungsempfehlungen während eines Cybervorfalles oder die fehlerhafte Einordnung regulatorischer Anforderungen können unmittelbar Auswirkungen auf Sicherheitsmaßnahmen, Compliance oder operative Entscheidungen haben.

Der produktive Einsatz generativer KI in sicherheitskritischen Domänen erfordert daher Systeme, die nicht nur sprachlich überzeugende Antworten liefern, sondern ihre Aussagen auf belastbares Wissen stützen und deren Herleitung nachvollziehbar machen können.

Warum klassisches RAG Halluzinationen nur teilweise reduziert

Um Halluzinationen zu reduzieren, hat sich in den vergangenen Jahren der Ansatz des Retrieval-Augmented Generation (RAG) etabliert. Anstatt ausschließlich auf das im Sprachmodell enthaltene Wissen zurückzugreifen, werden zusätzliche Informationen aus Dokumentenbeständen, Datenbanken oder Wissenssystemen abgerufen und dem Modell als Kontext bereitgestellt.

Dieser Ansatz stellt einen wichtigen Fortschritt dar. Das Modell kann auf aktuelle Richtlinien, Sicherheitskonzepte, technische Dokumentationen oder regulatorische Anforderungen zugreifen und seine Antworten auf konkrete Quellen stützen. Dadurch sinkt das Risiko freier Erfindungen erheblich.

Allerdings löst klassisches RAG das Halluzinationsproblem nicht vollständig. Das Modell erhält zwar zusätzliche Informationen, muss diese jedoch weiterhin interpretieren und in einen Antwortkontext einordnen. Die Qualität der Antwort hängt daher wesentlich davon ab, ob überhaupt die richtigen Dokumente gefunden wurden.

Genau hier liegen die Grenzen vieler heutiger RAG-Systeme. Die Dokumentensuche basiert häufig auf Vektorähnlichkeiten oder statistischen Repräsentationen von Texten. Das System erkennt, welche Dokumente sprachlich ähnlich erscheinen, versteht jedoch nicht notwendigerweise deren fachliche Bedeutung. Es kann deshalb zwar die richtigen Begriffe finden, aber dennoch den falschen organisatorischen oder regulatorischen Kontext berücksichtigen.

Gerade im Cyber-Security-Umfeld hängen Entscheidungen selten von einzelnen Dokumenten ab. Vielmehr entstehen sie aus komplexen Beziehungen zwischen Bedrohungen, Schwachstellen, Sicherheitsmaßnahmen, Verantwortlichkeiten, Geschäftsprozessen und regulatorischen Vorgaben. Eine reine Ähnlichkeitssuche kann solche Zusammenhänge nur eingeschränkt erfassen.

Warum Knowledge Graphs allein nicht ausreichen

Um die Grenzen dokumentenbasierter RAG-Systeme zu überwinden, werden zunehmend Knowledge Graphen (Wissensgraphen) eingesetzt. Diese ermöglichen die strukturierte Abbildung von Entitäten und Beziehungen und schaffen dadurch zusätzliche Kontextinformationen für KI-Systeme.

Knowledge Graphen stellen zweifellos einen wichtigen Fortschritt dar. Sie können beispielsweise abbilden, welche Systeme zu einer Infrastruktur gehören, welche Organisationseinheiten verantwortlich sind oder welche Komponenten miteinander verbunden sind.

Allerdings beantworten Wissensgraphen primär die Frage, welche Beziehungen existieren. Sie beantworten nur eingeschränkt die Frage, was diese Beziehungen bedeuten.

So kann ein Knowledge Graph beispielsweise erfassen, dass ein bestimmtes System zu einer kritischen Infrastruktur gehört oder dass eine Sicherheitsmaßnahme mit einem Risiko in Zusammenhang



steht. Er definiert jedoch nicht automatisch die fachliche Bedeutung dieser Begriffe, ihre Eigenschaften, Einschränkungen oder Regeln.

Genau hier liegt der entscheidende Unterschied zu Ontologien. Ontologien beschreiben nicht nur Objekte und Beziehungen, sondern spezifizieren deren Semantik. Sie legen fest, was ein Risiko ist, wann eine Maßnahme als Sicherheitskontrolle gilt, welche regulatorischen Anforderungen miteinander zusammenhängen oder welche Bedingungen erfüllt sein müssen, damit ein Vorfall als meldepflichtig eingestuft wird.

Während Knowledge Graphen primär Wissen abbilden, schaffen Ontologien ein gemeinsames Begriffs- und Regelwerk zur Interpretation dieses Wissens. Sie reduzieren Interpretationsspielräume und ermöglichen eine konsistente, organisationsübergreifende Wissensnutzung.

Ontologien als semantische Governance-Schicht

Ontologien können daher als semantische Governance-Schicht für KI-Systeme verstanden werden. Sie schaffen eine explizite Spezifikation des organisationalen Wissens und definieren, welche Konzepte in einer Domäne relevant sind und wie diese zueinander in Beziehung stehen.

Im Cyber-Security-Umfeld lassen sich beispielsweise Bedrohungen, Schwachstellen, Assets, Schutzmaßnahmen, Geschäftsprozesse, regulatorische Anforderungen und Verantwortlichkeiten in einer Ontologie spezifizieren. Gleichzeitig können fachliche Regeln und Einschränkungen explizit modelliert werden.

Dadurch entsteht eine Wissensarchitektur, die über einzelne Dokumente oder isolierte Datenbestände hinausgeht. Informationen werden nicht nur gesammelt, sondern in einen fachlichen Zusammenhang gebracht. Für KI-Systeme entsteht damit ein semantischer Kontext, der über bloße Textähnlichkeiten hinausgeht.

Ontologien schaffen somit die Grundlage für eine nachvollziehbare, konsistente und domänenspe-

zifische Wissensrepräsentation und bilden die Voraussetzung für die nächste Evolutionsstufe von RAG-Systemen.

Ontology-RAG: Die Verbindung von Sprachmodellen und Domänenwissen

Ontology-RAG erweitert klassische RAG-Architekturen um genau diese semantische Dimension. Neben Dokumenten und Wissensgraphen fließen explizite Domänenspezifikationen in den Retrieval- und Antwortprozess ein.

Bei einer Anfrage identifiziert das System zunächst die relevanten Konzepte der zugrunde liegenden Ontologie. Anschließend werden nicht nur passende Dokumente selektiert, sondern auch semantisch relevante Entitäten, Beziehungen, Regeln und Kontextinformationen berücksichtigt.

Dadurch erhält das Sprachmodell einen deutlich stärker strukturierten Wissensraum. Es verarbeitet nicht mehr lediglich Textfragmente, sondern Wissen über Risiken, Prozesse, Assets, Verantwortlichkeiten, regulatorische Vorgaben und deren Zusammenhänge.

Das Ergebnis sind Antworten, die stärker kontextualisiert, fachlich konsistenter und nachvollziehbarer ausfallen. Halluzinationsrisiken werden zwar nicht vollständig eliminiert, jedoch deutlich reduziert, da die Wissensbasis nicht mehr ausschließlich auf statistischen Ähnlichkeiten, sondern auf explizit spezifiziertem Domänenwissen beruht.

Mehrwert für Nachvollziehbarkeit, Auditierung und Compliance

Die größten Vorteile von Ontology-RAG entstehen dort, wo Nachvollziehbarkeit und Revisionssicherheit von zentraler Bedeutung sind.

Im Kontext von NIS2, KRITIS-Vorgaben, Informationssicherheitsmanagement oder Audits genügt es nicht, eine Antwort zu erhalten. Vielmehr muss nachvollziehbar sein, auf welchen Informationsquellen und welchen fachlichen Annahmen diese Antwort beruht.

Durch die Kombination aus Ontologien, Wissensgraphen und Dokumentenretrieval lassen sich Antworten auf konkrete Quellen, regulatorische Anforderungen und semantische Zusammenhänge zurückführen. Organisationen erhalten damit nicht nur Ergebnisse, sondern auch eine transparente Begründungsstruktur.

Ontology-RAG unterstützt dadurch die Auditierbarkeit von KI-Systemen und schafft eine wichtige Voraussetzung für vertrauenswürdige und governance-konforme KI-Anwendungen.

Anwendungsfälle in KRITIS, Cyberabwehr und öffentlicher Sicherheit

Besonders deutlich werden die Potenziale von Ontology-RAG in sicherheitskritischen Einsatzszenarien.

Im Bereich der Incident Response können Sicherheitsanalysten nach einem Cyberangriff unmittelbar erkennen, welche betroffenen Systeme mit welchen Geschäftsprozessen verbunden sind, welche regulatorischen Meldepflichten bestehen und welche Organisationseinheiten einzubinden sind. Statt Dokumente manuell zu durchsuchen, werden Zusammenhänge automatisch bereitgestellt.

Für KRITIS-Betreiber kann Ontology-RAG als intelligenter Wissenszugang für Sicherheitsrichtlinien, Risikoanalysen, Asset-Verzeichnisse und regulatorische Vorgaben dienen. Dadurch lassen sich Auswirkungen von Sicherheitsvorfällen schneller bewerten und Gegenmaßnahmen zielgerichteter planen.

In Sicherheitsbehörden und Lagezentren können Lageinformationen, Einsatzkonzepte, rechtliche Vorgaben und Erfahrungswissen in einem gemeinsamen semantischen Wissensraum zusammengeführt werden. Entscheidungsträger erhalten kontextbezogene Informationen über natürliche Sprache, ohne die Nachvollziehbarkeit der zugrunde liegenden Informationen zu verlieren.

Darüber hinaus eröffnet Ontology-RAG neue Möglichkeiten im Bereich des organisationalen Lernens. Frühere Vorfälle, Lessons Learned und bewährte

Vorgehensweisen können mit aktuellen Situationen verknüpft werden. Dadurch wird Erfahrungswissen nicht nur archiviert, sondern aktiv für zukünftige Entscheidungen nutzbar gemacht.

Fazit: Ontology-RAG als Grundlage vertrauenswürdiger KI

Die Diskussion über vertrauenswürdige KI wird sich künftig weniger um die Frage drehen, wie leistungsfähig Sprachmodelle sind, sondern vielmehr darum, wie belastbar ihre Wissensgrundlagen ausgestaltet werden können.

Größere Modelle allein lösen weder Halluzinationen noch Probleme der Nachvollziehbarkeit, Governance oder Compliance. Entscheidend wird vielmehr die Integration generativer KI in strukturierte Wissensarchitekturen sein.

Ontology-RAG stellt hierfür einen vielversprechenden Ansatz dar. Durch die Verbindung von Large Language Models, Dokumentenwissen, Wissensgraphen und formalen Ontologien entsteht eine Architektur, die sprachliche Flexibilität mit semantischer Präzision verbindet. Die eigentliche Innovation liegt dabei nicht im Sprachmodell selbst, sondern in der expliziten Modellierung des organisationalen Wissens.

Gerade im Umfeld von Cyber-Resilienz, NIS2, Kritischen Infrastrukturen und öffentlicher Sicherheit könnte Ontology-RAG damit zu einer Schlüsseltechnologie werden. Denn die Zukunft vertrauenswürdiger KI liegt nicht allein in immer leistungsfähigeren Modellen, sondern vor allem in besseren Wissensstrukturen. Ontologien schaffen dafür die semantische Grundlage und machen KI-Systeme nachvollziehbarer, auditierbarer und letztlich resilient gegenüber den Herausforderungen einer zunehmend komplexen digitalen Welt. -v-





Breaking the Chain: Kontrolle macht KI-Handlungen sicherer

MIKE GOERLICH

Wenn über sichere KI-Agenten gesprochen wird, geht es erstaunlich oft zuerst um das Modell. Kann es manipuliert werden? Wird der Auftrag richtig verstanden?

Das sind berechnete Fragen. Aber ein guter Prompt ist keine Sicherheitskontrolle. Sobald ein Agent nicht nur antwortet, sondern Tools auswählt und über APIs auf Systeme zugreift, beginnt das eigentliche Risiko häufig erst hinter dem Modell: dort, wo ein Aufruf reale Wirkung entfaltet.

Ein Beispiel: Ein Agent bearbeitet eine Lieferantenrechnung. Die Rechnung wird gelesen, das Lieferunternehmen mit den Stammdaten abgeglichen und die Zahlung vorbereitet. Vielleicht dürfen bei Abweichungen sogar Kontodaten aktualisiert werden. Jeder Schritt kann erlaubt und plausibel sein. Trotzdem kann am Ende Geld auf dem falschen Konto landen.

Das Risiko liegt in der Handlungskette

Agenten arbeiten selten isoliert. Sie wählen ein Tool, das über eine API eine Änderung im Zielsystem auslöst. Das Ergebnis wird zur Grundlage für den nächsten Schritt.

Das Risiko steckt nicht nur in den einzelnen Komponenten, sondern auch darin, wie sie zusammenspielen. Auftrag, Kontext, Berechtigung und mögliche Wirkung können sich an jedem Übergang verändern.

Ein Toolname beschreibt nur eine Funktion. „E-Mail senden“ kann heißen, einen Entwurf intern zu teilen oder sensible Daten nach außen zu übertragen. Das Risiko ist ein völlig anderes.

Identität ist der Anfang

Agenten brauchen verlässliche Identitäten. Sonst lässt sich kaum nachvollziehen, wer einen Vorgang

ausgelöst hat. Das gilt erst recht, wenn weitere Agenten oder Dienste beauftragt werden.

Identität allein reicht aber nicht. Zu wissen, welcher Agent handelt, sagt noch nichts darüber aus, was in diesem Moment erlaubt ist. Es ist ein Unterschied, ob eine Zahlung vorbereitet, ausgelöst oder ob Stammdaten verändert werden. Auftraggebende Stelle, Ziel, Betrag und mögliche Folgen gehören ebenfalls in die Entscheidung.

In vielen Architekturen wird der Zugriff zu früh und zu pauschal festgelegt. Ein Agent erhält ein Token für mehrere Funktionen eines Dienstes, obwohl für den konkreten Auftrag vielleicht nur eine benötigt wird. Ändern sich Auftrag, Ziel oder Kontext, kann diese Berechtigung bereits zu weit reichen.

Secure the Chain

Secure the Chain bedeutet nicht, Agenten bei jedem Schritt anzuhalten. Sie sollen ihre Aufträge erledigen können. Dafür brauchen sie den geringsten ausreichenden Kontext, um zu entscheiden, und die geringste ausreichende Berechtigung, um zu handeln.

Ändern sich Auftrag, Ziel, Kontext, Risiko oder mögliche Wirkung, muss diese Berechtigung am nächsten relevanten Übergang neu bewertet werden. Das ist der praktische Kern von Continuous Authorization: neu entscheiden, wenn sich die Grundlage der nächsten Handlung verändert hat.

APIs spielen dabei eine besondere Rolle. An ihnen wird aus dem Auftrag eines Agenten eine konkrete Handlung im realen System. Sie sind dabei Kontroll- und Durchsetzungspunkte. Je nach Architektur kann die Durchsetzung auch am Gateway stattfinden.

Entscheidend ist, dass dieselben Regeln dort greifen, wo die Handlung erfolgt.

Sehen, entscheiden, unterbrechen

Nicht jeder Kontrollpunkt ist ein Break Point. Trace Points machen den Weg einer Handlung sichtbar. Sie verbinden Auftrag, Entscheidung und Wirkung im Zielsystem. Es geht nicht um möglichst viele Logdaten, sondern darum, erkennen zu können, wer in wessen Auftrag gehandelt hat und was daraus geworden ist.

Zugriffskontrollen prüfen den Kontext und begrenzen die Berechtigung. Ein Break Point geht weiter und hält die Ausführung an, blockiert den nächsten Aufruf oder entzieht eine Berechtigung. Eine Warnung reicht nicht, wenn im Hintergrund die Zahlung bereits ausgeführt wird.

Break the Chain

Fehlt entscheidender Kontext, gehen Agenten über den jeweiligen Auftrag hinaus oder ist der nächste Schritt nicht mehr vertretbar, muss die Kette warten können. Dann wird eine Berechtigung enger gefasst, ein Token widerrufen oder ein Aufruf blockiert. Manchmal ist eine menschliche Entscheidung nötig.

Hier gilt es, die Balance zu finden. Wer Dutzende Agenten betreibt und jeden Schritt freigeben lässt, hat keine Kontrolle gebaut, sondern eine Warteschlange. Menschen werden dort gebraucht, wo eine Handlung kaum rückgängig zu machen ist oder ein Restrisiko bewusst übernommen werden soll.

Dafür braucht es verständlichen Kontext. Ein roter Warnhinweis ohne Zusammenhang hilft wenig. Die entscheidenden Personen müssen erkennen können, wer handelt, in wessen Auftrag und was

unmittelbar passieren würde. Bis die Entscheidung gefallen ist, darf der Prozess nicht weiterlaufen.

Was passiert nach dem Stopp?

Auch das Unterbrechen kann Folgen haben. In einem kritischen Prozess darf nicht vorsorglich alles zum Stillstand kommen. Ein brauchbarer Break Point begrenzt den betroffenen Teil und lässt sichere Abläufe weiterlaufen. Hier treffen Zugriffskontrolle, Resilienz und Business Continuity aufeinander.

Im eingeschränkten Betrieb dürfen Agenten vielleicht noch Informationen lesen, aber keine Änderungen mehr vornehmen. Möglicherweise übernimmt ein vorbereiteter manueller Ablauf eine wichtige Funktion.

Eine Organisation muss im Vorhinein festlegen, wer den Krisenbetrieb ausruft, wer Berechtigungen sofort entziehen darf und welche Funktionen weiterlaufen müssen. Auch für die Übernahme eines Restrisikos und den Wiederanlauf braucht es klare Zuständigkeiten.

Agenten können bereits handeln. Sicherer werden sie, wenn ihre Handlungsketten sichtbar, begrenzt und an den richtigen Stellen unterbrechbar sind.

Secure the Chain heißt, Kontext und Berechtigung vor dem nächsten Schritt zu prüfen und eng zu begrenzen. Break the Chain heißt, die Ausführung rechtzeitig anzuhalten, wenn diese Grundlage nicht mehr trägt.

Unternehmen werden nicht jedes Modellverhalten perfekt kontrollieren können. Aber sie können kontrollieren, worauf Agenten zugreifen dürfen, wie weit ihre Wirkung reicht und ob sie noch rechtzeitig eingreifen können. -v-





Wenn die Systeme laufen, aber die Gesellschaft stillsteht

EDGAR WEIPPL

Warum menschliche Urteilkraft zur kritischen Infrastruktur des KI-Zeitalters wird

Das Stromnetz ist online, die Leitwarte auch. Kein Server wurde kompromittiert. Trotzdem verliert der Betreiber die Kontrolle. Während einer regionalen Störung treffen Tausende Warnungen, Lageberichte und Lieferantenmeldungen ein. Manche sind dringend. Andere doppelt. Einige wurden gezielt erzeugt. Fast alle wirken glaubwürdig genug, dass sie geprüft werden müssen.

Dasselbe kann in einem Krankenhaus passieren oder bei einem Telekommunikationsanbieter, der mit Störungsmeldungen geflutet wird. Oder in einer Behörde, die mehr plausible Eingaben erhält, als ihre Fachleute bearbeiten können.

Das ist Denial of Service auf Layer 8 und 9: auf der menschlichen und organisatorischen Ebene. Dafür muss niemand einen Server kompromittieren, eine Datenbank verschlüsseln oder Schadsoftware einschleusen. Es reicht, glaubwürdiges Material schneller zu erzeugen, als Menschen es, selbst unter Verwendung von AI-Tools, beurteilen können.

Die neue Asymmetrie ist sehr einfach. Generative KI hat die Kosten für Texte, Code, Analysen und Berichte beinahe auf 0 gesenkt. Die Kosten des Prüfens und Entscheidens sind kaum gefallen. Mithilfe von LLMs formuliert ein:e Angreifer:in in Sekunden eine überzeugende Störungsbeschreibung, deren Validierung beispielsweise eine Netztechnikerin, eine Ärztin oder einen Security-Analysten benötigt.

Institutionen hatten lange eine unsichtbare Mengenbegrenzung. Ein ernsthaft wirkender Bericht setzte meist menschlichen Aufwand voraus. Wer Stunden in das Verfassen von Dokumenten investierte, konnte diese Zeit nicht in hundert weitere stecken. Diese Verbindung zwischen Menge und Einsatz bricht weg.

Die Gefahr ist also nicht, dass Maschinen schlechte Inhalte produzieren. Gefährlich wird es, wenn sie ausreichend gute Inhalte schneller ausstoßen, als Menschen sie prüfen können. Sie müssen nicht wahr

sein. Sie müssen nur ausreichend plausibel sein, damit die gewohnten Filter versagen.

Wir schützen Kraftwerke, Netze, Rechenzentren, Verkehrswege und Lieferketten gegen Sabotage und Unterbrechung durch technische und organisatorische Sicherheitsmechanismen, beachten dabei noch nicht Angriffe auf Layer 8 und 9. Jedes dieser Systeme hängt von Organisationen ab, die unter Druck vernünftig entscheiden müssen.

Bei kritischer Infrastruktur bleibt diese Lähmung nicht in einer Organisation. Eine Telekommunikationsstörung belastet Rettungsdienste. Ein kompromittierter Lieferant schafft Arbeit bei Dutzenden Kunden. Widersprüchliche Meldungen während eines Stromausfalls treffen Verkehr, Krankenhäuser und öffentliche Kommunikation zugleich.

Layer-8/9-Angriffe können Organisationsgrenzen überschreiten, ohne dass Schadsoftware von einem System zum nächsten wandert. Die Ansteckung ist „kognitiv“.

Eine weitere Gefahr ist, dass Fairness von offenen Prozessen gefährdet wird. Gut ausgestattete Akteure dominieren mit KI und koordinierten Kampagnen die Entscheidungskanäle fluten. Kleine Zulieferer, Gemeinden und Bürgerinnen sprechen mit einer Stimme; LLM-gestützte Verstärkung produziert Tausende plausibel wirkende Eingaben.

Was tun Institutionen heute? Oft das Naheliegende.

Sie verlangen Identifikation. Doch Identität beweist keine Aufmerksamkeit. Ein verifizierter Mensch kann Hunderte Anfragen automatisieren oder koordiniert handeln. Gleichzeitig gefährdet Identitätszwang legitime Anonymität: beim Whistleblowing, bei Sicherheitsmeldungen oder im politischen Widerspruch.

Sie setzen starre Quoten. Die lassen sich über Partner umgehen. Je höher der Druck, desto mehr wird vorsortiert. Menschen und Maschinen passen

ihre Eingaben an die Filter an. Alles klingt ähnlicher. Wichtige Signale verschwinden. Am Ende erzeugen Maschinen die Anfragen, andere priorisieren sie, und ein Mensch bleibt als Name unter der verantworteten Entscheidung.

Wir brauchen deshalb einen anderen Blick auf Sicherheit

Das Industriezeitalter lernte, Energie, Verkehr und Produktion zu schützen. Das digitale Zeitalter nahm Netze, Software und Daten hinzu. Im KI-Zeitalter gehört menschliche Urteilkraft auf diese Liste.

Mehr Rechenleistung erzeugt kein verantwortliches Urteil. Fachliche Bewertung braucht Zeit, Kontext, Erfahrung und jemanden, der für eine Entscheidung einsteht. Sind diese Ressourcen aufgebraucht, ist eine Institution nicht wirklich verfügbar.

Ein sinnvolles Sicherheitsversprechen wäre „humane Verfügbarkeit“: Ein legitimer, angenommener Vorgang erhält innerhalb vertretbarer Zeit ein Mindestmaß ernsthafter menschlicher Aufmerksamkeit.

Betreiber wesentlicher Dienste müssen ihre Aufmerksamkeitsbudgets sichtbar machen. Abgeschlossene Tickets verraten nicht, ob Fälle geprüft oder bloß entfernt wurden. Eingangslast, Prüfaufwand und Expertenstunden gehören zusammen betrachtet. Menschliche Entscheidungskapazität gehört in Risikoregister, Notfallpläne und Lieferkettenprüfungen.

Auch Reserven brauchen wir. Für Server ist Redundanz selbstverständlich, für menschliche Urteilkraft kaum. Übungen sollten testen, ob eine Organisation noch entscheiden kann, wenn glaubwürdige Informationen mit Maschinengeschwindigkeit eintreffen.

Zugangsmechanismen sollten nicht fragen: „Mensch oder Maschine?“ Sinnvoller ist: Gibt es Anzeichen ernsthafter Auseinandersetzung? Datenschutzfreundliche Nachweise könnten zeigen, dass eine berechnete Person Zeit mit einem bestimmten Gegenstand verbracht hat. Das darf keine Identität

offenlegen oder Verständnis vortäuschen. Es könnte aber die Verbindung zwischen einem Vorgang und knappem menschlichem Einsatz teilweise wiederherstellen.

Und der Schutz darf nicht selbst zur Überwachungsinfrastruktur werden. Lückenlose Verhaltensbeobachtung, biometrische Identifikation und detaillierte Aktivitätsprofile mögen eine Warteschlange absichern, beschädigen aber womöglich die Gesellschaft dahinter. Datensparsamkeit, anonyme Berechtigungsnachweise, grobe Zeitangaben, klare Löschregeln und unabhängige Kontrolle müssen von Anfang an eingebaut sein.

Die entscheidende Wahl ist am Ende keine kryptografische

Führungskräfte müssen akzeptieren, dass ein Eingabekanal weit offen sein kann, während das Verfahren dahinter längst nicht mehr zugänglich ist. Ein System, das alles annimmt und nichts mehr angemessen würdigen kann, simuliert Beteiligung.

Vorstände, Behördenleitungen und Krisenstäbe sollten unangenehme Fragen stellen: Wie viel menschliche Aufmerksamkeit verspricht dieser Dienst? Was fällt zuerst aus, wenn Urteilkraft überlastet wird? Wessen Signale unterdrücken unsere Filter? Was dürfen Maschinen vorbereiten, was müssen Menschen verantworten? Wie abhängig sind wir von einem Anbieter oder Modell?

Auch Lieferkettensicherheit muss breiter werden. Kann ein Anbieter alle nachgelagerten Organisationen mit ungeprüften Behauptungen fluten? Kognitive Last ist ein Lieferkettenrisiko. Heute steht das in kaum einem Audit.

KI aus kritischen Infrastrukturen zu verbannen wäre trotzdem die falsche Antwort. Sie kann Muster erkennen, Fachwissen übersetzen, Personal unterstützen und Institutionen zugänglicher machen. Gerade deshalb darf ihre Skalierbarkeit nicht jene Räume zerstören, in denen Belege geprüft, Alternativen abgewogen und Verantwortung übernommen werden. -v-



ZRK – Gemeinsam Zukunft sichern

Stellen Sie sich eine Welt vor, in der wir auf jede Krise vorbereitet sind: In Organisationen, Unternehmen, Städten, Gemeinden – oder in Ihrem eigenen Team. Wo Wissen nicht nur gespeichert, sondern geteilt wird. Wo Lösungen entstehen, bevor Probleme eskalieren. Genau dafür steht das Zentrum für Risiko- und Krisenmanagement (ZRK) – Österreichs führende Plattform für innovative, vernetzte und interdisziplinäre Sicherheitsarbeit.

Was ist das ZRK?

Das ZRK ist Verein, Think Tank und Kompetenzzentrum in einem. Seit seiner Gründung im Jahr 2007 bringt es Fachleute aus Wirtschaft, Wissenschaft, Verwaltung, Einsatzorganisationen und NGOs international zusammen – mit einem gemeinsamen Ziel: Risiken besser zu verstehen und Krisen souverän zu meistern.

Mit Sitz in Wien und aktiver Präsenz im gesamten D-A-CH-Raum verknüpft das ZRK Forschung, Praxis und Lehre – und bietet seinen Mitgliedern ein starkes Netzwerk für Sicherheit, Resilienz, Leadership, Strategie und Zukunftsgestaltung.

Wofür steht das ZRK?

Für Vernetzung. Wissenstransfer. Verantwortung. Ob Cybersecurity, Krisenkommunikation, Katastrophenschutz oder neue Risiken durch Digitalisierung – das ZRK erkennt Entwicklungen frühzeitig und gestaltet aktiv mit. Dabei entstehen praxisnahe Konzepte, fundierte Analysen und konkrete Handlungsstrategien.

Das Leitbild ist klar: Qualität, gesellschaftlicher Nutzen und Innovationskraft stehen im Mittelpunkt. Ziel ist nicht Theorie, sondern anwendbares Wissen – damit Sie und Ihre Organisation sicherer, belastbarer, resilienter und zukunftsfähiger werden.

Wer ist im ZRK aktiv?

Ein starkes Netzwerk aus Persönlichkeiten und Institutionen: Vom Sicherheitschef eines Konzerns über die Leiterin eines Gesundheitsamts, dem ehemaligen Präsidenten des THW bis zum Cyber-Experten im Bundesheer – sie alle verbindet eine Überzeugung: Gute Vorbereitung ist der beste Schutz.

Das ZRK wird von einem interdisziplinären Team geleitet und beraten – strategisch durch ein hochkarätiges Präsidium und einen engagierten Vorstand, operativ durch erfahrene Expert:innen für Forschung, Netzwerkentwicklung, Kommunikation und Bildung.

Was macht das ZRK konkret?

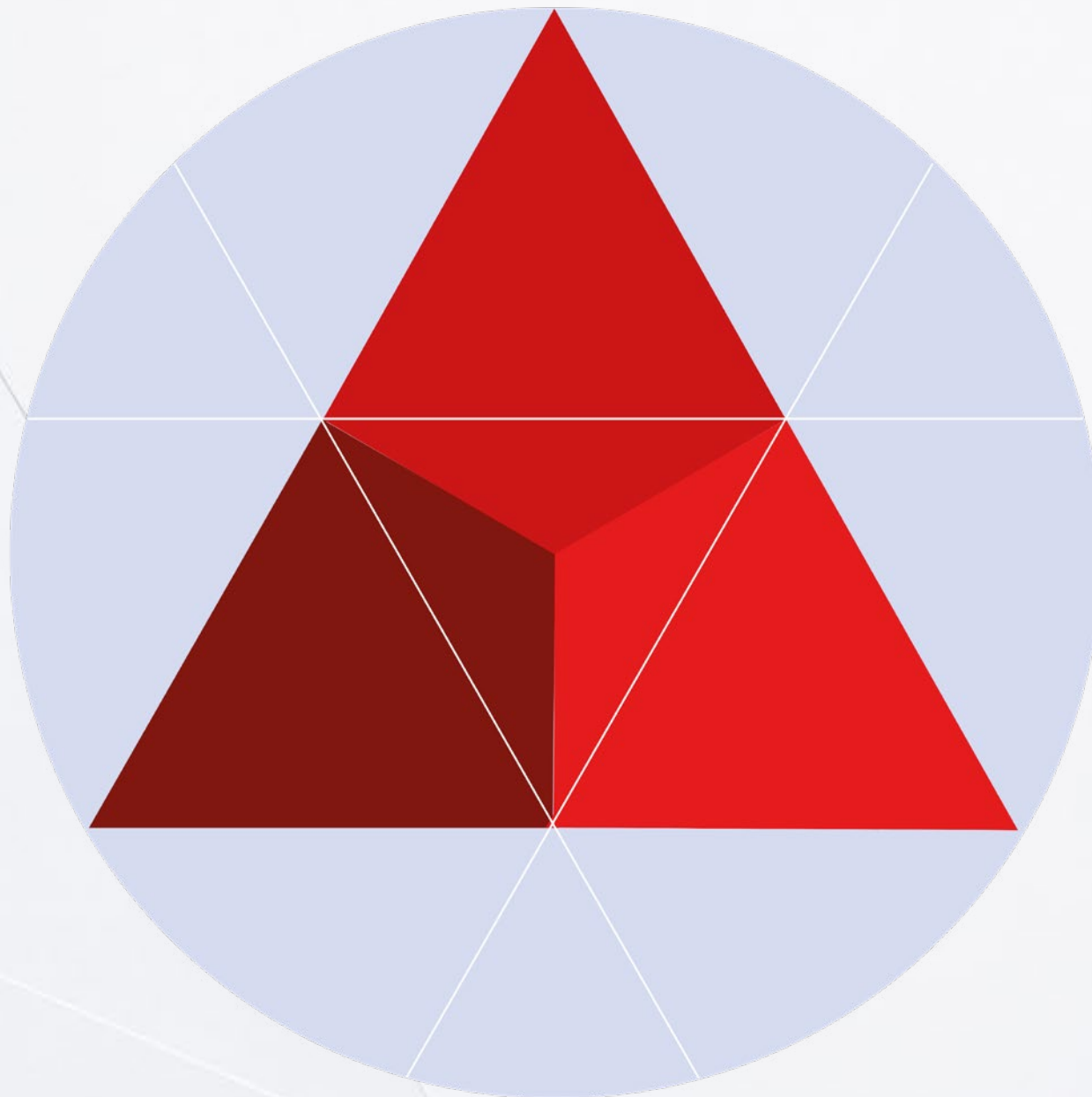
Das ZRK bietet praxisorientierte Programme, Fachpublikationen und exzellente Veranstaltungen:

- ZRK-Expert-Talks & Science-Talks: Kompakte Online- und Hybridformate zu aktuellen Themen
- Internationale Konferenzen: CYSMEC & VSSC als Plattformen für Cybersecurity, Resilienz und Space Security
- ZRK-Morgenimpulse: 60 Minuten komprimierter Wissenstransfer – ideal für Entscheidungsträger:innen (Remote)
- Magazin VANGUARD & Podcast #magic15minutes: Impulse, Analysen und Perspektiven für die Praxis

Darüber hinaus ist das ZRK in über 20 Fachbereichen und Kompetenzzentren aktiv – u. a. zu Cyber-Resilienz, Smart Cities, Wirtschaftsmediation, Gesundheitswesen und Sicherheitspolitik. Hier wird Wissen nicht nur vermittelt, sondern konkret angewendet.

Warum jetzt Mitglied werden?

Weil Sicherheit kein Zufall ist – sondern das Ergebnis von Kompetenz, Austausch und Weitblick.





Als Mitglied im ZRK profitieren Sie von:

- Exklusivem Zugang zu Veranstaltungen, Studien & Weiterbildungen
- Austausch auf höchstem fachlichem Niveau
- Mitgestaltung nationaler und internationaler Sicherheitsstrategien
- Sichtbarkeit im größten Sicherheitsnetzwerk Österreichs
- Praxisnahe Unterstützung für Ihre Organisation

Ob Einzelperson oder Institution – Ihre Stimmen zählen. Ihre Erfahrungen stärken unser Netzwerk.

Für wen ist das ZRK ideal?

- IT- & Cybersecurity-Expert:innen
- Führungskräfte in Unternehmen & öffentlicher Verwaltung
- Einsatzkräfte, NGO-Vertreter:innen & Berater:innen
- Wissenschaftler:innen & Studierende im Sicherheitskontext
- Organisationen mit kritischer Infrastruktur

Wie werde ich Mitglied?

Einfach diesen QR-Code scannen, den Antrag online ausfüllen – und Teil einer Bewegung werden, die Sicherheit neu denkt.

Sichern Sie sich den Wissensvorsprung – gestalten Sie mit uns die resiliente Zukunft. Willkommen im ZRK! -v-



EU-Maßnahmen für digitale Souveränität

HEINZ STIASTNY

Die im Juni 2026 vorgestellten Maßnahmen sollen Europa resilienter und unabhängiger machen

Die kritische Infrastruktur Europas – ob Krankenhäuser oder die Stabilität der Energienetze – hat einen Abhängigkeitsgrad von außereuropäischen Technologieanbietern erreicht, der ein existenzielles Risiko darstellt. Die Europäische Kommission hat deshalb ein Paket zur technologischen Souveränität Europas mit umfassenden Regulierungsvorhaben vorgestellt, um a) die Abhängigkeiten Europas zu reduzieren und b) die digitale Resilienz des Kontinents zu stärken. Europa kann es sich auf Dauer nicht leisten, besonders bei kritischen Infrastrukturen abhängig zu sein.

Europa hat Talente, Exzellenz in der Forschung, eine starke industrielle Basis und einen ausgeprägten Binnenmarkt – diese Stärken gilt es gemeinsam in technologische Souveränität umzuwandeln.

Die steigende Nachfrage nach Rechenzentrumskapazitäten im Zuge des KI-Booms verschärft das Problem. Obwohl es seit 2023 ein Chip-Gesetz auf europäischer Ebene gibt, bleibt Europa insbesondere bei fortschrittlichen Produktionsanlagen, aber auch beim Chip-Entwurf an sich, stark von Drittländern außerhalb der Europäischen Union abhängig. Ziel ist es, auch hier eine umfassende „digitale Autonomie“ auf allen Ebenen zu etablieren. Der Bogen spannt sich vom physischen Siliziumchip bis zur darüberlaufenden Softwarearchitektur.

Was sind nun die beschlossenen vier Säulen des Souveränitätspakets? Das Paket ist kein einzelnes Gesetz, sondern ein Bündel verknüpfter Maßnahmen, die diese vier Hauptbereiche adressieren.

Chips und Hardware

Die Chipverordnung 2.0 ist eine direkte Antwort auf die zunehmend kritischen Schwachstellen in den globalen Lieferketten. Während das erste Chip-Gesetz (1.0) die Fertigungswerke stärkte, zielt nun die Nachfolgeregelung darauf ab, die europäische Wertschöpfungskette für Chips umfassend zu

sichern und strukturelle Engpässe bei Kernkomponenten zu minimieren.

Aufbau der Cloud- und KI-Kapazitäten in Europa

Im Bereich KI sollen nicht nur technologische Kapazitäten aufgebaut, sondern die Entwicklung soll auch reguliert werden. Die Regelung zur Cloud- und KI-Entwicklung soll einen europäischen Rahmen schaffen, der Transparenz sichert und sicherstellt, dass kritische Anwendungen – besonders im Gesundheitswesen und in der Energieversorgung – künftigen europäischen Standards entsprechen. Ziel ist es, die Kapazitäten der Rechenzentren in Europa in den nächsten fünf bis sieben Jahren zu verdreifachen. Die Regelung soll die Forschung im Bereich moderner und nachhaltiger Technologien unterstützen und gleichzeitig ein Gleichgewicht zwischen den KI-Zielen und den Klimaschutzverpflichtungen herstellen, wobei der Großteil des EU-Marktes für gleichgesinnte Partner offen bleiben soll. Dies soll dazu beitragen, kritische Anwendungen und sensible Daten zu schützen und die Entwicklung moderner Cloud- und KI-Technologien zu unterstützen. Weiters soll dadurch ein besser koordiniertes, EU-weites Vorgehen bei der KI-Einführung in den einzelnen Mitgliedsstaaten erreicht werden – unter anderem durch die Erfassung von KI-Erfahrungen sowie durch neue Beschleunigungszentren zur Unterstützung der KI-Integration.

Stärkung der digitalen Autonomie durch Open Source

Derzeit tragen in Europa mehr als drei Millionen Menschen zu Open-Source-Lösungen bei. Die Open-Source-Strategie baut auf diese Stärke auf, um souveräne Lösungen nachhaltig zu entwickeln. Mit ihr werden quelloffene Alternativen etwa in den Bereichen Cloud, KI, Internettechnik, Cybersicherheit und Halbleiterproduktion ausgebaut. Weiters sollen ein stärkeres



Open-Source-Ökosystem gefördert und quelloffene Start-up-Unternehmen unterstützt werden.

Zudem soll die stärkere Nutzung quelloffener Lösungen in der öffentlichen Verwaltung durch Leitlinien für Auftragsvergaben und bewährte Verfahren in der Praxis vorangetrieben werden. Sie soll die Übernahme europäischer Lösungen fördern und Normung sowie Interoperabilität unterstützen, auch durch die Initiative „Open Internet Stack“.

Digitalisierung des europäischen Energiesystems

Ein weiterer kritischer Engpass betrifft die Rechenleistung selbst. Hohe Energiepreise belasten die Wettbewerbsfähigkeit der europäischen Industrie und schmälern gleichzeitig die Kaufkraft der Haushalte.

Gleichzeitig wird das Wachstum der digitalen Infrastrukturen in Europa die Stromnachfrage erheblich steigern. Durch die Regelung sollen energieeffiziente Rechenzentren auf nachhaltige und transparente Weise in das europäische Energiesystem integriert und eine nachhaltige Basis für die gesamte digitale Expansion geschaffen werden. Damit positioniert

sich Europa von einem rein regulierenden Akteur hin zu einem aktiven Gestalter seiner digitalen Zukunft. Durch die Verknüpfung von Gesetzgebung, Infrastrukturstrategie und Open-Source-Förderung versucht die Europäische Kommission, eine europaweite Wertschöpfungskette zu etablieren, deren Resilienz nicht von globalen geopolitischen Spannungen oder Abhängigkeiten kritischer Drittstaaten bedroht wird. Die Umsetzung dieser komplexen Strategie erfordert jedoch massive Investitionen und eine Koordination über alle Mitgliedsstaaten hinweg.

Zu all diesen strategischen Ansätzen sind bereits eine Vielzahl europäischer Unternehmen beteiligt – zuletzt sei noch auf das im Hub der AI Factory Austria (AI:AT) verankerte österreichische KI-Unternehmen Eustella hingewiesen. Eustella ist eine europäische Plattform für KI-Agenten, die laut ihrem Entwickler komplexe, mehrstufige Arbeitsabläufe eigenständig unterstützen soll – etwa bei Recherchen, Präsentationen, Medienproduktionen, Reise- und Lifestyle-Projekten, aber auch bei wissensintensiven Workflows.

Klar ist: Der Weg Europas in die digitale Unabhängigkeit wird nicht leicht, nichts kann über Nacht erreicht werden – aber die ersten wichtigen Schritte sind nun gesetzt. -v-

Souveränität duldet keine Rückkopplung

HEIKO FRIEDRICH

Warum der österreichische Sicherheitsraum mehr braucht als lokale Datenhaltung

Österreich will seine digitale Souveränität stärken. Der politische Anspruch ist formuliert, die strategischen Leitplanken stehen. Mit dem Digitalen Aktionsplan, den definierten Handlungsbereichen zur digitalen Souveränität und dem Digital Austria Act 2.0 hat die Republik ein klares Signal gesetzt: Digitale Abhängigkeiten sollen sichtbar gemacht, bewertet und dort reduziert oder vermieden werden, wo sie selbstbestimmtes Handeln, Resilienz und Sicherheit beeinträchtigen.

Doch ausgerechnet an jener Stelle, an der digitale Kontrolle operativ wirksam wird, bleibt dieser Anspruch in vielen Organisationen unvollendet: bei der Steuerung von Endgeräten. Hier werden administrative Zugriffsrechte vergeben, Sicherheitsrichtlinien technisch durchgesetzt und oftmals tausende Geräte zentral gesteuert.

Lokale Datenhaltung ist nur der Anfang

Der Widerspruch wird deutlich, wenn man den Blick auf die heutige IT-Praxis richtet. Daten werden mit großem Aufwand in österreichischen oder europäischen Rechenzentren verortet. Compliance-Programme, Zero-Trust-Modelle und Sicherheitsrichtlinien werden sorgfältig dokumentiert. Gleichzeitig erfolgt die operative Steuerung von Endgeräten in vielen Fällen über internationale SaaS-Plattformen, deren rechtlicher und technischer Kontrollraum außerhalb der eigenen Jurisdiktion liegt.

Das schafft eine trügerische Sicherheit. Für digitale Souveränität ist nicht allein entscheidend, wo Daten gespeichert werden, sondern wer Konfigurationen ändern, Richtlinien ausrollen, Geräte sperren, kryptographische Schlüssel verwalten und administrative Zugriffe kontrollieren kann.

Genau diese zentralen Steuerungsfunktionen werden im Unified Endpoint Management gebündelt. Damit ist UEM weit mehr als ein Werkzeug zur Gerätever-

waltung. Auf dieser Ebene werden Sicherheitsvorgaben technisch umgesetzt, Zugriffsrechte durchgesetzt, Endgeräte mit Identitäts- und Sicherheitsstrukturen verknüpft, Patch-Zyklen gesteuert und Compliance-Anforderungen in den laufenden Betrieb übersetzt. Die Kontrolle über diese Steuerungsebene ist deshalb unmittelbar mit der Handlungsfähigkeit einer Organisation verbunden und gerade dann relevant, wenn digitale Prozesse unter erhöhtem Druck stabil und beherrschbar bleiben müssen.

Wo Resilienz operativ entschieden wird

Für öffentliche Verwaltung, Landesverteidigung, Betreiber kritischer Einrichtungen und regulierte Branchen in Österreich ist diese Frage weder theoretisch noch rein technischer Natur. Mit NISG 2026, DORA und RKEG sowie den Anforderungen aus DSGVO und DSG gewinnen tatsächliche Steuerbarkeit, nachvollziehbare Verantwortlichkeiten, belastbare Risikokontrollen und operative Resilienz weiter an Bedeutung. Wer Informations- und Kommunikationsrisiken wirksam begrenzen will, benötigt deshalb Architekturen, in denen administrative Zugriffe kontrolliert, Rollen sauber getrennt, Aktivitäten revisionsfähig protokolliert und Drittparteirisiken beherrscht werden.

Liegen wesentliche Steuerungsfunktionen außerhalb des eigenen Rechts- und Kontrollraums, entsteht ein strukturelles Abhängigkeitsrisiko. Dieses kann sich in extraterritorialen Rechtszugriffen, konzernrechtlichen Bindungen, begrenzten Support- und Eskalationswegen oder geopolitischen Entwicklungen ergeben, die plötzlich operative Folgen entfalten. Unter Krisenbedingungen zählt dann nicht allein, was im Architekturpapier dokumentiert ist, sondern ob eine Organisation ihre digitale Umgebung eigenständig absichern, steuern und aufrechterhalten kann.

Entscheidend ist daher nicht nur die Leistungsfähigkeit eines UEM, sondern auch sein Betriebsmodell.





Dieses muss Kontrolle, Nachweisfähigkeit und Krisenfestigkeit gewährleisten. Ein souverän gestaltetes UEM schafft dafür die Voraussetzungen durch klare Datenhoheit, eine nachvollziehbare Trennung von Rollen und Verantwortlichkeiten sowie eine Architektur, in der die Steuerungsebene nicht dauerhaft an Herstellerzugriffe oder intransparente technische Rückkanäle gekoppelt ist. Souveränität wird damit von einer politischen Zielsetzung zu einer überprüfbaren Eigenschaft der digitalen Betriebsarchitektur.

Woran sich souveränes Endgeräte-Management bemisst

Ob ein UEM tatsächlich souverän betrieben werden kann, ist in erster Linie in der Architektur seines Betriebsmodells verankert. Konkret lässt sich das an drei Anforderungen festmachen, die Datenhoheit, technische Kontrolle und strategische Unabhängigkeit miteinander verbinden.

Erstens erfordert ein souveränes UEM vollständige Transparenz darüber, welche Telemetrie-, Protokoll- und Konfigurationsdaten anfallen, wo sie verarbeitet werden und welche Stellen darauf zugreifen können.

Zweitens setzt es voraus, dass administrative Eingriffe technisch hart abgesichert sind, etwa durch starke Authentifizierung, granulare Rollenmodelle, nachvollziehbare Protokollierung und eine möglichst weitgehende kryptographische Schlüsselhoheit auf Seiten des Nutzers.

Drittens braucht es eine Entkopplung vom Hersteller dort, wo sie strategisch relevant ist, insbesondere wenn dieser nicht aus dem Land oder der Region stammt. Gemeint ist eine Architektur, in der zentrale Steuerungsfunktionen weder von Fernzugriffen des Herstellers abhängen noch voraussetzen, dass externe Stellen Einsicht in produktive Daten erhalten, um den Betrieb aufrechtzuerhalten.

Souveränität sichert Handlungsfähigkeit

Damit ist weder Abschottung noch technologische Autarkie gemeint. Im Kern geht es um digitale

Handlungsfähigkeit: also um die Fähigkeit, auch in einer vernetzten und von Abhängigkeiten geprägten Umgebung souverän und sicher zu handeln. Dazu gehört, zwischen eigenen Lösungen und den Angeboten vertrauenswürdiger Partner frei und verantwortungsbewusst wählen zu können. Genau diesem Verständnis folgt auch der Digitale Aktionsplan Austria im Kapitel „Digitale Souveränität für Österreich“: Nicht der Verzicht auf internationale Technologie steht im Vordergrund, sondern die systematische Bewertung von Abhängigkeiten, die Sicherung von Handlungsoptionen und die Hoheit über jene Kompetenzen, die für Sicherheit, Resilienz und Betrieb im eigenen Verantwortungsbereich notwendig sind.

Betroffen sind alle Sektoren, in denen digitale Infrastrukturen, sensible Daten, kritische Prozesse und regulatorische Anforderungen zusammenkommen. Für sie ist Endgeräte-Management kein peripheres IT-Thema, sondern Teil der operativen Sicherheitsarchitektur. An seiner Ausgestaltung entscheidet sich, ob Sicherheitsvorgaben, administrative Zugriffe und digitale Abhängigkeiten tatsächlich unter eigener Kontrolle bleiben.

Und darin liegt die eigentliche Pointe: Weder „EU-Hosting“ noch „AT-Hosting“ machen eine Infrastruktur für sich genommen souverän. Souverän ist eine Architektur erst dann, wenn ihre zentrale Steuerungsebene unter eigener rechtlicher, technischer und organisatorischer Kontrolle steht. Alles andere ist gut gemeinte Compliance. Aber noch keine belastbare Souveränität. -v-

Quellen

Digitaler Aktionsplan Austria: <https://www.digitalaustria.gv.at/verwaltung/strategien/digitaler-aktionsplan.html>

Digitaler Souveränitätskompass, S. 12: https://www.digitalaustria.gv.at/dam/jcr:8a8a4469-0945-444f-8083-566feb44fdd9/2023_11_27_KommPaper_DAA_Sicherheit_Souveraenitaet%20AT.pdf

Digital Austria Act 2.0: https://www.bundeskanzleramt.gv.at/dam/jcr:25e542d4-887a-44f9-8076-63a6e524e83b/30_13_mrv.pdf

Handlungsbereiche Digitale Souveränität: <https://www.digitalaustria.gv.at/dam/jcr:24aa98c6-f9c7-45c7-8f8e-daf534513b5c/Handlungsbereiche%20Digitale%20Souver%C3%A4nit%C3%A4t.pdf>





Wenn niemand mehr eingreift

ROBERT-P. PELIKAN



Am 6. Mai 2010 verlor der Dow Jones Industrial Average innerhalb weniger Minuten fast 1.000 Punkte, rund neun Prozent seines Werts, und vernichtete kurzzeitig rechnerisch etwa eine Billion Dollar an Marktwert. Ausgelöst wurde der sogenannte "Flash Crash" durch einen einzelnen automatisierten Verkaufsauftrag über 75.000 E-Mini-Kontrakte im Wert von rund 4,1 Milliarden Dollar, den ein Algorithmus ohne Rücksicht auf Preis oder Zeitpunkt in den Markt drückte. Andere automatisierte Handelssysteme reagierten in Sekundenbruchteilen darauf, verstärkten die Verkaufswelle, und binnen Minuten brach der Markt ein. Erst rund zwanzig Minuten später erholte er sich wieder fast vollständig. Menschliche Händler saßen währenddessen vor ihren Bildschirmen und sahen zu. Eingreifen konnte in dieser Zeitspanne niemand - die Systeme agierten schneller, als ein Mensch überhaupt erfassen konnte, was gerade geschah.

Diese Geschichte wird in Risikomanagement-Kreisen meist als Warnung vor fragmentierten Märkten und Hochfrequenzhandel erzählt. Das greift zu kurz. Der eigentliche Kern ist ein anderer: Organisationen bauen zunehmend Systeme, die schneller handeln, als Menschen sie überwachen können, und verlassen sich gleichzeitig darauf, dass im Ernstfall ein Mensch eingreift. Diese Kombination ist eine strukturelle Zeitbombe, und sie betrifft längst nicht mehr nur den Börsenhandel. Sie betrifft jede Organisation, die KI-gestützte Systeme in Entscheidungsprozesse mit echtem Zeitdruck einbaut: automatisierte Fraud-Detection, KI-gestützte Netzwerküberwachung, algorithmische Lieferkettensteuerung, Frühwarnsysteme im Krisenmanagement.

Die zwei Fehler, die sich gegenseitig verstärken

Der erste Fehler ist eine Illusion von Kontrolle. Viele Organisationen implementieren KI-Systeme mit der beruhigenden Formel "der Mensch bleibt in der Schleife". In der Praxis bedeutet das oft: Ein Mitarbeiter sitzt vor einem Dashboard und soll im Zweifel eingreifen. Doch wenn ein System in Sekunden Entscheidungen trifft, die sich in Minuten kumulieren,

ist diese menschliche Aufsicht eine Fiktion. Niemand kann eine Entscheidungskette sinnvoll unterbrechen, deren Geschwindigkeit für menschliche Reaktionszeiten nicht ausgelegt ist. Das Problem ist nicht die Kompetenz der Aufsichtsperson, sondern die Architektur: Wer Eskalationsschwellen, Not-Aus-Mechanismen und Interventionsfenster nicht von Anfang an technisch mitdenkt, hat de facto keine menschliche Kontrolle eingebaut, sondern nur ein Feigenblatt dafür.

Der zweite Fehler ist subtiler und wurde in der Luftfahrt lange vor dem KI-Zeitalter beschrieben: der Verlust manueller Fähigkeiten durch Automatisierungsgewöhnung, im Fachjargon "skill fade" genannt. Der Absturz von Air France 447 im Jahr 2009 ist dafür das bekannteste Beispiel. Als die Geschwindigkeitssensoren wegen Vereisung ausfielen und sich der Autopilot abschaltete, übernahmen die Piloten manuell - und reagierten mit einer Steuerbewegung, die einen Strömungsabriss verursachte, statt ihn zu beheben. Die Untersuchung zeigte: Jahre der Automatisierungsgewöhnung hatten die Routine im Umgang mit genau jenen Grenzsituationen erodieren lassen, für die menschliches Eingreifen eigentlich vorgesehen war. Das Paradoxe daran: Je zuverlässiger ein automatisiertes System im Normalbetrieb funktioniert, desto seltener trainiert der Mensch daneben genau jene Fähigkeit, die im Ausnahmefall gebraucht wird.

Für Führungskräfte, die heute KI-Systeme in Sicherheits-, Risiko- oder Entscheidungsprozesse integrieren, ergibt sich daraus eine unbequeme Konsequenz. Es reicht nicht, ein System zu bauen und einen Menschen "zur Sicherheit" danebenzusetzen. Wer Resilienz ernst meint, muss zwei Dinge parallel sicherstellen: erstens eine Systemarchitektur, die menschliches Eingreifen technisch tatsächlich ermöglicht, mit klar definierten Zeitfenstern, Schwellenwerten und Abschaltmechanismen, die zur tatsächlichen Reaktionsgeschwindigkeit des Menschen passen. Zweitens eine bewusste Praxis, mit der genau jene Fähigkeiten trainiert werden, die im Normalbetrieb durch Automatisierung überflüssig erscheinen. Piloten üben deshalb regelmäßig im Simulator

Ausnahmesituationen, obwohl der Autopilot 99 Prozent der Flugzeit übernimmt. Organisationen, die KI-gestützte Entscheidungsprozesse einführen, brauchen ein Äquivalent dazu: regelmäßige, bewusst inszenierte Situationen, in denen Menschen ohne das System entscheiden müssen, damit die Fähigkeit dazu im Ernstfall noch vorhanden ist.

Verantwortung darf nicht im System verschwinden

Damit verbunden ist eine zweite, oft übersehene Verschiebung: die Diffusion von Verantwortung. Wenn eine Entscheidung von einem KI-System vorgeschlagen oder getroffen wurde, entsteht in Organisationen leicht eine implizite Entlastung - "das System hat es so berechnet" wird zur Rechtfertigung, ohne dass jemand die Berechnung tatsächlich geprüft hätte. Genau das war auch beim Flash Crash ein Teil des Problems: Die beteiligten Handelsalgorithmen folgten jeweils für sich genommen plausiblen, korrekt programmierten Regeln. Niemand hatte in Echtzeit die Befugnis oder die Werkzeuge, das Zusammenspiel dieser Regeln zu hinterfragen, bevor sich die Verkaufswelle selbst verstärkte. Führung im KI-Zeitalter bedeutet deshalb auch, explizit festzulegen, wer für eine KI-gestützte Entscheidung haftet und rechenschaftspflichtig bleibt - nicht als Formalie im Compliance-Dokument, sondern als gelebte Praxis, die regelmäßig getestet wird, bevor der Ernstfall sie testet.

Resilienz entsteht nicht dadurch, dass man ein System für ausfallsicher erklärt. Sie entsteht dadurch, dass man ehrlich zugibt, wo die Grenzen menschlicher Reaktionsfähigkeit liegen, und die Architektur genau darauf ausrichtet, statt sich auf eine Aufsicht zu verlassen, die im entscheidenden Moment gar nicht mehr eingreifen kann. -v-





Wenn der Gegner in der eigenen Cloud sitzt

RICHARD WERNER



Souveränität bedeutet, selbst entscheiden zu können, ohne von anderen abhängig zu sein. Wer diesen Anspruch erhebt, braucht eigene Handlungsfähigkeit, politisch wie technologisch. Und genau hier wird es unbequem, denn im digitalen Raum gibt es keine Grenzen, die man ziehen könnte: Es gibt Verträge, Rechtsräume und Vertrauensketten. Eine aktuelle Untersuchung staatsnaher Cyberangriffe (Advanced Persistent Threats, APTs) durch die Sicherheitsexperten von TrendAI zeigt, dass diese Akteure solche Vertrauensketten inzwischen als bevorzugten Angriffsweg nutzen. Damit wird digitale Souveränität von einem Compliance-Thema zur Frage der Verteidigungsfähigkeit.

Der Angriff kommt nicht durch die Mauer, sondern durch das Vertrauen

Eine zentrale Erkenntnis des Berichts: Staatsnahe Cyberakteure verstecken ihre Steuerungsinfrastruktur bevorzugt in Diensten, die Behörden ohnehin nutzen, wie Cloud-Plattformen und Entwicklerwerkzeuge. Eine China-nahe Gruppe steuerte ihre Schadsoftware ausschließlich über E-Mail-Entwürfe, die nie versendet wurden. Die Angreifer suchen also nicht mehr die Lücke im Zaun, sondern nutzen das Tor, das offen bleiben muss. Denn wer den Verkehr zur Office-Cloud blockiert, blockiert die eigene Verwaltung.

Vom Perimeter zur Entscheidungsfähigkeit

Damit verschiebt sich die Cyber-Verteidigung von der Frage „Wohin verbindet sich das?“ zu „Was passiert hier gerade?“. Diese zweite Frage kann nur beantworten, wer die eigenen Sicherheitsdaten sieht, versteht und behält. Sicherheitstelemetrie ist kein technischer Datenberg. Sie enthält Organisationsstrukturen, Zuständigkeiten, Nutzerverhalten und Netzabbildungen. Für eine Behörde ist sie ein Lagebild über sich selbst. Wer dieses Lagebild außerhalb des eigenen Rechtsraums verarbeiten lässt, gibt einen Teil seiner Entscheidungsfähigkeit ab, ohne dass es dafür einen Angriff braucht.

Abhängigkeit ist eine Verwundbarkeit, auch ohne Angriff

Ein zweites Muster: Angreifer setzen dort an, wo Vertrauen konzentriert ist. Ein einziges kompromittiertes Entwicklerkonto reichte für nordkoreanische Akteure schon aus, um über ein weltweit verbreitetes Software-Paket Organisationen in 21 Ländern zu erreichen.

Somit ist jede zentrale Plattform auf ihre möglichen Risiken hin zu betrachten. Das umfasst auch die Sicherheitsplattform selbst, denn sie hat die tiefsten Rechte im Netz. Souveränität ist deshalb Teil der Schutzwirkung: Sie umfasst die Frage, was passiert, wenn ein Dienst ausfällt, ein Rechtsstreit eskaliert oder eine Lizenz nicht mehr verfügbar ist. Wer diesen Fall nie durchgespielt hat, hat keinen Plan, sondern eine Hoffnung.

KI verschiebt die Zeitverhältnisse – und damit die Machtverhältnisse

Im ersten Halbjahr 2026 dokumentierten die Experten erstmals, dass ein Angreifer einen KI-Agenten überredete, selbstständig in einem fremden Netzwerk zu arbeiten: aufklären, Zugangsdaten sammeln, weiterkommen – nicht als Experiment, sondern in einer laufenden Operation. Eine Cyberverteidigung, die in Ticketlaufzeiten gemessen wird, verliert zwangsläufig gegen einen Gegner, der in Maschinenzeit arbeitet.

Gleichzeitig behandeln alle beobachteten Akteure KI-Fähigkeit als strategisches Gut: China treibt Autarkie bei Chips und Modellen voran, Russland treibt das Thema als staatliche Initiative voran, Nordkorea leiht sich fremde Modelle, weil Sanktionen eigene verhindern. Wenn Rechenleistung auf der Gegenseite eine Staatsangelegenheit ist, sollte die Frage auf unserer Seite nicht dem Einkauf überlassen werden: Wo läuft das Modell, mit welchen Daten, unter welcher Rechtsordnung?

Souveränität ist kein Autarkieprojekt

Ein wichtiges Missverständnis gehört dabei ausge-

räumt: Souveränität bedeutet nicht Abschottung. In der heutigen vernetzten Welt kann sich das praktisch kein Land leisten. Souveränität heißt vielmehr, selbstbestimmt entscheiden zu können, was man selbst macht, was man abgibt und welche Daten wohin fließen.

Dafür gibt es tragfähige Cybersecurity-Betriebsmodelle: Werden moderne Sicherheitsplattformen innerhalb der selbst gewählten Souveränitätsgrenze ausgerollt, bleiben die Daten im eigenen Verantwortungsbereich, ohne Abhängigkeit von einer herstellerseitig betriebenen Infrastruktur. Bereitgestellt werden kann das bei einem nationalen Cloud-Anbieter, im eigenen Rechenzentrum oder auch vollständig „air-gapped“ für die sensibelsten Bereiche.

Vier Fragen, die Cybersecurity-Verantwortliche klären sollten:

- Souveränitätsgrenze definieren: Welche Daten, Metadaten und Schlüssel dürfen den eigenen Rechtsraum verlassen – und welche unter keinen Umständen?
- Souveränität als Bewertungskriterium verankern, nicht als Anhang zur Compliance-Prüfung. Was nicht gewichtet wird, wird wegverhandelt.
- Den Ausfall üben: Handlungsfähigkeit bei Störung, Abschaltung oder Rechtskonflikt gehört in Übungen, nicht in Präsentationen.
- KI-Governance: Wer KI zur Verteidigung einsetzt, muss wissen, wo sie rechnet und wer im Haus schon welche KI-Werkzeuge nutzt.

Fazit

Cyberakteure haben verstanden, dass Vertrauen die effizienteste Angriffsfläche ist. Sie nutzen unsere Cloud-Dienste, unsere Lieferketten, unsere Updates und inzwischen unsere KI-Werkzeuge. Wer darauf mit Compliance-Nachweisen antwortet, verwaltet ein Risiko, statt es zu senken. Für einen neutralen Staat ist digitale Souveränität kein Prestigethema, sondern die Voraussetzung, im Ernstfall selbst zu entscheiden und selbst zu handeln. -v-



APT-Bedrohungslage · 1. Halbjahr 2026

GEORG LANZINGER

Wie staatliche Angreifer im Zeitalter der KI

unser Vertrauen zur Waffe machen



Regierungsnahe Angreifer feilten im ersten Halbjahr 2026 spürbar an ihren Methoden. Künstliche Intelligenz dringt tief in sämtliche Phasen der Attacken ein – sie veredelt Schadcode, beschleunigt das Auskundschaften von Zielsystemen und steuert eigenständige Software-Einheiten durch fremde Netzwerke. Wer die Schritte von Gruppen mit Drahtziehern in China, Russland, Nordkorea oder dem Iran analysiert, erkennt rasch den Stempel regionaler Machtpolitik auf Zielen sowie Vorgehensweisen. Sämtliche dieser Cyber-Netzwerke arbeiten heutzutage deutlich professioneller.

Schwachstellen gerieten blitzschnell ins Visier, während Angriffe über Zulieferer hoch im Kurs blieben. Kriminelle verlagerten ihre Befehlszentralen vermehrt in vertrauenswürdige Werkzeuge: bekannte Cloud-Speicher, Entwickler-Zugänge, verknüpfte Datenbanksysteme oder Online-Textspeicher. Böartige Signale verschmelzen mit dem alltäglichen Datenstrom in Firmenbüros und entziehen sich der Löschung. Selbst greifbare Technik rückte ins Blickfeld – manipuliertes Messgerät an Kraftstofftanks zeugte davon ebenso wie das Tracken von Standortdaten über digitale Werbenetzwerke ganz ohne Schadsoftware: dem Tracking über Werbedaten, kurz ADINT.

KI-Ambitionen und ihre Grenzen in den großen Bedrohungs-ökosystemen

Vier Lager, vier sehr unterschiedliche Strategien: So gehen die großen staatsnahen Ökosysteme derzeit mit künstlicher Intelligenz um.

China – „Der Skalierer im Staatsauftrag“

China-nahe Gruppen setzten KI in diesem Halbjahr an fast jeder Station der Angriffskette ein. Earth Krahang machte mit generativer KI aus einem öffentlichen Exploit einen Scanner für den großflächigen Einsatz, Earth Naga ließ sich einen Backdoor-Loader regelrecht „zusammenvibecoden“, und ein weiterer Akteur schickte einen KI-Agenten los, der eigenständig Netzwerke durchsuchte, Zugangsdaten abgriff und sich seitwärts durch die Umgebung des Opfers bewegte. Andere versteckten ihre Steuerkanäle in Microsoft-365-Entwürfen und Blockchain-Transaktionen, während SHADOW-EARTH-067 diese Tarnung mit einem BYOVD-Rootkit kombinierte, das die Endpunkterkennung (EDR) direkt auf Kernel-Ebene blind schaltete.

Nordkorea – „Der diebstahlfinanzierte Aufsteiger“

Zellen mit DPRK-Bezug blieben ihrer Kernaufgabe treu: Geld für den Staat beschaffen. BlueNoroff kaperte das Konto des Axios-Maintainers und verteilte über ein Paket mit mehr als 100 Millionen wöchentlichen Downloads einen



Fernzugriffstrojaner, während Void Dokkaebi Schadsoftware über gefälschte Repositories für Bewerbungsgespräche streute. Ein mutmaßlich nordkoreanischer Akteur erbeutete 285 Millionen US-Dollar vom Drift Protocol, ein weiterer zog 292 Millionen US-Dollar aus KelpDAO ab – zusätzlich zu den stetigen Einnahmen eingeschleuster IT-Kräfte. Sanktionen und ein marodes Stromnetz halten moderne KI im eigenen Land außer Reichweite und zwingen diese Gruppen auf ausländische Server und fremde Modelle, etwa für KI-gestützte Raketentests.

Russland – „Der Militarisierte am Hardware-Limit“

Russland-nahe Gruppen agierten schnell und blieben dabei erstaunlich unsichtbar. Pawn Storm verwandelte eine frische Office-Zero-Day-Lücke binnen weniger Wochen in eine einsatzfähige Waffe und nahm ein breites Spektrum kriegsrelevanter Ziele ins Visier, von Verteidigungsministerien bis zur Grenzpolizei, während Earth Dahu weiter eine längst bekannte WinRAR-Schwachstelle ausnutzte, die eben nicht überall gepatcht war. Turla setzte auf besonders zählebige Infrastruktur und baute sein Kazuar-Toolset zu einem Botnetz um, bei dem pro Netzwerk nur ein einziger Knoten nach außen kommuniziert. Laundry Bear wählte einen anderen Weg, tarnte sich als Hilfsorganisation für Kriegsoffer und wickelte seine Steuerung über Wegwerf-Paste-Seiten ab.

Iran und weitere Regionen „Der Eskalierer von der Stange“

Iran-nahe Aktivität verwischte die Grenze zwischen Spionage und Kriminalität. CyberAv3ngers wurde mit IOCONTROL in Verbindung gebracht, einer wiederverwendbaren Malware-Plattform für Angriffe auf Betriebstechnik wie Treibstoffsysteme. Parallel traf eine

mutmaßlich Iran-nahe Welle internetexponierter Tankfüllstandsmesser an US-Standorten, während Earth Vetala (MuddyWater) eigene Werkzeuge mit einer auf einer kriminellen Plattform gemieteten Backdoor kombinierte und ihre C&C-Adressen über öffentliche Blockchain-Abfragen auflöste. Aktivitäten aus anderen Regionen zeigten zudem, wie sich Personen über ADINT in großem Stil verfolgen lassen – ganz ohne den Einsatz von Schadsoftware.

Die bemerkenswertesten TTPs des Halbjahres

1. KI-gestützte Entwicklung und agentisches Lateral Movement

Zum ersten Mal dokumentierten die Forschungsteams von TrendAI™, dass China-nahe Akteure wie Earth Krahang, Earth Naga (mit Verbindungen zu

Flax Typhoon) und ein bislang nicht zugeordneter Angreifer generative KI aktiv in mehrere Phasen ihres Angriffszyklus integrieren. Die Spanne reichte von der Verfeinerung bekannter Einbruchsskripte über per Prompts geschriebene Programme bis hin zu KI-Agenten. Letztere spionierten Firmennetze aus, fischten Passwörter ab und arbeiteten sich eigenmächtig von Rechner zu Rechner vor. Bislang testen diese Gruppen die Werkzeuge vor allem, doch die Hürde für hochgefährliche Digitalkörper sinkt rapide.

2. Legitime Dienste als C&C-Kanäle

Chinesische Formationen wie Earth Baxia sowie SHADOW-EARTH-067 machten ihre eigene Serverinfrastruktur entbehrlich. Sie steuerten Angriffe stattdessen über geläufige Werkzeuge: die Schnittstellen von Microsoft-Diensten, Entwickler-Tunnel, dynamische Netzwerk-Adressen oder digitale

Währungsnetzwerke. Die Befehle und erbeuteten Daten fließen getarnt durch Alltagskanäle. Abwehrsysteme schlagen bei diesem gewohnten Datenverkehr kaum noch Alarm.

3. Mehrstufiges Phishing mit Ködern und Social Engineering

Spear-Phishing blieben das Werkzeug erster Wahl für den Einbruch. Die Angreifer schraubten die Qualität ihrer Köder jedoch deutlich nach oben. Mehrstufige Mail-Wechsel bauten schrittweise Vertrauen auf, passgenau zugeschnittene Dokumente spiegelten politische Relevanz vor, gefälschte Update-Dateien verlockten zum Klick und manipulierte Webseiten erzeugten scheinbar echte Sicherheitswarnungen im Browser. Sämtliche Kniffe zielten darauf ab, Bedenken zu zerstreuen.

4. BYOVD zur Umgehung von EDR und Virenschutz

Erstmals wurde „Bring Your Own Vulnerable Driver“ als dedizierte Rootkit-Komponente beobachtet – eine deutliche Eskalation der Verschleiерungsfähigkeiten China-naher Akteure, allen voran bei SHADOW-EARTH-067. Indem verwundbare, aber legitim signierte Treiber in den Kernel geladen werden, hebeln die Angreifer Schutzmechanismen genau dort aus, wo Sicherheitsprodukte eigentlich ihre stärkste Stellung haben.

Wie KI und politische Verschiebungen die APT-Kampagnen neu definieren

„In einem Fall führte ein KI-Agent seine Aufklärung und Lateralbewegung selbst durch – per Jailbreak überredet von einem Akteur, der die Operation wahrheitswidrig als legitimen Penetrationstest ausgab.“





KI ist für APT-Gruppen keine experimentelle Spielerei mehr, sondern ein operativer Baustein, der direkt in Kampagnen eingebettet wird. China-nahe Akteure schärften mit generativer KI einen öffentlichen Proof-of-Concept-Exploit zu einem großflächigen Scan-Werkzeug und entwickelten Schritt für Schritt einen bössartigen Loader aus PowerShell und C#. In einem Fall, der möglicherweise einer Earth-Lamia-Operation zuzurechnen ist, wurde ein autonomer KI-Agent per Jailbreak dazu gebracht, gegen ein Ziel in Südostasien selbstständig Netzwerk-Scans, Exploits, Credential-Diebstahl und Password-Spraying durchzuführen. Auch Russland- und Nordkorea-nahe Akteure greifen zu kommerzieller KI, bislang allerdings eher unterstützend und in begrenztem Umfang.

Der politische Unterbau dieser Kampagnen ist dabei alles andere als flüchtig. Der Krieg in der Ukraine hat sich zu einem langen Abnutzungskampf verfestigt, während Russland vor seinen Parlamentswahlen im September die Informationskontrolle spürbar verschärft. Nordkorea richtet sich dauerhaft als nuklear bewaffneter Staat ein, der sich über Cyberdiebstahl finanziert. China balanciert seine Rivalität mit den USA aus und treibt zugleich die Eigenständigkeit bei Chips und KI voran, und Iran-nahe Operationen eskalierten im Gleichschritt mit den Spannungen in der Region. Keiner dieser Trends dürfte sich bis zum Jahresende umkehren – und damit werden auch die darauf aufbauenden Kampagnen aus KI-geschärfter Ausnutzung, missbrauchter Vertrauensinfrastruktur und gemietetem Werkzeug weiter reifen. Für Verteidiger heißt das im Umkehrschluss: Wer die geopolitische Motivlage seiner Angreifer versteht, kann deutlich besser einschätzen, welche Sektoren, Datenbestände und Systeme als Nächstes ins Visier geraten dürften.

Was das für Sicherheitsverantwortliche bedeutet

Diese Entwicklungen betreffen praktisch jede Ebene einer Sicherheitsorganisation, wenn auch auf unterschiedliche Weise. Für CISOs und Security-Direktoren verschiebt sich das langfristige Risikoprofil: Die Kombination aus KI-Adaption, dem Missbrauch vertrauenswürdiger Infrastruktur und klarer geopolitischer

Ausrichtung verlangt nach Budget- und Architektur-entscheidungen, die über das nächste Quartal hinausdenken – und nach Vorstandsbriefings, die genau diese Zusammenhänge verständlich machen. SOC-Teams und Threat-Intelligence-Analysten wiederum müssen sich darauf einstellen, dass Angreifer im Alltag längst mit KI-gestützter Exploit-Entwicklung arbeiten und ihre Steuerkanäle in Cloud-Diensten und Blockchains verbergen, wo klassische Blocklisten ins Leere laufen. Engineers stehen vor der Aufgabe, ihre Erkennungslogik für BYOVD-Rootkits, Cloud- und Identitätsmissbrauch sowie kompromittierte Lieferketten nachzuschärfen, während Risiko-, Policy- und Governance-Teams den geopolitischen Unterbau brauchen, um nachvollziehbar zu erklären, warum gerade bestimmte Regionen, Branchen und Betriebstechnik im Fadenkreuz stehen.

Prioritäre Maßnahmen für Verteidiger

- Verlagern Sie die Erkennung stärker auf Identitäten, Cloud und Endpunktverhalten, denn C&C versteckt sich zunehmend in vertrauenswürdigen Cloud-Plattformen, Entwickler-Tunneln und Blockchains. Verantwortlich: Security Operations und Identity-Teams.
- Behandeln Sie die Software-Lieferkette und die Entwickler selbst als Teil der Angriffsfläche: Abhängigkeiten fixieren und verifizieren, Installationsskripte überwachen. Verantwortlich: Governance und Security Operations.
- Verkürzen Sie das Patch- und Expositionsfenster bei Edge-Systemen und unverwalteter Software, besonders bei Werkzeugen ohne automatische Updates. Verantwortlich: Risikomanagement.
- Nehmen Sie Betriebstechnik und kritische Infrastruktur vom öffentlichen Internet, segmentieren und überwachen Sie Ihre Steuerungsnetze. Verantwortlich: Risikomanagement und Security Operations.
- Planen Sie für KI-beschleunigte Gegner – einschließlich der KI-Werkzeuge, die bereits im eigenen Haus laufen, etwa Coding-Assistenten und Agenten-Frameworks. Verantwortlich: Security Operations und Governance. -v-



SASE für Österreich: Weniger Baustellen, mehr Steuerung



In vielen IT-Landschaften sieht es ähnlich aus. VPN, Firewall, Web-Gateway, SD-WAN, DLP, CASB sind über Jahre als getrennte Projekte entstanden, jedes mit eigener Begründung und eigenem Budget. In Summe entsteht daraus genau das, was eigentlich vermieden werden sollte: mehrere Konsolen, konkurrierende Regelwerke, verstreute Vertragslaufzeiten und Sicherheitsentscheidungen, die im Zweifel niemand mehr sauber erklären kann.

NIS2 erhöht den Druck auf diese gewachsene Struktur. Risiken müssen belegbar gesteuert, Zugriffe nachvollziehbar kontrolliert, Vorfälle schneller erkannt und Lieferketten samt digitaler Dienste robuster abgesichert werden. Wer das mit sechs Werkzeugen und vier Logquellen nachweisen soll, verbringt mehr Zeit mit Berichten als mit Sicherheit.

SASE ist eine Architekturfrage, kein Produktname

An dieser Stelle wird SASE relevant, und zwar nicht als Buzzword, sondern als Entscheidung über die Bauart. SASE bündelt die zentralen Netzwerk- und Sicherheitsfunktionen: Zero Trust Network Access als Ablöse für das klassische VPN, ein Secure Web Gateway für Internetverkehr, CASB und DLP für Cloud- und Datenkontrolle, dazu SD-WAN und Netzwerkdienste für Standorte und hybride Umgebungen.

Die Feature-Liste ist dabei nicht der Unterschied. Fast alle Anbieter zeigen dieselben Kästchen. Interessant wird es eine Ebene tiefer, bei der Frage, wo diese Funktionen tatsächlich laufen. Cloudflare betreibt

sie auf einem globalen Anycast-Netzwerk, in dem jeder Dienst in jedem Rechenzentrum verfügbar ist. Prüfungen finden dort statt, wo Nutzerin, Standort oder Anwendung sind, statt den Verkehr über wenige zentrale Knoten zu ziehen. Das Ergebnis ist praktisch messbar: weniger Latenz, ein Regelwerk statt mehrerer, und die Möglichkeit, bestehende VPN- und Security-Architekturen schrittweise abzulösen, ohne einen Stichtag mit Rückfahrkarte planen zu müssen.

Für Österreich kommt ein handfester Punkt dazu. Cloudflare betreibt Infrastruktur im Land und verfügt global über mehr als 500 Tbit/s Netzwerkkapazität. Richtlinien lassen sich damit lokal performant durchsetzen und trotzdem weltweit einheitlich halten.

Datenkontrolle bleibt Chefsache

Wo Daten verarbeitet, entschlüsselt und gespeichert werden, ist längst keine rein technische Fußnote mehr. Mit der Data Localization Suite lässt sich genau das steuern, passend zu DSGVO, NIS2 und internen Governance-Vorgaben. Der Punkt dabei: es braucht keine zweite, parallele Sicherheitsarchitektur nur für die Compliance-Anforderungen.

KI ist der nächste blinde Fleck

Die nächste Welle läuft bereits, und sie läuft an vielen Sicherheitsteams vorbei. Mitarbeitende nutzen KI-Dienste, ob freigegeben oder nicht. Fachbereiche bauen erste Assistenten. Entwicklerteams verdrahten Modelle direkt in Anwendungen. Drei Fragen bleiben offen: Welche Dienste sind erlaubt? Welche Daten verlassen dabei das Unternehmen? Und was passiert

mit dem Rest, der ohnehin passiert?

Der erste Teil ist klassische SASE-Arbeit. Secure Web Gateway und CASB machen sichtbar, welche KI-Anwendungen im Einsatz sind, DLP verhindert, dass Quellcode, Kundendaten oder Vertragsentwürfe im Prompt landen. Shadow AI wird damit kein Rätsel mehr, sondern eine Liste, über die man entscheiden kann.

Der zweite Teil betrifft die KI-Nutzung, die das Unternehmen selbst aufbaut, und hier hilft ein Baustein, den viele SASE-Diskussionen noch auslassen: AI Gateway. Der Dienst liegt als Proxy zwischen den eigenen Anwendungen und den Modellanbietern. Jeder Aufruf läuft über einen kontrollierten Punkt, an dem Logging, Kostentransparenz, Caching, Rate Limiting sowie Retries und Fallbacks auf ein Alternativmodell greifen. Aus einer Blackbox wird damit ein Datenpfad mit Protokoll.

Sicherheitsseitig ist das der eigentliche Gewinn. Prompts und Antworten lassen sich mit Guardrails auf unerwünschte Inhalte prüfen, bevor sie beim Modell oder beim Nutzer ankommen, und die DLP-Funktion erkennt personenbezogene oder finanzielle Daten im laufenden Verkehr. Wer wie oft welches Modell

aufruft, ist auswertbar. Ein kompromittierter oder schlicht zu teurer Anwendungsfall fällt auf, bevor die Rechnung kommt. Und weil Modellanbieter über eine einheitliche Schnittstelle angebunden sind, bleibt der Wechsel eine Konfiguration statt eines Refactorings.

Zusammen ergibt das eine durchgehende Linie: Kontrolle über die KI, die Beschäftigte nutzen, und Kontrolle über die KI, die das Unternehmen selbst betreibt. Beides auf derselben Plattform, mit denselben Identitäten und derselben Protokollierung.

Klein anfangen ist die richtige Strategie

Ein SASE-Einstieg muss kein Zweijahresprogramm sein. Die meisten Organisationen starten mit einem Standort, einer Nutzergruppe oder einer einzelnen kritischen Anwendung, sammeln Erfahrung und erweitern dann. Mit erfahrenen lokalen Partnern funktioniert dieser Weg vom KMU bis zum Konzern.

Beim ITK am 16.09.2026 in Linz zeigt Cloudflare live, wie das in der Praxis aussieht: einfach einzuführen, lokal performant und vorbereitet auf Cloud, hybrides Arbeiten, NIS2 und KI. -v-

Cybersecurity: wenn Komplexität zum größten Risikofaktor wird

PETER HERMANN

Die digitale Bedrohungslage erreicht eine neue Dimension. Bereits der Global Cybersecurity Outlook 2026 des Weltwirtschaftsforums (WEF) vom Frühjahr dieses Jahres dokumentiert eine Welt, in der geopolitische Spannungen, künstliche Intelligenz (KI) und fragile Lieferketten die Sicherheitslandschaft grundlegend verändern. Für Unternehmen wird klar: Klassische Abwehrstrategien reichen nicht mehr aus, Resilienz wird zur Schlüsselkompetenz.

Die Zahlen sind eindeutig. 87 Prozent der Befragten identifizieren KI-bezogene Schwachstellen als das am schnellsten wachsende Cyber-Risiko. 77 Prozent berichten von einer Zunahme von Cyber-Betrug und Phishing, 65 Prozent von wachsenden Lieferkettenrisiken. Die Herausforderung besteht heute weniger darin, Angriffe zu verhindern, sondern den Betrieb nach einem Vorfall schnell wiederherzustellen. Cyberbedrohungen entwickeln sich zu komplexen Multi-Payout-Angriffen, bei denen Daten verschlüsselt, erpresst und weiterverkauft werden. Intelligente Dateninfrastrukturen mit Anomalie-Erkennung, Breach-Analytik und automatisierter Isolation werden zum Fundament moderner Cyber-Resilienz.

KI als Komplexitätstreiber

Künstliche Intelligenz verstärkt diese Dynamik: 94 Prozent der Befragten gehen davon aus, dass KI im Jahr 2026 der bedeutendste Veränderungsfaktor in der Cybersicherheit sein wird. Die Studie zeigt: Der Anteil der Organisationen, die die Sicherheit von KI-Tools vor deren Einsatz prüfen, hat sich im Vergleich zum Vorjahr nahezu verdoppelt.

Gleichzeitig identifizieren 87 Prozent der Befragten KI-bezogene Schwachstellen als das am schnellsten wachsende Cyberrisiko. Die weitverbreitete Integration von KI-Systemen schafft neue Angriffsflächen, für die herkömmliche Kontrollen nicht ausgelegt sind. Angreifer nutzen generative KI, um Social-Engineering-Angriffe zu automatisieren und zu skalieren. Mit realistischen Phishing-Mails, Deepfakes und gefälschten Dokumenten umgehen sie Erkennungssysteme und menschliche Prüfungen.

Doch KI ist auch ein entscheidender Faktor für die Verteidigung. Wird sie in die Kerninfrastruktur eingebettet, können Unternehmen Bedrohungen in Echtzeit erkennen, automatisiert reagieren und prädiktive Analysen durchführen. Gerade bei knappen personellen Ressourcen sind diese Fähigkeiten besonders wertvoll.

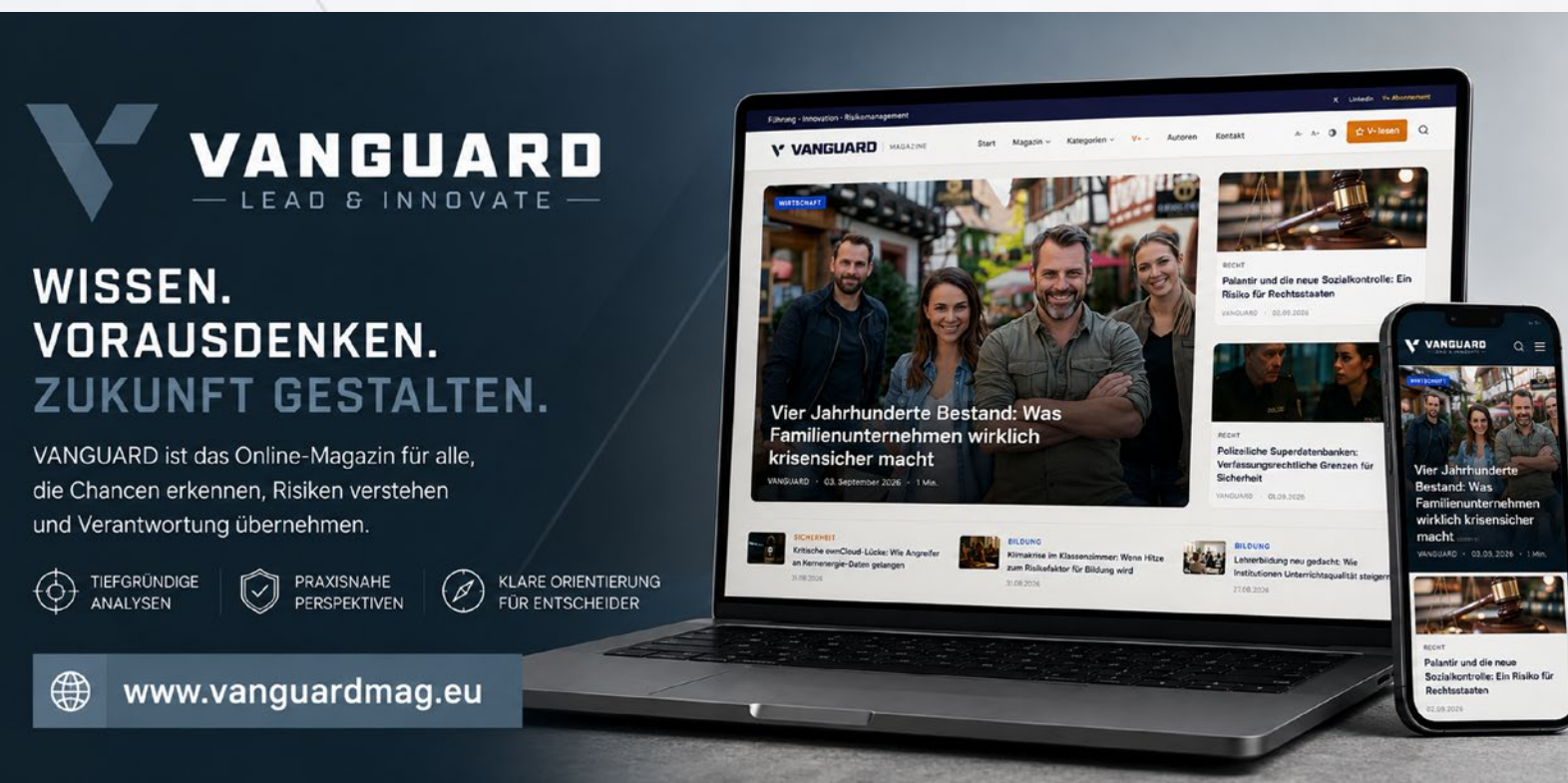
Auffallend ist auch, dass sich die Risikowahrnehmung verschiebt. CEOs stufen Cyber-Betrug und Phishing mittlerweile als größtes Risiko ein – noch vor Ransomware, das 2025 an erster Stelle stand. CISOs hingegen priorisieren weiterhin Ransomware und Lieferkettenrisiken. Beide Perspektiven erfordern jedoch denselben Lösungsansatz: unveränderliche Backups, die auch bei einem Ransomware-Angriff intakt bleiben, kombiniert mit einem Zero-Trust-Sicherheitsmodell, bei dem kein Nutzer und kein System automatisch als vertrauenswürdig gilt.

Doch KI-gestützte Angriffe sind nicht die einzige aufkommende Bedrohung, auf die sich Unternehmen heute vorbereiten müssen. Hinzu kommt das Risiko „Harvest now, decrypt later“: Verschlüsselte Daten werden heute gesammelt, um sie künftig mit Quantencomputern zu entschlüsseln. Experten erwarten, dass Quantencomputer zwischen 2028 und 2033 klassische Verschlüsselungsverfahren wie RSA oder ECC in kurzer Zeit knacken können – der sogenannte Q-Day. Damit könnten heute gestohlene Daten künftig offen lesbar werden.

Trotz des wachsenden Handlungsdrucks haben laut aktueller Studien noch über 90 Prozent der Unternehmen weltweit keine Post-Quanten-Kryptographie (PQC) Roadmap. Die Umstellung auf quantensichere Verschlüsselung dauert bei großen Organisationen geschätzt 12 bis 15 Jahre – wer jetzt nicht beginnt, riskiert unzureichenden Schutz zum Q-Day.

Lieferketten als systemisches Risiko

Ein weiterer Komplexitätstreiber sind die Abhängigkeiten in digitalen Lieferketten. 65 Prozent der großen Unternehmen nennen Schwachstellen bei Drittanbietern als größtes Hindernis für ihre Cyber-



VANGUARD
— LEAD & INNOVATE —

WISSEN. VORAUSDENKEN. ZUKUNFT GESTALTEN.

VANGUARD ist das Online-Magazin für alle, die Chancen erkennen, Risiken verstehen und Verantwortung übernehmen.

 TIEFGRÜNDIGE ANALYSEN
  PRAXISNAHE PERSPEKTIVEN
  KLARE ORIENTIERUNG FÜR ENTSCHEIDER

www.vanguardmag.eu



Resilienz – ein Anstieg gegenüber 54 Prozent im Vorjahr.

Viele Unternehmen können die Integrität von Lösungen ihrer Partner nur eingeschränkt sicherstellen. Während 66 Prozent der Organisationen die Sicherheit ihrer Lieferanten bewerten, simulieren nur 27 Prozent Cybervorfälle oder üben die Wiederherstellung mit ihren Geschäftspartnern. Diese Lücke erhöht das systemische Risiko erheblich.

Resilienz als Antwort auf Komplexität

Deshalb vollzieht sich ein Paradigmenwechsel. Cyber-Resilienz bedeutet, die Auswirkungen schwerwiegender Cybervorfälle auf Geschäftsziele zu minimieren. Entscheidend sind schnelle Recovery-Fähigkeiten, die Ausfallzeiten reduzieren.

Die Merkmale resilienter Organisationen sind messbar: Hochresiliente Unternehmen (76 Prozent) beziehen ihre Sicherheit deutlich häufiger in Beschaffung und Lieferantenmanagement ein.

In diesem Kontext spielt die Demokratisierung von Cybersicherheit eine entscheidende Rolle. Die Kluft zwischen Organisationen, die sich eine robuste Sicherheit leisten können und jenen, die es nicht können, wächst. KMUs sowie der öffentliche Sektor sind dabei besonders gefährdet. Skalierbare Lösungen, die Enterprise-Grade-Resilienz auch für

kleinere Organisationen zugänglich machen, können diese Lücke schließen. Automatisierte Bedrohungserkennung und Managed Backup Services reduzieren den Bedarf an internem Fachwissen und helfen gegen Fachkräftemangel.

Selbstverteidigende Infrastrukturen als neuer Maßstab für Resilienz

Mehrere Entwicklungen werden die Antwort auf zunehmende Komplexität prägen. Dazu gehören:

- Schnellere Erkennung und Wiederherstellung
- Automatisierte Isolation und Recovery
- Intelligente Dateninfrastrukturen mit Anomalie-Erkennung, Breach-Analytik und Post-Quanten-Kryptographie

KI-gestützte Cybersicherheitstools entwickeln sich vom Experiment zum Standard. Prädiktive Analytik und KI-gestützte Forensik zur Erkennung abnormaler Verhaltensweisen werden breit eingesetzt. Zudem rückt Data Governance in den Fokus: Zugriffskontrollen, Sicherheit und Herkunftsverfolgung über den gesamten Datenlebenszyklus werden zur Grundlage vertrauenswürdiger KI. Erfolgreich sind Unternehmen, die Resilienz als strategische Aufgabe verstehen und ihre Wiederherstellungsfähigkeit kontinuierlich stärken. -v-



Vom Patchen zur Risiko-Strategie: Exposure Management als Grundlage moderner Cybersicherheit

ROGER SCHEER

Cybersicherheit steht an einem Wendepunkt: Isolierte Schwachstellenmeldungen allein helfen Unternehmen wenig, wenn der Bezug zum Geschäftsrisiko fehlt. Warum es jetzt einen strategischen Perspektivwechsel braucht und wie Sicherheit konsequent an geschäftlichen Risiken ausgerichtet werden kann, erläutert Roger Scheer, Regional Vice President Central Europe bei Tenable.

In einer Zeit, in der digitale Geschäftsmodelle immer stärker vernetzt und komplexer werden, reicht es nicht mehr aus, nur Schwachstellen zu erkennen und zu beheben. Klassische Schwachstellenscans liefern zwar wertvolle Daten, zeigen jedoch selten, welche Risiken für das Geschäftsmodell tatsächlich relevant sind. Moderne Cyberrisiken verlangen einen strategischen Blick auf die gesamte Risikolage eines Unternehmens – ein Ansatz, der als Exposure Management bezeichnet wird und weit über traditionelle Schwachstellenanalysen hinausgeht.

Die Grenzen klassischer Schwachstellenanalyse

Seit vielen Jahren folgen Sicherheitsprogramme einem eingespielten Zyklus: scannen, bewerten, patchen, wiederholen. Dabei entstehen enorme Datenmengen, die kaum noch sinnvoll priorisiert werden können. Zudem

werden Schwachstellen häufig isoliert betrachtet, ohne sie in den Kontext von Geschäftsprozessen, Angriffspfaden oder der tatsächlichen digitalen Infrastruktur einzuordnen.

In der Praxis führt dies nicht selten zu Alarmmüdigkeit. Sicherheitsteams arbeiten umfangreiche Listen technischer Einzelbefunde ab, ohne sicherstellen zu können, dass damit die realen Risiken für das Unternehmen wirksam reduziert werden. Mit jeder neuen Cloud-Anwendung, jeder vernetzten Produktionsanlage und jeder zusätzlichen Schnittstelle wächst zudem die Angriffsfläche – und damit die Komplexität der Risikosteuerung.

Exposure Management: Ein Perspektivwechsel

Exposure Management setzt an einem anderen Punkt an. Statt ausschließlich zu fragen, welche Schwachstellen vorhanden sind, steht die Frage im Mittelpunkt, welche konkreten Risiken das Geschäftsmodell bedrohen und auf welchen Wegen Angreifer diese Risiken ausnutzen könnten. Dieser Perspektivwechsel verändert die Priorisierung grundlegend.

Ein solcher Ansatz erfordert zunächst Transparenz über sämtliche relevanten Assets – von klassischen IT-Systemen über Cloud-Dienste und Identitäten bis

hin zu OT- und IoT-Umgebungen. Entscheidend ist jedoch nicht nur die Inventarisierung, sondern die intelligente Verknüpfung dieser Informationen. Schwachstellen, Fehlkonfigurationen, übermäßige Berechtigungen oder exponierte Zugangsdaten entfalten ihr tatsächliches Gefahrenpotenzial oft erst im Zusammenspiel. Gerade sogenannte „toxische Risikokombinationen“ – etwa ein kompromittiertes Benutzerkonto mit weitreichenden Rechten auf einem verwundbaren System – lassen sich nur erkennen, wenn Datenquellen zusammengeführt und in Beziehung gesetzt werden.

Damit verschiebt sich der Fokus von einer reaktiven Abarbeitung technischer Mängel hin zu einer strategischen Bewertung tatsächlicher Risiken. Sicherheitsmaßnahmen werden nicht mehr primär nach Schweregrad einzelner Schwachstellen priorisiert, sondern nach ihrer Bedeutung für das Geschäftsrisiko.

Sichtbarkeit über Silos hinweg

Traditionelle Schwachstellen-scanner betrachten häufig nur Teilbereiche der IT-Landschaft. Netzwerk, Server, Anwendungen oder Identitäten werden separat analysiert. In hochgradig vernetzten Umgebungen entsteht so jedoch ein fragmentiertes Bild der Sicherheitslage.



Exposure Management führt diese Perspektiven zusammen und macht sichtbar, welche Angriffspfade tatsächlich existieren. Ein Cloud-Dienst mag für sich genommen unkritisch erscheinen. Treffen jedoch eine unzureichende Netzwerkkonfiguration, weitreichende Zugriffsrechte und eine bekannte, aktiv ausnutzbare Schwachstelle aufeinander, kann daraus ein direkter Weg in sensible Kernsysteme entstehen. Die isolierte Betrachtung einzelner Komponenten würde dieses Szenario möglicherweise nicht erkennen.

Gerade in hybriden Infrastrukturen, in denen On-Premises-Systeme, Multi-Cloud-Architekturen und industrielle Steuerungstechnik ineinandergreifen, ist eine solche ganzheitliche Sicht Voraussetzung für wirksames Risikomanagement.

Vom Datenberg zur Entscheidungsgrundlage

Für Führungskräfte ist weniger die Anzahl entdeckter Schwachstellen entscheidend als die Frage,

welche davon das Unternehmen tatsächlich gefährden. Exposure Management transformiert technische Detailinformationen in kontextbezogene Erkenntnisse über geschäftskritische Risiken. Dadurch wird es möglich, Ressourcen gezielt dort einzusetzen, wo sie den größten Effekt auf die Risikominimierung haben.

Sicherheitsberichte gewinnen so an strategischer Aussagekraft. Statt rein technischer Kennzahlen stehen belastbare Einschätzungen zur realen Gefährdungslage im Mittelpunkt. Das erleichtert die Kommunikation zwischen IT, Sicherheitsverantwortlichen und Geschäftsführung erheblich. Sicherheit wird damit nicht als Kostenfaktor oder Bremse wahrgenommen, sondern als integraler Bestandteil verantwortungsvoller Unternehmensführung.

Sicherheit als Bestandteil der Geschäftsstrategie

Mit zunehmender Digitalisierung steigt nicht nur die Innovations-

geschwindigkeit, sondern auch die regulatorische und operative Verantwortung. Anforderungen wie NIS-2 unterstreichen, dass Transparenz über Risiken und deren systematische Steuerung keine Option mehr ist, sondern zur unternehmerischen Pflicht wird.

Ein strategisch ausgerichtetes Exposure Management ermöglicht es, Angriffspfade frühzeitig zu erkennen, bevor sie ausgenutzt werden, begrenzte Sicherheitsressourcen auf die tatsächlich kritischen Bereiche zu konzentrieren und fundierte Entscheidungen auf Basis konsolidierter Risikoinformationen zu treffen. Damit entwickelt sich Cybersicherheit von einer rein technischen Disziplin zu einem zentralen Element des unternehmensweiten Risikomanagements. -v-



Identität ist die neue Frontlinie

Öffentliche Institutionen zwischen NIS2, DORA und wachsendem Angriffsdruck

Cyberangriffe auf Behörden, Kommunen, Verteidigungseinrichtungen und kritische Infrastruktur sind kein Ausnahmefall mehr. Sie sind Tagesgeschäft. Angreifer kennen keine Feiertage, keine Budgetzyklen, keine Dienstwege. Sie suchen den Weg des geringsten Widerstands – und finden ihn zunehmend über gestohlene, missbrauchte oder überprivilegierte Identitäten statt über die klassische Netzwerkgrenze.

Der Gesetzgeber hat reagiert. Mit NIS2 verpflichtet die EU Betreiber wesentlicher und wichtiger Einrichtungen – von Verwaltung über Energie bis Gesundheitswesen – zu belegbarem Risikomanagement, verbindlicher Vorfallmeldung und geprüfter Lieferkettensicherheit. Geschäftsführung und Behördenleitung haften persönlich für Versäumnisse. Für Finanzinstitute und ihre IKT-Dienstleister kommt DORA hinzu: operative Resilienz, Drittparteirisiko und Reaktionsfähigkeit sind Pflicht, keine Kür. Beide Regelwerke verlangen dasselbe Prinzip: Eine Institution muss Sicherheit nachweisen, nicht nur behaupten.

Der Nachweis beginnt bei der Identität. Wer hat Zugriff, auf was, warum, und seit wann? Diese Frage stellen Prüfer, Aufsichtsbehörden und Angreifer gleichermaßen. Ohne durchgängige Identitätssicherheit lässt sich weder Risikomanagement nach NIS2 belegen noch operative Stabilität nach DORA herstellen. Identität ist damit kein IT-Thema unter vielen mehr. Sie ist die Grundlage, auf der Compliance und Resilienz stehen oder fallen.

RSA sichert seit Jahrzehnten die Identitäten, auf die Regierungen, Verteidigungseinrichtungen und Behörden weltweit ihre Mission stützen. RSA schützt Behördenbetrieb in 67 Ländern; mehr als 9.000 sicherheitskritische Organisationen setzen auf die RSA Unified Identity Platform. Das Fundament dafür ist ein einziges Prinzip: Identität zuerst, in jeder Umgebung.

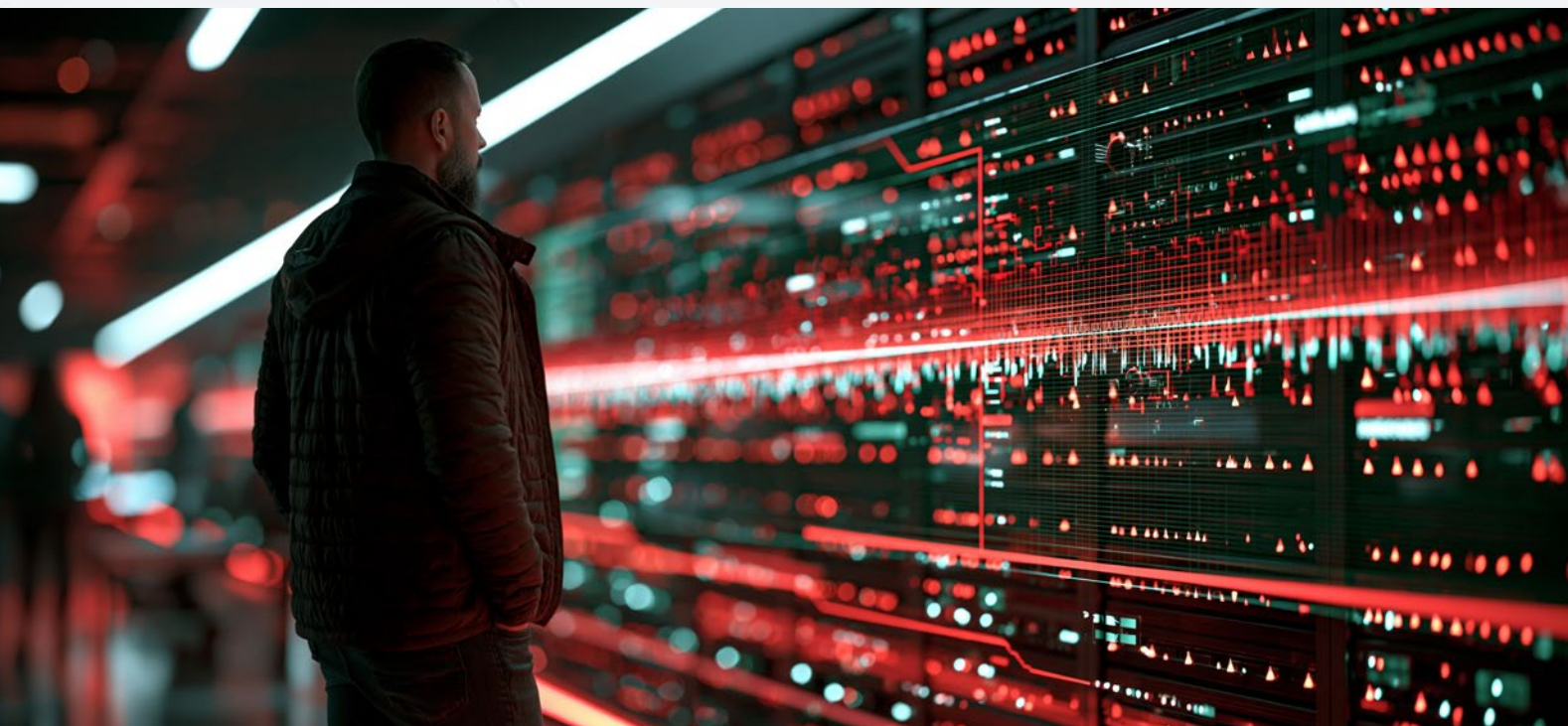
RSA ID Plus liefert phishing-resistente Multi-Faktor-Authentifizierung und passwortlosen Zugriff über Cloud-, Hybrid- und On-Premises-Umgebungen hinweg – bis in abgeschottete, luftgetrennte Netzwerke, wie sie Verteidigung und kritische Infrastruktur voraussetzen. RSA Hybrid Failover hält Behörden auch dann arbeitsfähig, wenn die Verbindung zur Cloud ausfällt. Genau diese Betriebskontinuität fordert DORA konkret ein.

RSA Governance & Lifecycle automatisiert Zugriffsprüfungen, erkennt überprivilegierte und verwaiste Konten, bevor Angreifer sie finden, und liefert prüfungsfeste Audit-Trails auf Knopfdruck statt manueller Zertifizierungsrunden. Das ist die Dokumentation, die NIS2 verlangt – kontinuierlich erzeugt, nicht einmal jährlich zusammengetragen. RSA Risk AI setzt dort an, wo klassische Regeln nicht mehr ausreichen: mit risikobasierten, adaptiven Zugriffsentscheidungen nach Zero-Trust-Prinzipien.

Compliance ist bei RSA nicht nachgelagert, sondern eingebaut: FedRAMP, NIS2, DORA, FIPS, NIST, CMMC. Die Anforderungen wechseln je nach Land und Branche, das Fundament bleibt dasselbe. Das entscheidet darüber, ob eine Institution unter Prüfungsdruck bestehen kann oder nachbessern muss – und ob sie im Ernstfall handlungsfähig bleibt oder stillsteht.

Öffentliche Institutionen in Österreich und der gesamten EU stehen an einem Punkt, an dem Regulierung und Bedrohungslage in dieselbe Richtung zeigen: Identität muss die Grundlage der Sicherheitsarchitektur sein, nicht ein Baustein darunter. RSA bringt die Erfahrung aus Regierungseinsätzen in 67 Ländern dorthin, wo sie jetzt gebraucht wird.

RSA ist mit einem eigenen Stand auf der IKT-Sicherheitskonferenz 2026 in Linz vertreten (15. bis 17. September, veranstaltet vom Bundesministerium für Landesverteidigung). Vor Ort zeigt RSA, wie sich NIS2- und DORA-Anforderungen mit einer identitätszentrierten Sicherheitsarchitektur in der Praxis umsetzen lassen – von der Authentifizierung bis zur prüfungsfesten Governance. www.rsa.com/solutions/government -v-





ZRK

ZENTRUM FÜR
RISIKO- UND
KRISENMANAGEMENT

WIR SCHAFFEN RESILIENZ.

Strategische Resilienz beginnt vor der Krise.



FORSCHUNG



BILDUNG



CONSULTING



VERNETZUNG



Gemeinsam für
eine widerstandsfähige Zukunft.

www.zfrk.org

VERSTEHEN.
VORBEREITEN.
HANDELN.
GESTALTEN.



SICHERHEIT

Was macht Kritische Infrastruktur heute besonders kritisch?

BJÖRN HAWLITSCHKA

Der Begriff Kritische Infrastruktur klingt nach moderner Technik und Industrieanlage. Doch schon die Macht Roms begründete sich auf funktionierende Infrastruktur. Straßen, Aquädukte, Brücken und Häfen - sie brachten Truppen, Wasser, Nahrung und Waren in Bewegung. Auch im Mittelalter entschieden Handelswege, Mühlen, Brunnen und Stadtbefestigungen über Wachstum oder Not. Ein vergifteter Brunnen, eine blockierte Straße waren bereits damals ein Angriff auf die Gesellschaft.

Die Besonderheit der Kritische Infrastruktur des 21. Jahrhunderts zeichnet sich dagegen durch ihre Vielzahl, ihre Vernetzung und die damit bedingte Abhängigkeit voneinander aus. Der mittelalterliche Brunnen funktionierte, auch wenn die Windmühle am Ortsrand stillstand. Das moderne Wasserwerk dagegen braucht Strom, Telekommunikation, digitale Steuerung und oft externe Dienstleister. Fällt ein Baustein aus, gerät das ganze System unter Druck. Kritische Infrastruktur ist kein Sammelkasten besonderer Einzelexemplare mehr. Sie ist ein zusammenhängender hochkomplexer Organismus. Strom, Telekommunikation, Verkehr, Gesundheit, Finanzen, Logistik und digitale Dienste greifen so eng ineinander, dass sie nicht länger getrennt betrachtet werden können. Die Abhängigkeiten laufen in beide Richtungen: Ohne Strom keine Mobilfunknetze. Ohne Telekommunikation können Energieversorger ihre Netze nicht steuern. Ohne funktionierende Rechenzentren stehen Logistik, Zahlungsverkehr und Verwaltung still.

Die Anfälligkeit der Kritische Infrastruktur des 21. Jahrhunderts ist daher auch durch Kaskadeneffekte gekennzeichnet. Die Digitalisierung hat diese Entwicklung beschleunigt. IT- und OT-Systeme haben Kritische Infrastrukturen leistungsfähiger gemacht - und zugleich verwundbarer. Früher brauchte es physische Sabotage. Heute reichen digitale Zugänge aus der Ferne, um Abläufe zu manipulieren, Informationen zu verfälschen oder Anlagen stillzulegen.

Auch die Bedrohungslage hat sich verändert.

Zwar standen im Kalten Krieg ebenso Brücken, Staudämme, Kraftwerke und Kommunikationszentren im Fokus. Doch waren hier die Szenarien klar, die Bedrohung physisch und meist einem staatlichen Akteur zuzuordnen. Heute verschwimmen die Grenzen. Der russische Angriff auf die Ukraine zeigt, wie moderne Konflikte über klassische Militärschläge hinausgehen. Energieanlagen werden digital und physisch angegriffen, Kommunikationsnetze und Stromversorgung gleichzeitig. Ziel ist oft nicht allein Zerstörung, sondern die Schwächung staatlicher Handlungsfähigkeit und gesellschaftlicher Widerstandskraft.

Europa ist davon nicht ausgenommen. Die Sabotage der Nord-Stream-Pipelines machte klar: Auch komplexe Infrastrukturprojekte weitab klassischer Krisengebiete sind verwundbar. Cyberangriffe auf Energieversorger, Krankenhäuser, Wasserwerke und Behörden nehmen zu. Unterseekabel, Satellitensysteme und digitale Plattformen spielen heute eine ähnlich zentrale Rolle wie einst Eisenbahnlinien oder Seewege. Und die Schwelle für Angriffe ist gesunken. Neben Staaten agieren organisierte Kriminalität, ideologisch motivierte Gruppen oder einzelne Angreifer. Wobei diese nicht mal hochqualifiziert zu sein brauchen: Ein kleines Flugobjekt zu steuern, erforderte vor Jahrzehnten noch die Praxis geübter Modellflugzeug-Piloten - insbesondere bei Start und Landung. Heutige Drohnen übernehmen einen Großteil dieser Aufgaben selbst und machen aus einer fliegerischen Fähigkeit eine Softwarefunktion.

Die Herausforderung der kommenden Jahre liegt nicht allein darin, jeden Angriff zu verhindern. Entscheidend wird sein, Resilienz zu erhöhen, Redundanzen zu schaffen und Kaskadeneffekte beherrschbar zu machen. Spätestens an dieser Stelle kommt der händeringende Experten-Call, die Gesellschaft müsse endlich resilienter werden.

Nur leider ist für die Kritische Infrastruktur des 21. Jahrhunderts auch ihre Wahrnehmung in der Gesellschaft kennzeichnend: Sie wird stets als gegeben

vorausgesetzt. Strom kommt aus der Steckdose, Wasser auf dem Hahn, Sprit von der Tankstelle, omnipräsente W-Lan-Zugänge sind gefühltes Menschenrecht. Wer dagegen in den ärmsten Regionen der Welt lebt, ist es täglich gewohnt weite Wege zur nächsten Wasserstelle zu gehen, um zu überleben. In fast allen urbanen Zentren Europas wüsste der Großteil der Menschen nicht, wo der nächste Notwasserbrunnen steht. Und wenn er es wüsste, würde er es als Zumutung empfinden, wenn ihm eine ungewisse Zeit an Tagen bevorstünde, in der das gewohnte Selbstoptimierungsleben massiv gestört ist.

Wenn wir diesen Konsumentenanspruch als unveränderliche Variable akzeptieren, lassen sich zumindest weitere Appelle an die Gesellschaft zum Resilienzaufbau sparen. „Gesellschaft hat keine Adresse“ wusste Niklas Luhmann schon im 20. Jahrhundert. Wir können heute pointiert hinzufügen: Gesellschaft erwartet, dass jede Adresse online ist. Daher sollte der Resilienzaufbau besser fokussiert werden – auf den für Vorsorge und Bewältigung zuständigen Sicherheitsbereich unter Einbeziehung aller erforderlichen und bereitstehenden Akteure. Der Stromausfall im Südwesten Berlin im Januar 2026 zeigte welche großen Kapazitäten der Blaulichtorganisationen in der Krise notwendig waren, um einen dagegen prozentual kleinen Bevölkerungsanteil der Millionenmetropole zu versorgen. Hier werden auch Sicherheitsdienstleister mit einzubeziehen sein. Wir müssen davon ausgehen, dass sich solche Vorfälle jederzeit wiederholen werden und die Gefahr besteht, dass die zuständigen Ressourcen an ihre Grenzen kommen. Daher sollte das gemeinsame Vorgehen vor der nächsten Krise abgestimmt werden und nicht erst mittendrin.

Bildunterschrift: Die Zahl kritischer Infrastrukturen hat sich seit dem Römischen Reich etwa vervielfacht. Die Veränderungsgeschwindigkeit hat sich wiederum um den Faktor 20 erhöht. Die Zahl der Vernetzung und damit Abhängigkeiten wächst nicht linear, sondern nahezu quadratisch. -v-

G D C I M
GENOSSENSCHAFT FÜR DIGITALISIERUNG
CHALLENGE- & INNOVATIONSMANAGEMENT

**GEMEINSAM
STARK!**



**Das IKT- & CYBER
Kompetenzzentrum
für KMU und freie
Berufe**



WWW.GDCIM.COOP



Resilienz kritischer Infrastruktur ist eine Planungs- und Führungsaufgabe

CHRISTIAN PAGITSCH

Krankenhäuser, Energiezentralen, Verkehrsleitstellen, Produktionsanlagen und Rechenzentren zählen zu den Gebäuden kritischer Infrastruktur: Sie sichern zentrale Funktionen unserer Gesellschaft, und ihre bauliche und technische Struktur bildet die Grundlage für Prozesse, deren Unterbrechung weitreichende Folgen haben kann. Sie müssen kritische Funktionen auch unter außergewöhnlichen Belastungen aufrechterhalten und anschließend kontrolliert in einen stabilen Betriebszustand zurückkehren.

Genau an diesen Anforderungen zeigt sich, dass der klassische Sicherheitsbegriff zu kurz greift. Der Sicherheitsgedanke zielt darauf, Risiken vorab zu identifizieren, die Eintrittswahrscheinlichkeiten zu minimieren und damit das Schadensausmaß zu reduzieren – und meint dabei mehr als Cybersicherheit im engeren Sinn, die nur den Schutz von Informations- und Kommunikationssystemen vor unbefugtem Zugriff, Manipulation oder Ausfall bezeichnet. Sicherheit im umfassenden Sinn schließt daneben physische, bauliche und organisatorische Schutzmaßnahmen ein. Resilienz beschreibt darüber hinaus die Fähigkeit eines Systems, Störungen aufzunehmen, ihre Auswirkungen zu begrenzen und wesentliche Funktionen innerhalb definierter Zeiträume stabil zu halten.

Viele Voraussetzungen hierfür werden bereits in den frühen Planungsphasen geschaffen, in die Umfeld- und Gefahrenanalysen einfließen: bei der Wahl des Standorts, der Erschließung, des Tragwerks, der Brandabschnitte und Sicherheitszonierungen sowie der infrastrukturellen Ver- und Entsorgung. Werden sie erst während der Ausführung oder im Betrieb berücksichtigt, bleiben meist nur aufwendige Nachrüstungen und funktionale Kompromisse.

Dass Architektur die Widerstandsfähigkeit eines Gebäudes gegenüber äußeren Einwirkungen – seismischer, klimatischer oder manipulativer Art – grundsätzlich mitzudenken hat, gehört zum Berufsbild und ist etwa im DGNB-Kriterienkatalog als Querschnitts-

thema verankert. Der vorliegende Beitrag konzentriert sich auf einen Ausschnitt daraus: gezielt herbeigeführte Störungen, wo das Zusammenspiel von baulicher Struktur, technischer Infrastruktur und digitalen Systemen besondere Wichtigkeit erlangt.

Resilienz ist keine technische Zusatzleistung am Ende eines Projekts – sie ist eine strategische Planungsentscheidung und damit eine Führungsaufgabe. Wie sich diese Prinzipien planerisch konkret auswirken, lässt sich besonders deutlich am Beispiel von Rechenzentren zeigen.

Redundanz allein schafft noch keine Resilienz

Für Rechenzentren lässt sich die planerische Bedeutung von Redundanz anhand der EN 50600 oder Tier-Klassifizierung des Uptime Institute verdeutlichen. Letztere beschreibt vier Topologien der versorgungskritischen Standortinfrastruktur, unterschieden nach Kapazitäten, Verteilwegen und Wartungsmöglichkeiten. Konkrete Anforderungen an Perimeterschutz, Videoüberwachung oder Zutrittskontrolle sind dagegen nicht Bestandteil dieser Klassifizierung und verlangen ein entsprechendes Konzept, das sich aus den Schutzzielen des Betreibers sowie einer standortspezifischen Umfeld- und Gefahrenanalyse ableitet. Verfügbarkeit und Sicherheit sind damit zwei unterschiedliche Achsen. Resilienz verbindet beide und ergänzt sie um die Fähigkeit, den Betrieb im Störfall aufrechtzuerhalten oder zügig wiederherzustellen.

Die Qualität einer Redundanzstruktur bestimmt sich daher nicht allein durch die Anzahl ihrer Komponenten, sondern durch die räumliche Unabhängigkeit der Versorgungswege. Zwei Einspeisungen oder zwei USV-Systeme bilden etwa keine belastbare Redundanz, wenn beide über denselben Schacht oder dieselbe Gebäudeeinführung geführt werden. Für Rechenzentren mit erhöhtem Schutzbedarf sieht der IT-Grundschutz daher getrennte Trassen für redundanzgebende Leitungen sowie eigenständige



USV-Systeme für die beiden Versorgungswege vor. In der Praxis bedeutet das: die Sicherstellung von zwei unabhängigen Versorgungswegen, zwei räumlich getrennten Gebäudeeinführungen, zusätzlichen Brandabschnitten sowie Nutzungs- und Sicherheitszonierungen. Diese systemrelevanten Anordnungen müssen zum Beispiel im Grundriss und Tragwerkskonzept sowie allen anderen baurelevanten Konzepten von Anfang an vorgesehen werden – nachträglich lassen sie sich kaum oder nur mit erheblichem Aufwand einfügen.

NIS2 und NISG 2026 verbinden digitale und physische Resilienz

Die NIS2-Richtlinie schafft seit Januar 2023 einen gemeinsamen europäischen Rahmen für die Cybersicherheit wesentlicher und wichtiger Einrichtungen; in Österreich wird sie durch das NISG 2026 umgesetzt, das am 1. Oktober 2026 in Kraft tritt und die Aufsicht dem neu geschaffenen Bundesamt für Cybersicherheit im Bundesministerium für Inneres überträgt. Anbieter von Rechenzentrumsdiensten zählen im Sektor Digitale Infrastruktur zu den von NIS2 erfassten Einrichtungen – mit unmittelbaren Konsequenzen für ihre Architektur und Ausgestaltung. Für ihre Planung ergeben sich daraus konkrete Anforderungen. Übergeordnet relevant ist der All-Hazard-Ansatz des Art. 21 der Richtlinie. Er verlangt die Berücksichtigung aller relevanten Gefahrenarten – Betriebskontinuität, Wiederherstellung, Lieferkettensicherheit, Zugangskontrolle und physischer Schutz gelten als Teile eines gemeinsamen Risikomanagements. Physische und digitale Sicherheitsanforderungen können damit nicht länger unabhängig definiert und erst bei Inbetriebnahme zusammengeführt werden; sie müssen bereits in einem frühen Stadium der Projektentwicklung in ein gemeinsames Schutzkonzept übersetzt werden.

Diese regulatorische Verbindung von physischer und digitaler Resilienz hat unmittelbare Konsequenzen für die Planung. Gerade bei großmaßstäblichen Rechenzentrumsprojekten greifen Infrastrukturversorgung, redundante Anbindungen,

Abwärmenutzung, Verkehrserschließung und Sicherheitstechnik eng ineinander. Ihre Wechselwirkungen lassen sich deshalb nicht isoliert betrachten, sondern müssen bereits in frühen Projektphasen gemeinsam bewertet und koordiniert werden.

Wie komplex diese Aufgabe in der Praxis werden kann, zeigt das Datacenterprojekt der Schwarz-Gruppe in Lübbenau, für das ATP architekten ingenieure als Generalplaner tätig ist. Mit einem Investitionsvolumen von rund 11 Milliarden Euro handelt es sich um die größte Einzelinvestition in der Unternehmensgeschichte der Gruppe. Zugleich verfolgt das Projekt das erklärte Ziel, die digitale Souveränität Deutschlands zu stärken. Bei Vorhaben dieser Größenordnung wird deutlich, dass technische Verfügbarkeit, Sicherheit, Energieversorgung und betriebliche Anforderungen nur innerhalb einer durchgängigen Planungsstruktur sinnvoll aufeinander abgestimmt werden können. Integrale Planung schafft dafür die Voraussetzung, Abhängigkeiten früh zu erkennen und fachübergreifend zu bearbeiten.

Das Risiko liegt an den Systemverbindungsstellen

Gebäudeautomation, Energieverteilung, Kühlung, Zutrittskontrolle und technische Überwachung gehören zur Operational Technology (OT). Die internationale Normenreihe IEC 62443 – gemeinsam von der International Electrotechnical Commission und der International Society of Automation entwickelt – ordnet Gebäudeautomation ausdrücklich den OT-Umgebungen zu und hält fest, dass dort anders als in der IT nicht die Vertraulichkeit von Daten im Vordergrund steht, sondern Verfügbarkeit und Integrität – mit entsprechenden Konsequenzen für die Priorisierung von Schutzmaßnahmen.

Moderne Rechenzentren zum Beispiel nutzen zentrale Leitstände, digitale Plattformen und externe Fernwartungszugänge. Dadurch entstehen vielfältige Verbindungen zwischen baulicher Struktur, OT und IT – sicherheitsrelevant sind dabei auch Zugriffsrechte und betriebliche Abhängigkeiten. Bereits in

der Planung muss deshalb geklärt werden, welche Systeme betriebskritisch sind, welche Funktionen bei einem Teilausfall erhalten bleiben müssen und welche Systeme räumlich oder logisch zu trennen sind. Das verändert etwa Raumfolgen, Erschließungswege und die Lage technischer Zentralen.

Geteilte Verantwortung braucht klare Führung

Ein Generalplaner ersetzt keine Cybersicherheits-Abteilung und übernimmt nicht die Verantwortung für IT- oder OT-Sicherheit. Seine Rolle liegt vielmehr in der räumlichen, funktionalen und technischen Koordination jener Schnittstellen, an denen unterschiedliche Systeme und Zuständigkeiten zusammentreffen. Die Bauherrschaft definiert dafür verbindliche Schutzziele, IT- und Sicherheitsverantwortliche übersetzen sie in technische Anforderungen, Fachplaner integrieren sie in die Gebäudestruktur, Integratoren übernehmen Konfiguration und Inbetriebnahme, Hersteller verantworten die Sicherheit ihrer eigenen Produkte, Betreiber steuern Berechtigungen und Notfallorganisation im laufenden Betrieb. Dieses Modell geteilter Verantwortung funktioniert nur mit klaren Entscheidungswegen – ohne koordinierende Struktur entstehen Lücken zwischen Leistungsbildern und Zuständigkeiten, während einzelne Anforderungen formal erfüllt, im Zusammenspiel aber ungeprüft bleiben.

Integrale Planung kann diese Abhängigkeiten früh sichtbar machen – vorausgesetzt, Informationen aus allen Disziplinen lassen sich durchgängig und konsistent zusammenführen. Genau dafür setzt ATP architekten ingenieure seit 2010 auf Building Information Modeling (BIM): Architektur, Tragwerksplanung und Technische Gebäudeausrüstung inkl. der Gebäudeleittechnik werden in einem gemeinsamen Informationsmodell koordiniert. So lassen sich räumliche, technische und funktionale Wechselwirkungen früh erkennen und gemeinsam bewerten. Auf dieser langjährigen Praxis basiert die Koordination unterschiedlicher Gebäude kritischer Infrastruktur – von Krankenhäusern und Flughäfen bis

hin zu militärischen Anlagen. In der Datacenterplanung arbeiten dafür spezialisierte Teams in Wien, Zürich, Frankfurt, Krakau und Innsbruck standortübergreifend zusammen.

Entscheidend ist dabei die digitale Durchgängigkeit über den gesamten Lebenszyklus. Wie andere Assetklassen wird auch ein Rechenzentrum bei ATP architekten ingenieure nicht nur im Entwurf modelliert. Die strukturierte Datenbasis wird von Planung und Bau bis zu Betrieb, Wartung, Umbau und Weiterentwicklung fortgeführt. Informationen zu Bauteilen, technischen Anlagen, Versorgungspfaden und räumlichen Abhängigkeiten bleiben damit über Projektphasen hinweg verfügbar und nachvollziehbar. Gerade bei hochverfügbaren Infrastrukturen schafft diese Kontinuität eine wesentliche Grundlage für Wartung, Änderungsmanagement und spätere Eingriffe in den Bestand.

BIM unterstützt damit weit mehr als die geometrische Koordination. Die gemeinsame Datenumgebung bildet auch Systemgrenzen, betriebliche Anforderungen und relevante Abhängigkeiten ab. Versorgungswege, technische Zentralen, Sicherheitszonen und Wartungswege können dadurch im Zusammenhang betrachtet und über Planungsphasen hinweg konsistent weitergeführt werden.

Damit gewinnt auch die Qualität der zugrunde liegenden Daten sicherheitsrelevante Bedeutung. Entscheidend ist nicht allein das gemeinsame Modell, sondern dessen Governance: Wer darf Informationen lesen oder verändern? Wie werden Versionen und Freigaben dokumentiert? Welche Daten werden an Betreiber übergeben? Und wie bleibt ihre Verfügbarkeit langfristig gesichert? Erst wenn diese Fragen geklärt sind, wird digitale Durchgängigkeit zu einer belastbaren Grundlage für Planung, Betrieb und sicherheitsrelevante Entscheidungen über den gesamten Lebenszyklus eines Gebäudes hinweg.

Der integrale Planungsanspruch endet damit nicht bei der räumlichen Koordination der Fachdisziplinen. Er umfasst ebenso die Informations- und System-schnittstellen zwischen Gebäude, OT, IT und Betrieb.





Drei Entscheidungen, die später kaum korrigierbar sind

Erstens müssen kritische Funktionen und Abhängigkeiten früh identifiziert werden – anhand gemeinsamer Ausfallszenarien, die bauliche, technische, digitale und organisatorische Folgen zusammenführen. Zweitens müssen redundante Systeme funktional und räumlich unabhängig bleiben; der Grundriss wird damit unmittelbar zur Resilienzentscheidung. Drittens benötigen die Verbindungsstellen zwischen baulicher Struktur, OT und IT eine klare Governance, die bereits früh in der Planungsphase definiert ist – nicht nur für den Regelbetrieb, sondern auch für Wartung, Notbetrieb und Wiederherstellung. Diese Entscheidungen lassen sich nicht vollständig an einzelne Fachdisziplinen delegieren; die Bauherrschaft braucht dafür einen kompetenten Partner, der sie in die Lage versetzt, Schutzziele frühzeitig zu formulieren und sicherheitsrelevante Entscheidungen verantwortungsvoll zu treffen.

Fazit

Wer Resilienz erst im Betrieb behandelt, setzt viel zu spät an. Die entscheidenden Voraussetzungen entstehen bereits in der Planung: durch belastbare Versorgungstopologien, räumlich getrennte Redundanzen, klar definierte Systemgrenzen und eine eindeutige Zuordnung von Verantwortung. Integrale Planung ersetzt dabei weder IT- noch OT-Sicherheit. Sie schafft jedoch die räumlichen, technischen und organisatorischen Voraussetzungen, unter denen Sicherheitskonzepte wirksam werden können. Gerade an den Schnittstellen zwischen Gebäude, technischer Infrastruktur, OT, IT und Betrieb entscheidet sich, ob einzelne Schutzmaßnahmen tatsächlich zu einem resilienten Gesamtsystem zusammenwirken.

Resilienz kritischer Infrastruktur ist damit eine Planungs- und Führungsaufgabe: Schutzziele müssen früh definiert, Abhängigkeiten sichtbar gemacht und Verantwortlichkeiten über den gesamten Lebenszyklus hinweg eindeutig organisiert werden. -v-

Fußnoten

DGNB – Deutsche Gesellschaft für Nachhaltiges Bauen: DGNB-Kriterienkatalog, Resilienz als Querschnittsthema in der Gebäudeplanung. In Österreich vertreten durch die ÖGNI (Österreichische Gesellschaft für Nachhaltige Immobilienwirtschaft) als Systempartner.

Uptime Institute: Tier Standard: Topology. uptimeinstitute.com/tiers

Uptime Institute: Myths and Misconceptions Regarding the Uptime Institute's Tier Certification System. journal.uptimeinstitute.com

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Baustein INF.2 (Rechenzentrum sowie Serverraum).

Richtlinie (EU) 2022/2555 (NIS2), Art. 21 und Anhang I.

Republik Österreich: Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026), BGBl. I Nr. 94/2025, Inkrafttreten 1.10.2026.

igor'sLAB: „Schwarz-Gruppe startet Milliardenprojekt für neue Rechenzentrumsleistung in Lübbenau“, 18.11.2025.

IEC 62443 (International Electrotechnical Commission / International Society of Automation): Normenreihe zur Cybersicherheit von Industrial Automation and Control Systems (IACS) und Operational Technology.



ICHW
INTERNATIONALES
CYBER-HILFSWERK



WWW.CYBER-HW.ORG



Sicherheitspolitische und strategische Risikoana

JOHANNES GÖLLNER

Märkte entstehen und vergehen. Unabhängig vom Sektor stellt sich im strategischen Management immer wieder die Frage, wann sich Investitionsmöglichkeiten ergeben, wann sich Forschung auszahlt und wann sich Risiken aufbauen, die es zu vermeiden gilt. Deshalb ist es wichtig sich mit qualitäts-gesichertem Wissen über die globale bzw. unternehmerische Zukunft auseinander zu setzen.

Erfolgreiche Sicherheitspolitik und das Design von Sicherheitsstrategien für den öffentlichen und privaten Sektor –im globalen Kontext-, insbesondere bei der Entwicklung von zukunftsweisenden Konzepten zu Resilienz und zum Schutz kritischer Infrastrukturen, benötigt den offenen und unvoreingenommenen Gedankenaustausch aller Akteure einer Gesellschaft, der Politik, der Wirtschaft, der öffentlichen Verwaltung, sowie der Wissenschaft und der Forschung.

Die Diskussion der Komplexität und die Veränderung der Komplexität im Verlauf der Zeit sowie die Rückschlüsse aus dem Verhalten eines Systems oder Teilsysteme sind wesentliche Aspekte zur Generierung sicherheitspolitischer Konzepte und davon abgeleiteter Strategien von und für individuelle und kollektive soziale Akteure.

Die Diskussion und Entwicklung einer umfassenden und ganzheitlichen sicherheitspolitischen und strategischen Sichtweise im Sinne des Securitization-Konzepts¹, das societal security, political security, economical security, environmental security, public security, cyber security und space security umfasst, ist für ein Unternehmen das Fundament zur strategischen Risikoanalyse und diese wiederum die Grundlage zur Sicherstellung seiner Unternehmenssicherheit. Der Themenkomplex Cybersicherheit und Weltraumsicherheit, und deren globale Wechselwirkungen und Auswirkungen wurde vom Autor 2022 infolge des Entstehens neuer EU rechtlicher Grundlagen, wie die EU-directive NIS2 hinzugefügt, um gesamtheitliche Modellierung und Simulationen

für strategische und sicherheitspolitische Analysen für Unternehmen und andere Stakeholder ermöglichen zu können.

Verlässliches und qualitätsgesichertes Wissen über zukünftige Trends, Entwicklungen und über Trendbrüche sowie über innovative Lösungen und Methoden war immer schon relevant für das strategische Management und die [Neu]ausrichtung von [großen] Organisationen und Unternehmen. In den letzten 20 Jahren hat sich Foresight und Horizon Scanning zunehmend in der strategischen Planung und in der Transformation von großen Organisationen etabliert. In Zeiten von Big Data, künstlicher Intelligenz (ohne kognitive Fähigkeiten), medialen Filterblasen und zunehmend höher werdender Innovationsgeschwindigkeit stellt sich umso mehr die Frage nach zuverlässigem Wissen über Trends, Trendbrüche, sowie über zukünftige geschäftliche, unternehmerischen Optionen und Risiken. Im strategischen Management kann es nur zu leicht passieren, dass Investitionschancen und Transformationsrisiken verpasst werden.

Der Themenkomplex: Cyber Security, Space Security und Supply Chain Security und deren globale Wechselwirkungen sowie wirtschaftlichen, rechtlichen und politischen Auswirkungen, stellt unter anderem auch in Hinblick auf die neue EU NIS2-Richtlinie (12/2022), eine strategische und eventuell existentielle Diskussion für Unternehmen und Ihrer Produkte dar.

Die Diskussion der komplexen Zusammenhänge und permanenter Interaktionen wie z.B. zwischen „Space Security, Cyber Security und Supply Chain Security“ und die Einflüsse auf und durch die globalen sicherheitspolitischen Rahmenbedingungen sind mindestens für alle Unternehmen hoch relevant, um nicht zu sagen existentiell notwendig in der unternehmerischen Risikoanalyse – und -modellierung.

Anmerkung: Innovative sowie robuste Sicherheits-



lyse als Fundament für Unternehmenssicherheit

konzepte für die Wirtschaft und die Weltgemeinschaft zur Nutzung und Ökonomisierung des Weltraums durch private und staatliche Akteure sind von Nöten, da z.B. die weltraumbasierten kritischen Infrastrukturen (z.B. Satelliten für Informations- und Kommunikation, Navigation, Erdbeobachtung, etc) mittlerweile für das Funktionieren unserer Wirtschaft, der Logistik, Supply Chain, etc. existentiell und mittlerweile unverzichtbar sind.

Zukunftsdenken und Foresight in der strategischen Langfristplanung²

Historische Nachweise über die Verwendung von Zukunftsdenken und Zukunftsanalysen treten, soweit historische Quellen darauf hindeuten, erst relativ spät in der Menschheitsgeschichte in Erscheinung, wenn man einmal von Orakeln, Wahrsagern, Propheten und Magiern absieht. Es ist nicht verwunderlich, dass verschiedene Quellen darauf hindeuten, dass im Mittelalter, wo naturwissenschaftliche Debatten im Wettbewerb mit theologischen Diskursen standen, Zukunftsvorhersage methodenkritisch diskutiert wurde. Zu dieser Zeit waren geringe Abweichungen von „allgemeinakzeptierten Wahrheiten“ schon gefährlich, weil die gerade im Entstehen begriffenen staatlichen Institutionen ihre Legitimierung darauf aufbauten, dass ihre Bürger dieselben Anschauungen und Erwartungshaltungen vertraten. Auch heute noch zeigt sich in Diskussionen über Zukunftsszenarien, dass eine saubere Trennung zwischen Szenarien-Szenarienportfolios-Frameworkszenarien, Visionen, Ideologien und Glaubensparadigmen nicht immer einfach ist. Immerhin haben sich die Konsequenzen deutlich geändert.

Es ist deswegen nicht überraschend, dass besonders im Umfeld des amerikanischen Pragmatismus der wissenschaftliche Umgang mit Zukunftserwartungen im Fach „Future studies“ entstanden ist. Der deutsche Begriff Futurologie wurde 1943 von Ossip K. Flechtheim eingeführt. Eine umfangreiche

Darstellung der Entstehung der Zukunftsforschung würde den Rahmen dieses Artikels überschreiten. Einen Überblick über die klassische Zukunftsforschung gibt jedoch u.a. Rolf Kreibich (Kreibich, 2009).

Kreibich definiert Zukunftsforschung 2006 als „die wissenschaftliche Befassung mit möglichen, wünschbaren und wahrscheinlichen Zukunftsentwicklungen und Gestaltungsoptionen sowie deren Voraussetzungen in Vergangenheit und Gegenwart.“³ Diese Definition wird in der wissenschaftlichen Zukunftsforschung weitgehend akzeptiert, wobei ihre Wissenschaftlichkeit „in Abgrenzung zu zahlreichen pseudowissenschaftlichen Tätigkeiten wie ‚Trendforschung‘, ‚Prophetie‘ oder ‚Science Fiction‘ grundsätzlich allen Qualitätskriterien [unterliegt], die in der Wissenschaft an gute Erkenntnisstrategien und leistungsfähige Modelle gestellt werden: Relevanz, logische Konsistenz, Einfachheit, Überprüfbarkeit, terminologische Klarheit, Angabe der Reichweite, Explikation der Prämissen und der Randbedingungen, Transparenz, praktische Handhabbarkeit u. a.“

Typische Methoden der Zukunftsforschung sind z.B. Trendextrapolation und DelphiBefragung. Methoden, wie Roadmapping, Technikfolgen-Abschätzung und historische Analogie beschäftigen sich hauptsächlich mit der Zukunft von Technologien. Methoden wie Szenario-Analyse, Systemanalyse, Verflechtungsmatrix, Nutzwertanalyse, Relevanzbaum und Cross-Impact-Analyse beschäftigen sich mit Szenarien der Zukunft und deren Ausgestaltung. Neben Methode 635 und Synektik gibt es eine Reihe an Methoden in der Zukunftsforschung, die sich mit der Steigerung der Kreativität beschäftigen. Fantasie, Vorstellungsvermögen und Gestaltungswille sind unabdingbar von Nöten.

Die großen Herausforderungen des technisch-ökonomischen Wettbewerbs zwischen den Industriestaaten verlangen sowohl im Hinblick auf Chancennutzung als auch Gefahrenerkennung



immer dringlicher verlässliches Zukunftswissen und das Aufzeigen von Handlungsoptionen zur Zukunftsgestaltung.⁴

Auch wenn sich der Gebrauch des Wortes „Strategie“ schon relativ früh in der Menschheitsgeschichte nachweisen lässt (Sunzi⁵, Aeneas Tacticus⁶), so ist das dahinterliegende Konzept nach der heute üblichen Wortbedeutung ein neuzeitliches, welches ganz wesentlich von Clausewitz⁷ und im Weiteren von der Wissenschaftsdisziplin der Spieltheorie geprägt wurde. Üblicherweise wird unter strategischer Vorgehensweise⁸ die Fähigkeit zur geplanten und beabsichtigten Erreichung eines gewünschten Zustandes unter Verwendung aller verfügbaren Mittel verstanden.

CYBER-DEMOCRACY – CYBER DEVELOPMENT – CYBER DEFENCE:

„Digital verursachte Unfälle passieren häufiger, als wir denken. Wenn man technische Schlampeigkeiten wie bei CrowdStrike und gezielte Cyber-Angriffe auf Unternehmen oder Ministerien zusammenrechnet, dann haben IT-Ausfälle in Deutschland allein im Jahr 2022 einen Schaden von 206 Milliarden Euro verursacht.“⁹

Alle reden von Cybersicherheit, aber keiner tut was dafür. Das scheint derzeit allgemeine Wahrnehmung zu sein. Es fehlt nicht an Erkenntnissen und Experten, um zu wissen, was zu tun ist oder zu tun wäre. Sobald es darum geht die angemessenen Maßnahmen umzusetzen und Ressourcen bereitzustellen,

prallen sie oft am Festhalten an Gewohnheiten oder Handlungszwängen ab. So laden offenstehende Schwachstellen Hacker mit [organisierten] kriminellen Absichten und Energie zum Missbrauch ein. Seit den letzten Jahrzehnten erlebt der technische Fortschritt im Bereich der Computertechnik eine revolutionäre Entwicklung. Die ersten Großrechner in der Mitte des 20. Jahrhunderts füllten noch Räume mit einer Rechenleistung, die längst von unseren Smartphones in der Hosentasche übertroffen wird. Mit dem Aufkommen des Internets in den 1990er Jahren erfuhr die Welt eine grundlegende Veränderung in der Art und Weise, wie Menschen kommunizieren, Informationen austauschen und Geschäfte tätigen. Die ständige Weiterentwicklung von Netzwerktechnologien hat zu einer global vernetzten Gesellschaft geführt, die in Echtzeit Informationen austauscht. Effizienz und Produktivität steigerten sich in zahlreichen Branchen und neue Geschäftsmodelle und soziale Interaktionen entstanden, die zuvor undenkbar waren.¹⁰

Innovative Geschäftsmodelle (Smart Business Models) auf Basis von digitalen Technologien erobern stetig alle Bereiche der Privatwirtschaft und der öffentlichen Verwaltung. Gleichzeitig steigen im Einzelnen die Cyberrisiken und Supply Chain Risiken an. In Kombination können diese Ereignisbilder krisenhafte und möglicherweise auch katastrophale Zustände für Unternehmen, Unternehmenscluster und Staaten ein- bzw. annehmen.

Cybersicherheit: Berücksichtigung 2500 Jahre alten strategischen Denkens

Die Steigerung der digitalen Widerstandsfähigkeit und die Gewährleistung von Cybersicherheit in der digitalen Welt insgesamt sind für die Sicherheit eines Staates oder eines z.B. global agierendes Unternehmens von großer Bedeutung. Dies drückt sich beispielweise in der „Österreichischen Strategie für Cybersicherheit“ (ÖSCS) aus dem Jahr 2021 aus, wo als Vision die langfristige Schaffung eines sicheren Cyberraumes als Beitrag zur Steigerung der Resilienz Österreichs und der Europäischen Union durch einen gesamtstaatlichen Ansatz festgehalten ist. Strategien bzw. deren Umsetzung haben auch strategisches Denken potenzieller Mitbewerber/Gegner zu berücksichtigen. Die Herausforderungen der Cybersicherheit im strategischen Bereich machen insbesondere auch eine Auseinandersetzung mit dem eher wenig bekannten strategischen Gedankengebäude der im Werk „Kunst des Krieges“ dargelegten dreizehn Grundprinzipien, verfasst vermutlich um 500 v.Chr. durch einen chinesischen General namens Sun Tsu, lohnenswert; dies umso mehr, als diese Prinzipien an chinesischen Bildungseinrichtungen nach wie vor als aktuell gelten und dementsprechend gelehrt werden. Klar kommt die entscheidende Bedeutung der Sicherheit und damit in Verbindung die Bedeutung des Krieges zum Ausdruck: „Die Kunst des Krieges ist für den Staat von entscheidender Bedeutung. ... Deshalb darf sie unter keinen Umständen vernachlässigt werden.“ Heute ist dies wohl auf die umfassende Bedeutung dieser Begriffe zu beziehen. Gerade der Bereich der Kriegführung im Cyberraum folgt folgenden Gedanken: „In all deinen Schlachten zu kämpfen und zu siegen, ist nicht die größte Leistung. Die größte Leistung besteht darin, den Widerstand des Feindes, ohne einen Kampf zu brechen.“ Sun Tsu betont damit auch die grundsätzliche Überlegenheit der indirekten Strategie gegenüber der direkten Strategie. Die indirekte Strategie beruht vor allem auf

Täuschung und List, wobei hier konkrete Handlungsanweisungen gegeben werden: „Wenn wir also fähig sind anzugreifen, müssen wir unfähig erscheinen; wenn wir unsere Streitkräfte einsetzen, müssen wir unfähig scheinen; ... greife den Feind an, wo er unvorbereitet ist; tauche auf, wo Du nicht erwartet wirst.“ Als eine zentrale Forderung formuliert Sun Tsu die Notwendigkeit einer richtigen Beurteilung der gegnerischen und eigenen Mittel: „Wenn du den Feind und dich selbst kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten. ... Wenn du weder den Feind noch dich selbst kennst, wirst du in jeder Schlacht unterliegen.“¹¹

Die Diskussion und Erarbeitung einer umfassenden und ganzheitlichen sicherheitspolitischen Sicht im Sinne eines Security¹²-Konzeptes, welches Societal Security, Cyber Security, Space Security, Economical Security, Environmental Security, Political Security und Public Security umfasst, ist für jeden Staat, seinen Institutionen und Unternehmen existenziell notwendig.

Verlässliches und qualitätsgesichertes Wissen über zukünftige Trends, Entwicklungen und über Trendbrüche sowie über innovative Lösungen und Konzepten-Modellen-Methoden-Tools war immer schon relevant für das strategische Management und die [Neu]ausrichtung von [großen] Organisationen und Unternehmen.

In den letzten 20 Jahren hat sich Foresight und Horizon Scanning zunehmend in der strategischen Planung und in der Transformation von großen Organisationen etabliert. In Zeiten von Big Data, künstlicher Intelligenz, medialen Filterblasen und zunehmend höher werdender Innovationsgeschwindigkeit stellt sich umso mehr die Frage nach zuverlässigem Wissen über Trends, Trendbrüche, sowie über zukünftige geschäftliche Chancen und Risiken. Im strategischen Management kann es nur zu leicht passieren, dass Investitionschancen und Transfor-





mationsrisiken -somit- verpasst werden, und so z.B. krisenhafte Situationen in ganzen Wirtschaftssektoren entstehen können.

Im Spannungsfeld von Globalisierung, Digitalisierung und Automatisierung liegt das Interesse an einer holistischen Betrachtung der Verletzbarkeit der Supply Chain, der Value Chain und seiner Netzwerke (Basis-, Versorgungs- und Public Netzwerke) als Summe der primären- und Hilfsprozesse (insbesondere Lagerung und Transport von Waren, Informationen und Geld) unter Berücksichtigung der Einbettung in transnationale und internationale Versorgungssysteme (Energie, Rohstoffe, Lebensmittel, medizinische Verbrauchsgüter, Informationen, etc.), die durch politische, rechtliche, ökonomische, zivile, technische, sowie Natur- und Umweltereignissen - „man-made“ und „non man-made“ - zu Unterbrechungen und Engpässen in der Versorgung führen können.

In punkto strategischer Risikoanalyse im Themenkomplex: Digitalisierung und Cyber Security dehnt z.B. eine neue Richtlinie (NIS2-Richtlinie) ihre Reichweite aus, um mehr Sektoren und Unternehmen einzubeziehen. Sie führt auch detaillierte Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit, strengere Aufsichts- und Durchsetzungs- und Haftungsanforderungen sowie harmonisierte Sanktionen ein. Sie regelt die Cyber- und Informationssicherheit von Unternehmen und Institutionen. Bis Oktober 2024 hätten alle EU-Mitgliedsstaaten diese in nationales Recht überführen (transformieren) müssen.

Die NIS2-Richtlinie („The Network and Information Security (bzw. auf Deutsch Netzwerk und Informationssicherheit) (NIS) Directive“) wurde am 27.12.2022 im EU-Amtsblatt veröffentlicht und ist am 16.01.2023 in Kraft getreten. Sie regelt die Cyber- und Informationssicherheit von Unternehmen und Institutionen. Bis Oktober 2024 mussten die EU-Mitgliedsstaaten diese in nationales Recht übergeführt haben.

Die NIS2-Richtlinie zielt darauf ab, die Cybersicherheit in der gesamten Europäischen Union zu stärken, indem der Umfang der regulierten Sektoren und Einrichtungen erweitert wird und strengere Anforderungen eingeführt werden (Noack, 2023; Vogel & Ziegler, 2023; Lucini, 2023). Sie ersetzt die bisherigen Kategorien von Betreibern durch „wichtige“ und „wesentliche“ Einrichtungen, die in erster Linie anhand der Unternehmensgröße und nicht anhand von Entscheidungen der nationalen Behörden bestimmt werden (Sievers, 2021). Die Richtlinie führt neue Verpflichtungen und geänderte Verfahrensbedingungen ein, die sich auf zuvor ausgenommene Betreiber auswirken und eine Neubewertung derjenigen erfordern, die bereits unter die NIS 1 fallen. Die EU-Mitgliedsstaaten hatten bis zum 17. Oktober 2024 Zeit, ihre Gesetzgebung an die NIS2 anzupassen¹³. Die Richtlinie zielt darauf ab, einen kohärenteren regionalen Cybersicherheitsrahmen zu schaffen, der die fragmentierte Annahme der Vorgängerrichtlinie behebt und die Widerstandsfähigkeit der Mitgliedsstaaten erhöht (Noack, 2023)¹⁴.

Es wird erwartet, dass diese EU-Richtlinie die Cybersicherheitsmaßnahmen und die Meldepflichten für die betroffenen Sektoren -einschließlich Weltrauminfrastrukturen und deren Provider- weiter verschärfen wird.

Cyber Security, Space Security und Supply Chain Security und deren globale Wechselwirkungen und wirtschaftlichen, rechtlichen und politischen Auswirkungen, stellt unter anderem auch in Hinblick auf die neue EU NIS2-Richtlinie (12/2022), eine strategische und eventuell existentielle Diskussion für Unternehmen und Ihrer Produkte und Services dar.

Der Themenkomplex Cybersicherheit und Weltraumsicherheit, und deren globale Wechselwirkungen und Auswirkungen, muß in strategischen Unternehmensbeurteilungen und -planungen berücksichtigt werden, um gesamtheitliche Modellierung und Simulationen für strategische und sicherheits-

politische Analysen und Entscheidungsfindung für Unternehmen und andere Stakeholder ermöglichen zu können.

Erfolgreiche Sicherheitspolitik und das Design von Sicherheitsstrategien für den öffentlichen und privaten Sektor – im globalen Kontext –, insbesondere bei der Entwicklung von zukunftsweisenden Konzepten zu Resilienz (Robustheit) und zum Betrieb und Schutz kritischer Infrastrukturen (Supply Chain Networks), benötigt den offenen und unvoreingenommenen Gedankenaustausch aller Akteure einer Gesellschaft, der Politik, der Wirtschaft, der öffentlichen Verwaltung, sowie der Wissenschaft und Forschung.

Die Diskussion der Komplexität und die Veränderung der Komplexität im Verlauf der Zeit sowie die Rückschlüsse aus dem Verhalten eines Systems (Meta- bis Subsystem) sind wesentliche Aspekte zur Generierung sicherheitspolitischer Konzepte und davon abgeleiteter Strategien von und für individuelle und kollektive soziale Akteure.

Die Entwicklung von risikoreduzierenden Strategien und Resilienz-Strategien bedürfen Innovationen bei qualitativen und quantitativen Konzepten, Modellen, Methoden und Werksezeugen im Bereich Risk Assessment sowie Modeling und Simulation, um den Grad der erforderlichen Resilienz (Bevorratung, Eigenfertigung, Rohstoffselbstversorgung) auf staatlicher und unternehmerischer Ebene festzustellen.

Technologien im Supply Chain haben eine strategische Bedeutung als Backbone der Optimierung der Lieferketten um Effizienz, Sicherheit und Wirtschaftlichkeit zu gewährleisten.

Dazu sollen Technologien (z.B. DLT/Blockchain) oder Anwendungen für die Supply Chain Prozesse identifiziert werden, insbesondere die zur Synchronisation innerhalb und zwischen den Lieferketten, vom Rohstoff-Lieferanten bis zum Endkunden, erforderlich sind.

Intelligente Dienste erzeugen eine höhere Kundenzufriedenheit und verschaffen Unternehmen entscheidende Wettbewerbsvorteile. Vernetzte datenge-

triebene Systeme können dank Internet of Things (IoT) auch Sensoren, Maschinen und Fahrzeuge integrieren, große Mengen erfasster Daten über Big Data Techniken verarbeiten und mit Hilfe von Artificial Intelligence (AI) neue Erkenntnisse zum Nutzen des Menschen gewinnen. Das Finden von Lösungen zur sicheren Anwendung von Informations- und Kommunikationstechnologien und das zugehörige Risiko- und Krisenmanagement sind ein existentieller Bestandteil jeglicher Informations- und Kommunikationsinfrastruktur einer Organisation, unter Berücksichtigung von organisationsinternen und -externen handelnden Personen.

Zukunftsweisende Anwendungen bedürfen einer flexibel skalierbaren, hochverfügbaren und sicheren Infrastruktur. Neben der Cloud spielen dabei auch die Blockchain, Distributed Ledger Technologien (DLT) und dezentralisierte Speicherlösungen eine zunehmend wichtige Rolle. Sie können verteilte Systeme ohne zentrale Betreiber dank kryptografischer Verfahren gegen Angriffe von außen und innen schützen. Die darauf aufbauenden Anwendungen ermöglichen zum Beispiel fälschungssichere Aufzeichnungen entlang von Lieferketten, einen sicheren anonymen Datenaustausch, die Monetarisierung von Wirtschaftsgütern, selbstsouveräne Identitäten und vieles mehr.

Im Zusammenhang mit dieser Informationsgesellschaft ist die Digitale Souveränität ein wesentlicher Aspekt hinsichtlich der Eigenverantwortung und der Verfügungsvollmacht über die dabei entstehenden Informationen. Diese Autonomie einer natürlichen Person, einer juristischen Person und der Verwaltung eines Staates muss vom Gesetzgeber entsprechend berücksichtigt und über die rechtlichen Rahmenbedingungen sichergestellt werden. In diesem Zusammenhang ergibt sich die Schnittstelle zu einem Managementsystem. Ein Managementsystem muss sicherstellen, dass eine Organisation sowohl die gesetzlichen als auch moralisch-ethischen Grenzen und Rahmenbedingungen im Zusammenhang mit der Digitalen Souveränität innerhalb seiner Grenzen bestimmt.





Supply Chain Resilienz und Security Management und innovative Lösungsbeiträge für Unternehmen

Globalisierung, Digitalisierung und Automatisierung sind die Treiber für eine holistischen Betrachtung der Verletzbarkeit der Supply Chain und seiner Netzwerke (Basis-, Versorgungs- und Public Netzwerke) als Summe der primären- und Hilfsprozesse (insbesondere Lagerung und Transport von Waren, Informationen und Geld) -in Beziehung zum CYBER-Raum und -Events. Unter Berücksichtigung der Einbettung in transnationale und internationale Versorgungssysteme (Energie, Rohstoffe, Lebensmittel, medizinische Verbrauchsgüter, Informationen, etc.), die durch politische, rechtliche, ökonomische, zivile, technische, sowie Natur- und Umweltereignissen, „man-made“ und „non man-made“ zu Unterbrechungen und Engpässen in der Versorgung führen können, ist diese holistische Betrachtung die essentielle Grundlage zur Entwicklung von Strategien für Risikoreduktion und Resilienz-Design in der Supply Chain. ICT/CYBER-Ereignis-/Bedrohungsbilder, die zu Unterbrechungen und Engpässen in der regionalen, nationalen, supranationalen und internationalen Versorgung beitragen können sind in Korrelation zu Supply Chain Unterbrechungen in das Risk Assessment mit einzubinden.

Die Schäden infolge Supply Chain Unterbrechungen können sehr vielfältig sein. Bei der Gestaltung finanzieller Diskussionen über Verluste aufgrund von Lieferkettenrisiken ist es wichtig, die betrieblichen Auswirkungen einer Störung und die damit verbundenen finanziellen Auswirkungen zu analysieren. Zu den zu untersuchenden Bereichen gehören ¹⁵:

- Produktionsstopp oder -verlangsamung: Direkte Verluste entstehen, wenn Produktionslinien stillgelegt werden müssen, weil wichtige Komponenten oder Inputs nicht verfügbar sind. Die täglichen Kosten einer angehaltenen Produktionslinie sind die offensichtlichsten Kosten, aber es können auch andere damit verbundene

Kosten anfallen.

- Höhere Frachtkosten: Um Ausfallzeiten zu reduzieren, können Vormaterialien oder sogar Fabrikaurüstung eingeflogen werden, dies ist jedoch mit Kosten verbunden.
- Umsatzeinbußen: Längere Unterbrechungen bei bestehender Marktnachfrage können zu Umsatzeinbußen führen.
- Verlust von Marktanteilen: In einigen Branchen können Umsatzeinbußen zu einem Verlust von Marktanteilen führen, wenn das Produkt eines Mitbewerbers als ebenso gut oder besser eingestuft wird.
- Reputation: Das Reputationsrisiko ist schwer zu messen, aber wichtig, da die Kundenerwartungen an Service und Umweltschutz steigen. Selbst wenn die Ursache einer Störung unvermeidbar ist, wird von Unternehmen erwartet, dass sie bestimmte Dinge getan haben, um sich auf Störungen vorzubereiten und darauf zu reagieren. Unternehmen, die sich darin auszeichnen, können ihren Ruf verbessern, indem sie als letzte schließen und als erste öffnen.

Jedes Unternehmen befindet sich in einer Lernphase, wenn es darum geht, für jedes Glied seiner Lieferkette das richtige Gleichgewicht zwischen Agilität und Redundanz zu finden. Diejenigen, die als erste die Lösung finden, werden als Branchenführer hervorgehen.

Digitale Technologien -im Einsatz entlang dem Supply und Value Chain- haben zunehmend eine strategische Bedeutung als Backbone der Optimierung der Lieferketten, um Effizienz, Sicherheit und Wirtschaftlichkeit zu gewährleisten. Der Beachtung der Nachhaltigkeit der Supply Chain (ökologische, ökonomische- und soziale Aspekte, als Abkehr vom 1 Kriterium Konstruktionsprinzip der minimal möglichen Kosten) und damit der Kreislaufwirtschaft (Circular Economy) sowie steady state economy ist ein weiterer wichtiger und integrierter Bestandteil von risikoreduzierenden

Strategien und Resilienz Strategien für physische und digitale Supply und Value Chains.

Ein umfassendes und ganzheitliches Cyber Security & Supply Chain Resilience (Security) Monitoring, Rating und Auditing Konzeptes ist in einem Unternehmen unabdingbar, weil Cyber Events (weltweit: 34%; AT: 40%; GE: 40%; CH: 57%) und Supply Chain Interruptions-Betriebsunterbrechungen (weltweit: 34%; AT: 32%; GE: 46%; CH: 41%) zu den 10 weltweit größten Risiken¹⁶ gehören.

Bereits 2018 hat das NCSC-National Cyber Security Centre, U.K. den thematischen Zusammenhang zwischen Supply Chain Security und Cyber Security in seinen „Supply Chain Security: 12 Principles“^{17, 18} dokumentiert und veröffentlicht, wie folgt:

- Understand the risks
- Principle 1: Understand what needs to be protected and why
- Principle 2: Know who your suppliers are and build an understanding of what their security looks like
- Principle 3: Understand the security risk posed by your supply chain
- Establish control
- Principle 4: Communicate your view of security needs to your suppliers
- Principle 5: Set and communicate minimum security requirements for your suppliers
- Principle 6: Build security considerations into your contracting processes and require that your suppliers do the same
- Principle 7: Meet your own security responsibilities as a supplier and consumer
- Principle 8: Raise awareness of security within your supply chain

- Principle 9: Provide support for security incidents
- Check your arrangements
- Principle 10: Build assurance activities into your approach to managing your supply chain
- Continuous improvement
- Principle 11: Encourage the continuous improvement of security within your supply chain
- Principle 12: Build trust with suppliers

Deshalb reagieren die nationalen Gesetzgeber, wie z.B. Deutschland, mit dem Lieferkettensorgfaltspflichtengesetz, welches 1. Januar 2023 in Kraft getreten ist und auch mögliche Auswirkungen auf österreichische und globale Zulieferanten Auswirkungen haben könnte bzw. hat. Das Gesetz regelt z.B. unter anderem die unternehmerische Verantwortung und Haftung für die Einhaltung von Menschenrechten in den globalen Lieferketten.

Der supranationalen Gesetzgeber (EU) reagiert -wie bereits vorhin beschrieben- darauf mit zum Beispiel der EU NIS2-Directive (Directive (EU) 2022/2555¹⁹ of the European Parliament and of the Council of 14 December 2022), welche auch ab 18.10.2024 in Deutschland, Österreich und allen EU-Mitgliedschaften für spezifische KMU (wesentliche und wichtige Einrichtungen) gelten sollten. Betroffen sind KMU, welche sogenannte wesentliche oder wichtige Einrichtungen und dem Kriterienkatalog dieser EU-Directive entsprechen. Das wesentliche ist, daß zum ersten Mal Cyber Security mit Supply Chain Security (IT-Supply Chain, Tier 1) und zugehörigen Krisenmanagement und Business Continuity Management kombiniert werden, und welche bei der Auditierung nach ISO 27001 in Korrelation mit anderen Standards abgefragt werden müssen. Bei den wichtigen Einrichtungen der „Abfallbewirtschaftung“ werden indirekt, möglicherweise auch KMU der Kreislaufwirtschaft (Circular Economy) adressiert (Anmerkung: Autor).





Die Risikomanagementmaßnahmen (Cybersecurity risk-management measures), gemäß Artikel 21 Abs (2) der NIS2-Directive (EU) 2022/2555 müssen auf einem gefahrenübergreifenden Ansatz „All-hazard-approach“ beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen²⁰:

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
- Bewältigung von Sicherheitsvorfällen;
- Aufrechterhaltung des Betriebs (business continuity), wie Backup-Management und Wiederherstellung nach einem Notfall (disaster recovery), und Krisenmanagement (crisis management);
- Sicherheit der Lieferkette (supply chain security) einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
- Konzepte und Verfahren für den Einsatz von

Kryptografie und gegebenenfalls Verschlüsselung;

- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Die internationale Standardisierung, vertreten durch NSA²¹ (Nato Standardization Agency, Brüssel) und ISO (International Organisation for Standardization, Genf), haben bereits 2004 bzw. 2007 mit der Herausgabe von Critical Infrastructure und Supply Chain Security-Standards²² (Regelwerken) -reagiert bzw. herausgegeben und die Relevanz damit mehr als dokumentiert, unabhängig davon, ob der Inhalt dieser als Wissensanleihe in Unternehmen, speziell in global agierenden Industrieunternehmen, angewendet oder nicht angewendet werden oder wurden.

Solche internationalen und nationalen Standards sind, zum Beispiel für²³:

- Risikomanagement:
- ISO 31000:2018 (1. Fassung: 2009)
- DIN EN IEC 31010 VDE 0050-1:2024-12 (1. Fassung: 2010-11)
- Supply Chain Security Management:
- ISO 28000 (Specification for security management systems for the supply chain), First edition: 2007-09-15; aktueller Stand: ISO 28000:2022; Revision in Vorbereitung.

- ISO 28001 (Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans Requirements and Guidance), First edition 2007-10-15
- ISO 20858 (Ships and marine technology — Maritime port facility security assessments and security plan development), First edition 2007-10-15; aktueller Stand: ISO 28000:2012
- Krisenmanagement:
- ISO 22361 (Security and resilience — Crisis management — Guidelines), First edition 2021-11-05; aktueller Stand: ISO 22361:2022
- Business Continuity Management
- ISO 22301 (Security and resilience – Business continuity management systems – Requirements, the International Standard for implementing and maintaining effective business continuity plans, systems and processes), First edition 2019²⁴
- ÖNORM EN ISO 22313:2020 (Sicherheit und Resilienz - Business Continuity Management Systems - Anleitung zur Verwendung von ISO 22301 (ISO 22313:2020))
- ÖNORM EN ISO 22301:2020 (Sicherheit und Resilienz - Business Continuity Management System – Anforderungen) & ÖNORM EN ISO 22301/A1:2024 (Sicherheit und Resilienz - Business Continuity Management System - Anforderungen - Änderung 1: Änderung der Klimaschutzmaßnahmen)²⁵

Die Strategische und operationelle Risikomodellierung und -analysis von CYBER/Supply Chain Resilience-Produkte- und Service-Lösungen -insbesondere für Klein- und Mittelbetrieben (KMU)- ist mittlerweile für sehr viele Unternehmen -heute und in Zukunft- von strategischer und existentieller

Relevanz und Bedeutung, und nicht nur seit CORONA und dem UKRAINE-Konflikt -sei angemerkt-.

FAZIT

Die Entwicklung von risikoreduzierenden Strategien und Resilienz Strategien für physische und digitale Supply und Value Chains und Verbindung mit deren Supply Chain Networks (Strategische [Kritische Infrastrukturen] Infrastrukturen) bedürfen Innovationen bei qualitativen und quantitativen Konzepten, Modellen, Methoden und Werkzeugen im Bereich Risk Assessment sowie Modeling und Simulation, um den Grad der erforderlichen Resilienz der Supply und Value Chain (z.B. Bevorratung, Eigenfertigung, Rohstoffselbstversorgung) auf staatlicher und unternehmerischer Ebene festzustellen, um zur Strategie- und Produkt-Entwicklung beitragen zu können.

Das strategische Management -der Vorstand, die Aufsichtsräte sowie Unternehmenseigentümer und Investoren haben zur Beantwortung der z.B. der Fragen, wann sich Investitionsmöglichkeiten ergeben, wann sich Forschung auszahlt und wann sich Risiken aufbauen, die es zu vermeiden gilt, unternehmerische organisationale Kompetenzen in Ihren Unternehmen aufzubauen, damit sie ihre entsprechenden unternehmerischen Optionen- Entscheidungen treffen können und im Unternehmen Handlungsfähigkeit (Resilienz) in einer global fragiler werdenden Welt sicherstellen können.

Deshalb ist es Wichtig sich mit qualitätsgesichertem Daten, Informationen und Wissen – unterstützt durch Risikoanalyse als mindestens zeitgleichen Prüfprozess - über die globale bzw. unternehmerische Zukunft, im Sinne einer strategischen Langfristplanung und der damit verbundenen Capacity Building auseinander zu setzen. -v-





IT-Governance: Zwischen Pflicht und Überlebensnotwendigkeit

RALF KIMPEL

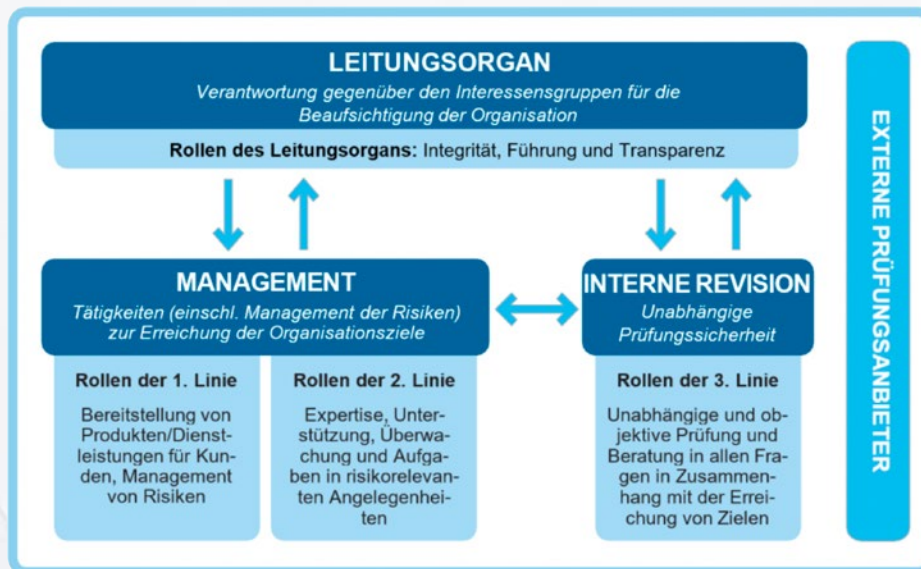
Stellen Sie sich vor: Ein international tätiger Mittelständler wird über Nacht lahmgelegt – sämtliche Systeme verschlüsselt, Daten unzugänglich, das Telefon klingelt unaufhörlich. Der IT-Leiter erkennt schnell: Ein gezielter Ransomware-Angriff hat nicht nur die Produktion, sondern auch den Vertrieb und die komplette Lieferkette stillgelegt. Lösegeldforderungen und die Angst vor Datenleaks setzen das Management unter Druck. In diesem Moment wird deutlich: IT-Governance ist keine lästige Pflichtübung, sondern das Sicherheitsnetz, das im Ernstfall das Überleben des Unternehmens sichert.

Die digitale Transformation hat in den vergangenen Jahren nicht nur Geschäftsmodelle revolutioniert, sondern auch die Bedrohungslage für Unternehmen dramatisch verschärft. Cyberangriffe, regulatorische Anforderungen, Datenfluten und immer komplexere IT-Landschaften zwingen das Unternehmen zu handeln. Wer heute noch glaubt, IT-Governance sei nur ein bürokratisches Pflichtprogramm, irrt gewaltig. Sie ist längst ein entscheidender Faktor für Überleben, Wettbewerbsfähigkeit und Reputation von Unternehmen.

Ein weiteres Beispiel: In einem großen deutschen Verkehrsunternehmen offenbaren forensische Analysen nach einem Angriff mit Schadsoftware, dass sich die Angreifer bereits seit Monaten unbemerkt im System aufhielten. Erst nach dem geplanten Wechsel auf eine cloudbasierte Lösung würden gravierende Sicherheitslücken entdeckt werden können – zu spät, die Schadenshöhe geht in die Millionen. Hier zahlt sich eine vorausschauende und konsequent gelebte IT-Governance aus, die regelmäßig Risiken bewertet und Gegenmaßnahmen einleitet.

Governance als Fundament der Unternehmenssteuerung

Das in der Welt der Internen Revisoren anerkannte 3-Linien-Modell beschreibt, wie ein funktionsfähiges und wirksames Steuerungs- und Überwachungssystem in Unternehmen aussehen kann. Es zeigt die Zuordnung der verschiedenen Rollen und Aufgaben in drei „Verteidigungslinien“: in der ersten Management-Linie werden Produkte/Dienstleistungen bereitgestellt und die damit verbundenen Risiken gesteuert. In der zweiten Management-Linie unterstützen und überwachen Funktionen wie Compliance, Datenschutz und ein zentrales Risikomanagement die erste Linie. Die dritte Linie unterstützt die interne Revision durch unabhängige und objektive Prüfungs- und Beratungsleistungen beim Erreichen der Unternehmensziele – einschließlich der Risikomanagementziele:



IT-Governance fügt diesem Modell eine neue Dimension hinzu: Sie sorgt dafür, dass IT-Ressourcen, Prozesse und Systeme nicht Selbstzweck sind, sondern konsequent auf Unternehmensziele

einzuwirken. Oder um es mit der Definition des Gabler-Wirtschaftslexikons zu sagen: IT-Governance ist der Ordnungsrahmen, der sicherstellt, dass IT nicht nur funktioniert, sondern Mehrwert schafft – sicher, effizient und compliant.

Warum IT-Governance gerade jetzt überlebenswichtig ist

Die Bedrohungslage hat sich in den letzten Jahren dramatisch zugespitzt:

- Komplexität der IT-Systeme: Heterogene Systeme, Cloud-Lösungen, Legacy-Infrastrukturen und hybride Architekturen fordern eine Governance, die flexibel und adaptiv ist.
- Cyberangriffe: Kriminelle nutzen zunehmend KI-gestützte Angriffsmethoden. Schutzstrategien müssen kontinuierlich nachgeschärft werden.
- Datenflut: Die Verarbeitung und Sicherung großer Mengen personenbezogener Daten (pD) stellt Unternehmen vor massive organisatorische und technische Herausforderungen.
- Regulatorischer Druck: Gesetze wie NIS-2, DORA oder das deutsche Lieferkettensorgfaltspflichtengesetz erhöhen die Anforderungen an Compliance und Transparenz – oft mit empfindlichen Sanktionen bei Verstößen.

Die Botschaft ist klar: Wer IT-Governance vernachlässigt, riskiert nicht nur Sicherheitslücken, sondern auch Haftungsfälle, Reputationsschäden und im schlimmsten Fall den Fortbestand des Unternehmens.

Modelle und Standards: Orientierung im Dschungel

Um diesen Herausforderungen zu begegnen, haben sich in der Praxis verschiedene Modelle bewährt, zum Beispiel:

- COBIT bietet ein Rahmenwerk für IT-Governance

und Risikomanagement.

- ISO/IEC 27000 fokussiert auf Informationssicherheit.
- ITIL definiert Best Practices für IT-Service-Management.
- ISO/IEC 38500 richtet sich an die Unternehmensführung und legt Grundsätze für IT-Governance fest.

Entscheidend ist weniger, welchem Modell man folgt, sondern dass Governance nicht als Einmalprojekt verstanden wird, sondern als kontinuierlicher Verbesserungsprozess. Reifegradmodelle können dabei helfen, Fortschritte sichtbar zu machen.

Praxis bei Hubert Burda Media: dezentral erfassen, zentral überwachen

Am Beispiel Hubert Burda Media wird im Folgenden verdeutlicht, wie IT-Governance in einem internationalen Konzern praktisch umgesetzt werden kann:

- Regelwerk: Konzernrichtlinien, Prozessvorgaben und Detailanweisungen schaffen einen verbindlichen Rahmen, der laufend angepasst wird.
- Klare Zuständigkeiten: Vom Compliance Board über ein Data Governance Board bis hin zum CISO (Chief Information Risk Officer) sind Verantwortlichkeiten klar definiert.
- Dezentrale Erfassung: Geschäftsbereiche identifizieren eigenständig ihre kritischen Anwendungen und Risiken.
- Zentrales Monitoring: Ein konzernweites System konsolidiert die Informationen, überwacht Risiken und integriert diese in das GRC-System.

Bei der Gestaltung der IT-Governance von Burda sind verschiedene Standards eingeflossen, insbesondere die ISO 27000.

Die zentralen Vorgaben werden über Konzern-Richt-



linien zur IT kommuniziert, die für alle Tochtergesellschaften verbindlich sind. Dabei wird nach Adressaten

Konzernrichtlinien	Adressaten
Informationssicherheit (Leitlinie)	Alle Mitarbeitenden
Nutzung von IT- und Kommunikationssystemen	Alle Mitarbeitenden
Informationssicherheit für IT-Services	Interne IT
Informationssicherheit & externe Dienstleister	Management, das externe Dienstleister einsetzt
Richtlinie für externe Dienstleister	Externe Dienstleister

unterschieden:

Mit der Leitlinie zur Informationssicherheit werden die grundlegende Verantwortung und Organisation, Aufgaben, Ziele und Strategie sowie das Richtlinienkonzept der Informationssicherheit bei Burda festgelegt.

Die Konzernrichtlinie Nutzung von IT- und Kommunikationssystemen (ITK) regelt die Grundsätze der dienstlichen Nutzung von ITK durch Burda-Mitarbeitende für alle Gerätekategorien (z. B. Arbeitsplatzrechner, mobile Endgeräte, Workstation) („IT-Systeme“).

Sie richtet sich außerdem an Mitarbeitende, die eine Rolle in der Informationssicherheitsorganisation bzw. in der IT innehaben. Für die interne IT und für externe IT-Dienstleister existieren zusätzliche Vorgaben (Konzernrichtlinie Informationssicherheit für IT-Services bzw. Richtlinie für externe Dienstleister).

Aufgrund der dezentralen Verantwortung für geschäftsbereichsspezifische IT ist eine lokale Erfassung geschäftskritischer Anwendungen unter Einbindung zentraler Instanzen wie den Konzern-Datenschutz notwendig:

- Dezentrale Systeme zur Erfassung und

- Risikobewertung digitaler Assets (z. B. über MS Forms) durch die User im jeweiligen Geschäftsbereich
- Ausgenommen: Standard-Software-Produkte, die von der zentralen IT bereitgestellt werden (z. B. MS O365)
 - Schnittstellen wie Datenschutz, Informationssicherheit oder Betriebsrat werden automatisch informiert

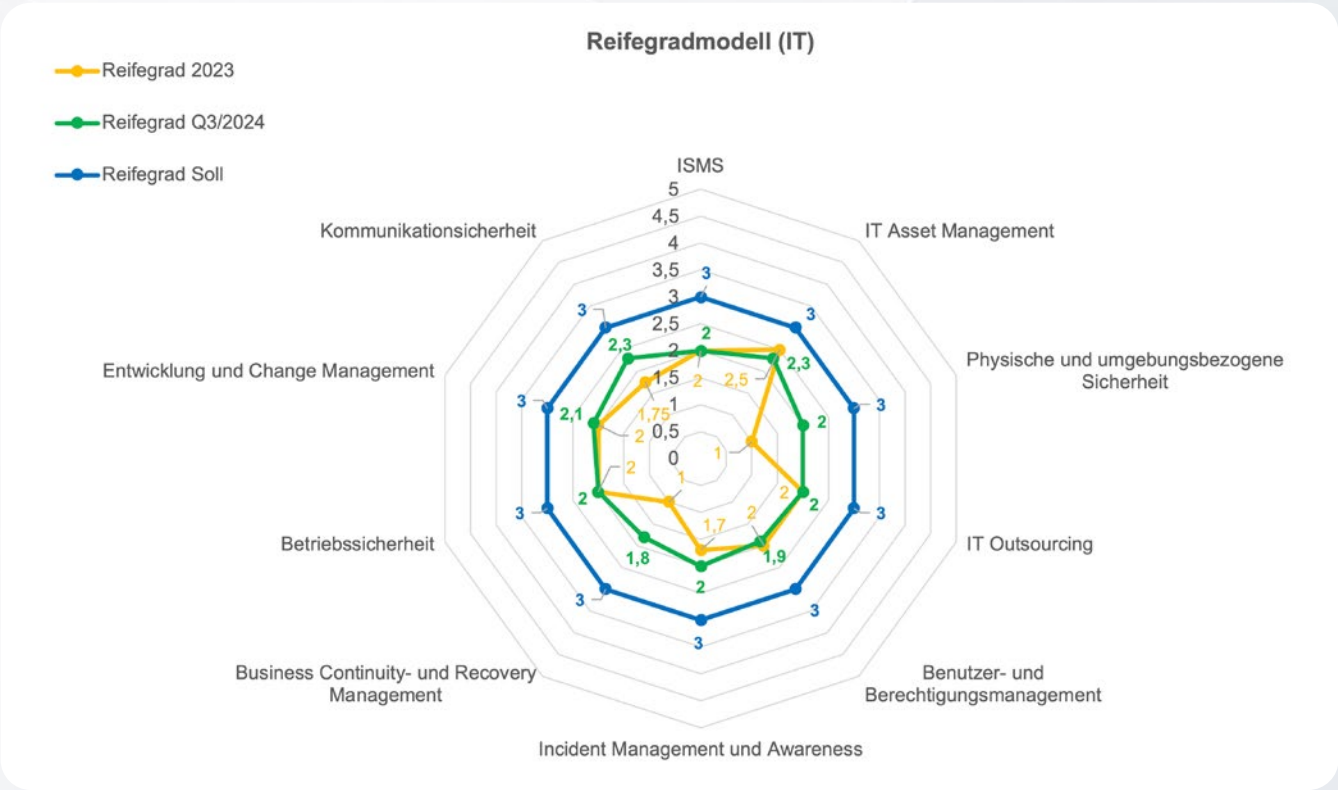
Vor diesem Hintergrund ist ein zentrales Monitoring digitaler Assets aus Konzernsicht notwendig. Digitale Assets, die aus Konzernsicht geschäftskritisch sein könnten, werden daher entsprechend der Bewertung des Schutzbedarfs und der IT-/Informationssicherheitsrisiken in ein zentrales System und Monitoring überführt.

Wesentliche IT-/Informationssicherheitsrisiken werden darüber hinaus in das unternehmensweite Risikomanagementsystem übernommen, um in der Geschäftsführung ein möglichst vollständiges Risiko-Lagebild zu geben.

Diese Kombination aus dezentraler Verantwortung und zentraler Überwachung stellt sicher, dass möglichst kein Risiko übersehen wird, gleichzeitig aber die Eigenverantwortung der Geschäftsbereiche erhalten bleibt.



Die Interne Revision prüft regelmäßig den Reifegrad der Informationssicherheit und vereinbart mit den Geprüften auf Basis der Ist-Analyse das Ziel- bzw. den Soll-Reifegrad und mit welchen Maßnahmen dieses erreicht werden soll. Der Reifegrad kann exemplarisch wie folgt abgebildet werden:



Chancen durch robuste IT-Governance

Eine gute Governance ist nicht nur ein Schutzschild, sondern auch ein Hebel für Wertschöpfung:

- Effizienzsteigerung: Klare Prozesse und abgestimmte IT-Strategien senken Kosten und erhöhen Synergien.
- Rechtssicherheit: Standards und Richtlinien minimieren Haftungsrisiken.
- Innovation: Governance schafft Freiräume für Digitalisierung, KI-Einsatz und neue Geschäftsmodelle.
- Resilienz: Durch präventives Risikomanagement werden Bedrohungen frühzeitig erkannt und Schäden reduziert.

Kurz: Governance macht Unternehmen nicht langsamer, sondern schneller, sicherer und zukunftsfähiger. -v-



Supply Chain Resilienz Management und „NIS 2 – die neue Cybersecurity Richtlinie“ der Europäischen Union

JOHANNES GÖLLNER

Globalisierung, Digitalisierung und Automatisierung sind die Treiber für eine holistische Betrachtung der Verletzbarkeit der Supply Chain und ihrer Netzwerke (Basic-, Supply- und Public Networks) in Beziehung zum CYBER-Raum und zu Cyber-Events. Unter Berücksichtigung der Einbettung in transnationale und internationale Versorgungssysteme (Energie, Rohstoffe, Lebensmittel, medizinische Verbrauchsgüter, Informationen, etc.), die durch politische, rechtliche, ökonomische, zivile, technische sowie Natur- und Umweltereignisse, „man-made“ und „non man-made“, zu Unterbrechungen und Engpässen in der Versorgung führen können, ist eine holistische Betrachtung die essentielle Grundlage zur Entwicklung von Strategien für Risikoreduktion und Resilienz-Design in der Supply und Value Chain und ICT/CYBER Security. ICT/CYBER-Ereignis-/Bedrohungsbilder, die zu Unterbrechungen und Engpässen in der regionalen, nationalen, supranationalen und internationalen Versorgung bzw. Lieferkette beitragen können, sind in Korrelation zu Supply Chain Unterbrechungen in das Risk Assessment mit einzubinden.

Infolge von digitalen Innovationen, zum Beispiel im Bereich Robotik, Language und Artificial Intelligence, neuer plattformökonomischer Geschäftsmodelle (Smart Businesses, Smart Products und -Services), werden Themen wie das Bewusstsein für Risiken, technische und strategische Gestaltungsoptionen sowie innovative Konzepte zur Sicherstellung von Rechtskonformität aufgezeigt und weiterentwickelt, um für Konsumenten sowie für die Unternehmen Handlungsfähigkeit und Sicherheit zu gewährleisten.

Weiterhin müssen Maßnahmen erarbeitet und priorisiert werden, um die Risiken zu bewältigen, die mit der Digitalisierung und/oder geopolitischen Ereignissen einhergehen und verbunden sind. Die notwendigen Maßnahmen und deren Umfang zur Risikobewältigung sind natürlich individuell verschieden und müssen aus dem Unternehmenskontext, der Risikotoleranz, der Strategie sowie dem Anspruch auf Handlungsfähigkeit abgeleitet werden.

Dafür werden hinreichend transparente und quantitative, belastbare Informationen sowie sehr viel Expertise benötigt.

Digitalisierung ist einer der zentralen Transformationsprozesse in der Wirtschaft, in dem für Cybersecurity wichtige Themen reguliert werden, um Risiken zu vermindern sowie Resilienz (Robustheit) zu erhöhen und gleichzeitig digitale Souveränität einzufordern. Die Aufrechterhaltung der Handlungsfähigkeit einer Organisation/eines Unternehmens ist das Gebot der Stunde – mehr denn je.

Zum Beispiel verarbeitet Data Science enorme Datenmengen, und mit Künstlicher Intelligenz erhofft man sich Tools, um komplexe Probleme bzw. Situationen zu beherrschen bzw. effizienter und effektiver bearbeiten und verarbeiten zu können. Damit verbunden sind Ereignisbilder bzw. Risiken wie enorme Steigerungen des Energieverbrauchs, um den Betrieb der dafür notwendigen Rechen- und Datenzentren sicherstellen zu können. Auch der Themenkomplex Cyber Security, Space Security und Supply Chain Security und deren globale Wechselwirkungen sowie wirtschaftliche, rechtliche und politische Auswirkungen stellt, unter anderem auch im Hinblick auf die neue EU-NIS2-Richtlinie (12/2022) und die nationalen Umsetzungsgesetze z. B. in Deutschland und Österreich (5.12.–6.12.2025), eine strategische und eventuell existenzielle Diskussion für Unternehmen und ihre Produkte dar. Mittlerweile werden erste Tests zum Errichten und Betreiben von Datacentern im Orbit durchgeführt – Science-Fiction oder in Bälde Realität. Deutschland plant z. B. den Aufbau eines eigenen, souveränen militärischen Satellitennetzwerks, das oft als „deutsches Starlink“ bezeichnet wird. Dazu haben sich für dieses Großprojekt die Unternehmen Airbus, Rheinmetall und der Bremer Raumfahrtkonzern OHB zusammengeschlossen.

Die geopolitische Lage macht eine Neuorganisation der Wirtschafts-/Industriestruktur notwendig, und Risiken müssen angesichts komplexer, langfristiger

Abhängigkeiten und dominanter Plattformen (neu) bewertet und (re-)strukturiert werden.

Erfolgreiche Sicherheitspolitik und das Design von Sicherheitsstrategien für den öffentlichen und privaten Sektor – im globalen Kontext –, insbesondere bei der Entwicklung von zukunftsweisenden Konzepten zu Resilienz und zum Schutz kritischer Infrastrukturen, benötigt den offenen und unvoreingenommenen Gedankenaustausch aller Akteure einer Gesellschaft: der Politik, der Wirtschaft, der öffentlichen Verwaltung sowie der Wissenschaft und der Forschung.

Die Diskussion der Komplexität und die Veränderung der Komplexität im Verlauf der Zeit sowie die Rückschlüsse aus dem Verhalten eines Systems oder Teilsystems sind wesentliche Aspekte zur Generierung sicherheitspolitischer Konzepte und davon abgeleiteter Strategien von und für individuelle und kollektive soziale Akteure.

Supply Chain Resilienz Management

(Auszug aus: Johannes Göllner, Ralf A. Huber; Supply Chain Resilienz Management, Hrsg. Controller Magazin, Ausgabe 3: Mai/Juni 2025, VCW Verlag für ControllingWissen AG, Freiburg, 2025, S. 104.)

Das Supply Chain Resilienz Management wandelt sich und nimmt dabei die Herausforderungen der Gesellschaft an. Mit der digitalen Transformation und der ökologischen Transformation sowie den Veränderungen der Gesellschaft und des Konsumverhaltens ändert sich der Kontext. Regulierungen aus den Themenfeldern der Informationssicherheit, der Resilienz, des Lieferkettensorgfaltspflichtengesetzes und der weitergehenden auch persönlichen Verantwortung und Haftung setzen dem Supply Chain Resilienz Management neue Ziele. Beispiele sind das IT-Sicherheitsgesetz, die NIS-Richtlinien (1 & 2) und die Europäische Strategie für wirtschaftliche Sicherheit und die Nationale Sicherheitsstrategie Deutschland:

„Die deutsche Bundesregierung entwickelt ihre Strategie für die Rohstoffversorgung mit den Schwerpunkten Versorgungssicherheit, Diversifikation, Nachhaltigkeit und Innovation fort. Damit schaffen

wir einen Rahmen für ein konsequentes Monitoring von Rohstofflieferketten, die Stärkung diversifizierter Wertschöpfungsketten und für die Vermeidung einseitiger Abhängigkeiten von einzelnen Zulieferern.“ (vgl. Nationale Sicherheitsstrategie Deutschland, S. 55, <https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf>)

Ziel der Europäischen Strategie für wirtschaftliche Sicherheit ist es, die wirtschaftliche Sicherheit in der EU zu schützen, die Resilienz unserer Wirtschaft zu stärken und gleichzeitig dafür zu sorgen, dass wir unseren technologischen Vorsprung vergrößern. Um diese Ziele zu erreichen, brauchen wir einen klaren Überblick über die Risiken und ihre Entwicklung im Laufe der Zeit. Aus diesem Grund werden die Kommission und die Mitgliedstaaten kritische Lieferketten eingehender analysieren, sie Stresstests unterziehen und das Risikoniveau festlegen. (siehe Europäische Strategie für wirtschaftliche Sicherheit, S. 6, Pkt. 2, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52023JC0020>)

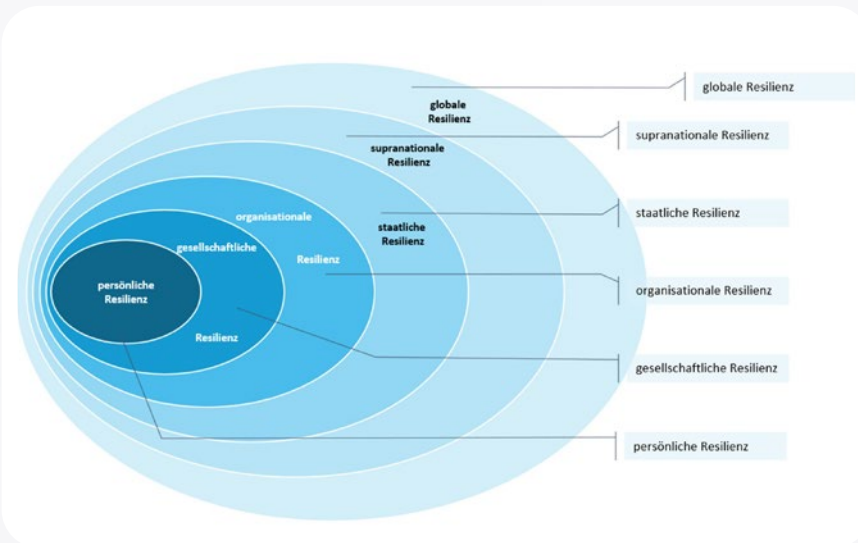
Im Wirtschaftsschutz 2024+, der sich als Gemeinschaftsleistung staatlicher und privatwirtschaftlicher Akteure auf die Stärkung der Resilienz der Wertschöpfungs- und Lieferketten ausrichtet, erhält der Schutz der KRITIS (Kritische Infrastruktur) daher eine besondere Bedeutung (siehe Grünbuch ZMZ 4.0, Hrsg. Zukunftsforum öffentliche Sicherheit e. V., Sandra Bubendorfer-Licht MdB, Leon Eckert MdB, Dr. André Hahn MdB, Dr. Günter Krings MdB, Ingo Schäfer MdB, Fallbeispiel 6.4, S. 51).

Vernetzung, insbesondere der kritischen oder strategischen Infrastrukturen, sowie multiple, sich wechselseitig verstärkende Krisen stellen eine Herausforderung für ein SCRM dar.

Die BME-Logistikstudie 2024 „Risikomanagement und Resilienz in Supply Chains“ liefert zentrale Erkenntnisse zur aktuellen Lage der Lieferketten-Resilienz. Zusammenfassend zeigt die Studie, dass trotz gewisser Verbesserungen die Lieferketten vieler Unternehmen noch nicht ausreichend widerstandsfähig sind und ein umfassendes, proaktives Risikomanagement weiterhin eine Herausforderung bleibt.



Supply Chain Resilienz Management ist ein Spannungsfeld, das durch ein Größerwerden des Verantwortungsraums geprägt wird. Das Lieferkettensorgfaltspflichtengesetz fordert die Verantwortung für Risiken der gesamten Supply Chain. Das Spannungsfeld wird auch geprägt durch den Wunsch und die Notwendigkeit, den Wettbewerb zu wahren. Transparenz über die gesamte Supply Chain, wie sie durch moderne Technologien möglich wird und von einzelnen Unternehmen für eine gesamte Supply Chain (extern und intern) gefordert und durchgesetzt wird, beeinflusst den Wettbewerb – Informationen über Beschaffung und Märkte werden sichtbar, und das verändert die Position von Teilnehmern der Supply Chain. Die Konsequenzen von schlechtem Risikomanagement oder einer Nichteinhaltung der gesetzlichen Vorgaben werden spürbar.



Die Entwicklung von **risikoreduzierenden Strategien und Resilienzstrategien** für physische und digitale Supply und Value Chains sowie deren Verbindung mit den zugehörigen Supply Chain Networks (strategische [kritische Infrastrukturen]) bedarf Innovationen bei qualitativen und quantitativen Konzepten, Modellen, Methoden und Werkzeugen im Bereich Risk Assessment sowie Modeling und Simulation, um den Grad der erforderlichen Resilienz der Supply und Value Chain auf staatlicher und unternehmerischer Ebene festzustellen und um zur Strategie- und Produktentwicklung positiv und wertschöpfend beitragen zu können.

Resilienz, organisatorische, Cyber- und Supply-Chain-Resilienz haben sich in den letzten Jahren zu absoluten Schlagwörtern entwickelt. Zahlreiche Consulting-Unternehmen nutzen das Thema Resilienz als Werbeslogan, um ihre Produkte zu verkaufen. Auch auf internationalen Konferenzen erfreut sich der Themenbereich wachsender Aufmerksamkeit.

Resilienz ist jedoch kein fixer Werkzeugkasten, sondern eine Fähigkeit, und sollte daher als strategischer Mehrwert oder Steuerungstool für Organisationen betrachtet werden. Hierfür ist es notwendig, den Terminus „Strategische Resilienz“ als neuen Begriff zu prägen. Richtig angewendet, kann sie als Integriertes Management System (IMS) in Organisationen dienen.

Abbildung 1: RESILIENZ © Christian PAUL, Johannes GÖLLNER, Helmut PISECKY, Susanne LUDESCHER [1]

Als Resilienz von Organisationen bezeichnet man die Fähigkeit einer Organisation, auf interne und externe Einschlüsse und Veränderungen der Rahmenbedingungen zu reagieren und sich diesen anzupassen. Gegenwärtig erleben wir eine Zeit, die von Veränderungen, Krisen und Polykrisen geprägt ist; die vielzitierte VUCA-Welt (Volatility, Uncertainty, Complexity, Ambiguity) ist längst Realität. Gerade unter diesen Umfeldbedingungen ist die Fähigkeit zur Anpassung überlebenswichtig, für Individuen ebenso wie für Gesellschaften, Staaten und Organisationen: Jedes System ist nur so widerstandsfähig wie die Subsysteme, die es ausmachen.

Die internationale Standardisierung, vertreten durch ISO (International Organisation for Standardization, Genf), hat bereits 2007 mit der Herausgabe von Supply-Chain-Security-Standards [2][3][4] reagiert und die Relevanz dokumentiert. Bereits 2018 hat

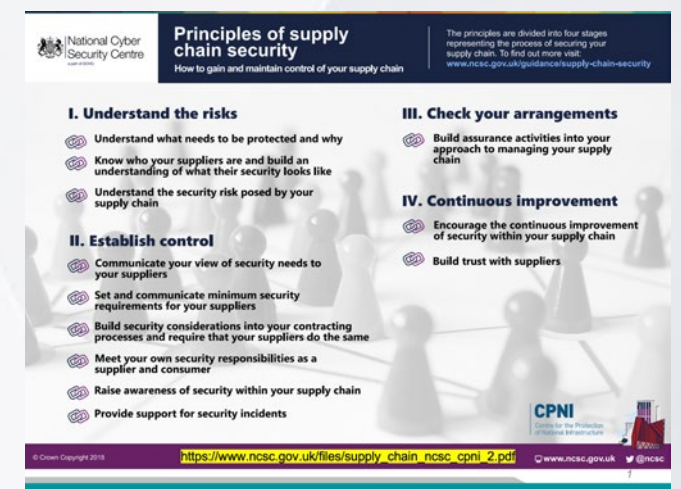
das National Cyber Security Centre, U.K., den thematischen Zusammenhang zwischen Supply Chain Security und Cyber Security dokumentiert und veröffentlicht.

Der supranationale Gesetzgeber (EU) reagierte darauf – unter anderem – mit der EU-NIS2-Directive (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022), welche ab 18.10.2024 in Österreich und allen EU-Mitgliedstaaten auch für spezifische KMU (wesentliche und wichtige Einrichtungen) gelten sollte. [5]

Die Transformation in nationale Gesetzgebung erlangte in Österreich das sogenannte „NISG 2026“ am 23.12.2025 (gültig ab 01.10.2026) im nationalen BGBl. [6] und in Deutschland mit dem NIS-2-Umsetzungsgesetz am 06.12.2025 seine Gültigkeit.

Betroffen sind alle Unternehmen und spezifische KMU, welche sogenannte wesentliche oder wichtige Einrichtungen sind und dem Kriterienkatalog dieser EU-Directive entsprechen. Das Wesentliche ist unter anderem, dass zum ersten Mal Cyber Security mit Supply Chain Security, gemäß Artikel 21 [7] (2) d) [8] der NIS-2-Richtlinie, verknüpft werden – und dass diese bei der Auditierung nach ISO 27001 in Korrelation mit anderen Standards analysiert werden müssen.

II. NIS-2 Richtlinie: NIS-2: Wesentliche und Wichtige Einrichtungen	
Wesentliche Einrichtungen (Anhang I)	Wichtige Einrichtungen (Anhang II)
Energie (Elektrizität, Fernwärme/kälte, Öl, Gas, Wasserstoff)	Post- und Kurierdienste
Verkehr (NIS 1: Luft, Wasser, Schiene, Straße)	Forschung
Bankwesen	Chemie (Herstellung & Handel)
Finanzmarktaufsichtsinfrastrukturen	Lebensmittel (Produktion, Verarbeitung, Vertrieb)
Gesundheitswesen (Gesundheitsdienstleister, EU-Referenzlaboratorien, Forschung und Herstellung pharmazeutischer und medizinischer Produkte & Geräte)	Verarbeitendes & Herstellendes Gewerbe (Medizinprodukte, Datenverarbeitungs- elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste, Suchmaschinen, Online-Marktplätze, Plattformen für soziale Netzwerke
Abwasser	Abfallbewirtschaftung (Anmerkung GÖLLNER: „Kreislaufwirtschaft/Circular Economy integriert JANEIN ?!“)
Digitale Infrastruktur (IXP, DNS, TLD, Cloud Computing, Rechenzentren, Inhaltsspeichernetze, Vertrauensdiensteanbieter, und öffentliche elektronische Kommunikationsnetze)	
IKT-Service Management	
Öffentliche Verwaltung	
Weltraum	



Zusammenfassung & Ausblick

Im Nachfolgenden sind einige Herausforderungen angeführt, welche für NIS-2-betroffene Unternehmen „Wesentliche und Wichtige Einrichtungen“ – und im Besonderen KMU – relevant sind:

Entwicklung und Anwendung eines standardisierten, fakten- und mathematisch-modellbasierten Cyber-Event- und Bedrohungs-Monitorings sowie eines Risikoanalyse- und -bewertungsmodells, sowie der notwendigen – teils permanenten – Dokumentation der Zusammenhänge und Wechselwirkungen, basierend auf den aktuell relevanten gesetzlichen Innovationen zwischen Cyber- und Supply-Chain-Regelwerken.

Die Anforderungen und strategischen Ansätze – Status quo und Innovationen für die Risikomodellierung & -monitoring in Bezug auf Zertifizierungen, Audits und Bonitätsprüfungen im Rahmen einer M&A-Due-Diligence – werden die Unternehmen (Einrichtungen) vor große Herausforderungen stellen, um Vertrauen bei bzw. in den betroffenen Unternehmen, Investoren und den national zuständigen Aufsichtsbehörden zu begründen und um eine reduzierte Innovationsfreude – besonders bei KMU – oder Druck auf die digitale Transformation der KMU zu vermeiden.



Die Verfügbarkeit qualitätsgesicherter, modellbasierter Cyber-/Lieferketten-Event- und -Bedrohungs-Monitoring-, Risikoanalyse- und Risikobewertungswerkzeuge ist fachlich nur eingeschränkt gegeben.

Die Mitentwicklung von Leitfäden und einheitlichen, qualitätsgesicherten und getesteten Zertifizierungsstandards ist relevant, um die entstehenden Kosten (wie z. B. infolge zusätzlicher Überwachung, zusätzlicher – womöglich permanenter – Berichterstattung von Vorfällen und Bedrohungen, Supply Chain Security, zusätzlicher Vollzugskosten, einschließlich des zusätzlichen Rahmens für das Krisenmanagement, etc.) bei der Erfüllung der NIS-2-Richtlinien-Vorgaben reduzieren zu können.

Initiierung einer Aus-, Fort- und Weiterbildungskampagne zur Bewältigung des existierenden facheinschlägigen IT-/Cyber-Fachkräftemangels bei Unternehmen sowie der Ausbildung verfügbarer NIS-2-Zertifizierungsexperten, um die nach ISO 27001 etc. zu erwartende große Anzahl zu auditierender Unternehmen fachlich und zeitnah bedienen zu können.

Hinweis: Ein geeigneter Weg könnte hier z. B. in Österreich auch in der Nutzung der mit dem Ingenieurgesetz (IngG 2017) geschaffenen Möglichkeit liegen, auf der Niveaustufe VI des NQR/EQR (Bachelorniveau) selbst geeignete Fachkräfte auszubilden und damit die Lücke an fehlenden Hochschulabsolvent:innen zu schließen.

Darüber hinaus wurde 2025 ein Kontaktstudium zum hochschulgeprüften „Resilienz Manager“ durch das Zentrum für Risiko- und Krisenmanagement – unter der Leitung von Christian Paul und Johannes Göllner – entwickelt.

Derzeit existiert noch kein verfügbares, inhaltlich qualitätsgesichertes Top-Management-Ausbildungskonzept für die Zielgruppe Top-Management (Geschäftsführer, Vorstände, Aufsichtsräte, Beiräte, etc.) im Sinne der Verantwortlichkeit des

Top-Managements gemäß NIS-2-Richtlinie.

Hinweis: Das Zentrum für Risiko- und Krisenmanagement erarbeitet seit 2025 ein solches Ausbildungskonzept für den D-A-CH-Raum.

Die Umsetzung eines Supply Chain Risk Management steckt weiterhin in den Kinderschuhen. Der Reifegrad des SCRM hat deutlich Luft nach oben. (vgl. BME-Logistikstudie 2024: Risikomanagement und Resilienz in Supply Chains, Fazit und Handlungsempfehlungen, S. 58, https://a.storyblok.com/f/104752/x/bf5bd97da2/bme-leitfaden-logistikstudie-2024_final.pdf) -v-

Quellenangaben

- [1] siehe <https://www.zfrk.org/bereich/publikationen/positionspapiere>
- [2] ISO 28000 (Specification for security management systems for the supply chain), First edition: 2007-09-15; aktueller Stand: ISO 28000:2022; Revision in Vorbereitung.
- [3] ISO 28001 (Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans, requirements and guidance), First edition 2007-10-15.
- [4] ISO 20858 (Ships and marine technology – Maritime port facility security assessments and security plan development), First edition 2007-10-15; aktueller Stand: ISO 20858:2012.
- [5] Bis zum 17.10.2024 erlassen und veröffentlichen die Mitgliedschaften die erforderlichen Vorschriften, um diese Richtlinie umzusetzen.
- [6] siehe https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2025_I_94
- [7] Risikomanagementmaßnahmen im Bereich der Cybersicherheit.
- [8] Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern.

CHW AT

CYBER-HILFSWERK ÖSTERREICH

Deine Freunde und Helfer



DIGITAL ANGELS



AT.CYBER-HW.ORG

Von der Feldererkennung zur Kommandoentscheidung

TUDOR ANDRONIC, RENÉ DÖHRING

Verteidigungsorganisationen stehen zunehmend vor einer Aufgabe, die zwei bislang oft getrennt betrachtete Fragen verbindet: Wie lässt sich aus der physischen Umgebung belastbare Lageinformation gewinnen, und wer behält die Kontrolle über die Systeme, in denen diese Informationen verarbeitet werden? Ein Sensor kann eine Bedrohung erkennen und ein KI-Modell daraus strukturierte Daten erzeugen. Ihr Wert hängt davon ab, wo die Software läuft, wer diese Umgebung kontrolliert und ob die Verarbeitung bei Veränderungen verfügbar bleibt.

Anwendungsfähigkeit und digitale Souveränität

Anwendungsfähigkeit und digitale Souveränität werden damit zu zwei Seiten derselben Betriebsfrage. Verarbeitung am Einsatzrand kann bei eingeschränkter Kommunikation notwendig sein, während Simulation und Analyse zentrale Systeme benötigen können. Sensible Anwendungen müssen zwischen privater Infrastruktur, souveränen Cloud-Umgebungen und anderen kontrollierten Betriebsorten verlagert werden können, ohne dass die Anwendung dafür grundlegend neu entwickelt wird.

ASSIST Software veranschaulicht die Anwendungsseite dieses Problems. Das 1992 im rumänischen Suceava gegründete Unternehmen entwickelt kundenspezifische Software und KI-Systeme und ist mit der ASSIST Software GmbH im Technologiezentrum Augsburg im DACH-Raum vertreten. ASSIST Software ist zudem eines der ersten Unternehmen in Rumänien mit einer Zertifizierung nach ISO/IEC 42001 für KI-Managementsysteme.

Die Verteidigungsaktivitäten des Unternehmens führen von der physischen Wahrnehmung bis in Simulation und Entscheidungsunterstützung. Ein aktueller Demonstrator basiert auf einer vierbeinigen Roboterplattform mit 360-Grad-Kamera und lokal betriebenem Computer-Vision-Modell. Das System erkennt militärisch relevante Objekte wie



Schusswaffen, handgeführte Sprengkörper und Gefahrenindikatoren. Die Verarbeitung erfolgt auf der Plattform; Live-Bild und Erkennungsdaten werden über XR-Brillen an den Bediener übertragen.

Lokale Verarbeitung verringert die Abhängigkeit von permanenter Konnektivität, während die Erkennung mit wechselnden Umgebungsbedingungen und unvollständigen Informationen umgehen muss.

Infrastrukturunabhängigkeit als Architekturprinzip

ASSIST Software führt diese Kette in die Simulation weiter. Zum Portfolio gehören KI-gestütztes Verhalten von Einheiten, Szenariengenerierung, physikbasierte Gefechtsmodellierung und KI-gestützte After-Action-Reviews in Verteidigungssimulationsumgebungen. Eine Beobachtung aus dem Einsatzraum kann damit als strukturierte Information in Systeme einfließen, die Ereignisse analysieren, Alternativen modellieren und eine Bewertung auf Führungsebene unterstützen.

Aus dieser Verbindung ergibt sich eine Infrastrukturfrage. Anwendungen am taktischen Rand können keine permanente Verbindung zu einer einzigen zentralen Umgebung voraussetzen. Ist die Software eng an einen bestimmten Infrastrukturbetreiber gekoppelt, verliert die Organisation einen Teil der Flexibilität, die verteilte Operationen erfordern.

Codesphere adressiert diese zweite Ebene mit seiner Virtual Cloud Platform. Das Unternehmen stellt eine Software- und Steuerungsschicht oberhalb der zugrunde liegenden Infrastruktur bereit. Anwendungen lassen sich damit über Public Clouds, souveräne Cloud-Anbieter, private Umgebungen und lokale Systeme hinweg entwickeln, bereitstellen, absichern, betreiben und verwalten.

Für Verteidigung und öffentliche Verwaltung ist diese Unterscheidung wesentlich. Souveränität entsteht nicht allein durch den Standort eines Rechenzentrums. Eine Anwendung kann in einem europäischen Rechenzentrum laufen und dennoch von proprietären Diensten oder Kontrollmechanismen außerhalb des tatsächlichen Einflussbereichs der Organisation

abhängen. Codesphere versucht, die Infrastruktur austauschbarer zu machen und ein konsistentes Kontrollmodell für die Anwendungen zu erhalten.

Resiliente Systeme für verteilte Operationen

Hier wird das Verhältnis beider Unternehmen zu einem konkreten Beleg für eine technische Architektur, nicht zu einer klassischen Partnerschaftsgeschichte. ASSIST Software entwickelt Systeme, die einsatzrelevante Informationen erfassen, auswerten und in Simulation und Entscheidungsunterstützung überführen. Codesphere stellt eine Betriebs- und Steuerungsebene bereit, auf der die dafür benötigte Software über unterschiedliche Infrastrukturumgebungen hinweg kontrolliert werden kann.

Für eine Verteidigungsorganisation kann diese Trennung darüber entscheiden, ob eine Architektur nach ihrer Einführung anpassungsfähig bleibt. Ein robotisches Sensorsystem kann lokal verarbeiten, ausgewählte Daten an geschützte Infrastruktur übertragen und Informationen an eine getrennte Simulationsumgebung weitergeben müssen. Die Anwendung muss auch bei einem Wechsel des Betriebsorts funktionsfähig bleiben. Umgekehrt hat souveräne Infrastruktur nur begrenzten Wert, wenn spezialisierte Missionssoftware nicht ohne umfangreiche Anpassungen darauf betrieben werden kann.

Verteidigungs- und Behördenarchitekturen setzen stärker auf Edge-Verarbeitung, verteilte Sensorik und softwaredefinierte Funktionen, während Anforderungen an Souveränität und Resilienz zunehmen. Infrastrukturunabhängigkeit wird damit zu einer Eigenschaft der Anwendungsarchitektur und nicht nur zu einer Beschaffungsentscheidung über den Standort von Servern. Der entscheidende Maßstab ist, ob Missionssoftware belastbare Informationen über wechselnde Betriebsumgebungen hinweg verarbeiten kann, während die verantwortliche Organisation die Kontrolle über diese Verarbeitung behält. Genau diese Trennung von Anwendungsintelligenz und Infrastrukturabhängigkeit wird für sicherheitskritische Systeme zu einem grundlegenden Architekturprinzip. -v-

VANGUARD

— LEAD & INNOVATE —



TIEFGRÜNDIGE
ANALYSEN



PRAXISNAHE
PERSPEKTIVEN



KLARE ORIENTIERUNG
FÜR



JETZT ONLINE LESEN!
www.vanguardmag.eu





Wenn öffentliche Sicherheit zur Vertrauensfrage wird

HERBERT HENNINGER

Ein Stromausfall legt eine ganze Region lahm, während in einem Krankenhaus Notfallpläne greifen und Behörden Krisenstäbe über mehrere Standorte koordinieren. In solchen Momenten entscheiden Sekunden über Stabilität, Versorgung und Vertrauen.

Szenarien wie diese gehören längst zur Realität. Sie zeigen, wie hoch der Druck auf die öffentliche Sicherheit geworden ist.

Für Österreich ist diese Frage besonders relevant. Öffentliche Einrichtungen, Betreiber kritischer Infrastruktur und Organisationen mit Versorgungsauftrag müssen auch dann funktionieren, wenn Systeme unter Druck geraten. Gefragt sind Lösungen, die Risiken früh sichtbar machen und im Ernstfall klare Entscheidungen ermöglichen.

Genau hier setzt Primion an. Im österreichischen Markt steht künftig Herbert Henninger als erfahrener Ansprechpartner zur Verfügung. Er begleitet Kunden von der ersten Beratung bis zur passenden Sicherheitslösung.

Denn öffentliche Sicherheit ist mehr als die Kontrolle an Türen oder Schranken. Sie beschreibt die Fähigkeit einer Stadt, Behörde oder Organisation, auch in belastenden Situationen arbeits- und handlungsfähig zu bleiben. Energieversorgung, Verwaltung, Gesundheitswesen, Verkehr und nationale Sicherheit sind Bereiche, auf die sich Menschen jeden Tag verlassen. Wenn dort Systeme ausfallen, entsteht weit mehr als ein technisches Problem.

Sicherheit braucht Übersicht

Primion betrachtet Sicherheit deshalb als ein Zusammenspiel von Menschen, Prozessen und Technik. Im Mittelpunkt steht ein integriertes Lagebild, das Informationen aus verschiedenen Bereichen zusammenführt.

Verantwortliche erkennen schneller, was passiert, wer vor Ort ist, welche Bereiche geschützt werden müssen und welche Teams einsatzbereit sind. So entstehen Entscheidungen nicht auf der Basis von Vermutungen, sondern aus verlässlichen Daten.

Viele öffentliche Einrichtungen arbeiten mit getrennten Systemen: Zutrittskontrolle, Personalplanung, Alarmierung und Notfallorganisation werden getrennt voneinander betrieben. Im Alltag fällt das oft kaum auf, aber in einer Krise kann es wertvolle Zeit kosten. Denn wenn Informationen erst aus mehreren Quellen zusammengesucht werden müssen, entstehen Verzögerungen und genau diese Zeit fehlt, wenn eine Störung eskaliert oder eine schnelle Abstimmung notwendig ist.

Konvergente Sicherheit verändert diesen Ansatz. Sie verbindet Zutrittskontrolle, Sicherheitsmanagement, Personalprozesse und Notfalllösungen auf einer gemeinsamen Plattform. So wird sichtbar, welche Mitarbeitenden sich in welchen Gebäuden befinden, wer Entscheidungen treffen darf und welche Einsatzkräfte verfügbar sind. Auch zusätzliche Kräfte, etwa freiwillige Helferinnen und Helfer, lassen sich besser einplanen.

Für Behörden und öffentliche Einrichtungen ist das ein riesiger Vorteil, vor allem wenn Ressourcen und Personal knapp sind. Zugleich steigen die Anforderungen an die Bereitschaft, Dokumentation und Zusammenarbeit über mehrere Standorte hinweg. Moderne Systeme entlasten, weil sie eine Übersicht schaffen, die Abläufe beschleunigen und Risiken früher erkennbar machen.

Vernetzt in die Zukunft

Ein wichtiger Punkt ist der Schutz bestehender Investitionen. Viele öffentliche Gebäude und Infrastrukturen sind über Jahrzehnte gewachsen. Eine vollständige Modernisierung wäre teuer und würde den laufenden Betrieb belasten. Primion setzt deshalb auf Lösungen, welche vorhandene Systeme einbinden und schrittweise erweitern können. So entsteht Fortschritt, ohne die bewährten Strukturen unnötig zu ersetzen.

Hinzu kommt, dass sich die Bedrohungslage stark verändert hat. Physische Sicherheit, IT und Betriebstechnik lassen sich nicht länger getrennt voneinander betrachten. Ein Angriff kann digital beginnen, aber ganz reale Folgen haben. Umgekehrt kann ein Vorfall vor Ort massive Auswirkungen auf digitale Prozesse haben.

Wer das Thema Sicherheit ernst nimmt, braucht ein System, das Zusammenhänge erkennt und nicht nur einzelne Ereignisse meldet.

Für Österreich bietet dieser Ansatz klare Chancen. Das Land verfügt über leistungsfähige öffentliche Strukturen, eine kritische Infrastruktur und ein starkes Bewusstsein für Verlässlichkeit. Herbert Henninger bringt dafür umfassende Erfahrung im Vertrieb, Business Development und in Transformationsprojekten mit. Seine Aufgabe ist es, Anforderungen vor Ort zu verstehen und gemeinsam mit Kunden passende Lösungen zu entwickeln.

Die öffentliche Sicherheit wird damit zu einer Gestaltungsaufgabe. Es geht nicht nur darum, auf Vorfälle zu reagieren. Entscheidend ist die Vorbereitung, bevor eine Krise entsteht. Wer kritische Prozesse kennt, Verantwortlichkeiten klar abbildet und Infor-

mationen zentral verfügbar macht, gewinnt jede Menge Handlungsspielraum.

Fazit: Die Zukunft liegt in vernetzten, intelligenten und verständlichen Lösungen. Sie müssen im Alltag entlasten und im Ernstfall zuverlässig funktionieren. Für Behörden, Betreiber kritischer Infrastrukturen und öffentliche Organisationen wird diese Fähigkeit zum strategischen Schlüssel.

Denn wenn jede Sekunde zählt, darf Sicherheit nicht kompliziert sein. Sie muss vorbereiten, Orientierung geben und handlungsfähig machen. Genau darin liegt ihr Wert für die Gesellschaft, die sich auf ihre öffentlichen Systeme verlassen will.

Mehr: <https://primion.io/de/branchen/offentliche-sicherheit/> -v-



Die Psycho-Logik der Sicherheit – ein Auftrag an Führung und Organisation

ANJA EBERT-STEINHÜBEL

Warum Sicherheit im Unternehmen zuerst eine psychologische und erst dann eine technische Frage ist

Die Psycho-Logik der Organisation

Die Verbreitung von Angst und Unsicherheit in den Unternehmen gleicht einer stillen Erosion. Ganz gleich, welche physischen und technologischen Konzepte oder Regulatorien im Umgang mit unternehmerischen oder technologischen Risiken und Krisen bestehen, bleibt stets ein Bodensatz diffuser Empfindungen und impliziter Vorbehalte gegenüber der subjektiv erlebten Veränderungsdynamik unserer Zeit.

Die psychologische Bewältigung von Unsicherheit, Ambivalenz und Innovationsdruck ist von Person zu Person verschieden und in der Regel nicht explizit. Eben darin liegt die besondere Herausfor-

derung: Die unsichtbaren und unbewussten Hürden bremsen oder verhindern die Handlungsfähigkeit des gesamten Systems oft und gerade dann, wenn ein schnelles Agieren dringlich und strategisch geboten erscheint.

Tatsächlich erfüllt das Streben nach Sicherheit ein menschliches Grundbedürfnis – ganz unabhängig von Alter, Kultur, Generation etc.: Über den physischen Schutz und den Ausschluss einer potenziellen aktuellen Gefährdung hinaus, wirkt Sicherheit als Schutzbrief für die überlebensnotwendige Konsistenz, die besondere Waage zwischen Neuem und Altem, Vertrauen und Unbekanntem unserer Existenz. In der persönlichen und beruflichen Lebensgestaltung wird diese über

Bindung, Vertrauen und Stabilität realisiert. Die Zugehörigkeit in einer Beziehung, zu einem Team, Projekt oder Unternehmen wirkt dabei entlastend und kompensiert quasi innerlich die Erfahrung externer Dynamik, Brüche, Krisen und Konflikte.

Innere Sicherheit – eine Frage der Kompetenz

Kompetenz erfordert Mut in Form praktizierter Selbstwirksamkeit. Nach der psychologischen Selbstbestimmungstheorie sind wir immer dann am erfolgreichsten, wenn wir motiviert und selbstbewusst agieren, Sinn und Bedeutung erleben sowie Erfolge und Misserfolge selbst verantworten. Autonomie, Sinn und Kompetenz – das „Dreieck“ wirksamen Handelns – setzen

eine Art innerer Sicherheit, die im „Dreiklang“ persönlichen Wissens, Wollens und Könnens basiert, also voraus und bestärken diese zugleich.

Eine ausschließlich auf den Informations- oder Wissensaspekt hin orientierte Risiko-, Krisen- und Veränderungskommunikation läuft daher folgerichtig ins Nichts. Ganz im Gegenteil evoziert sie den Widerstand oder Rückzug derjenigen, die sich nicht fähig oder bereit genug fühlen. Und sie befördert darüber hinaus den Bias, nach dem die Wahrnehmung allzu häufig und umfassend präsentierter Informationen in ihrer Relevanz und Dringlichkeit verpufft.

Psychologische Sicherheit als Führungsanspruch

Der Hebel innerer Sicherheit funktioniert auch und gerade in sozialen Gruppen und Teams.

Edmondson beschreibt die Effekte „psychologischer Sicherheit“ einer vertrauensvollen, wertschätzenden, entwicklungsorientierten Kultur, die Unterschiede proaktiv fördert, Lernen ermöglicht und die Team-Performance in der bestmöglichen Entfaltung der Einzelnen generiert.

In der modernen Führungslehre wird diese Leitidee in der Sicherung des sozialen Freiraums und Befähigung und Stärkung der Teammitglieder, diesen auch zu nutzen, normativ gesetzt.

Damit verbunden sind die Aspekte der Bindung und Kompetenz, aber auch der persönlichen Wertschätzung und Rückversicherung, dass gerade in Situationen von großer Unsicherheit, Ambivalenz oder Komplexität Fehler keine Schwächen bedeuten, sondern Lernen ermöglichen und damit Zukunftsfähigkeit.

Die Balance, die durch ein erfolgreiches Leadership immer wieder neu zu vermitteln ist, liegt weniger zwischen den Polen Unsicherheit und Sicherheit, denn zwischen Entwicklung und Integration bzw. Konsistenz. Zur Bewältigung und proaktiven Gestaltung der Transformation ist deshalb nicht nur eine andere Art von Führung erforderlich, sondern eine neue Art von Organisation, in der ein Nebeneinander von Flexibilität und Stabilität, Innovation und Optimierung, Freiraum und Schutz gleichzeitig möglich sind. Sicherheit offenbart sich darin als ein primär psycho- und führungslogisches Konzept. -v-





Meta-Leadership

Führung jenseits traditioneller Grenzen

THOMAS BENESCH

In einer Arbeitswelt, die durch Dynamik, Komplexität und permanente Veränderung gekennzeichnet ist, reichen klassische Führungsansätze nicht mehr aus. Das Konzept des Meta-Leadership hat daher in den letzten Jahren zunehmend an Bedeutung gewonnen, da es Führungskräfte dazu befähigt, strategische, emotionale und interdisziplinäre Kompetenzen zu vereinen, um den Herausforderungen moderner Organisationen gerecht zu werden (Marcus et al., 2019).

Im Kern des Meta-Leadership stehen drei miteinander verwobene Dimensionen: Person, Situation und Konnektivität. Während die Dimension Person die Selbstführung und Reflexion als Kernkompetenzen betont, fokussiert Situation die Kontextanalyse und Konnektivität die Vernetzung mit Stakeholdern (Marcus et al., 2020). Dieser integrative Ansatz ermöglicht es Führungskräften, nicht nur ihre eigene Wirkung zu reflektieren, sondern auch komplexe Systeme zu durchschauen und effektive Verbindungen zwischen verschiedenen Organisationen und Menschen herzustellen.

Die Entwicklung interner Kapazitäten bildet das Fundament erfolgreicher Führung. Dabei spielen emotionale Intelligenz und Selbstwahrnehmung eine zentrale Rolle. Goleman (1995) hat gezeigt, dass emotionale

Intelligenz für Führungserfolg oft wichtiger ist als der kognitive. Das Verständnis der eigenen Emotionsregulation – insbesondere die Überwindung des sogenannten „emotionalen Kellers“ – sowie die Förderung eines resilienten Mindsets sind entscheidend, um in herausfordernden Situationen selbstbewusst und lernbereit zu bleiben (Dweck, 2006). Dwecks Konzept des Wachstumsmindsets ist dabei essenziell für die kontinuierliche persönliche und berufliche Entwicklung von Führungskräften.

Neben der inneren Ausrichtung erfordert Meta-Leadership die gezielte Entwicklung externer Fähigkeiten. Die Erstellung einer Situation Connectivity Map ermöglicht die systematische Analyse und Verknüpfung von Stakeholdern, während der POP-DOC Loop als kontinuierliches Verfahren zur Verbesserung des Situationsbewusstseins und der Handlungsfähigkeit in komplexen Führungssituationen dient (Marcus et al., 2020). Diese Methoden der kooperativen Führung und interdisziplinären Zusammenarbeit sind unverzichtbar, um in dynamischen Umgebungen effektiv agieren zu können.

Die moderne Arbeitswelt stellt Führungskräfte vor zusätzliche Herausforderungen: Remote-Leadership, digitale Kommunikationsstrategien und ethische Entscheidungen in virtuellen

Räumen erfordern neue Kompetenzen. Gleichzeitig wird die Fähigkeit zur Krisenbewältigung und Risikoprävention immer relevanter. Marcus et al. (2019) betonen, dass Meta-Leadership gerade in Krisenzeiten seine volle Wirkung entfaltet, wenn Führungskräfte emotionale Intelligenz mit analytischer Klarheit verbinden. Heifetz, Grashow und Linsky (2009) ergänzen dies mit dem Konzept der adaptiven Führung, das praktische Werkzeuge für den Umgang mit komplexen Veränderungen bereitstellt.

Ein weiterer zentraler Baustein ist das Innovationsmanagement. Design Thinking und agile Methoden werden dabei als Werkzeuge für die Umsetzung innovativer Konzepte in die Praxis eingesetzt (Senge, 1990). Senges Prinzipien des systemischen Denkens zeigen, wie Organisationen lernen und wachsen können. Dabei gilt es, ein Wachstumsmindset nicht nur bei sich selbst, sondern auch in Teams und Organisationen zu fördern (Dweck, 2006). Nachhaltigkeitskompetenzen werden zunehmend in Führungsprozesse integriert, um Visionen zu entwickeln, die Ganzheitlichkeit und Wirtschaftlichkeit vereinen.

Fazit

Meta-Leadership ist kein statisches Konzept, sondern ein kontinuierlicher Lern- und Entwicklungsprozess. Es verbindet

Selbstführung mit systemischem Denken und kooperativer Vernetzung. Wie Covey (2020) in seinen Prinzipien persönlicher Effektivität zeigt, beginnt erfolgreiche Führung stets bei der eigenen Haltung. Brown (2018) ergänzt dies mit dem Appell an Mut und Verletzlichkeit als Grundlage positiver Unternehmenskultur. Führungskräfte, die diese Dimensionen integrieren, sind bestens gerüstet, die komplexen Anforderungen der modernen Arbeitswelt nicht nur zu bewältigen, sondern aktiv mitzugestalten.. -v-

Literaturverzeichnis

- Brown, B. (2018). Dare to lead: Brave work. Tough conversations. Whole hearts. Random House.
- Covey, S. R. (2020). The 7 habits of highly effective people. Simon & Schuster.
- Dweck, C. S. (2006). Mindset: The new psychology of success. Random House.
- Goleman, D. (1995). Emotional intelligence: Why it can matter more than IQ. Bantam Books.
- Heifetz, R., Grashow, A., & Linsky, M. (2009). The practice of adaptive leadership: Tools and tactics for changing your organization and the world. Harvard Business Press.
- Marcus, L. J., McNulty, E. J., Henderson, J., & Dorn, B. C. (2019). You're it: Crisis, change and how to lead when it matters most. Public Affairs.
- Marcus, L. J., McNulty, E. J., Flynn, L. B., Henderson, J. M., Neffenger, P. V., Serino, R., & Trenholm, J. (2020). The POP DOC loop: A continuous process for situational awareness and situational action. Industrial Marketing Management, 88, 272-277.
- Senge, P. M. (1990). The fifth discipline: The art & practice of the learning organization. Doubleday/Currency



Wenn der Titel nicht mehr ausreicht

ALEXANDER GOMERINGER

Warum wir Führung neu denken müssen, bevor uns die Realität dazu zwingt

Wenn Führung plötzlich sichtbar wird

Es gibt einen Moment, auf den keine Führungskraft vollständig vorbereitet wird. Er taucht in keinem Lehrbuch auf, lässt sich nur begrenzt simulieren und steht in keiner Stellenbeschreibung. Es ist der Augenblick, in dem Gewissheiten verschwinden.



Informationen sind unvollständig, die Zeit drängt, Entscheidungen lassen sich nicht mehr vertagen. Menschen blicken auf die Person, die führen soll, und suchen nach Orientierung. In diesem Moment verliert ein Titel seinen größten Vorteil. Nicht

dauerhaft, aber entscheidend. Denn plötzlich interessiert niemanden mehr, wie groß das Büro ist, welche Position auf der Visitenkarte steht oder wie beeindruckend der Lebenslauf aussieht. Es zählt eine andere Frage: Wem können wir jetzt vertrauen?

Vielleicht beginnt genau hier echte Führung: nicht mit einer Ernennung, einem Organigramm oder einer Beförderung, sondern in dem Augenblick, in dem Menschen freiwillig entscheiden, jemandem zu folgen.

Über Jahrzehnte haben Unternehmen Führung mit Hierarchie gleichgesetzt. Dieses Verständnis war nicht grundsätzlich falsch. Es passte zu einer Welt, in der Märkte berechenbarer, Strategien langlebiger und Erfahrungen ein verlässlicherer Kompass für die Zukunft waren. Heute verfügen Organisationen über mehr Daten als je zuvor und gleichzeitig über weniger Gewissheit. Technologien verändern Branchen innerhalb weniger Monate, künstliche Intelligenz verschiebt Aufgaben und Rollen, geopolitische Konflikte treffen Lieferketten innerhalb kürzester Zeit.

Viele Organisationen reagieren darauf mit den Werkzeugen der Vergangenheit: mehr Prozesse, mehr Freigaben, mehr Kennzahlen, mehr Kontrolle. Das ist nachvollziehbar. Kontrolle kann Abläufe stabilisieren und Risiken reduzieren. Was sie nicht automatisch schafft, ist Orientierung. Und Vertrauen lässt sich ohnehin nicht verordnen. Es entsteht zwischen Menschen.

Die eigentliche Währung moderner Führung heißt deshalb nicht Macht, sondern Glaubwürdigkeit. Sie entsteht nicht mit einer Beförderung, sondern jeden Tag neu: in Entscheidungen, in Gesprächen, im Umgang mit Fehlern und in der Bereitschaft, Verantwortung zu übernehmen, wenn die richtige Antwort noch niemand kennt. Früher legitimierte der Titel die Führung. Heute muss Führung den Titel legitimieren.

Führung beginnt dort, wo Gewissheit endet

Noch immer hält sich die Vorstellung, gute Führungskräfte seien vor allem diejenigen, die die richtigen Antworten kennen. Je höher die Position, desto größer die Erwartung, Sicherheit auszustrahlen. Doch moderne Führung bewegt sich nur noch selten zwischen eindeutig richtig und eindeutig falsch. Häufig geht es um mehrere Möglichkeiten, von denen keine vollkommen ist.

Damit verändert sich die entscheidende Frage. Sie lautet nicht mehr nur: Welche Entscheidung

ist richtig? Sondern immer häufiger: Welche Entscheidung können wir unter den heutigen Bedingungen verantworten?

In vielen Unternehmen werden Entscheidungen so lange abgesichert, bis möglichst alle Informationen vorliegen. Analysen werden ergänzt, Risiken neu bewertet, weitere Meinungen eingeholt. Jeder einzelne Schritt kann vernünftig sein. In Summe entsteht jedoch ein Preis: Zeit. Während eine Organisation auf Gewissheit wartet, verändert sich die Realität weiter. Eine fachlich hervorragende Entscheidung kann wertlos werden, wenn sie zu spät kommt.

Nicht jede schlechte Entscheidung entsteht deshalb durch mangelnde Informationen. Manche entstehen, weil niemand bereit war, rechtzeitig Verantwortung zu übernehmen.

Verantwortung bedeutet dabei nicht, Unsicherheit zu überspielen. Menschen erwarten von Führungskräften keine Unfehlbarkeit. Sie wollen nachvollziehen können, warum eine Entscheidung getroffen wurde. Sie wollen erleben, dass unterschiedliche Perspektiven berücksichtigt wurden. Und sie wollen sehen, dass jemand zu einer Entscheidung steht, auch wenn sie sich später als unvollkommen erweist.

Glaubwürdigkeit entsteht nicht durch den Anspruch, niemals Fehler zu machen, sondern durch den Umgang mit ihnen. Eine Führungskraft, die offen sagen kann: „Nach heutigem Wissen halte ich diesen Weg für richtig. Wenn sich die Lage verändert, überprüfen wir unsere Entscheidung“, zeigt keine Schwäche. Sie verbindet Entscheidungsfähigkeit mit der Bereitschaft, die eigene Einschätzung an einer veränderten Realität zu messen.

Für mich ist das keine theoretische Erkenntnis. Während einer Winterexpedition in Schwedisch Lappland gerieten wir in einen schweren Schneesturm. Innerhalb kurzer Zeit verschwand die Orientierung, die Sicht wurde nahezu null. Es gab keinen Vorgesetzten, den ich hätte fragen können. Kein Lehrbuch und keine Checkliste konnten mir sagen, welche Entscheidung die richtige war. Menschen und Tiere warteten darauf, dass jemand Verantwortung übernimmt. Nicht irgendwann. Sofort.

In diesem Moment ging es nicht darum, Sicherheit auszustrahlen, die nicht vorhanden war. Es ging



darum, die Lage so gut wie möglich einzuschätzen, eine Entscheidung zu treffen und bereit zu sein, ihre Konsequenzen zu tragen. Diese Erfahrung hat mein Verständnis von Führung stärker geprägt als jedes Modell. Unter realen Bedingungen zeigt sich nicht nur die Qualität einer Entscheidung. Es zeigt sich die Haltung des Menschen, der sie trifft.

Druck erschafft dabei keinen neuen Charakter. Er macht vorhandene Muster sichtbar. Wer Verantwortung grundsätzlich meidet, wird sie unter Druck eher abgeben. Wer Kontrolle mit Führung verwechselt, versucht Unsicherheit durch noch mehr Kontrolle zu kompensieren. Wer Vertrauen aufgebaut hat, kann dagegen auf etwas zurückgreifen, das kein Notfallplan kurzfristig erzeugen kann.

Deshalb greift auch die Vorstellung zu kurz, Führung lasse sich allein durch Wissensvermittlung entwickeln. Seminare, Modelle und Methoden haben ihren Wert. Sie schaffen Sprache, Struktur und Orientierung. Doch zwischen Wissen und Verhalten liegt ein Raum, den keine Präsentation schließen kann: die Realität. Erst dort zeigt sich, ob aus einer Methode eine Haltung geworden ist.

Je intelligenter die KI, desto menschlicher muss Führung werden

Künstliche Intelligenz macht diese Frage noch dringlicher. Die Debatte konzentriert sich häufig auf Automatisierung, Effizienz und Produktivität. Die tiefere Veränderung betrifft jedoch die Rolle des Menschen und damit zwangsläufig die Rolle der Führung.

Über Jahrzehnte war Wissen ein entscheidender Vorsprung. Wer mehr Informationen besaß, Zusammenhänge schneller erkannte und bessere Analysen erstellen konnte, hatte Einfluss. Heute können Systeme innerhalb von Sekunden Datenmengen auswerten, für die früher ganze Abteilungen notwendig waren. Künstliche Intelligenz fasst Studien zusammen, analysiert Märkte, entwickelt Szenarien und bereitet Entscheidungsoptionen vor.

Das macht den Menschen nicht überflüssig. Es verschiebt den Ort, an dem sein Wert entsteht. Wenn Information leichter verfügbar und Analyse zunehmend automatisierbar wird, gewinnt Urteilsvermögen an Bedeutung.

Zwischen Information und Entscheidung liegt Verantwortung. Genau diese Lücke kann Technologie nicht schließen. Ein System kann Risiken berechnen, Szenarien vergleichen und eine wirtschaftlich effiziente Option identifizieren. Es steht aber keinem verunsicherten Team gegenüber. Es führt kein schwieriges Gespräch. Und es trägt keine moralische Verantwortung für die Folgen einer Entscheidung.

Je intelligenter Maschinen werden, desto wichtiger wird deshalb die Qualität der Menschen, die ihre Ergebnisse bewerten. Nicht jede rechnerisch optimale Antwort ist automatisch eine verantwortbare Entscheidung. Führung muss Fragen stellen, die über die reine Analyse hinausgehen: Welche langfristigen Folgen hat dieser Weg? Was bedeutet er für unsere Kultur? Welche Werte stehen auf dem Spiel? Welche Konsequenzen sind wir bereit zu tragen?



Damit verändert KI auch den Maßstab für Autorität. Wer seine Stellung vor allem daraus bezog, mehr zu wissen als andere, verliert einen Teil dieses Vorsprungs. Was bleibt, sind Fähigkeiten, die sich nicht einfach delegieren lassen: Orientierung geben, Vertrauen schaffen, Konflikte austragen, Verantwortung übernehmen, Entscheidungen erklären und durch das eigene Verhalten Kultur prägen.

Technologie macht Führung deshalb nicht kleiner. Sie macht sie anspruchsvoller. Wenn leistungsfähige Systeme für immer mehr Organisationen verfügbar werden, entsteht Differenzierung nicht allein durch Technologie. Sie entsteht auch durch die Art, wie Menschen mit deren Möglichkeiten umgehen und welche Verantwortung sie für ihre Entscheidungen übernehmen.

Glaubwürdigkeit wird dabei zu einem Vorteil, der sich nicht installieren lässt. Vertrauen entsteht langsam: durch nachvollziehbare Entscheidungen, eingehaltene Zusagen, den Umgang mit Fehlern und die Bereitschaft, zu den eigenen Werten zu stehen, wenn es unbequem wird. Gerade unter Druck zeigt sich, ob Unternehmenskultur Realität oder Fassade ist.

Vielleicht erleben wir deshalb neben einer technologischen auch eine menschliche Verschiebung. Je mehr Antworten Maschinen liefern können, desto wichtiger wird die Fähigkeit, die richtigen Fragen zu stellen. Je präziser Prognosen werden, desto sichtbarer wird die Verantwortung dessen, der entscheidet. Je intelligenter unsere Technologie wird, desto menschlicher muss Führung werden.

Was bleibt, wenn der Titel verschwindet?

Jede Karriere endet. Irgendwann wird das Büro geräumt, der Laptop zurückgegeben, die E-Mail-Adresse deaktiviert. Ein anderer Name erscheint im Organigramm. Die Organisation geht weiter.

Der Titel bleibt als Funktion. Der Mensch geht. Gerade deshalb lohnt sich eine Frage, die erstaunlich selten gestellt wird: Was bleibt von einer Führungskraft, wenn ihre Position nicht mehr existiert?

Menschen erinnern sich selten an perfekt formulierte Präsentationen oder einzelne Quartalszahlen. Sie erinnern sich an den Vorgesetzten, der in einer schwie-

rigen Situation ruhig geblieben ist. An die Geschäftsführerin, die Verantwortung übernommen hat, obwohl sie den Fehler nicht selbst verursacht hatte. An den Teamleiter, der zugehört hat, bevor er entschied. An den Menschen, der Orientierung gegeben hat, als Orientierung fehlte.

Führung ist deshalb keine Belohnung für eine erfolgreiche Karriere. Sie ist eine Verpflichtung gegenüber anderen Menschen. Wer führt, beeinflusst nicht nur Ergebnisse, sondern Motivation, Entwicklung, Selbstvertrauen und die Bereitschaft anderer, selbst Verantwortung zu übernehmen. Diese Wirkung entsteht meist nicht in außergewöhnlichen Momenten, sondern im Alltag: in der Art, wie Kritik geäußert wird, wie mit Fehlern umgegangen wird, wie Anerkennung verteilt wird und wie über Menschen gesprochen wird, wenn sie den Raum verlassen haben.

Vielleicht gibt es am Ende eine Führungsfrage, die mehr über Autorität aussagt als jede Stellenbeschreibung: Würden Menschen dieser Person auch dann folgen, wenn sie morgen keinen Titel mehr hätte?

Wer diese Frage mit Ja beantworten kann, besitzt eine Form von Autorität, die kein Organigramm verleihen kann. Titel schaffen Zuständigkeiten. Vertrauen schafft Gefolgschaft.

Vielleicht haben wir Führung über viele Jahre zu stark mit Position, Hierarchie, Macht und Status verbunden. Dabei beginnt sie an einem anderen Punkt: dort, wo Menschen freiwillig Vertrauen schenken. Ein Titel kann Verantwortung übertragen, Zuständigkeiten definieren und Türen öffnen. Führung kann er nicht verleihen.

Sie entsteht im täglichen Handeln: in Entscheidungen, die niemand kontrolliert; in einer Haltung, die auch dann bestehen bleibt, wenn sie unbequem wird; in der Bereitschaft, Verantwortung zu übernehmen, obwohl keine perfekte Lösung existiert.

Nicht der Titel entscheidet darüber, ob Menschen folgen. Nicht das Organigramm. Nicht die Visitenkarte. Sondern der Mensch. Denn am Ende erinnert sich niemand an die Bezeichnung auf einer Tür. Menschen erinnern sich daran, wie sie geführt wurden. Und genau deshalb reicht der Titel nicht mehr aus. -v-





Visionärer Pragmatismus und Future Leadership

STEFAN SELKE

Vom Risikodenken zur euphorischen Transformation

Unsere Welt ist auch deshalb ein trostloser Ort, weil wir in einer risikoscheuen Sprache und Vermeidungsimperativen (von „Nulltoleranz“ bis „Risikominimierung“) über sie sprechen. Vieles wurde in letzter Zeit richtig gemacht, eines jedoch vergessen: Future Leadership braucht Zukunftseuphorie, um Erwartungen zu bündeln und zum Aufbruch anzuleiten.

Zwei Kontrastbeispiele: Bei einem lange vorbereiteten Satellitenstart bei der Europäischen Raumfahrtagentur ESA gehen Manager nach kaum fünf Minuten wieder zurück in ihre Büros – kein Jubel, kein Abklatschen, keine Party. Anders hingegen der CEO des Start-ups Bake in Space, das versucht, eine krümelfreie Brotmischung für Weltraumreisen zu entwickeln: Auf einem Kongress präsentiert er sein Produkt derart voller Begeisterung, dass niemand im Raum ungerührt bleibt. Der Unterschied: Die ESA verfolgte schlaue Pläne, Bake in Space lieferte emotionale Beteiligung mit überspringender Überzeugungskraft. Genau das ist der Unterschied zwischen Projekten und Missionen. Deshalb basiert Future Leadership auf positiver Zukunftsbejahung, weil sich nur so die allgegenwärtige Krisenerstarre auflockern lässt.

An der Schwelle zur Perspektivlosigkeit

Warum ist das so? Erstens lässt sich empirisch belegen, dass viele Gesellschaften an der Schwelle zur Perspektivlosigkeit stehen. Gerade die Vermessung von Gemütszuständen junger Menschen ist besorgniserregend. Zahlreiche Studien (v. a. in der DACH-Region) belegen, dass Resignation das Grundrauschen bildet. Auch Erwachsene sind zunehmend überfordert. Post-Corona-Studien und Studien zur Kritikalität der Welt zeichnen ein tendenziell pessimistisches Zukunftsbild. Kontingenzangst, die Mischung aus Ungewissheit, Orientierungslosigkeit und überfordernder Optionsvielfalt, führt zur Eintrübung langfristiger Zukunftserwartungen. Allerdings sind Wut, Resignation und Hoffnungslosigkeit

schlechte Ratgeber für Zukunftsfragen.

Zweitens ist Zukunftsgestaltung aus anthropologischer Sicht eine praktische Kompetenz. Was wir Zukunft nennen, ist eine kollektive Anstrengung und soziale Praxis. Zukunft ist nicht nur ein technischer Raum, sondern in Erzählungen, Bildern und Kulturerzeugnissen von Affekten und Empfindungen durchdrungen. Wer Zukunft sagt, sollte besser zwei Dimensionen im Blick haben: In der kognitiven Dimension geht es um Planung, Berechnung und Prognosen. In der korrespondierenden affektiven Dimension um die Verbindung abstrakter Zukunftsvisionen mit positiven Emotionen und Motiven.

Die Psychologie der Transformation fordert deshalb, Gefühlszustände nicht aus Kränkungs-erlebnissen, sondern aus sich selbst verstärkenden positiven Affekten herzuleiten. Statt aus dem Druck der Vergangenheit sollten Gefühle aus dem Sog der Zukunft resultieren. Kurz: Der Attraktor sollte die euphorische Betrachtung der Zukunft sein. In soziologischer Perspektive dient Zukunftseuphorie der Veränderung kollektiver Bewusstseinszustände, bricht hierarchische soziale Ordnungen auf, fördert neue Gruppenbindungen und hilft somit, herrschende Konventionen zu überwinden und sich auf mutige Experimente einzulassen.

Euphorie verändert die Wahrnehmung der eigenen Umwelt vom Krisenmodus hin zur Vorstellung, Teil einer besseren Welt zu sein. Dies motiviert zur aktiven Teilnahme an Gestaltungsprozessen. Wir brauchen deshalb nicht nur bessere Zukunftsbilder, sondern vor allem eine starke, positive emotionale Verbindung mit diesen Bildern.

Kritiker werden bemängeln, dass der Ruf nach euphorischer Bejahung des Kommenden in einer Epoche, der langsam Begriffe für Negativbeschreibungen ausgehen, wie ein Frevel wirkt. Gleichwohl gibt es ein starkes Gegenargument: Jede Krise hat

ein Danach. In Krisenzeiten über Zukunftseuphorie nachzudenken, ist deshalb nicht obszön. Gerade weil Polykrisen unsere Wahrnehmung dominieren, macht es Sinn, den Blick prophylaktisch auf Polyoptionen zu richten. In einer erschütterten Welt braucht es radikale Perspektivwechsel. Trotz problematischer Gegenwart bereitet Zukunftseuphorie auf das Kommende vor, hilft, der allgegenwärtigen Resignation zu entkommen, Zukunft wieder vorstellbar zu machen und schlussendlich Handlungsoptionen zu entdecken.

Das wäre allemal zielführender, als weiterhin in die Nostalgie zu flüchten, Märchen von (techno-utopischen) Idealwelten zu verbreiten oder sich spekulativen Verheißungen und Vertröstungen hinzugeben. Auch passives Warten auf Veränderungen oder das allgegenwärtige Durchwursteln sind keine Lösungen. Politik wandelt Begeisterung für die Zukunft in normative Richtlinien oder operative Nützlichkeitsregeln um und reproduziert dabei lediglich Standardwelten. Und die akademische Welt wird immer wieder als Abklingbecken für Kreativität erlebt. Selbst in Unternehmen geht es zu oft um die Verhinderung eines Übels anstatt um das Erreichen eines Zieles.

Future Leadership beginnt deshalb damit, ein Leitbild über Bord zu werfen, das (meist unhinterfragt) auf Anpassung beruht, denn Anpassung ist ein Symbol des Stillstands. Wir dürfen nicht zulassen, dass passives und angetriebenes Warten zur Grundeinstellung unserer Gesellschaft wird. Aufbruch steht hingegen für eine Transformation in Richtung lebenswerter Zukünfte. Vor allem gilt: Sich auf die Zukunft einzustellen, bedeutet gerade nicht, sich alternativlos anzupassen.

Visionärer Pragmatismus als Grundlage für Future Leadership

Zukunftsfähigkeit bedeutet die Fähigkeit, die widerspenstige Wirklichkeit gerade nicht zu leugnen und trotz aller Krisenwahrnehmungen konsequent Anreize für einen optimistischen Wandel zu entwickeln. Diese Haltung nenne ich visionären Pragmatismus – der dritte Weg zwischen Pessimismus

oder Optimismus. Visionärer Pragmatismus ist die illusionsfreie Anerkennung von Realitäten, gleichzeitig aber auch das mutige, von Zukunftseuphorie getragene Denken darüber hinaus. Der Rausch des Kommenden ist weder Flucht, noch Eskapismus oder nur kurzes Hochgefühl, sondern eine emotionale Investition in die wertvollste Ressource, die wir besitzen: Zukunft.

Für gesamtwirtschaftliche Effekte braucht es nicht nur Geld oder schlaue Pläne, es braucht vor allem eine positive emotionale Grundierung: Zukunftseuphorie. Erst auf dieser Grundlage kann der Shift von angst- zu wunschgetriebener Zukunftsgestaltung – von „future by disaster“ zu „future by design“ – gelingen. Es lohnt sich, über Zukunftseuphorie als das „Missing Link“ von Future Leadership nachzudenken. Denn Aufbruch beginnt dort, wo wir uns selbst überraschen. -v-





Das Sisyphus-Syndrom

WOLFGANG LUSAK

Warum Sicherheitsarbeit ohne gesellschaftliche Mitte nie ans Ziel kommt

Erkennen wir die wahren Dimensionen der Bedrohungs- und Krisen-Lawine, die uns gerade in Europa überrollt? Ist uns klar, dass die Wild-West-Methoden der Unsicherheitsverbreiter eine neue Dimension globaler Sicherheitskonzepte erfordern? Schwierige Frage. Können wir uns darauf einigen, dass nichts so bleibt, wie es einmal war? Das wäre ein Anfang dafür, den Überblick zurückzugewinnen.

Den Überblick darüber, wie wir jetzt unsere Landesverteidigung gestalten, hybride Kriegsführung, Drohnenangriffe und Sabotage an Infrastruktur abwehren sowie Terroranschläge, Kriminalität und illegale Migration verhindern. Darüber, wie wir Bränden, Wasserverknappung, Ernteausfällen, Energieengpässen und Blackouts begegnen. Wie wir unsere digitalisierten Daten vor Hackern schützen, gleichzeitig Menschen zum richtigen Umgang mit Handys und Internet bringen. Wieso es wenigen Menschen gelingt, auf Kosten vieler unermesslich reich zu werden und damit gewaltige gesellschaftliche Schieflagen zu erzeugen. Wie globale Verführungssysteme Menschenmassen mit Drogen, Spielen, Erzählungen und Genüssen zu Alltags-Junkies machen. Wie heute Top-Manager die Einführung von KI in ihren Konzernen befehlen – ohne zu wissen, was sie damit zerstören und auslösen. Wie wir aus verwöhnten und anspruchsvollen wieder verantwortungsvolle, resiliente und wehrfähige Menschen machen. Wie man angesichts Klimawandel und Ressourcen-Verknappung aus Feindbildern heraus wieder in kooperative Partnerschaften hineinfindet. Warum sich die Mehrheit der Menschen von ihren vordergründig demokratischen Regierungen oder auch hintergründigen diktatorisch-monopolistischen Mächtigen unverstanden, ignoriert und ausgebeutet fühlt. Wie sich der Zyklus wachsender Gewalt beschleunigt.

Macht es nicht wie Sisyphus

Es wird uns ja täglich vor Augen geführt, dass es nicht genügt, einzelne Firewalls aufzubauen, KI-gesteuerte Raketen-Abwehrsysteme zu installieren, Wasser-Stauseen anzulegen, Zucker zu verbieten, E-Bike-Fahrern Helme aufzusetzen, zu Selbstverteidigungskursen zu verpflichten, usw. Solange wir in einem von Menschen- und Umweltverachtung dominierten System leben, das Gier, Dummheit und Gewalt zu viel Platz gibt. Solange in dieser Welt begrenzter Ressourcen immer mehr Ungerechtigkeit und damit Unsicherheit entsteht. Solange alle um partielle Sicherheitslösungen bemühten Experten, Wissenschaftler oder Entscheider im Sisyphus-Arbeitsmodus verharren. Sich dabei – bei allem Respekt – zu nützlichen Idioten der diktatorisch-monopolistischen Mächtigen machen.

Tatsächlich ist unsere Welt unsicherer geworden. Weil sie gezielt unsicherer gemacht wurde, weil wir das Unsicherheitsgefühl selbst bis hin zur Hysterie medial verbreiten. Weil extremistische Machtmenschen sowie Manager monopolistischer Big-Data-Konzerne trotz schlimmer Kollateralschäden ihre Wege fortsetzen. Und sich gut bezahltes, system-konformes Sicherheitspersonal ins Fäustchen lacht. Es wird also nicht genügen, die technischen und oberflächlichen Symptome der Unsicherheit einzeln zu bekämpfen, wir müssen ihre wahren Ursachen gesamthaft verstehen und daraus Strategien für eine neue, weltweit krisen-feste Gesellschaft ableiten.

Meine Kernaussage ist: Solange wir in einer ungerechten Welt leben, wird sich die Sicherheitslage weiter verschlechtern. Wir brauchen einen gesellschaftlichen Wandel zur Errichtung einer gerechten und verantwortungsvollen Sicherheits- und Demokratie-Struktur. Die Mitte wird dabei eine entscheidende Rolle spielen.

Wie die „unheilige Allianz“ dominiert und Mitte zerstört

Ich bin seit Jahrzehnten mit der Durchsetzung nachhaltig-digitaler Innovationen beschäftigt und beobachte als Coach politischer Organisationen die Lobby-Netzwerke der Macht in den westlichen Demokratien. Diese Macht schafft eine künstliche Spaltung zwischen Links und Rechts, Jung & Alt, Arm & Reich, Arbeitenden & Sozialhilfe-Bedürftigen, Insidern & Outsidern. Was letztlich nur der „unheiligen Allianz“ zwischen Monopol-Kapitalisten und Links- oder Rechts-Populisten zugutekommt. Weil das zu einer Gesellschaft führt, die wie eine Schachfigur aussieht, in der oben im Kopf der Rahm abgeschöpft wird, in der unten die sozial Schwachen mit „Brot & Spielen“ sowie „Teilen & Herrschen“ ruhiggestellt werden und dazwischen die am meisten zum Brutto-sozialprodukt beitragende Mitte ausgepresst wird.

Dazu kommt, dass rund 70 % der Weltbevölkerung in Diktaturen lebt, dass autoritäre Regime sogar wieder zunehmen und teilweise auch Europa bedrohen. Russland betreibt territoriale Angriffskriege, China aggressive Wirtschaftspolitik, USA Big-Tech-Monopole und Militäraktionen für Ressourcen-Zugriffe.

In den westlichen, vor allem europäischen Demokratien bilden der unternehmerische Mittelstand und die vollzeitarbeitende, angestellte Mittelschicht die „Mitte der Gesellschaft“, welche als „Nettozahler“ den wichtigsten Leistungsträger stellt. Sie macht als Wertegemeinschaft der Werte Leistung, Eigentum, Nachhaltigkeit und Fairness gut ein Drittel der Bevölkerung aus. Sie leidet unter Steuerungerechtigkeit, Bürokratie sowie schlechtem Zugang zu Kapital und monopolisierter Technologie. Sie erhält Staat und Gesellschaft mit Konsum, Inves-

tion, Innovation, Verantwortungsbewusstsein und ausgleichendem Verhalten. Von ihr wird zu Arm und Reich umverteilt, weil es superreiche Investoren und monopolistische Konzerne immer wieder schaffen, Steuerzahlungen zu vermeiden. Aber wenn die Mitte zu sehr belastet wird, verliert sie ihre Kreativität, Innovationskraft und Wettbewerbsfähigkeit. Wenn sie zugrunde geht, geht auch der Staat zugrunde.

So entstand die „Schachfiguren-Gesellschaft“

Trotz gegenteiliger Aussagen populistischer Politiker hat die Mitte der Gesellschaft nicht nur eine sehr schwache Interessenvertretung und Lobby, sie wird auch medial zwischen extremistischen Polarisierungen auf einen Punkt reduziert, was die unsere Existenz gefährdende „Schachfiguren-Gesellschaft“ (© Lusak) zur Folge hat: Oben den Kopf des gierigen Monopol-Kapitalismus mit seinen Handlangern und Politikern. Unten die sozial Schwachen und eine Working-Poor-Masse. Dazwischen die Mitte der Gesellschaft, die sich kaum mehr durchsetzen kann, weiter ausgehöhlt wird und damit den immer dünner werdenden Hals der Schachfiguren-Gesellschaft bildet.

Dass sich der Monopol-Kapitalismus der Superreichen und Konzerne so leicht an der Spitze der Schachfiguren-Gesellschaft halten kann, liegt an dem Umstand, dass populistische Politik mit Kapitalismus gerne kollaboriert. Weil sie gleiche Ziele und Strategien haben: den eigenen Machterhalt und die Beherrschung der Massen. Konzerne brauchen billige Arbeitskräfte für alles, was noch nicht digitalisiert ist, sowie Käufer ihrer billigen, oft auch gesundheitsgefährdenden Massenprodukte und Marken. Populistische Politik will mit ihren Gewerkschaften





genau von der gleichen Zielgruppe ihre Stimme bei der Wahl. Monopolisten können situationselastisch sowohl mit Links- wie mit Rechtspopulisten kollaborieren. Mit den Linken schwören sie auf Wokeness, Antirassismus und Klimawende, mit den Rechten auf Heimat, Nationalstolz und Religion. „Wer braucht da noch die Mitte?“ ist die dabei unausgesprochene und kurzsichtige Frage.

Mit jedem Tag, an dem der Krieg weitergeht, das Weltklima heißer wird, Inflation und Arbeitslosigkeit wächst, Kriminalität und Gewalt steigt, KI wuchert, digitale Souveränität sinkt und die Unsicherheit zunimmt, brauchen wir mehr denn je Sicherheit mit zentrierter Vernetzung.

Die Lösung liegt in der runden Mitte

Damit die Menschheit überlebt, braucht es daher mehr Platz für Übersicht, Balance und Mitte. In der runden, kugelförmigen, widerstandsfähigen, krisenfesten Gesellschaft der Mitte gibt es wenige Superreiche und Arme und dafür viele fair behandelte Leistungsträger. Zu diesen Leistungsträgern der Mitte gehören die Führungskräfte und Experten von vitalen, sicherheitsbezogenen Diensten wie Militär, Polizei, Medizin, Technologie, Digitalisierung, Lebensmittel-, Wasser- und Energiewirtschaft usw. Entscheidend wird sein, dass nicht mehr Reichtum und Armut bekämpft wird, sondern die Mitte so sehr befreit und gestärkt ist, dass exorbitanter Reichtum und fürchterliche Armut quasi automatisch vermieden werden.

Um so einen stabilen Staat aufzubauen, ist zuerst einmal ein umfassendes Mitte-Monitoring, eine neue Kultur der Mitte in Körper, Geist, Seele und Gesellschaft, eine Demokratiereform mit einer echten Repräsentanz der Mitte in einem schlanken, sparsamen Staat aufzubauen. Dann sind noch faire Rahmenbedingungen für KMU und Mittelschicht und vor allem Unterstützung bei deren Entwicklung von Innovationen für globale Wettbewerbsfähigkeit und neue Einkommensmöglichkeiten zu erreichen.

Leadership, Human-Ressource-Management & White Lobbying sind gefragt

Als engagierter Mensch und Coach nachhaltiger Innovations-Prozesse möchte ich auf die Leadership- und Human-Ressource-Management-Skills hinweisen, die erforderlich sind, um die runde Gesellschaft der Mitte zu realisieren und damit auch weltweite Verbesserungen in den Bereichen Sicherheit, Resilienz und Krisenbewältigung zu ermöglichen. Diese Skills sollten in die auf Einzelslösungen, auf vernetzte Lösungssysteme und auf komplette Sicherheits-, Souveränitäts- und Resilienzkonzepte ausgerichteten Fachkreise aufgenommen werden. Im Geist der Balance, Gerechtigkeit, Friedfertigkeit und Kooperation. Und wohl auch im Geist des immer gültigen „kategorischen Imperativs“ von Immanuel Kant, der vereinfacht bedeutet: „Was du nicht willst, das man dir tut, das füg auch keinem anderen zu.“ Das alles braucht Führungspersönlichkeiten, die vorangehen und die Fähigkeit haben, Menschen überzeugend anzusprechen, zu motivieren und zu mobilisieren.

Ich lade ein, dazu Vorschläge zu machen, und erlaube mir vier erste Empfehlungen auszusprechen, die ich somit zur Diskussion stelle:

- Bekenntnis zur ideologischen und wirtschaftlichen Unabhängigkeit der Wissenschaft, Expertise und Praxis-Erfahrung aus dem Fachbereich Sicherheit, Souveränität, Datenschutz, Resilienz, Risiko- und Krisenmanagement von Einflüssen der Monopole und Politik.
- Forcierung von sicherheitsrelevanten Forschungen, Entwicklungen und Innovationen sowie Open-Innovation-Prozessen im Rahmen von Arbeitsgruppen, Plattformen, Kooperationen und Vereinigungen – nach den Prinzipien der „runden Gesellschaft der Mitte“, weil Innovationen der Quell aller humanen Fortschritte sind.

WE SHAPE THE FUTURE

NEXT LEVEL EDUCATION
Excellent.Connected.Individual.



SCHOOL OF EXCELLENCE
FOR LEADERSHIP, RISK- AND
INNOVATION MANAGEMENT

powered by
**ZRK Beteiligungs-, Service
und Management GmbH**

SOE.ZRK.ACADEMY

CYSMEC

CYber SMart EConomy Conference

RESILIENT TODAY. SECURE TOMORROW.

Internationale Konferenz zu Cyber 3D, Smart Products, Supply Chain Management sowie Resilienz- und Krisenmanagement.

Wirtschaft, Wissenschaft und Politik im Dialog.

WIRTSCHAFT.
WISSENSCHAFT.
POLITIK.

CYBER 3D

SMART
PRODUCTS

SUPPLY CHAIN
MANAGEMENT

RESILIENZ &
KRISENMANAGEMENT



MEHR ERFAHREN

www.cysmec.eu

12.-13. MAI 2027

PARLAMENT
WIEN

NTS

RELAX, WE CARE

NTS NETZWERK TELEKOM SERVICE AG
NETWORK | DATA CENTER & PLATFORM | SECURITY | COLLABORATION | SUPER SERVICES
GRAZ | WIEN | LINZ | INNSBRUCK | SALZBURG | DORNBIRN | KLAGENFURT

www.nts.eu

TALKS.
PANELS.
WORKSHOPS.
NETWORKING.

FOTO: Lupi Spuma

Zuschriften:

ZRK Beteiligungs-, Service und Management GmbH
c/o Office Center Graben 28, Graben 28/1/12, 2.5, A-1010 Wien

Leserbriefe & Reaktionen:

per eMail an leserbrief@vanguardmag.eu

Presseanfragen:

per eMail an presse@vanguardmag.eu

Einschaltungen, Inserate udgl.:

per eMail an inserat@vanguardmag.eu