VANGUARD

— LEAD & INNOVATE —

SEITE 9

DIGITALE SCHATTEN WIRTSCHAFT

AUS KRIMINELLEN SCRIPTS WERDEN GLOBALE SERVICES

SEITE 36

SICHERHEIT NEU DENKEN

EIN AUFRUF ZU FÜHRUNGS-VERANTWORTUNG UND RESILIENZ

SEITE 48

KI TRIFFT 5G

WIE TECHNOLOGIE EUROPAS SOUVERÄNITÄT VERÄNDERT

AUSGABE 01/25

IMPRESSUM - *Medieninhaber & Verleger:* ZRK Beteiligungs-, Service und Management GmbH, Reisnerstrasse 5/20a, A-1030 Wien, Tel: +43 650 2252991, Mail: office@zrk.gmbh, ***Herausgeber:*** DI Johannes Göllner, Robert-P. Pelikan, ***Redaktion:*** Zentrum für Risiko- & Krisenmanagement, Reisnerstrasse 5/20a, 1030 Wien, ***Chefredaktion:*** DI Johannes Göllner, Robert-P. Pelikan, ***Vertrieb & Logistik:*** ZRK Beteiligungs-, Service und Management GmbH, Reisnerstrasse 5/20a, A-1030 Wien, ***Konzept, Gestaltung & Layout:*** Robert-P. Pelikan – iKnooow, ***Marketing & Kommunikation:*** Robert-P. Pelikan – iKnooow, ***Kundenservice & Aboservice:*** ZRK Beteiligungs-, Service und Management GmbH, Reisnerstrasse 5/20a, A-1030 Wien, ***Vorsitzender des Redaktionsbeirates:*** Tit.-Univ-Prof. Dr.habil. DDr. Thomas Benesch, ***Strategisches Marketing & PR:*** Mag. Manfred Oschounig, ***Druck:*** Bösmüller Print Management, Wien - Stockerau, www.boesmueller.at, ***Autoren dieser Ausgabe:*** siehe www.vanguardmag.eu, ***Bildquellen, sofern nicht anders gekennzeichnet:*** Zentrum für Risiko- und Krisenmanagement, iKnooow, Pexels, Midjourney, Wikipedia Commons, die Autoren bzw. Unternehmen der jeweiligen Artikel, ***Offenlegung gemäß § 25 Mediengesetz:*** Das Magazin „VANGUARD" versteht sich als Fachmagazin für Führungskräfte, Entrepreneure, IT-Verantwortliche und Abteilungsleiter, die in der digitalen Ära erfolgreich sein und Vorreiterrollen in ihren Bereichen übernehmen wollen. Ziel der Publikation ist die Information und Weiterbildung der Leser sowie die Förderung des Austauschs innerhalb der Fachgemeinschaft. ***Haftungsausschluss:*** Alle in dieser Publikation veröffentlichten Inhalte wurden sorgfältig geprüft. Dennoch übernehmen Herausgeber, Autoren und Verlag keine Haftung für die Richtigkeit und Vollständigkeit der Angaben. Alle Angaben erfolgen ohne Gewähr. ***Website:*** www.vanguardmag.eu | ***DISCLAIMER:*** Aus Gründen der besseren Lesbarkeit haben wir auf das Gendern verzichtet. Selbstverständlich beziehen sich alle in diesem Magazin verwendeten Begriffe und Formulierungen auf Personen jeglichen Geschlechts.

Sicherheit denken. Verantwortung gestalten. Zukunft ermöglichen.

Mit dieser zweiten Ausgabe von **VANGUARD – Lead & Innovate** setzen wir bewusst ein Zeichen: Sicherheit ist heute nicht mehr bloß ein technisches Thema, ein Compliance-Kapitel oder ein punktuelles Projekt. Sie ist zur strategischen Führungsaufgabe geworden – und damit zum Prüfstein moderner Organisationen, resilienter Systeme und verantwortungsvoller Führungskultur.

Wir leben in einer Zeit, in der klassische Sicherheiten brüchig geworden sind: Lieferketten reißen, Desinformation zirkuliert schneller als Fakten, Cyberangriffe treffen nicht mehr nur Großkonzerne, sondern zunehmend auch öffentliche Institutionen, KMU und kritische Infrastrukturen. Gleichzeitig bringen technologische Entwicklungen wie generative KI eine neue Qualität an Komplexität und Geschwindigkeit mit sich – sowohl in den Risiken als auch in den Chancen.
Was heute zählt, ist die Fähigkeit, Wandel nicht nur zu überstehen, sondern ihn aktiv zu gestalten. Und genau hier beginnt Sicherheit – nicht als Einschränkung, sondern als Ermöglichung. Nicht als starres Korsett, sondern als dynamisches Prinzip, das Orientierung gibt, wo Unsicherheit wächst. Wer Sicherheit ganzheitlich denkt – als Verbindung von Technologie, Kultur, Führung und Verantwortung – schafft die Grundlage für Zukunftsfähigkeit.

Die Beiträge dieser Ausgabe spannen ein breites thematisches Feld auf: von Social Engineering und KI-basiertem Phishing über resiliente Kommunikationsstrukturen und strategisches Risikomanagement bis hin zu europäischer Souveränität, normativer Führung und der Rolle der Sicherheit auf Messen und Großveranstaltungen. In all diesen Bereichen wird eines deutlich: Die Bedrohungen sind vernetzter, die Angriffsflächen vielfältiger – und einfache Lösungen greifen zu kurz.

Besonderes Augenmerk gilt dem Menschen – als Angriffsfläche, aber vor allem als Schutzfaktor. Sicherheit beginnt im Kopf. In der Art, wie wir kommunizieren, entscheiden, Verantwortung übernehmen. Und wie wir Organisationen befähigen, mit Unsicherheiten produktiv umzugehen. Klassische Awareness-Maßnahmen allein reichen nicht mehr. Es braucht eine neue Sicherheitskultur – geprägt von Vertrauen, Klarheit und echter Beteiligung.
Sicherheit ist dabei kein Selbstzweck. Sie ist der Möglichmacher für Innovation, die Voraussetzung für mutiges Handeln. Nur wer weiß, wie er mit Risiken umgeht, kann bewusst Neues wagen. Nur wer vorbereitet ist, bleibt entscheidungsfähig – auch dann, wenn die Welt um ihn herum aus den Fugen gerät.

VANGUARD – Lead & Innovate versteht sich in diesem Kontext als Plattform für Vordenker:innen, Strateg:innen und Verantwortungsträger:innen. Als Ort für mutige Fragen, konkrete Impulse und vernetztes Wissen. Wir möchten Orientierung geben – nicht im Sinne fertiger Antworten, sondern durch Perspektiven, die zum Weiterdenken und Handeln einladen.
Diese zweite Ausgabe ist nicht nur eine Sammlung analytischer Beiträge. Sie ist ein Plädoyer für einen Perspektivwechsel: Weg vom reaktiven Risikodenken, hin zu einem gestaltenden Sicherheitsverständnis. Denn Zukunft passiert nicht. Sie wird gemacht – von Menschen, die bereit sind, Verantwortung zu übernehmen.

In diesem Sinne: Lassen Sie sich inspirieren. Hinterfragen Sie Routinen. Bauen Sie Strukturen, die auch unter Druck tragen. Und gestalten Sie mit uns eine resiliente, handlungsfähige Zukunft – lokal, regional, international.

Robert-P. Pelikan
Herausgeber & Chefredakteur

Inhaltsverzeichnis

3 Editorial

6 Risikomanagement und IKT-Sicherheit: Kommunale Verwaltungen brauchen mehr als Passwörter und Cyberversicherungen

7 Geopolitische Spannungen und ihre Auswirkungen auf die öffentliche Sicherheit

9 Die Schattenwirtschaft im Netz: Wie Cybercrime-as-a-Service zur realen Gefahr wird

14 Unsere Demokratie: Gefährdung durch Cyberangriffe im Rahmen hybrider Kriegsführung

15 Sei keine Schwachstelle!

16 Mobiles Arbeiten und Sicherheit

18 Phishing: Wenn Digitalisierung zur Gefahr wird

20 Wenn KI zum Angreifer wird: Was uns in Zukunft erwartet und wie die BPN Group mit AI Driven Tools Cyber Attacken entgegenwirkt

22 META KI bringt neue Spielregeln – das betrifft auch Events und Messen

24 Kryptografie im Umbruch: Warum Unternehmen jetzt ihre Post-Quantum-Strategie planen müssen

26 Finanzielle Betrugsdelikte und Steuerhinterziehung im Zeitalter der Cyberkriminalität: Bedrohung für Staat und Gesellschaft – Herausforderungen und Lösungsansätze für die Aufklärung

29 Risikominimierung durch Technologie: Computervision in der Logistiksicherheit

32 Phishing im Zeitalter von KI: Neue Herausforderungen und ein innovativer Lösungsansatz

Inhaltsverzeichnis

34 SOCIAL ENGINEERING – Sicherheit beginnt im Kopf

36 Zukunft gestalten heißt: Sicherheit neu denken

38 Neue Spannungsverhältnisse und Interdependenzen im Kontext der Cybersecurity und neuer regulatorischer Anforderungen

40 Kritische Infrastrukturen im Fadenkreuz: Wie sicher ist unsere Versorgung wirklich?

45 Digitale Souveränität als strategische Herausforderung für Cybersicherheit und Unternehmensentscheidungen

46 Chinese Social Credit System

49 5G-AI Integration is reshaping technology and digital sovereignty

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

53 Strategische Resilienz

55 Gelebte IT-Sicherheit – Projekt CONTAIN verbindet Forschung und Praxis

56 Von der digitalen Resilienz gemäß der DORA-VO (EU) 2022/2554 zur integrierten operationellen Resilienz im Banksektor

58 ZRK – Gemeinsam Zukunft sichern

60 Ist der Leitfaden für Compliance-Management-Systeme in kleinen und mittleren Unternehmen ein Lichtblick?

63 Quantitatives und qualitatives strategisches und operatives Risikomanagement in Unternehmen in Relation zu NIS-2

64 Cybersicherheit 2025: Resilient. Intelligent. Vernetzt.

Mario GUBESCH, *BA MA MBA*

Risikomanagement und IKT-Sicherheit: Kommunale Verwaltungen brauchen mehr als Passwörter und Cyberversicherungen

Digitale Angriffe, Datenverlust oder Systemausfälle sind keine hypothetischen Bedrohungen mehr. Vielmehr stellen sie reale Herausforderungen für Städte und Gemeinden dar. Risikomanagement in der kommunalen Praxis wird häufig auf IKT-Sicherheitsthemen wie Passwörter, Firewall-Einstellungen oder Cyberversicherungen reduziert. Diese technische Sichtweise greift jedoch zu kurz. Risikomanagement ist weit mehr als nur IKT-Sicherheit; es ist ein integraler Bestandteil einer strategisch ausgerichteten und widerstandsfähigen Verwaltung.

Kommunale Verwaltungen agieren sowohl hoheitlich als auch wirtschaftlich. Sie verwalten Steuern, vergeben Aufträge, betreiben kritische Infrastrukturen und erbringen Dienstleistungen für Bürgerinnen und Bürger. All diese Tätigkeiten sind mit Risiken behaftet, sei es personell, rechtlich, finanziell oder zunehmend digital. Ein systematisches Risikomanagement muss daher die gesamte Organisation erfassen und strukturieren und nicht nur ihre IT-Abteilung.

Ein zentrales Ergebnis aus der Masterarbeit „Risikomanagement in der oberösterreichischen kommunalen Verwaltung“ ist die Entwicklung eines kommunalspezifischen Risikomodells, das auf nationalen und internationalen Standards wie ISO 31000 und dem COSO-Rahmenwerk basiert. Es differenziert zwischen normativer, strategischer und operativer Ebene und stellt sicher, dass Risikomanagement nicht isoliert, sondern als durchgängiger Steuerungskreislauf nach dem Prinzip Plan – Do – Check – Act implementiert wird.

Auf der **strategischen Ebene** liegt die Verantwortung bei politischen Entscheidungsträgern wie Bürgermeister, Gemeinderat und Amtsleitung. Sie definieren die Risikopolitik, schaffen Strukturen und weisen Ressourcen zu. Ihre Aufgabe ist es, Risiken nicht nur zu genehmigen oder zu verhindern. Sie müssen diese aktiv bewerten, Chancen erkennen und Prioritäten setzen.

Die **operative Ebene** besteht aus Amtsleitung, Risikomanagement-Beauftragten und Abteilungsleitungen. Sie ist für die Identifikation, Analyse und Steuerung konkreter Risiken zuständig. Hier müssen Risiken wie Personalausfälle, Vertragsverletzungen oder Datenschutzverletzungen frühzeitig erkannt und systematisch bearbeitet werden.

Ein oft vernachlässigter, aber zentraler Bestandteil ist die **normative Ebene**. Sie gibt den Werterahmen und das Selbstverständnis der Verwaltung vor. Nur wenn Risikobewusstsein und Verantwortungsgefühl fest in der Organisationskultur verankert sind, kann Risikomanagement langfristig wirken. Die besten Systeme nützen wenig, wenn Mitarbeitende Risiken nicht erkennen oder melden wollen.

IKT-Sicherheit ist in diesem Kontext nicht losgelöst zu betrachten. Vielmehr ist es ein kritischer Teilbereich. Kommunale IT-Systeme müssen nicht nur technisch abgesichert, sondern organisatorisch eingebettet werden. Dazu zählen Zugriffs- und Berechtigungskonzepte, Schulungen, die Trennung von operativer Umsetzung und Kontrolle sowie ein transparentes Reporting über Vorfälle und Schwachstellen. Automatisierung kann hier helfen, um die Mitarbeitenden zu entlasten und die Reaktionsgeschwindigkeit zu erhöhen.

Das **kommunale Risikomanagementmodell** zeigt, dass es keine isolierte Aufgabe der IT-Abteilung sein darf, Risiken abzusichern. Eine gesamtheitliche Sichtweise ist notwendig. Nur wenn Verwaltungsspitze, operative Führungskräfte und Kontrollorgane wie Prüfungsausschüsse oder Kontrollämter zusammenarbeiten, lassen sich Risiken wirkungsvoll steuern. So können Kommunen widerstandsfähig gegen technische, wirtschaftliche oder gesellschaftliche Krisen werden.

Fazit: IT-Sicherheit ist wichtig, aber nur ein Teil des Ganzen. Ein professionelles, strategisch eingebettetes Risikomanagement stärkt nicht nur die Sicherheit von Daten und Systemen. Es sichert langfristig die Leistungsfähigkeit und das Vertrauen in die kommunale Selbstverwaltung. -v-

Björn HAWLITSCHKA

Geopolitische Spannungen und ihre Auswirkungen auf die öffentliche Sicherheit

Die Welt befindet sich in einer Phase erhöhter geopolitischer Spannungen, die die öffentliche Sicherheit in Europa bedrohen. Drei zentrale Konfliktzonen – der Krieg in der Ukraine, die Instabilität im Nahen Osten (einschließlich der Houthi-Aktivitäten im Jemen) und die Spannungen um Taiwan – prägen die globale Sicherheitslage. Hinzu kommt die Unberechenbarkeit eines einstigen Hegemon. Die US-Politik unter der aktuellen Regierung erschwert die transatlantische Partnerschaft mit den EU-Staaten sowie die Bündnisstärke der NATO.

Ukraine/Russland: Ein Krieg mit globalen Folgen

Der Krieg Russlands gegen die Ukraine, der seit 2022 andauert, hat die europäische Sicherheitsarchitektur nachhaltig erschüttert. Inzwischen reift eine weitere Erkenntnis: ein Frieden über Nacht würde die alte Ordnung nicht wieder zurückbringen. Ein Russland, das weiter die Konfrontation mit dem Westens sucht, würde eine Entlastung der Militärverbände nutzen, um vor anderen osteuropäischen Grenzstreifen Drohkulissen zu erzeugen. Die gemeinsame europäische Stimme, die drei Jahre lang für die Ukraine zu selten im Einklang erscholl, wäre jetzt umso mehr gefordert, da es nun um die Unantastbarkeit des EU-Gebiets geht.

Dabei brächte ein Frieden in der Ukraine noch weitere Herausforderungen für die Öffentliche Sicherheit Europas. Beginnen die Waffen zu schweigen, eröffnen sich Möglichkeiten für ihre Zweitverwertung: dem Verkauf auf den Schwarzmarkt. Europa machte hier bereits Erfahrungen mit dem Nachlasshandel des jugoslawischen Bürgerkriegs. Gleiches ist im Hinblick auf die Ukraine zu erwarten. Allein mit Blick auf das dschihadistische Terrorismusmilieu in Europa besteht ein größerer Abnahmemarkt als Ende der neunziger Jahre des vergangenen Millenniums.

Mit dem russischen Überfall hat der Kreml aber nicht nur die geografische Grenze überschritten. Es begann der Angriff auf Kritische Infrastrukturen, sei es als Cyberattacke oder als Sabotageversuch – und das umfasste den gesamten Westen. Die dadurch entstehenden Spannungen mit Moskau sind zu heiß, um sie sich als neuen Kalten Krieg schönreden zu können. Vielleicht mögen die neoimperialen Bestrebungen Putins Fantastereien bleiben. Doch Zusammenbrüche von Kritische Infrastrukturen erzeugen ein Klima von Dysfunktionalität und Destabilisierung. Diese Effekte treffen die europäischen Gesellschaft ins tiefste Rückenmark.

Naher Osten: Instabilität mit globaler Reichweite

Schon vor dem Angriff der Hamas auf Israel am 7. Oktober 2023 war der Nahe Osten ein Pulverfass mit hohem Polarisierungsfaktor. Doch die Intensität hat seitdem zugenommen und nimmt weiter zu. Die neue Gaza-Offensive des israelischen Militärs hat international Kritik ausgelöst und die unbedingte Solidarität westlicher Staaten zu Israel im Kampf gegen die Hamas geschmälert. Die aktuelle Entwicklung begünstigt noch stärkere Alleingänge der israelischen Regierung, was wiederum den Unmut von pro-palästinensischen Aktivisten verstärken dürfte. Bereits jetzt kommt es häufiger zu Gewalt-Eskalationen bei Protesten in westlichen Staaten. Sollte es tatsächlich zu einer dauerhaften Besetzung des Gazastreifens durch Israel und zu einer Vertreibung der Einwohner kommen, dürften die Proteste dagegen eine neue Dimension erreichen.

Zum aktuellen Nahost-Konflikt zählen längst die Houthi-Rebellen im Jemen. Unterstützt vom Iran, haben sie ihre Angriffe auf den Schiffsverkehr im Roten Meer intensiviert, was den Suezkanal – durch den 12 % des Welthandels fließen – zu einem kritischen Spannungspunkt gemacht hat. Die Houthi-Angriffe bedrohen die globale Handelssicherheit, was sich direkt auf die EU auswirkt, da sie stark auf Importe angewiesen ist. Höhere Frachtkosten aufgrund alternativer Handelsrouten um das Kap der Guten Hoffnung sowie Lieferengpässe belasten die Wirtschaft und treiben die Inflation weiter. Auch hier entfaltet sich eine destabilisierende Wirkung auf die europäischen Gesellschaften.

Taiwan/China: Ein potenzieller globaler Brandherd

Die Spannungen um Taiwan stellen den zentralen Konflikt im Hegemonialwettbewerb zwischen China und den USA dar. Chinas innenpolitische Herausforderungen – Wirtschaftskrise, Arbeitslosigkeit, soziale Unruhen – erhöhen den Druck auf die Kommunistische Partei, ihren Anspruch auf Taiwan durchzusetzen. Gleichzeitig hat Taiwan, unterstützt von den USA, seine Verteidigung massiv ausgebaut, was eine Invasion kostspielig und riskant macht. Dennoch bleibt die Gefahr einer militärischen Eskalation hoch, da ein Konflikt in der Taiwanstraße schnell zu einem regionalen oder globalen Krieg eskalieren könnte.

Aber nicht allein eine militärische Intervention Chinas in Taiwan wäre katastrophal. Auch eine Blockade der Insel hätte erhebliche Auswirkungen auf die öffentliche Sicherheit in Europa, insbesondere durch die Störung globaler Lieferketten. Taiwan,

insbesondere durch Unternehmen wie TSMC, produziert etwa 60 % der weltweiten Halbleiter und über 90 % der modernsten Chips (Stand 2025). Europa, das stark auf diese Chips für Automobilindustrie, Elektronik, Medizintechnik und Verteidigung angewiesen ist, würde mit massiven Engpässen konfrontiert. Beispiel: Die Chipkrise 2021-2022 führte in Deutschland zu Produktionsausfällen in der Autoindustrie – ein Taiwan-Konflikt könnte das um ein Vielfaches übertreffen.

Eine Blockade könnte auch die Schifffahrtsrouten in der Taiwanstraße (ca. 50 % des globalen Warenverkehrs) gefährden. Europa wäre indirekt von gestörten Öl- und Gaslieferungen aus Asien betroffen, was Energiepreise steigen ließe. Sollten Unternehmen aufgrund einer Blockade oder Intervention ihre Produktion drosseln oder stoppen, würde sich die Arbeitslosigkeit und die wirtschaftliche Unsicherheit in Europa erhöhen. Soziale Spannungen, aber auch die Kriminalität würden zunehmen und damit auch wieder die Destabilisierung der Gesellschaft. Europa müsste um den Willen seiner Stabilität auf Diversifizierung der Lieferketten und strategische Lagerhaltung setzen, um solche Szenarien abzumildern. Doch auch hier gilt: die Zeit für präventives Handeln wird knapp. -V-

Robert-P. PELIKAN

Die Schattenwirtschaft im Netz: Wie Cybercrime-as-a-Service zur realen Gefahr wird

Ein Blick hinter die Kulissen einer wachsenden Parallelökonomie

Cybercrime-as-a-Service professionalisiert kriminelle Aktivitäten im Netz: Angriffe lassen sich mieten, Phishing-Kits kaufen, Datenlecks abonnieren. Die digitale Schattenwirtschaft wächst – und stellt Unternehmen wie Behörden vor neue strategische Herausforderungen.

Die Professionalisierung des Verbrechens

Cyberangriffe sind heute keine Ausnahme mehr – sie sind Alltag. Und immer häufiger stellt sich heraus: Der Angreifer war gar kein Profi. Die Infrastruktur, die Malware, das Zugangswissen – all das wurde eingekauft, gemietet oder im Abo bezogen. Willkommen im Zeitalter von Cybercrime-as-a-Service (CaaS).

Was früher das Terrain hochspezialisierter Hacker war, ist heute ein Geschäftsmodell: kriminelle Dienstleistungen auf Knopfdruck – gut dokumentiert, skaliert, anonymisiert. Unternehmen, Behörden, NGOs – alle können zum Ziel werden. Und die Täter? Oft geografisch und juristisch unerreichbar.

Was ist Cybercrime-as-a-Service (CaaS)?

CaaS beschreibt den Verkauf oder die Vermietung krimineller Werkzeuge und Dienstleistungen im digitalen Raum. Der Begriff orientiert sich bewusst an kommerziellen Softwaremodellen wie „Software-as-a-Service (SaaS)" – nur mit gegenteiliger Intention.

Zu den gängigen Angeboten zählen:

- **Ransomware-as-a-Service (RaaS):** Schadsoftware mit Backend-Support, Updates & Anleitungen
- **Phishing-as-a-Service:** Vorlagen, Landingpages & Hosting für Fake-Login-Seiten
- **Botnets-on-demand:** Mietbare Netzwerke kompromittierter Geräte
- **Access-as-a-Service:** Verkauf von Zugangsdaten zu kompromittierten Systemen
- **Malware-Kits:** Baukastensysteme für trojanische Pferde, Keylogger und Remote Access Tools

Dabei gleicht der „Kundenservice" oftmals professionellen Plattformen – mit FAQs, Foren, Testversionen und manchmal sogar Geld-zurück-Garantie.

Die Akteure: Anbieter, Nutzer, Geschäftsmodelle

In der Schattenwirtschaft gelten eigene Marktregeln – aber die Rollen sind klar verteilt:

- **Dienstleister Entwickler:** Sie stellen Tools bereit, warten diese und entwickeln neue Versionen. Viele operieren ausschließlich als Softwareanbieter.
- **Vertrieb & Support:** Ähnlich wie bei SaaS-Modellen kümmern sich Mittelmänner oder Plattformen um Reichweite, Transaktionen und Kommunikation.
- **Kunden:** Das sind häufig nicht-technische Kriminelle, Einzeltäter oder Kleingruppen, aber auch professionelle Cybercrime-Zellen oder staatlich geförderte Gruppen.
- **Affiliates / Partnerprogramme:** Bei Ransomware-as-a-Service existieren oft Provisionsmodelle: Wer erfolgreich infiziert, bekommt einen Anteil vom Lösegeld.

So entsteht ein wirtschaftlich motiviertes Ökosystem, das auf Effizienz, Skalierbarkeit und niedrige Einstiegshürden setzt.

Der Marktplatz im Untergrund: Darknet, Telegram & Co.

Lange Zeit galt das Darknet als Hauptumschlagplatz für CaaS-Angebote – und tatsächlich florieren dort nach wie vor einschlä-

gige Foren wie Exploit.in, RAMP oder BreachForums. Doch der Trend geht in Richtung dezentraler und öffentlich zugänglicher Plattformen, die schwerer kontrollierbar sind:

Telegram: Beliebte Kanäle mit bis zu 20.000 Mitgliedern bieten Malware, Phishing-Kits, gestohlene Daten und Zugangsdaten.
Discord-Server: Genutzt für Schulungen, Taktikaustausch oder Verkauf von Exploits.
Clearnet-Foren & Social Media: Tarnung unter dem Deckmantel „IT-Security" oder „Bug Bounty"-Programme.

Zahlungen erfolgen nahezu ausschließlich in Kryptowährungen – bevorzugt Monero (XMR) oder Bitcoin (BTC). Identitäten werden über TOR-Netzwerke, temporäre E-Mail-Adressen und anonyme Wallets verschleiert.

Warum das Geschäftsmodell so gefährlich ist

Cybercrime-as-a-Service ist nicht nur eine technische Entwicklung – es ist ein wirtschaftliches Modell mit einer gefährlichen Logik:

Demokratisierung des Verbrechens: Früher benötigte man tiefes technisches Wissen. Heute reicht ein Zugang zum Internet und etwas Startkapital, um Angriffe durchzuführen, die Unternehmen lahmlegen können.
Professionalisierung der Anbieter: Viele CaaS-Plattformen operieren wie echte IT-Dienstleister: Sie bieten Support-Chats, Upgrades, Community-Foren und sogar Promotion-Aktionen. Dokumentation und Installationshilfen sind benutzerfreundlich, und es gibt umfangreiche FAQs – ganz wie bei seriösen SaaS-Produkten.
Skalierung von Angriffen: Durch Automatisierung können mit geringem Aufwand tausende Ziele gleichzeitig angegriffen werden. Das betrifft besonders kleine und mittelständische Unternehmen, die oft nicht über ein SOC verfügen.
Preisdruck und Innovation: Da die Anbieter im Wettbewerb stehen, entstehen regelmäßig neue Angriffsmethoden, bessere Tarnmechanismen und aggressivere Monetarisierungsstrategien.
Verdrängung klassischer Angreiferprofile: Einzelne, hochbegabte Hacker werden durch Netzwerke ersetzt. Tätergruppen agieren arbeitsteilig – Entwicklung, Vertrieb, Support und Monetarisierung sind auf mehrere Schultern verteilt. Dadurch entsteht eine Parallelinfrastruktur, die weit entfernt ist vom Bild des Einzelhackers im Keller.

Realbeispiele: Wie CaaS in der Praxis funktioniert

Beispiel 1: LockBit – Ransomware mit Partnerprogramm
Die Gruppe „LockBit" war 2022–2023 für weltweit über 1.000 bekannte Angriffe verantwortlich. Das Geschäftsmodell: Affiliates infizieren Unternehmen, LockBit stellt die Ransomware und Infrastruktur zur Verfügung, kassiert dafür Provisionen von 20–40 %. Die Gruppe betreibt eigene Leak-Seiten im Darknet und einen automatisierten Verhandlungsbot für Lösegeldforderungen.

Cybercrime-as-a-Service

Beispiel 2: Genesis Market – Identitäten zum Mietpreis
Vor seiner Zerschlagung durch das FBI im Jahr 2023 war Genesis Market eine Plattform für gestohlene digitale Identitäten. Für wenige Dollar ließ sich der vollständige digitale Fingerabdruck eines Nutzers kaufen – inklusive Cookies, Systemkonfiguration und Passwörtern. Die Oberfläche war benutzerfreundlich wie Amazon, der Checkout-Prozess auf maximale Effizienz ausgelegt.

Beispiel 3: Telegram-Kanäle für Phishing-as-a-Service
Im Sommer 2023 wurde ein Telegram-Kanal entdeckt, der über 14.000 Abonnenten mit fertigen Phishing-Kits versorgte. Enthalten waren Fake-Websites im Look & Feel von Banken, E-Mail-Diensten und eCommerce-Plattformen. Der Service umfasste Anleitung, Hosting, Support und manchmal sogar Werbung („Summer Discount – 20 % off“).

Beispiel 4: Malware-Baukästen mit Update-Abos
Info-Stealer wie RedLine oder Raccoon wurden als „Pakete“ inklusive Update-Service verkauft. Für rund 200 USD erhielt der Käufer eine anpassbare Malware mit GUI, Optionen für Verschlüsselung, Exfiltration und Anti-Analyse-Maßnahmen. Updates und neue Module konnten monatlich bezogen werden.

Auswirkungen auf Unternehmen und Behörden
Die Folgen für Unternehmen sind tiefgreifend – denn CaaS senkt die Eintrittshürde für Angriffe drastisch und erhöht gleichzeitig deren Effizienz:

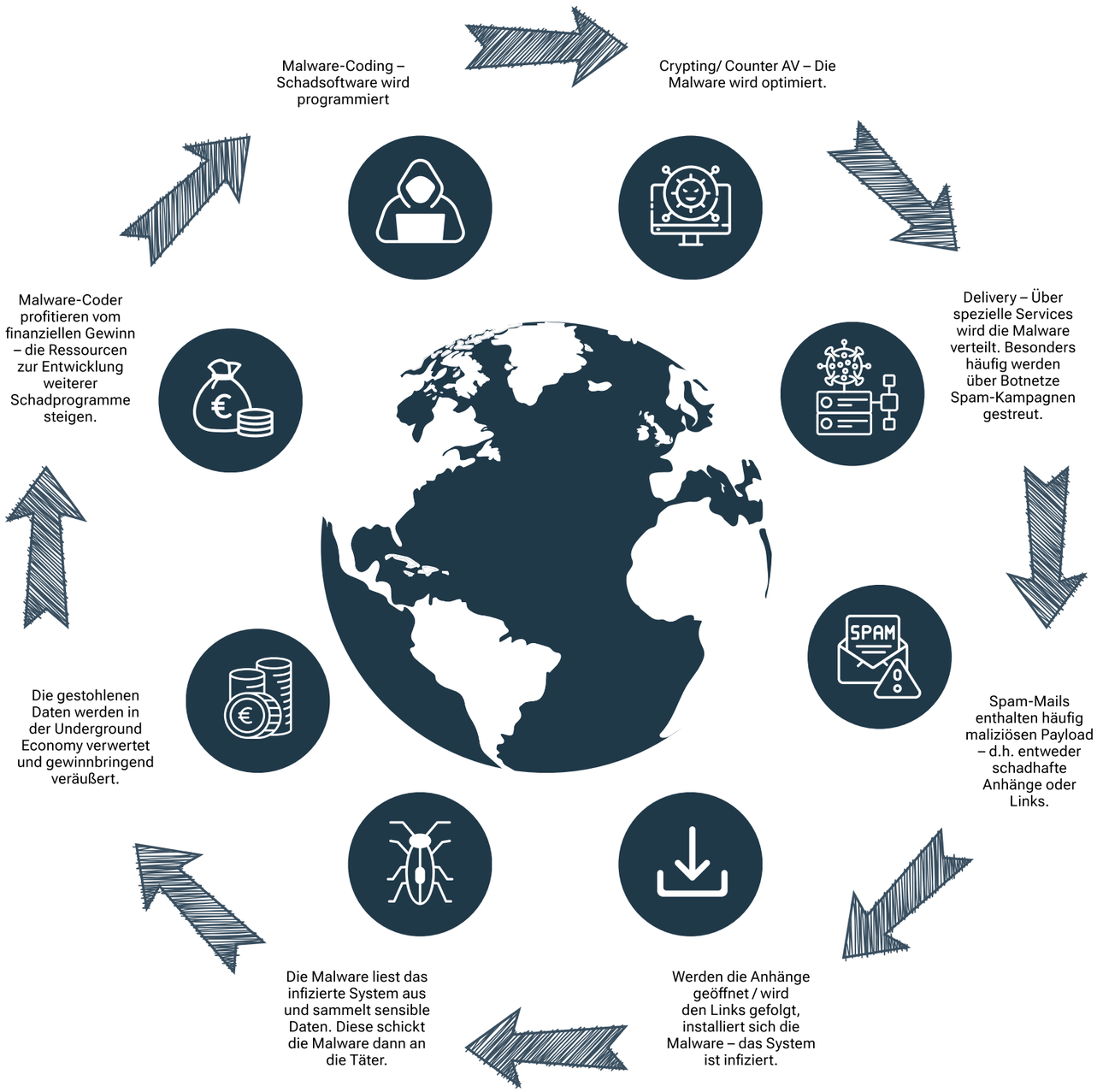
Verlust der Vorhersehbarkeit
Früher ließen sich Angreifer oft einem bestimmten Typ (Hacktivisten, Nationalstaaten, Wirtschaftskriminelle) zuordnen. Heute ist jeder potenzieller Angreifer – ein verärgerter Ex-Mitarbeiter, ein Cyberjugendlicher mit Krypto-Wallet, ein opportunistisches Syndikat.

Erhöhte Komplexität in der Verteidigung
CaaS-Tools werden laufend aktualisiert. Signaturbasierte Erkennung stößt an Grenzen. Auch Behavioral Analytics müssen immer schneller lernen, um mitzuhalten.

Unklare Attribution
Die Trennung zwischen Tool-Entwickler, Benutzer und Auftraggeber führt zu juristischer Grauzone: Wer ist verantwortlich? Und wie soll Strafverfolgung reagieren, wenn alle Beteiligten anonym operieren?

Wirtschaftlicher Druck steigt
Kleine und mittlere Unternehmen (KMU) werden besonders oft getroffen, weil sie als „leichte Beute“ gelten. Gleichzeitig fehlt es oft an Sicherheitsbudgets und Notfallprozessen.

Neue Anforderungen an Führung und Kommunikation
Geschäftsführungen müssen sich heute mit Cyberrisiken ebenso intensiv beschäftigen wie mit finanziellen oder rechtlichen Themen. Ein Angriff kann Reputation, Umsatz und Kundenvertrauen massiv beschädigen – selbst ohne erfolgreiche Datenexfiltration.



Auswirkungen auf kritische Infrastrukturen
Krankenhäuser, Energieversorger oder Behörden sind besonders gefährdet. Veraltete Systeme, geringe IT-Sicherheitsbudgets und fehlende Redundanzen machen sie anfällig – und aus Sicht der Angreifer: lukrativ.

Was Entscheider jetzt tun müssen

Cybercrime-as-a-Service lässt sich nicht stoppen – aber Unternehmen und Institutionen können sich schützen, wenn sie aktiv werden:

1. Bedrohungsanalyse professionalisieren
- Threat-Intelligence-Feeds einbinden
- CaaS-bezogene TTPs (Tactics, Techniques, Procedures) analysieren
- Frühwarnindikatoren (z. B. Darknet-Erwähnungen eigener Domains) etablieren

2. Security-Awareness realitätsnah gestalten
- CaaS-basierte Angriffsszenarien (Phishing, Ransomware, Credential Theft) simulieren
- Übungen auf Führungsebene durchführen
- Sicherheit als Teil der Unternehmenskultur verankern

3. Incident Response fit machen
- Playbooks regelmäßig aktualisieren und testen
- Offline-Kontaktlisten & Notfall-Zugänge vorbereiten
- Interne und externe Kommunikation frühzeitig planen

4. Strategisch investieren
- SOC, SIEM & MDR-Lösungen evaluieren
- Cloud-, Hybrid- und Endpoint-Sicherheit integrieren
- Partnernetzwerke und Dienstleister in Sicherheitsstrategie einbinden

5. Kooperationen nutzen
- Zusammenarbeit mit nationalen CERTs, Polizei, Brancheninitiativen
- Austauschformate wie IKT-Sicherheitskonferenz, Cybersecurity Forums besuchen
- Know-how länder- und branchenübergreifend nutzen

Sicherheitsdenken neu definieren

Cybercrime-as-a-Service ist kein Randphänomen – es ist das neue Normal. Es demokratisiert Angriffe, professionalisiert Kriminalität und unterwandert klassische Verteidigungsmechanismen.

Wer heute in Sicherheit denkt, muss ganzheitlich denken: nicht nur in Firewalls und Antivirenlösungen, sondern in Ökosystemen, Marktlogiken und verteilten Verantwortlichkeiten.

Die gute Nachricht: Der Wissensstand wächst, die Tools existieren, die Strategien sind verfügbar. Die Herausforderung liegt nun bei Führungskräften, diesen Wandel nicht nur zu erkennen, sondern aktiv zu gestalten. -V-

MMag. Franz HOLLERER

Unsere Demokratie: Gefährdung durch Cyberangriffe im Rahmen hybrider Kriegsführung

Mit der Gründung der Zweiten Republik vor 80 Jahren sowie der Wiedererlangung der Souveränität vor 70 Jahren begeht Österreich im Jahr 2025 zwei historisch bedeutsame Jubiläen, die unmittelbar mit den Werten unserer Demokratie verbunden sind. Das vorangegangene Jahr 2024 war das Jahr der Wahlen – rund die Hälfte der Weltbevölkerung wählte die diversen politischen Gremien. Der Anfang 2025 publizierte Demokratieindex des britischen „The Economist" bringt zum Ausdruck, dass zwar die überwiegende Mehrheit der Wahlen nach demokratischen Regeln abgelaufen sind, deren Ergebnisse aber interessanterweise jedoch viele Demokratien geschwächt hätten. Damit erreicht dieser seit 2006 erhobene Index im Jahr 2025 einen Tiefpunkt: vieles deutet darauf hin, dass wir in naher Zukunft einem entsprechenden breiten Spektrum undemokratischer Regierungsformen gegenüberstehen.

In dem Zusammenhang ist festzuhalten, dass wir zunehmend im Vergleich zu den letzten Jahrzehnten in unsichereren Zeiten leben. Der Krieg in seiner klassischen Form einer Auseinandersetzung mit militärischen Mitteln ist wieder im Osten Europas angekommen. Wenn man aber unter Krieg auch die diversen hybriden Bereiche, die wir insbesondere auch in Europa beobachten können, subsumiert, sind auch wir schon im Krieg.

Im Zusammenhang mit einer möglichen Gefährdung unserer Demokratie sind diverse Kampagnen näher zu betrachten. Die in jüngerer Vergangenheit zu beobachtenden einschlägigen Kampagnen können dahingehend subsumiert werden, insbesondere eine möglichst große Spaltung der Europäischen Union zu erreichen und die Solidarität innerhalb dieses Players möglichst zu minimieren. Gerade in der momentanen Phase, in der Europa mehr Selbstständigkeit zeigen und massiv in den raschen Aufbau militärischer Kapazitäten aufbauen muss, kommt es darauf an, diese Form der Angriffe erfolgreich abzuwehren. Als besondere Herausforderung ist dabei zu beachten, dass diese hybride Kriegsführung oft von der Bevölkerung gar nicht als solche wahrgenommen wird und teils schwer erkennbar ist.

Diese Form der Cyberangriffe stellen somit eine zunehmende Bedrohung für die Demokratie dar. Auswirkungen auf demokratische Werte können dabei durch verschiedene Maßnahmen erreicht werden; beispielhaft seien erwähnt:

Desinformationen: Es werden Desinformationen verbreitet, die das Vertrauen in politische Proponenten und auch Medien schwächen und damit die Glaubwürdigkeit der Demokratie untergraben.
Schädigung staatlicher Institutionen: Cyberangriffe können die Funktionsfähigkeit von stattlichen Einrichtungen gefährden und damit deren Handlungsfähigkeit einschränken und das Vertrauen in diese erschüttern
Wahlmanipulation: durch Cyberangriffe werden Zugänge zu elektronischen Wahlsystemen geschaffen und Wahlergebnisse manipuliert

Gegenmaßnahmen stellen sich insbesondere deswegen als herausfordernd dar, weil die Anzahl der Angriffe entsprechend hoch ist und man auf die Resilienz der Bevölkerung angewiesen ist. Daraus leiten sich beispielhaft folgende Maßnahmen ab:

Erhöhte Bewusstseinsbildung: Aufklärung sowie Sensibilisierung der Bürgerinnen und Bürger über die Gefahren von Cyberangriffen und die Notwendigkeit des Schutzes davor
Verstärkte Cybersicherheit: Stärkung der digitalen Infrastruktur
Zusammenarbeit Staat und Wirtschaft, auch im internationalen Bereich: Kooperation zur Erkennung und Abwehr von Cyberangriffen

Die Werte der Demokratie, wie wir diese verstehen, sind durchaus in Gefahr, in die Defensive zu geraten. Eine Beschäftigung mit anderen – uns nicht unbekannten – Regierungsformen macht klar, dass es diese Werte „wert" sind, sie zu verteidigen – insbesondere auch gegen im Rahmen einer hybriden Kriegsführung stattfindende Cyberangriffe! -v-

Dr. Roland KUNZ

Mobiles Arbeiten und Sicherheit

Wie Organisationen das Dilemma lösen

Mobiles Arbeiten eröffnet Organisationen und ihren Mitarbeitern neue Möglichkeiten, birgt aber auch einige Risiken, denn eine dezentrale IT-Landschaft bietet Cyberkriminellen zahlreiche Angriffspunkte. Nur mit einer ganzheitlichen Sicherheitsarchitektur, die alle Endgeräte, Anwendungen und Netzwerke einbezieht, können Organisationen eine geschützte Arbeitsumgebung schaffen. Dell Technologies erläutert, welche Aspekte dabei relevant sind.

Ultramobiles Arbeiten bedeutet, jederzeit und unabhängig vom Ort auf wichtige Ressourcen zugreifen zu können. Eine solche Arbeitsumgebung bringt automatisch eine neue Bedrohungslage mit sich: Klassische Schutzmaßnahmen stoßen an ihre Grenzen, wenn Netzwerkperimeter durchlässiger werden und zahlreiche neue Geräte angreifbar sind. Organisationen müssen daher in Technologien wie moderne Endpoint-Security-Lösungen, Zero-Trust-Architekturen, belastbare Cloud-Strategien, umfassende Notfallpläne und KI-basierte Sicherheitslösungen investieren, um sich gegen die stetig wachsenden Cyberbedrohungen zu wappnen.

Endpoint Security in einer verteilten Landschaft. Da Mitarbeiter von verschiedenen Standorten und Geräten auf Ressourcen zugreifen, ist der Schutz der Endgeräte ein entscheidender Aspekt in der Cybersicherheit. Organisationen brauchen moderne Endpoint-Security-Lösungen, um alle mit dem Firmennetzwerk verbundenen Devices zu schützen und offene Angriffsflächen für Cyberkriminelle zu schließen. Spezielle Detection- und Response-Systeme helfen ihnen dabei, Bedrohungen über verschiedene Endpunkte hinweg zu erkennen und zu entschärfen. Regelmäßige Software-Updates, Patch-Management und Geräteverschlüsselung sind weitere wesentliche Bestandteile einer umfassenden Sicherheitsstrategie.

Zero-Trust-Architektur für mehr Cybersicherheit. Der klassische Ansatz, Entitäten innerhalb des Organisationsnetzwerks zu vertrauen, hat sich angesichts der heutigen Cyberbedrohungen als überholt erwiesen. Die Zero-Trust-Architektur geht davon aus, dass jeder Benutzer und jedes Gerät innerhalb oder außerhalb des Firmennetzes ein Sicherheitsrisiko darstellt. Die Umsetzung eines Zero-Trust-Modells umfasst strenge Zugangskontrollen, kontinuierliche Überwachung und Multi-Faktor-Authentifizierung. Durch die Anwendung eines Least-Privilege-Ansatzes können Organisationen den Benutzerzugriff auf die für die jeweilige Rolle erforderlichen Ressourcen beschränken und so die potenziellen Auswirkungen einer Sicherheitsverletzung minimieren.

Cloud-Sicherheit in einer flexiblen Arbeitsumgebung. Die Cloud bietet Skalierbarkeit und Flexibilität, die für mobiles Arbeiten mit seinen Anforderungen an Kommunikation und Kollaboration unerlässlich sind. Wenn Mitarbeiter von den unterschiedlichsten Standorten und Geräten aus Cloud-Services nutzen, muss die dahinterliegende Infrastruktur entsprechend geschützt werden. Dazu gehört zunächst die Implementierung einer Identity- und Access-Managementlösung, um zu kontrollieren und zu regeln, wer auf was zugreifen darf. Die Verschlüsselung von Daten sowohl bei der Übertragung als auch im Ruhezustand, regelmäßige Sicherheitsüberprüfungen und die Überwachung der Compliance sind unerlässlich, um die eigene Widerstandsfähigkeit gegenüber Bedrohungen in der Cloud weiter zu verbessern.

Robuster Reaktionsplan für den Notfall. Keine Organisatione ist vor Cyberbedrohungen gefeit. Auch wenn viele immer noch hoffen, im Falle eines erfolgreichen Angriffs alle Daten zurückzubekommen, sieht die Realität oft anders aus: Die gestohlenen Informationen werden selbst nach Zahlung eines Lösegeldes nicht wieder freigegeben. Umso wichtiger ist ein umfassender Reaktionsplan mit klaren Abläufen, Rollen und Verantwortlichkeiten. Nur so können Organisationen bei einem Sicherheitsvorfall adäquat reagieren – von der Identifizierung über die Eindämmung und Beseitigung bis hin zur Wiederherstellung der Daten und dem Lernen aus dem Vorfall. Regelmäßige Tests des Reaktionsplans und entsprechende Anpassungen stellen seine Wirksamkeit sicher. Gleichzeitig müssen Standorte umfassende Strategien entwickeln, um im Falle eines Cyberangriffs wichtige Geschäftsprozesse aufrechtzuerhalten und so Ausfallzeiten und finanzielle Verluste zu minimieren.

KI für ein innovatives und sicheres Arbeitsumfeld. Künstliche Intelligenz ist ein wirksames Instrument zur Stärkung der Cyberabwehr. Sie kann Anomalien nahezu in Echtzeit erkennen und darauf reagieren. Durch die kontinuierliche Überwachung der Netzwerkaktivität lassen sich Angriffe frühzeitig isolieren und Schäden durch eine weitere Ausbreitung verhindern. Gleichzeitig können Berechtigungen auf Basis von Risikobewertungen angepasst werden. KI-basierte Rechner, die diese Technologie bereits integriert haben, heben den Schutz vor Cyberkriminellen auf ein neues Niveau, da alle notwendigen Funktionen lokal zur Verfügung stehen, ohne dass sensible Daten den Rechner verlassen müssen.

„Die Zukunft der Arbeit ist ultramobil – aber ohne einen ganzheitlichen Security-Ansatz, der alle Berührungspunkte innerhalb der IT-Umgebung abdeckt, ist diese Zukunft nur scheinbar sicher. Organisationen müssen in Technologien investieren, die nicht nur Innovationen ermöglichen, sondern auch Cyberbedrohungen in Echtzeit erkennen und abwehren“, erklärt Roland Kunz, Principal Systems Engineer for Emerging Technologies in EMEA bei Dell Technologies. „Was man auch nicht vergessen darf: Sicherheit ist kein statischer Zustand, sondern ein fortlaufender Prozess – gerade in einer Welt, in der mobiles Arbeiten neue Wege eröffnet und Herausforderungen mit sich bringt.“ -v-

Senator Heinz K. STIASTNY*, KommRat, RegKmsr*

Phishing: Wenn Digitalisierung zur Gefahr wird

…die Auswirkungen der Digitalisierung zeigen sich in nahezu allen Lebensbereichen. Damit einhergehende Technologien und deren positive Effekte sind aus unserem Alltag nicht mehr wegzudenken. Bringt dieser Fortschritt sicherlich viel Gutes mit sich, so muss man leider aber auch feststellen, dass viel Licht auch viel Schatten bringt.

Phishing ist kein wirklich neues Thema – es gab dieses Phänomen schon lange vor der Verbreitung des Internets. Per Mail verbreitete sich Phishing bereits in den 1990er- und 2000er-Jahren. Ein weiterer Schritt war die Verbreitung von Schadsoftware, genannt Trojaner. In weiterer Folge haben sich Spear-Phishing-Angriffe entwickelt (das gezielte Heraussuchen von Zielgruppen).

Aktueller Trend ist die Nutzung von QR-Codes – dahinter steht die Unmöglichkeit für Nutzer, einen Link zu prüfen. Die wenigsten Menschen sehen, dass sie an diesem Punkt schon ein Problem haben können. Täter springen auf Entwicklungen auf, wie etwa auf die Nutzung von QR-Codes im wirtschaftlichen Umfeld.

Die digitale (Schatten-)Welt wird auch für kriminelle Aktivitäten genutzt.

Der vermeintliche Deckmantel der Anonymität und die Möglichkeiten, eine Vielzahl von Menschen mit einem Mausklick zu erreichen bzw. zu kontaktieren, führen dazu, dass sich kriminelle Elemente zusehends in der virtuellen Welt bewegen. Eines dieser neu auftretenden Phänomene, die mittlerweile schon zu einem Teil unseres Alltags wurden, ist das sogenannte Phishing.

Wie ein Angler fischen die Täter im digitalen Raum nach potenziellen Opfern, nach deren Passwörtern und Daten. Auf täuschend echten Internetseiten sollen sie die Opfer dazu verleiten, ihre Daten – zumeist Bankdaten und Passwörter – anzugeben, um diese anschließend missbräuchlich zu verwenden und widerrechtliche Buchungen bzw. Finanztransaktionen durchzuführen.

Bei Phishing geht es in der Regel um eine Betrugshandlung oder deren Vorbereitung. Im Fokus steht nicht zwangsläufig ein technischer Ansatz. Für einen „gut geplanten Betrug" braucht es eine „gute Story". Rein technische Maßnahmen dagegen greifen oft zu kurz – auch wenn es das Ziel ist, Schadsoftware auf Geräten zu installieren, bleibt der zentrale Fokus vielfach die Erlangung von Zugangsdaten und Identitätsdaten.

Phishing ist der Versuch, über Kommunikationswege (gefälschte Webseiten, E-Mails oder Kurznachrichten) sensible (persönliche) Informationen der Internetbenutzer zu erlangen. Weiters stellt Phishing nicht nur ein technisches, sondern auch ein soziales Problem dar, da es auf die Manipulation und Ausnutzung menschlicher Schwächen abzielt. Es ist ein internationales Phänomen, darum ist die Notwendigkeit einer grenzübergreifenden Zusammenarbeit von zentraler Wichtigkeit.

Man kann Bits und Bytes nur mit Bits und Bytes bekämpfen. Dies erfordert technische Tools – gerade künstliche Intelligenz (KI) und Deepfakes sind von großer Bedeutung und werden der Cyberkriminalität einen weiteren Boost verleihen.

Die wichtigsten Prioritäten im Kampf gegen Phishing:

Breite Awareness und Aufklärung in der Bevölkerung
Bestmögliche Absicherung aller Online-Zugänge und Zugangsdaten durch Multifaktor-Authentifizierung als Mindeststandard (Ohne MFA bzw. Authentifizierungs-Apps hat man heute schon verloren.)
Kooperation und rascher Informationsaustausch auf allen Ebenen
(Telekommunikations- und Finanzdienstleister, Polizei, Konsumentenschutz, CERTs, Internet-Watchlisten …)
Präventionsmethoden weiterentwickeln
Verbreitungswege von Betrugsfallen erschweren
(z. B. Werbung für Fallen auf Plattformen)
Fallen automatisiert erkennen und das Datenmanagement zwischen den Stakeholdern verbessern

Der „Verteidiger" im Internet ist immer im Nachteil, er muss daher immer erfolgreich sein Oft ist der Informationsaustausch für Verteidiger aus rechtlichen Gründen (DSGVO) schwierig bzw. rechtlich nicht zulässig und möglich. Daher muss der Informationsaustausch massiv weiter betrieben werden, zumal Zusammenarbeit die wichtigste Waffe gegen immer neue Bedrohungen und Betrugsmuster ist.

Smishing: Phishing via SMS

Ein ebenfalls „neuer" Betrugstrend ist das sogenannte SMS-Phishing (Smishing). Dabei nutzen Täter vor allem SMS, E-Mails oder WhatsApp-Nachrichten. Die Täter bzw. Angreifer verwenden gehackte, gültige Telefonnummern, die im Darknet gehandelt werden.

Sie erwecken den Eindruck, dass die Nachricht z. B. von der eigenen Bank oder der Post kommt.

Kunden und Konsumenten denken daher, dass diese SMS legitim sein müssen. Oftmals wird gefordert, einen kleinen Geldbetrag bzw. Kostenbetrag zu überweisen – meist über einen Link, bei dem in der Folge alle Bank- oder Kreditkartendaten eingegeben werden.

Wichtige Maßnahmen gegen SMS-Phishing:

Sensibilisierung aller Beteiligten, dass Phishing mittels SMS nicht nur Banken betrifft, sondern ein Problem für unterschiedliche Industrien und die Gesamtbevölkerung ist (z. B. „Hallo Mama/Papa"-Ansprache als Initial-Vektor)
Wille zur Zusammenarbeit zwischen betroffenen Organisationen
(z. B. Finanzbranche, Logistikunternehmen, CERT …)
Rechtlich abgesicherte Möglichkeit für Telekomunternehmen, SPAM- und Phishing-SMS nicht zustellen zu müssen
Rechtssicherheit beim Austausch von Fraud-relevanten Daten
(z. B. zwischen Banken und Telekommunikationsunternehmen)
Optimierung der Zusammenarbeit mit der Exekutive bei erfolgreichen Betrugsfällen
Methoden entwickeln für den Opferschutz bei Identitätsdiebstahl

Fazit: Keine Wunderwaffe – aber viele Stellschrauben

Zusammenfassend ist zu sagen, dass es im Kampf gegen Phishing und andere Formen von Internetbetrug keine „Wunderwaffe" gibt. Die deutliche Erhöhung der Warnungen und Verbreitungskanäle muss weiter gesteigert werden. Sourcing-Tools wie der Fake-Shop-Detector sind genauso wichtig wie Kooperationen mit relevanten Stakeholdern.

Bei der Weiterentwicklung der Präventionsmethoden arbeiten neben der Suchmaschinenoptimierung auch Warnsysteme auf allen Suchkanälen, um diese möglichst nahe an den Fallen zu platzieren. Prävention funktioniert dann, wenn wir nicht über etwas reden, sondern mit den Zielgruppen darüber reden (Behörden, Sicherheitsexperten…). -v-

AWARENESS – KNOWLEDGE – ACTION

Patrick BARDEL

Wenn KI zum Angreifer wird: Was uns in Zukunft erwartet und wie die BPN Group mit AI Driven Tools Cyber Attacken entgegenwirkt.

Während sich Cyberbedrohungen in atemberaubender Geschwindigkeit weiterentwickeln, bleibt der Einsatz Künstlicher Intelligenz (KI) in österreichischen Unternehmen eher zurückhaltend. Laut **Statistik Austria** nutzten im Jahr 2024 lediglich **20 % der Betriebe KI-Technologien** – bei Dienstleistern sind es 23 %, in der produzierenden Industrie gar nur 15 %. Das ist zwar eine Verdopplung im Vergleich zum Vorjahr, doch der Abstand zur Bedrohungslage wächst.

Gleichzeitig setzen Angreifer längst auf KI – von **automatisierten Angriffen auf Web-Infrastrukturen** bis hin zu perfiden Social-Engineering-Taktiken mittels **Deepfakes**. Während also viele Unternehmen noch evaluieren, wie sie KI sicher einsetzen können, haben Hacker längst begonnen, sie produktiv zu nutzen.

Die Herausforderung: Web-Pentests und ihre blinden Flecken

In der Praxis verbringen Penetrationstester rund **30 % ihrer Zeit mit dem Reconnaissance-Prozess** – also der Analyse öffentlich zugänglicher Informationen über die Zielumgebung. Die Toollandschaft ist dabei fragmentiert, oft unzuverlässig, und variiert stark in ihrer Abdeckung. Noch gravierender ist die Tatsache, dass **durch wachsende Shadow IT** und dynamische Infrastrukturen wie Cloud-Services die Angriffspunkte laufend wachsen – und klassische Methoden nicht mehr Schritt halten.

Angreifen, um zu schützen: Die Zukunft des Pentestings

Mit ReconKraken hat BPN in Zusammenarbeit mit Ihrem Tocherunternehmen PWND Labs GmbH ein innovatives Werkzeug -made in Austria- geschaffen, dass diese Lücke schließt. **Die Software imitiert Aufklärungs- und zukünftig auch Angriffsverhalten – KI-gestützt, systematisch und skalierbar.**

Dabei geht ReconKraken über klassische Recon-Tools hinaus: Es denkt wie ein Angreifer, **führt automatisierte Enumeration durch**, sammelt Assets, Domains, Subdomains, Metadaten und **führt OSINT-gestützte Analyse** von Unternehmen, Mitarbeitern, Systemen und öffentlich zugänglichen Informationen durch. Auch geleakte Zugangsdaten, Social-Media-Profile, wirtschaftliche Informationen und API-Endpunkte fließen in die Analyse ein – ganz im Sinne eines KI-basierten Red Teamings.

Das Ziel: **Schwachstellen erkennen, bevor es echte Angreifer tun.**

Die KI gestützte Analyse von BPN vereint:

- Attack Surface Enumeration in Echtzeit
- KI-gesteuerte Mustererkennung & Risikoanalyse
- OSINT-Integration: Domains, Personen, Leaks, GitHub, Pastebin etc.
- Simulation von realistischen Angriffsvektoren – automatisiert, aber kontrolliert

Mehrwert für Unternehmen: Von Aufwand zu Erkenntnis

Die Vorteile liegen auf der Hand – und in der Bilanz:

Reduzierter Aufwand: Die KI gestützte Subscription automatisiert 70–80 % der sonst manuellen Recon-Tätigkeiten.
Höhere Präzision: KI erkennt Muster und Schwächen, die menschlichen Analysten häufig entgehen.
Frühzeitige Risikoeinschätzung: Shadow IT, falsch konfigurierte Cloud-Ressourcen und „vergessene" Web-Applikationen werden sichtbar.
Kürzere Pentest-Zyklen: Mehr Testzeit für Exploits, weniger für manuelle Informationsbeschaffung. Bei Bedarf auch kontinuierlich.

Vision & Verantwortung: KI in der Cyberabwehr

> „Wer die KI nicht für sich nutzt, wird erleben, wie andere sie gegen ihn einsetzen."

Diese Realität hat die BPN Group früh erkannt. Mit einem eigenen KI-Entwicklungsteam und dem strategischen Research-Unternehmen PWND Labs GmbH investieren wir gezielt in ethische offensive Security. ReconKraken **ist der erste Schritt in eine Zukunft, in der automatisierte Angriffs- und Abwehrmechanismen einander gegenüberstehen** – und Unternehmen einen entscheidenden Vorteil benötigen: Übersicht, Geschwindigkeit, Präzision.

BPN
bpn-group.com

Live auf der IKT-Sicherheitskonferenz in Dornbirn

Wir laden Sie ein, ein AI driven Assessment auf der IKT-Sicherheitskonferenz in Dornbirn am 25.und 26.06.2025 zu erleben. In unserem Vortrag zeigen wir, wie daraus ein Werkzeug entsteht, das Sicherheitsanalysen auf ein neues Niveau hebt. -v-

Weiterführende Infos finden sie auf unserer Webseite https://bpn-group.com/ikt-security-conference sowie hier:

Melanie Tajl, *BA*

META KI bringt neue Spielregeln – das betrifft auch Events und Messen

META (ehemals Facebook) hat angekündigt, seine KI künftig mit öffentlich zugänglichen Inhalten von Nutzer/innen zu trainieren. Eine Entscheidung, die in der Praxis heikel ist – insbesondere für Unternehmen. Denn: Auch öffentlich geteilte Inhalte wie Grafiken, Claims oder Kommentare fließen in die Datenbasis ein, auf der METAs KI weiterentwickelt wird. Eine Entwicklung, die nicht nur Datenschutzfragen aufwirft, sondern auch konkrete Auswirkungen auf die Kommunikation rund um Events und Messen hat.

Was META konkret ändert – und warum das auch Messen betrifft

Seit dem 27. Mai nutzt META **öffentlich zugängliche Inhalte**, um die hauseigene **KI weiterzuentwickeln**. Was auf den Plattformen geteilt wird, kann damit unter Umständen ohne ausdrückliche Zustimmung in die Trainingsdaten der KI einfließen – **mit potenziellen rechtlichen Risiken**.

Privatpersonen hatten die Möglichkeit, der Verwendung ihrer Inhalte zu widersprechen. Für Unternehmensseiten war dieser Widerspruch allerdings nicht direkt vorgesehen. Fachleute diskutieren derzeit, ob ein Opt-out dennoch greift, wenn die im Formular angegebene E-Mail-Adresse mit der der Unternehmensseite übereinstimmt.

Die Herausforderung: Künftig muss noch sorgfältiger darauf geachtet werden, was und wie kommuniziert wird. Häufig übersehen: Auch Event-Postings, Messestand-Videos, Speaker-Fotos oder Besucherszenen können von der KI weiterverarbeitet werden – ohne weitere Rückfrage.

Das betrifft nicht nur Aussteller/innen, sondern ebenso Veranstalter/innen, Agenturen sowie PR-Abteilungen in Konzernen und öffentlichen Institutionen.

Herausforderung Datenschutz: Öffentlich ist nicht gleich rechtssicher

Gerade in Europa ist der Umgang mit personenbezogenen Daten klar geregelt – die Datenschutz-Grundverordnung (DSGVO) setzt hier strenge Maßstäbe. Entscheidend ist dabei nicht, ob Inhalte auf Social Media gepostet wurden, sondern ob betroffene Personen nachvollziehen können, wofür ihre Daten verwendet werden.

Unternehmen, die etwa Gruppenfotos vom Messestand oder Videos mit erkennbaren Mitarbeiter/innen veröffentlichen, müssen künftig damit rechnen, dass diese Inhalte auch von META KI verarbeitet werden.

Gerade bei sensiblen Inhalten aus Unternehmen oder öffentlichen Einrichtungen kann das problematisch werden – nicht nur rechtlich, sondern auch im Hinblick auf Reputation und Vertrauen.

Was bedeutet das künftig für die Messe- und Eventpraxis?

Die neue META KI-Regelung hat spürbare Auswirkungen auf die zukünftige Marketingkommunikation rund um Veranstaltungen. Beiträge, Fotos und Videos von Messen und Events werden weiterhin veröffentlicht – insbesondere im laufenden Betrieb. Viele dieser Inhalte dienen gezielt der Markenbildung und Sichtbarkeit.

Umso wichtiger ist es für Veranstalter/innen, zu prüfen, ob zusätzliche Hinweise oder sichtbare Piktogramme notwendig sind, um Besucher/innen transparent über mögliche Aufnahmen und Veröffentlichungen zu informieren.

Auch im Bereich der Social Media Kommunikation gilt es, Inhalte künftig kritischer zu bewerten – insbesondere dann, wenn Personen deutlich erkennbar sind oder wenn sensible Informationen wie neue Produkte, Innovationen oder Partnerlogos zu sehen sind.

Kommunikation überdenken – Vertrauen stärken

Gerade die letzten Jahre zeigen, wie schnell sich die Technik weiterentwickelt – die META KI ist hierfür ein gutes Beispiel für die Geschwindigkeit, mit der sich die digitale Kommunikation verändert. Umso wichtiger ist ein bewusster Umgang mit Bildern, Plattformen und Daten. Wer heute bewusst kommuniziert, schafft die Grundlage für nachhaltiges Vertrauen – intern wie extern. -v-

Marko DJORDJEVIC

Kryptografie im Umbruch: Warum Unternehmen jetzt ihre Post-Quantum-Strategie planen müssen

Ein Blick in die nahe Zukunft

Quantencomputer könnten das kryptografische Fundament unserer digitalen Welt erschüttern. Was bislang durch Algorithmen wie RSA und ECC geschützt war, steht vor der realen Gefahr, durch quantenbasierte Berechnungen geknackt zu werden. Mit Blick auf diese Entwicklung fordern Experten und Institutionen wie das US-amerikanische NIST, Unternehmen dazu auf, bis spätestens 2030 ihre kryptografischen Infrastrukturen auf quantenresistente Verfahren umzustellen. Was nach Science-Fiction klingt, ist in Wahrheit ein dringender Aufruf zum Handeln.

Post-Quantum-Kryptografie: Mehr als nur neue Algorithmen

Post-Quantum-Kryptografie (PQC) bezeichnet Verschlüsselungs- und Signaturverfahren, die auch Angriffen durch leistungsstarke Quantencomputer standhalten sollen. Diese basieren auf mathematischen Problemen, für die selbst Quantenalgorithmen wie Shor oder Grover keine effiziente Lösung bieten. Projekte wie die NIST-Standardisierung von PQC-Verfahren haben bereits erste Algorithmen wie CRYSTALS-Kyber (Schlüsselaustausch) und CRYSTALS-Dilithium (digitale Signaturen) als zukünftige Standards identifiziert.

Diese neuen Verfahren basieren nicht mehr auf Primfaktorzerlegung oder diskreten Logarithmen, sondern auf gitterbasierten, hashbasierten oder multivariaten mathematischen Problemen. Sie gelten als deutlich resistenter gegenüber quantenbasierten Angriffen. Gleichzeitig gehen sie jedoch mit anderen Anforderungen an Speicher, Rechenzeit und Schlüsselgrößen einher als die etablierten Standards – was eine sorgfältige Evaluierung und Vorbereitung erforderlich macht.

Ein weiterer Ansatz ist die sogenannte hybride Kryptografie: Hierbei werden klassische Algorithmen wie RSA oder ECC gemeinsam mit einem PQC-Algorithmus in einem gemeinsamen Zertifikat oder Protokoll verwendet. So bleibt die Kompatibilität zu bestehenden Systemen erhalten, während gleichzeitig die Sicherheit gegenüber Quantenbedrohungen verbessert wird.

Die Implementierung von PQC ist jedoch nicht allein eine technische, sondern auch eine strategische Herausforderung. Unternehmen müssen genau wissen, an welchen Stellen ihrer Infrastruktur kryptografische Verfahren zum Einsatz kommen – etwa in VPNs, TLS/SSL-Verbindungen, Code-Signing-Prozessen, E-Mail-Verschlüsselung oder Cloud-Zugängen. Ohne ein vollständiges Inventar aller kryptografischen Assets droht eine fragmentierte, ineffiziente und im schlimmsten Fall unsichere Umstellung.

Deshalb gilt: PQC muss nicht nur eingeführt, sondern aktiv gemanagt werden. Und genau hier greifen Konzepte wie Cryptographic Posture Management (CPM) und Crypto-Agility ineinander – als methodische Voraussetzung für eine erfolgreiche Migration in eine quantensichere Zukunft.

Cryptographic Posture Management: Transparenz schafft Sicherheit

Cryptographic Posture Management (CPM) ist ein strategischer Ansatz zur Erfassung, Bewertung und Verwaltung sämtlicher kryptografischer Ressourcen in einer IT-Umgebung. Angesichts des PQC-Übergangs ist CPM unverzichtbar, um zu verstehen, wo und wie Kryptografie eingesetzt wird – und ob diese Einsätze sicher, regelkonform und zukunftsfähig sind.

Die zentrale Aufgabe von CPM besteht darin, Transparenz über alle kryptografischen Assets wie Schlüssel, Zertifikate und Geheimnisse zu schaffen – unabhängig davon, ob sie in On-Premises-Systemen, Cloud-Umgebungen oder hybriden Infrastrukturen liegen. Moderne Plattformen bieten dafür eine einheitliche Sicht („Single Pane of Glass") über die gesamte kryptografische Infrastruktur – inklusive Compliance-Dashboards, Risikobewertungen und einem unveränderbaren Audit-Trail.

Ein umfassendes CPM-Framework umfasst:

- automatisierte Erkennung und Inventarisierung aller kryptografischen Assets,
- Bewertung und Risikoeinstufung der Komponenten und ihres Kontextes,
- zentrale Richtlinienkontrolle und Compliance-Monitoring,
- Lifecycle-Management für Schlüssel und Zertifikate (z. B. Rotation, Erneuerung, Sperrung),
- sowie Integration in HSMs, PKI, Cloud-Dienste und DevOps-Umgebungen.

Zukunftsorientierte Unternehmen nutzen CPM als Grundpfeiler für Crypto-Agility: also der Fähigkeit, kryptografische Verfahren schnell und kontrolliert zu ändern. Mit automatisierten CPM-Tools lassen sich etwa schwache oder veraltete Algorithmen rasch identifizieren und ersetzen – ohne Geschäftsprozesse zu gefährden.

Doch CPM ist nicht nur ein Technologieprojekt. Die erfolgreiche Umsetzung erfordert klare Verantwortlichkeiten, regelmäßige Audits, gezielte Schulungen und eine strategische Verankerung im Risikomanagement. Nur wenn Menschen, Prozesse und Technologien harmonisch zusammenspielen, lässt sich Kryptografie wirklich nachhaltig und resilient steuern.

Ein bewährter Ansatz: Unternehmen etablieren ein interdisziplinäres Krypto-Gremium, das Standards definiert, Risiken bewertet, Maßnahmen priorisiert und für eine agile Umsetzungsstrategie sorgt. Wer heute damit beginnt, schafft die Grundlage für sichere Kommunikation im Zeitalter der Quantencomputer.

Fazit: Strategisch handeln, bevor der Druck steigt

Die Vorbereitung auf das Post-Quantum-Zeitalter ist keine rein technische Frage – sie ist eine strategische Aufgabe mit langfristigen Auswirkungen auf die Sicherheit, Compliance und Innovationsfähigkeit jedes Unternehmens. Wer jetzt handelt, gewinnt nicht nur Zeit und Flexibilität, sondern positioniert sich auch als zukunftsfähiger Marktteilnehmer.

Post-Quantum-Kryptografie bietet die Antwort auf eine absehbare technologische Disruption. Doch um von dieser Antwort profitieren zu können, müssen Unternehmen heute die richtigen Fragen stellen: Wo wird bei uns Kryptografie eingesetzt? Wie verwalten wir sie? Und wie können wir sie sicher, automatisiert und nachvollziehbar umstellen?

Cryptographic Posture Management und Crypto-Agility liefern dafür das organisatorische und technologische Fundament. Sie machen Kryptografie steuerbar, auditierbar und anpassungsfähig – Eigenschaften, die in einer dynamischen Bedrohungslandschaft zur Pflicht geworden sind.

Die Zeit drängt. Unternehmen, die heute die nötigen Weichen stellen, sichern sich morgen das Vertrauen ihrer Kunden, Partner und Regulierungsbehörden – und verteidigen die Integrität ihrer Daten in einer Ära, in der Quantencomputer Realität werden. -V-

Ing. Mag. Georg LANZINGER

Finanzielle Betrugsdelikte und Steuerhinterziehung im Zeitalter der Cyberkriminalität: Bedrohung für Staat und Gesellschaft – Herausforderungen und Lösungsansätze für die Aufklärung

Finanzielle Betrugsdelikte und Steuerhinterziehung sind große Gefahren für die wirtschaftliche und gesellschaftliche Stabilität moderner Staaten. Die Digitalisierung und Globalisierung der Finanzmärkte haben die Komplexität und Reichweite dieser Delikte vergrößert. Sie haben auch neue Angriffspunkte geschaffen. Cyberkriminelle nutzen moderne Technologien. Sie gefährden Finanzsysteme, verwischen digitale Spuren und erschweren Ermittlungen.

Die enge Verbindung von Finanzkriminalität, Cybercrime und Terrorismusfinanzierung stellt Ermittlungsbehörden, Geheimdienste und Cybersecurity-Experten vor große Aufgaben. Dieser Artikel betrachtet die jetzigen Gefahren, typische Betrugsmuster und die Rolle moderner Cybersecurity-Lösungen. Er gibt einen Ausblick auf nötige Strategien zur wirksamen Bekämpfung dieser Delikte.

Theoretische Grundlagen und Betrugsmuster im digitalen Zeitalter

Finanzielle Betrugsdelikte umfassen viele Straftaten. Sie zielen auf die unrechtmäßige Erlangung oder Verlagerung finanzieller Mittel. Zu den klassischen Delikten gehören:

Geldwäsche (Money Laundering): Eine Verschleierung der Herkunft illegal erworbener Gelder durch komplexe, oft internationale Transaktionsketten.
Steuerhinterziehung (Tax Evasion): Eine vorsätzliche Umgehung steuerlicher Verpflichtungen durch Falschangaben, Verschleierung von Einkünften oder die Nutzung von Steueroasen.
Korruption und Bestechung: Der Missbrauch von Machtpositionen zur persönlichen Bereicherung.
Bilanzfälschung (Accounting Fraud): Eine Manipulation von Unternehmensbilanzen zur Täuschung von Behörden, Investoren oder der Öffentlichkeit.
Insiderhandel: Eine Ausnutzung vertraulicher Informationen zum eigenen finanziellen Vorteil.
Terrorismusfinanzierung: Eine Bereitstellung oder Verschiebung von Geldern zur Unterstützung terroristischer Aktivitäten.

Mit der Digitalisierung entstanden neue Betrugsmuster. Sie kombinieren klassische und digitale Methoden. Dazu gehören der Einsatz von Kryptowährungen, anonymisierten Zahlungsströmen und digitalen Identitäten. Auch Offshore-Konten, Scheinfirmen und weitverzweigte Netzwerke aus Strohmännern und Briefkastenfirmen sind dabei. Cyberkriminelle nutzen gezielt Schwachstellen in IT-Systemen. Sie stehlen Finanzdaten, manipulieren Transaktionen oder gefährden digitale Identitäten.

Weiterführende Literatur über die theoretischen Grundlagen:

https://www.diw.de/documents/publikationen/73/diw_01.c.354167.de/diw_econsec0026.pdf
https://www.aeaweb.org/articles?id=10.1257%2Fjep.21.1.25
https://academic.oup.com/ijpor/article/36/3/edae035/7716344
https://virtusinterpress.org/IMG/pdf/rgcv9i1p1.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4899359
https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity

Cybersecurity als Schlüsselfaktor in der Betrugsbekämpfung

Die Digitalisierung des Finanzsektors hat die Angriffsfläche für Betrugsdelikte stark vergrößert. Cyberkriminelle agieren heute hochprofessionell und international vernetzt. Sie verfügen über erhebliches technisches Know-how. Zu den häufigsten Angriffsmethoden gehören:

Advanced Persistent Threats (APTs): Staatlich geförderte oder hochspezialisierte Hackergruppen infiltrieren Finanzsysteme über lange Zeiträume, um sensible Daten zu stehlen oder Transaktionen zu manipulieren.
Ransomware und Erpressung: Es sind Angriffe auf Finanzinstitute, bei denen kritische Daten verschlüsselt und Lösegeldforderungen gestellt werden – häufig in Kryptowährungen.
Phishing: nutzt gefälschte E-Mails, Webseiten oder Nachrichten. Ziel ist es, Mitarbeitende oder Kunden von Finanzinstituten zur Offenlegung von Zugangsdaten oder Authentifizierungscodes zu bewegen. Kann auch als Vektor für Malware-basierte Angriffe eingesetzt werden. Phishing tritt als Massenphänomen auf, aber auch vermehrt als gezielter Angriff, beispielsweise im Rahmen von BEC.
Business Email Compromise (BEC): Gezielte Phishing-Angriffe auf Finanzabteilungen, um Zahlungen umzuleiten oder vertrauliche Informationen abzugreifen. Hier ist eine gute Schulung jeder einzelnen Mitarbeiterin
Malware-basierte Angriffe: Einsatz spezialisierter Schadsoftware wie Banking-Trojaner zur Manipulation von Finanztransaktionen.
API-Manipulation: Ausnutzung von Schwachstellen in Finanz-APIs zur Umgehung von Sicherheitsmaßnahmen und Durchführung betrügerischer Transaktionen.
Identitätsdiebstahl und Social Engineering: Kompromittierung digitaler Identitäten und gezielte Täuschung von Mitarbeitenden zur Umgehung von Sicherheitskontrollen.

Steigende Anzahl der Beschwerden und Verluste

Die IC3 (Internet Crime Complaint Center vom FBI) erhielt in den letzten fünf Jahren durchschnittlich 758.000 Beschwerden jährlich. Diese Beschwerden thematisieren vielfältige Formen von Internetbetrug, die weltweit Einzelpersonen schädigen.

Quelle: FBI, Internet Crime Complaint Center (IC3). (2024). 2023 Internet Crime Report, https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

42,8% aller Phishing Angriffe gehen gegen Social Media Plattformen (Quelle: APWG Phishing Activity Trends Report, Q4 2023 http://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf). Um das Risiko eines Angriffes zu minimieren, ist die Implementierung umfassender Schulungsprogramme für alle Mitarbeitenden essenziell. Diese Programme schärfen das Bewusstsein für raffinierte Techniken und stärken die Fähigkeit zur Identifizierung potenzieller Bedrohungen. Solche Schulungen werden vom Cyberhilfswerk Österreich ab Q4 2025 angeboten.

Das Zusammenkommen von Cyberkriminalität und Finanzdelikten erschwert die Ermittlungsarbeit sehr. Täter operieren grenzüberschreitend. Sie nutzen Verschlüsselungstechnologien und anonymisierte Kommunikationskanäle. Die Zuordnung von Angriffen und die Identifikation der Täter sind oft nur mit großem technischem und forensischem Aufwand möglich.

Steuerhinterziehung im digitalen Kontext

Steuerhinterziehung bleibt ein zentrales Element finanzieller Kriminalität. Oft ist sie die Grundlage für Delikte wie Geldwäsche oder Terrorismusfinanzierung. Im digitalen Zeitalter haben sich die Methoden der Steuerhinterziehung weiterentwickelt:

Kryptowährungen als Steuerschlupfloch: Die Nutzung von Bitcoin, Monero und anderen Kryptowährungen zur Verschleierung von Vermögenswerten und zur Umgehung von Steuerpflichten.
Digitale Schattenwirtschaft: Der Betrieb von Online-Geschäftsmodellen in regulatorischen Grauzonen, die bewusst Steuerreporting vermeiden.
Automatisierte Steuervermeidungssysteme: Der Einsatz von Algorithmen zur kontinuierlichen Optimierung internationaler Steuerstrukturen an der Grenze zur Illegalität.
Blockchain-basierte Verschleierungstechniken: Die Nutzung von Smart Contracts und dezentralen Finanzplattformen (DeFi) zur Anonymisierung von Vermögenswerten.
Darknet-Marktplätze: Anonyme Handelsplattformen für illegale Finanzdienstleistungen, gefälschte Dokumente und Steuerumgehungstools.

Die systematische Umgehung von Steuerpflichten verursacht große staatliche Einnahmeverluste. Dies schwächt die Fähigkeit des Staates, wichtige Aufgaben wie Sicherheit, Infrastruktur und soziale Leistungen zu erfüllen. Durch Steuerhinterziehung generierte Mittel werden oft zur Finanzierung von Terrorismus, organisierter Kriminalität und politischer Destabilisierung eingesetzt. Im Jahr 2020 hat Deutschland laut Daten des Tax Justice Network durch Steuerhinterziehung („tax evasion") rund 10,67 Milliarden US-Dollar an Steuereinnahmen verloren.

Schnittstellen zwischen Cybersecurity, Finanzkriminalität und Terrorismusfinanzierung

Die Verbindung zwischen Cyberkriminalität, Finanzdelikten und Terrorismusfinanzierung ist eine besonders gefährliche Entwicklung. In den Berichten von FATF, Europol SOCTA und UNODC Reports wird auf die Zusammenhänge von Geldwäsche, Terrorismusfinanzierung und Steuerhinterziehung hingewiesen. Terroristische Organisationen und organisierte Kriminalität nutzen immer mehr digitale Infrastrukturen. Es dient dazu, Gelder zu beschaffen, zu transferieren und zu waschen. Typische Muster sind zb. Krypto-Fundraising, Hacktivismus mit terroristischem Hintergrund, Darknet-Finanzierung und Hybride Bedrohungen - die Kombination aus Cyberangriffen und physischen Terrorakten zur Maximierung der destabilisierenden Wirkung.

Die Analyse digitaler Spuren, Transaktionsmuster und Kommunikationsnetze braucht spezialisierte Cybersecurity-Expertise und moderne Analysewerkzeuge. Ermittlungsbehörden müssen in der Lage sein, große Mengen strukturierter und unstrukturierter Daten in Echtzeit auszuwerten. So können sie verdächtige Muster erkennen und verfolgen.

Moderne Softwarelösungen und Cybersecurity-Technologien

Angesichts der stark wachsenden Datenmengen und der zunehmenden Komplexität digitaler Angriffsvektoren sind moderne Technologielösungen unbedingt nötig. Zu den wichtigsten Werkzeugen gehören:

Threat Intelligence Plattformen: Echtzeit-Informationen über aktuelle Bedrohungen, Angriffsmuster und Schwachstellen im Finanzsektor.
Blockchain-Analyse-Tools: Spezialisierte Software zur Nachverfolgung und Deanonymisierung von Kryptowährungstransaktionen.
Künstliche Intelligenz und Machine Learning: Identifikation bisher unbekannter Betrugsmuster durch selbstlernende Systeme und Erkennung von Anomalien in Echtzeit.
Digital Forensics: Fortschrittliche Methoden zur Sicherung und Analyse digitaler Beweismittel aus kompromittierten Systemen.
Netzwerkanalyse mit Cybersecurity-Fokus: Visualisierung und Analyse von Verbindungen zwischen digitalen Identitäten, Transaktionen und Kommunikationsmustern.
Verhaltensbasierte Authentifizierung: Erkennung verdächtiger Aktivitäten durch Analyse von Benutzerverhalten und Abweichungen von normalen Mustern.
Secure Information Sharing: Sichere Plattformen für den Austausch sensibler Ermittlungsdaten zwischen Behörden unter Wahrung der Integrität und Vertraulichkeit.

Diese Technologien ermöglichen es Ermittlungsbehörden, auch komplexe und international verschachtelte Betrugsstrukturen gut zu durchdringen und aufzudecken. Die Integration von Cybersecurity-Expertise in traditionelle Finanzermittlungen ist entscheidend für den Erfolg.

Herausforderungen und Lösungsansätze für Ermittlungsbehörden

Die Bekämpfung von Finanzdelikten im Cyberraum erfordert neue Ansätze und Fähigkeiten. Dazu gehört der Aufbau spezialisierter Cyber-Finanz-Ermittlungseinheiten. Diese Einheiten benötigen interdisziplinäre Teams mit Expertise in Finanzermittlung, Cybersecurity und Datenanalyse. Ebenso wichtig ist die Implementierung fortschrittlicher Cybersecurity-Tools und Analysekapazitäten in Ermittlungsbehörden.

Eine verstärkte Zusammenarbeit zwischen nationalen Behörden ist unerlässlich, um grenzüberschreitende Cyber-Finanzdelikte effektiv zu bekämpfen. Des Weiteren sind rechtliche Anpassungen notwendig, um den rechtlichen Rahmen zur Verfolgung von Cyber-Finanzdelikten weiterzuentwickeln und die Beweisführung sicherzustellen.

Die Zusammenarbeit mit Finanzinstituten und Technologieunternehmen im Rahmen von Public-Private-Partnerships ist von Bedeutung, um Cyber-Finanzdelikte frühzeitig zu erkennen und präventive Maßnahmen zu ergreifen.

Fazit und Ausblick

Finanzielle Betrugsdelikte, vor allem Steuerhinterziehung, gefährden in Verbindung mit Cyberkriminalität die Stabilität und Sicherheit von Staaten und Gesellschaften stark. Die digitale Transformation hat die Komplexität und Reichweite dieser Gefahren dramatisch erhöht. Die Verknüpfung mit Terrorismusfinanzierung und organisierter Kriminalität zeigt, dass wirksame Gegenmaßnahmen nötig sind.

Nur der zielgerichtete Einsatz moderner Software, die Integration von Cybersecurity-Expertise in Finanzermittlungen und die intensive Kooperation zwischen Behörden ermöglicht die Bewältigung dieser Aufgaben. Die Entwicklung spezialisierter Fähigkeiten an der Verbindung von Finanzermittlung und Cybersecurity wird entscheidend sein. Es dient dazu, die Integrität des Finanzsystems zu schützen und die Finanzierung terroristischer und krimineller Aktivitäten wirksam zu bekämpfen.

Die Zukunft der Betrugsbekämpfung liegt in der intelligenten Verbindung von Finanzexpertise, Cybersecurity-Knowhow und fortschrittlichen Analysetechnologien. Nur so können Ermittlungsbehörden mit der schnellen Entwicklung digitaler Gefahren Schritt halten. Sie können auch den dauerhaften Schutz wichtiger Finanzinfrastrukturen garantieren. -V-

Dominic LACHAT

Risikominimierung durch Technologie: Computervision in der Logistiksicherheit

Ein Überblick über die Grundlagen der Computervision

Die Computervision ist ein interdisziplinäres Feld der künstlichen Intelligenz (KI), das sich mit der Fähigkeit von Computern befasst, visuelle Informationen aus der Welt um uns herum zu „sehen" und zu interpretieren. Ähnlich wie das menschliche Auge und das Gehirn zusammenarbeiten, um uns das Sehen zu ermöglichen, zielt die Computervision darauf ab, Computersysteme mit der Fähigkeit auszustatten, digitale Bilder und Videos zu erfassen, zu verarbeiten und zu analysieren.

Im Kern verwendet die Computervision Algorithmen und Modelle, um Muster in visuellen Daten zu erkennen und zu extrahieren. Diese Muster können dann verwendet werden, um Objekte zu identifizieren, Szenen zu verstehen und Entscheidungen zu treffen, die auf visuellen Informationen basieren.

Die Computervision umfasst eine breite Palette von Funktionen, die es ermöglichen, visuelle Daten auf unterschiedliche Weise zu analysieren. Einige der wichtigsten Funktionen sind:

Objekterkennung: Diese Funktion identifiziert und lokalisiert bestimmte Objekte innerhalb eines Bildes oder Videos. In der Logistik ann dies beispielsweise verwendet werden, um Gabelstapler, Container oder Pakete zu erkennen.
Objektklassifizierung: Hierbei wird ein erkanntes Objekt einer bestimmten Kategorie zugeordnet. Zum Beispiel könnte ein Objekt als „Lkw" oder „Person" klassifiziert werden.
Gesichtserkennung: Diese Funktion identifiziert und verifiziert Personen anhand ihrer Gesichter. In der Logistik kann sie für die Zugangskontrolle oder die Anwesenheitsverfolgung eingesetzt werden.
Nummernschilderkennung (LPR): LPR extrahiert automatisch Nummernschildinformationen aus Bildern oder Videos von Fahrzeugen. Dies ist nützlich für die Verfolgung von Fahrzeugen, die Verwaltung von Parkplätzen und die Zugangskontrolle.
Bewegungsanalyse: Durch die Analyse von Videosequenzen können Bewegungsmuster erkannt und verfolgt werden. Dies kann verwendet werden, um ungewöhnliche Aktivitäten zu erkennen oder den Personenfluss zu überwachen.
Bildsegmentierung: Bei dieser Technik wird ein Bild in verschiedene Regionen oder Objekte unterteilt, um eine detailliertere Analyse zu ermöglichen.
Merkmalsextraktion: Hierbei werden spezifische Merkmale aus einem Bild extrahiert, die für die weitere Analyse relevant sind.

Diese Funktionen ermöglichen es, Videoüberwachungssysteme intelligenter zu machen und automatisierte Analysen durchzuführen, was in der Logistik zu einer Vielzahl von Anwendungen führt.

Wichtige Funktionen und deren Bedeutung für die Logistik

Computervision bietet eine Reihe wichtiger Funktionen, die speziell auf die Anforderungen der Logistik zugeschnitten sind. Diese Funktionen tragen dazu bei, die Effizienz zu steigern, die Sicherheit zu verbessern und die Transparenz in der gesamten Logistikkette zu erhöhen.

Die Anwendungen von Computervision erstrecken sich über verschiedene Bereiche der Logistik:

Container-/Lkw-Management:
OCR/QR-Code/Containernummernerkennung: Diese Funktion automatisiert die Identifizierung von Containern und Lkw, indem sie optische Zeichenerkennung (OCR) und QR-Code-Lesung einsetzt. Dies beschleunigt die Erfassung von Frachtdaten und reduziert manuelle Fehler.
LPR (License Plate Recognition): Die Nummernschilderkennung ermöglicht die automatische Erfassung von Fahrzeugkennzeichen, was für die Zugangskontrolle, die Verfolgung von Fahrzeugbewegungen und die Verwaltung von Parkplätzen von Bedeutung ist.
Fahrzeugverfolgung/-zählung: Computervision kann Fahrzeuge auf dem Gelände verfolgen und zählen, um den Verkehrsfluss zu optimieren und die Auslastung von Parkplätzen zu überwachen.
Personennäherungserkennung an Lkw: Diese Funktion erkennt, wenn sich Personen in der Nähe von Lkw aufhalten, um Unfälle zu vermeiden und die Sicherheit auf dem Gelände zu gewährleisten.
Lagerhaus:
PPE (Personal Protective Equipment)-Erkennung: Computervision überwacht, ob Mitarbeiter die erforderliche Schutzausrüstung tragen (z. B. Helme, Sicherheitswesten), um die Einhaltung der Sicherheits-vorschriften zu gewährleisten.
Zugangskontrolle: Die Technologie kann zur automatischen Zugangskontrolle eingesetzt werden, um sicherzustellen, dass

nur autorisierte Personen bestimmte Bereiche betreten.
QR-Code-Erkennung: Ähnlich wie bei der Containeridentifizierung kann die QR-Code-Erkennung im Lagerhaus verwendet werden, um Waren zu verfolgen und Bestandsdaten zu verwalten.
Belegung: Computervision kann die Belegung von Bereichen im Lagerhaus überwachen, um die Raumnutzung zu optimieren.
Heatmapping: Die Erstellung von Heatmaps zeigt Bereiche mit hoher Aktivität oder Staus an, um Engpässe

zu identifizieren und die Effizienz zu verbessern.
Brand- und Raucherkennung: Computervision erkennt automatisch Brände und Rauch, um frühzeitig Warnungen auszulösen und Schäden zu minimieren.
Einbruchserkennung: Die Technologie erkennt unbefugtes Eindringen in Lagerbereiche, um Diebstahl und Vandalismus zu verhindern.
Personenfalldetektion: Diese Funktion erkennt Stürze von Personen, um schnell auf Notfälle reagieren zu können.
Verweilzeitanalyse: Die Verweilzeitanalyse misst, wie lange sich Objekte oder Personen in einem bestimmten Bereich aufhalten.
Personenverfolgung: Computervision verfolgt die Bewegungen von Personen im Lagerhaus, um Arbeitsabläufe zu analysieren und die Sicherheit zu verbessern.
ID-Verifizierung: Die Technologie kann zur automatischen Überprüfung von Ausweisen eingesetzt werden.
Büro-Bereich:
Videosuche: Computervision ermöglicht die schnelle Durchsuchung von Videomaterial, um bestimmte Ereignisse zu finden.
Die anderen oben genannten Funktionen (Heatmapping, Personenfalldetektion, Brand- und Raucherkennung, Personenverfolgung, ID-Verifizierung) sind auch im Bürobereich relevant.
Ladebereich:
Neben OCR/QR-Code/Containernummernerkennung und PPE-Erkennung sind hier auch die Personenfalldetektion, die Personennäherungserkennung an Lkw und die Personenverfolgung von Bedeutung.
Gelände:
LPR, Diebstahlerkennung, Fahrzeugverfolgung, Geschwindigkeitsüberwachung, PPE-Erkennung, Containernummerner-kennung, Brand- und Raucherkennung, Personenverfolgung und Personennäherungserkennung an Lkw sind wichtige Funktionen für die Überwachung des Geländes.
Parkplatz:
Computervision unterstützt die Erkennung von Falschparken, die Diebstahlerkennung, die Zählung/Belegung von Parkplätzen, LPR und Heatmapping.
Zufahrtsbereich:
LPR, OCR/QR-Code/Containernummernerkennung, Fahrzeugverfolgung/-zählung, Geschwindigkeitsüberwachung, Diebstahlerkennung, Personenverfolgung/-zählung und ID-Verifizierung sind in Zufahrts-bereichen relevant.

Diese detaillierte Aufschlüsselung zeigt, wie Computervision in verschiedenen logistischen Umgebungen eingesetzt werden kann, um spezifische Herausforderungen anzugehen und die Effizienz und Sicherheit zu verbessern.

Vorteile und Einsparungen durch Computervision

Der Einsatz von Computervision in der Logistik bietet eine Vielzahl von Vorteilen, die sich direkt in messbaren Einsparungen und einer gesteigerten Effizienz niederschlagen. Ein wesentlicher Vorteil ist die Reduzierung des Zeitaufwands für die manuelle Durchsicht von Videomaterial. Herkömmliche Überwachungssysteme erfordern oft, dass Sicherheitspersonal stundenlang Videomaterial sichtet, um bestimmte Ereignisse zu finden. Computervision automatisiert diesen Prozess, indem es Videodaten in Echtzeit analysiert und relevante Ereignisse sofort identifiziert. Dies ermöglicht es den Mitarbeitern, sich auf andere wichtige Aufgaben zu konzentrieren, was die Produktivität des Überwachungspersonals deutlich steigert.

Ein weiterer wichtiger Vorteil ist die Minimierung von Fehlalarmen. Traditionelle sensorbasierte Systeme erzeugen häufig eine hohe Anzahl von Fehlalarmen, da sie nicht in der Lage sind, zwischen verschiedenen Objekttypen zu unterscheiden. Computervision hingegen nutzt fortschrittliche Algorithmen, um Objekte präzise zu erkennen und zu klassifizieren, wodurch die Anzahl der Fehlalarme erheblich reduziert wird. Dies spart nicht nur Zeit und Ressourcen für die Untersuchung von Fehlalarmen, sondern erhöht auch die Akzeptanz und Effektivität des Sicherheitssystems.

Darüber hinaus ermöglicht Computervision eine effizientere Nutzung der vorhandenen Infrastruktur. Anstatt für jede spezifische Analyse eine separate Kamera zu installieren (zum Beispiel eine Kamera für die Gesichtserkennung und eine andere für die Nummernschilderkennung), können mit einer einzigen Kamera mehrere Analysen durchgeführt werden. Dies reduziert die Hardwarekosten und vereinfacht die Systemverwaltung.

Neben den direkten Kosteneinsparungen bietet Computervision auch eine Reihe von nicht-monetären Vorteilen. Dazu gehören eine schnellere Bearbeitung von Vorfällen, eine verbesserte Entscheidungsfindung und eine höhere Kundenzufriedenheit. Durch die Bereitstellung von Echtzeit-Warnmeldungen und die Möglichkeit, Videomaterial schnell zu durchsuchen, ermöglicht Computervision es Unternehmen, proaktiv auf potenzielle Probleme zu reagieren und ihre Abläufe kontinuierlich zu optimieren.

Zusammenfassung

Zusammenfassend lässt sich sagen, dass Computervision eine transformative Technologie für die Logistikbranche darstellt. Durch die Automatisierung von Videoanalysen, die Bereitstellung von Echtzeit-Informationen und die Ermöglichung einer proaktiven Gefahrenabwehr bietet Computervision Unternehmen die Möglichkeit, ihre Sicherheit zu erhöhen, ihre Effizienz zu steigern und ihre Betriebskosten zu senken. -v-

Andreas EKELHART, Sebastian SCHRITTWIESER & Edgar WEIPPL

Phishing im Zeitalter von KI: Neue Herausforderungen und ein innovativer Lösungsansatz

Phishing und andere Social-Engineering-Angriffe gehören nach wie vor zu den größten Cyber-Bedrohungen für Unternehmen. Gleichzeitig setzen Angreifer:innen zunehmend auf generative KI (in Form von sogenannten Large Language Models, LLMs), um solche Angriffe durchzuführen. Diese Entwicklung führt dazu, dass Phishing-Mails heute deutlich schwerer zu erkennen sind als noch vor einigen Jahren. Früher verrieten sich Phishing-Versuche oft durch offensichtliche Fehler – gebrochenes Deutsch oder Englisch, untypische Formulierungen oder plumpe inhaltliche Auffälligkeiten.

Mit LLMs sind diese Warnsignale nahezu verschwunden. Mit generativer KI können Angreifer qualitativ hochwertige E-Mails verfassen, die authentisch und professionell wirken. Gleichzeitig sind im Darknet sogar spezialisierte KI-Modelle wie WormGPT oder FraudGPT verfügbar. Diese wurden explizit für kriminelle Zwecke trainiert und generieren täuschend echte Phishing-Nachrichten, ohne die üblichen Rechtschreibfehler oder holprige Sprache, an denen man Betrug früher erkennen konnte. Mit anderen Worten: Die klassischen Erkennungsmerkmale greifen immer seltener. Aber es geht nicht nur um korrekte Grammatik. Moderne KI kann Inhalte kontextbezogen und individuell anpassen. So ist es beispielsweise möglich, öffentlich verfügbare Informationen (z.B. aus LinkedIn, Firmenwebseiten oder Social Media) auszuwerten und in die Phishing-Mail einzubauen. Eine solche KI-generierter Nachricht könnte beispielsweise den echten Namen eines Vorgesetzten nennen, auf ein aktuelles Firmenereignis Bezug nehmen oder persönliche Interessen des Empfängers einbeziehen, um möglichst glaubwürdig zu wirken. Diese hochgradige Personalisierung erhöht die Erfolgsquote erheblich – selbst sicherheitsbewusste Mitarbeitende haben Schwierigkeiten, solche gefälschten Nachrichten von legitimen Mails zu unterscheiden.

Neue Dimension der Bedrohung – und die Schwächen klassischer Schulungen

Generative KI ermöglicht es zudem, in kürzester Zeit eine Vielzahl unterschiedlicher Phishing-Texte zu produzieren. Angreifer können so kostengünstig Phishing-Kampagnen im großen Stil durchführen, ohne befürchten zu müssen, dass sich Muster wiederholen und auffallen. Unternehmen sehen sich somit einer neuen Dimension der Bedrohung gegenüber, bei der herkömmliche Abwehrstrategien an ihre Grenzen stoßen. Angesichts dieser Entwicklung gewinnt die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter weiter an Bedeutung. Schließlich sind geschulte und aufmerksame Mitarbeiter:innen die letzte Verteidigungslinie, wenn technische Filter versagen. Doch genau hier zeigt sich ein Problem: Herkömmliche Schulungsansätze reichen nicht mehr aus, um dem heutigen Tempo und der Raffinesse der Angriffe gerecht zu werden. Klassische Security-Awareness-Schulungen – etwa jährliche Seminare oder standardisierte E-Learning-Module – vermitteln oft nur theoretisches Wissen und erfüllen Compliance-Anforderungen, führen aber kaum zu einer nachhaltigen Verhaltensänderung. Die Ursache: „One-size-fits-all"-Trainings mit veralteten Inhalten, fehlender Praxisnähe und geringer Einbindung der Teilnehmenden.

Ohne kontinuierliche, interaktive Schulungen, die auf unterschiedliche Rollen und aktuelle Angriffsformen zugeschnitten sind, bleiben Mitarbeiter:innen oft unvorbereitet. Hier setzt das Forschungsprojekt Awareness 365 der Universität Wien an. Die Kernidee: Wenn Angreifer KI nutzen, um ihre Methoden zu verbessern, sollten wir die gleiche Technologie einsetzen, um unsere Abwehrmaßnahmen zu stärken. Konkret entsteht eine neuartige Awareness-Plattform, die generative KI für realitätsnahes Training nutzt. Dabei werden LLMs eingesetzt, um automatisch Phishing-Simulationen zu erzeugen, die von echten Angriffsmails praktisch nicht zu unterscheiden sind. Diese Simulationen können regelmäßig (im Idealfall ganzjährig, also „365 Tage im Jahr") an die Mitarbeiterinnen und Mitarbeiter versendet werden – ohne großen Mehraufwand für die IT-Sicherheitsverantwortlichen. Automatisierung ist hier ein Schlüssel: Bisher mussten Sicherheitsabteilungen viel Zeit investieren, um immer wieder neue Phishing-Testmails von Hand zu erstellen. Das KI-System von Awareness 365 übernimmt diese Aufgabe und generiert auf Knopfdruck eine Vielzahl glaubwürdiger Szenarien. Dabei lassen sich die Inhalte flexibel an aktuelle Bedrohungstrends, wie etwa neue Betrugsmaschen oder saisonale Themen, anpassen und auf die jeweilige Zielgruppe zuschneiden. So können beispielsweise Mitarbeiterinnen und Mitarbeiter aus dem Finanzbereich andere simulierte Angriffe erhalten als solche aus der Personalabteilung, jeweils abgestimmt auf die für sie plausiblen Themen.

Awareness 365: Realistisches Training durch KI-Simulatione

Forschungsergebnisse unterstützen diesen Ansatz: Individuell angepasste Trainingsinhalte sind deutlich effektiver, konnten bisher aber nur mit hohem Aufwand umgesetzt werden. Generative KI kann hier viele Schritte automatisieren und personalisierte Sicherheitstrainings skalierbar machen. Für die Mitarbeiterinnen und Mitarbeiter bedeutet dies eine deutlich praxisnähere Lernerfahrung. Statt abstrakter Warnungen oder veralteter Beispiele erleben sie in einem geschützten Rahmen, wie ein raffinierter Phishing-Angriff heute aussehen kann. Wenn eine simulierte KI-Phishing-Mail im Posteingang landet, müssen sie die gleiche Entscheidung treffen wie im Ernstfall. Durch diese wiederholte Übung in der Realitätsschleife prägt sich sicheres Verhalten viel stärker ein als durch bloße Theorie. Lernen wird zu einem kontinuierlichen Prozess und nicht zu einem jährlichen Pflichttermin. Die Mitarbeitenden bleiben über das Jahr hinweg für neue Maschen sensibilisiert und entwickeln ein Gespür für die subtilen Anzeichen von Social Engineering, auch wenn die Angriffe durch KI perfektioniert wurden. Langfristig führt dies zu einer messbaren Erhöhung der organisatorischen Resilienz gegenüber Cyberangriffen. Je mehr Übung die Mitarbeiter:innen haben, desto sicherer verhalten sie sich, unabhängig davon, ob die Phishing-Mail von einem Menschen oder einer KI stammt.

Traditionelle Schutzmechanismen wie Spam-Filter oder technische Lösungen bleiben wichtig, aber die jüngsten Entwicklungen machen deutlich, dass der „Faktor Mensch" immer mehr in den Mittelpunkt rücken muss. Angreifer:innen rüsten mit KI auf – Unternehmen sollten es ihnen gleichtun. Eine moderne Awareness-Plattform wie Awareness 365 zeigt, wie KI als Verteidigungsinstrument dienen kann: Sie ermöglicht ein immersives, aktuelles Training der Mitarbeiter und Mitarbeiterinnen und macht sie so fit für die neuen, KI-gestützten Betrugsmaschen. Mit diesem Ansatz können Unternehmen eine proaktive Sicherheitskultur etablieren, in der ihre Mitarbeiter zu einer widerstandsfähigen Firewall werden, gegen Angriffe der nächsten Generation ebenso wie gegen die klassischen Bedrohungen von gestern. -**v**-

Mag. Manfred OSCHOUNIG

SOCIAL ENGINEERING – Sicherheit beginnt im Kopf

Cybersicherheit gilt in der öffentlichen Wahrnehmung häufig als rein technisches Problem. Firewalls, Verschlüsselung und intelligente Überwachungssysteme stehen dabei im Fokus. Doch selbst die ausgereiftesten technischen Schutzmaßnahmen stoßen an ihre Grenzen, wenn die größte Schwachstelle im System nicht adressiert wird: DER MENSCH!

Social Engineering als Bedrohungskategorie

Social Engineering – die gezielte Manipulation menschlichen Verhaltens mit dem Ziel, sicherheitsrelevante Informationen zu erlangen oder sicherheitskritische Handlungen auszulösen – entwickelt sich zunehmend zur dominanten Bedrohung für Unternehmen und Institutionen. Dabei ist die Methode nicht neu. Der klassische Trickbetrug hat digitale Ausprägungen gefunden. Durch die Digitalisierung haben diese Angriffe eine neue Qualität erreicht: Sie sind schneller, gezielter und schwerer zu erkennen.

Angreifende agieren hochprofessionell und mit psychologischer Präzision. Sie nutzen soziale Muster, gewohnte Abläufe und menschliche Schwächen – etwa Vertrauen, Hilfsbereitschaft oder Zeitdruck –, um ihre Ziele zu erreichen. Besonders hinterhältig ist, dass sie ihre Angriffe zunehmend individuell zuschneiden und damit die Erfolgschancen drastisch erhöhen.

Neue Dimensionen durch Künstliche Intelligenz

Ein typisches Angriffsszenario beginnt mit einer scheinbar offiziellen E-Mail – beispielsweise mit einem dringenden Hinweis der Geschäftsleitung oder einer öffentlichen Institution. Die Nachricht wirkt seriös, der Absender scheint bekannt, der Handlungsdruck ist groß. Ein Klick genügt – und das Einfallstor für Schadsoftware, Datenklau oder finanzielle Verluste ist geöffnet.

Der Einsatz Künstlicher Intelligenz verschärft diese Dynamik. Generative Modelle erstellen täuschend echte, sprachlich korrekte und personalisierte Nachrichten. Deepfake-Technologien imitieren Stimmen von Vorgesetzten oder Kolleg*innen, um telefonisch Druck auszuüben. Mithilfe von OSINT (Open Source Intelligence) analysieren automatisierte Systeme öffentlich zugängliche Informationen über Zielpersonen, um Angriffe maßgeschneidert zu gestalten. Diese neuen Werkzeuge machen Social Engineering präziser und gefährlicher denn je.

Reale Vorfälle aus Österreich

Im Jahr 2022 wurde eine niederösterreichische Gemeinde Opfer eines Angriffs. Eine E-Mail im Design des Landesamts verwies auf angebliche Hygieneregeln. Ein Klick genügte – im Hintergrund wurde Schadsoftware installiert, das gesamte Verwaltungsnetzwerk fiel aus. Der Schaden war beträchtlich.

Ein weiteres Beispiel betrifft ein oberösterreichisches Bauunternehmen. Der Geschäftsführer wurde von einer angeblichen Microsoft-Mitarbeiterin kontaktiert, die ein dringendes Sicherheitsupdate ankündigte. Der gewährte Fernzugriff führte zur Kompromittierung sensibler Daten – einschließlich Bankkonten, über die mehrere tausend Euro abflossen.

Datenlage und Studien: Der Mensch als Einfallstor

Der „Human Factor Report 2025" von Proofpoint zeigt: 74 % aller erfolgreichen Cyberangriffe basieren auf Social Engineering. Besonders gefährdet sind KMU, öffentliche Einrichtungen, Schulen und soziale Dienste – Strukturen, in denen IT-Sicherheitsressourcen knapp sind und die Belegschaften oft überlastet oder unzureichend geschult sind.

Eine Studie von Edwards et al. (2023) zeigt, dass generative KI in simulierten Angriffsszenarien bei 43 % der Versuchspersonen erfolgreich war. Alshamrani et al. (2022) berichten von einer bis zu 30 % höheren Erfolgsquote bei KI-gestützten Angriffen im Vergleich zu herkömmlichen Methoden. Die Zahlen sprechen eine klare Sprache – und verlangen nach konsequentem Handeln.

Prävention beginnt bei der Kultur

Technik allein genügt nicht. Nachhaltige Cybersicherheit beginnt mit einem Kulturwandel. Organisationen müssen die menschliche Komponente in ihre Sicherheitsstrategie integrieren. Entscheidend sind:

- regelmäßige Schulungen und Awareness-Programme,
- realitätsnahe Trainings zur Angriffserkennung,
- eine offene Fehlerkultur, die das sofortige Melden verdächtiger Vorfälle ermöglicht.

Nur wer Fragen stellen und Zweifel äußern darf, entwickelt die kritische Distanz, die Social Engineering ins Leere laufen lässt.

Das ZRK – Kompetenzzentrum für Sicherheit

Das Zentrum für Risiko- und Krisenmanagement (ZRK) mit Sitz in Wien unterstützt Organisationen aller Größenordnungen beim Aufbau einer widerstandsfähigen Sicherheitskultur. Das ZRK bietet:

- praxisnahe Schulungen mit aktuellen Fallbeispielen,
- Awareness-Kampagnen, die individuell auf Zielgruppen abgestimmt sind,
- Social-Engineering-Simulationen (Phishing, Vishing, physische Angriffe),
- Red-Teaming-Übungen zur Identifikation organisatorischer Schwachstellen,
- Begleitung bei der Entwicklung von Notfallplänen und Meldeprozessen.

Das erklärte Ziel: die „Human Firewall" stärken – jene Schutzschicht, die durch informierte, sensibilisierte und selbstsichere Mitarbeitende entsteht. Das ZRK agiert dabei nicht nur beratend, sondern aktiv unterstützend, mit direkter Umsetzungshilfe und wissenschaftlich fundierten Methoden.

Sicherheitskompetenz ist Führungsaufgabe

Social Engineering ist die intelligenteste Form des digitalen Angriffs – und zugleich die menschlichste. Sie appelliert an Emotionen, Vertrauen und Reflexe. Organisationen, die diesen Faktor unterschätzen, riskieren nicht nur monetäre Verluste, sondern auch irreparablen Vertrauensschaden.

Cybersicherheit beginnt im Kopf – mit kritischem Denken, informierten Entscheidungen und klaren Prozessen. Das ZRK steht dabei als starker Partner zur Seite: praxiserprobt, lösungsorientiert und individuell. -**v**-

Literaturverzeichnis

Alshamrani, A. A., Alsadhan, N. A., Alghamdi, M. A., Alghamdi, W. H., & Alahmadi, A. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks. Applied Sciences, 12(12), 6042. https://doi.org/10.3390/app12126042

Edwards, B., Gentzel, P., & Zettlemoyer, L. (2023). Digital Deception: Generative AI in Social Engineering. arXiv preprint arXiv:2310.13715. https://arxiv.org/abs/2310.13715

Proofpoint. (2025). The Human Factor Report 2025: The Rise of Social Engineering. Abgerufen von https://www.proofpoint.com/us/resources/threat-reports/human-factor-social-engineering

Marcel LEHNER

Zukunft gestalten heißt: Sicherheit neu denken!

Ein Impuls zur strategischen Neuausrichtung von Sicherheit als Treiber für Resilienz, Innovation und moderne Unternehmensführung.

Oft fängt es leise an. Nicht mit einem Knall oder einer riesigen Katastrophe, die durch die Medien geht. Sondern mit kleinen Störungen, die kaum jemand bemerkt. Eine E-Mail kommt nicht an. Ein Zugriff wird verweigert. Ein Mitarbeiter sagt aus Unsicherheit nichts, obwohl er ein Problem sieht.

Früher schien das unwichtig. Heute ist es das erste Beben im Fundament. Sicherheit ist nicht mehr selbstverständlich und unsichtbar. Sie ist nicht mehr nur das Fundament, auf dem wir bauen. Sie ist eine aktive Bedingung geworden. Ohne sie hält kein Bau mehr.

Was bedeutet das? Wir müssen unser Denken über Sicherheit grundlegend ändern. Nicht aus Angst, sondern aus klarem Kopf. Nicht als Abwehr, sondern als Prinzip, das gestaltet. In einer Zeit, die sich ständig ändert, in der Sicherheiten schwinden, brauchen wir eine Sicherheitsphilosophie, die nicht fragt: Wie schützen wir uns? Sondern: Wie bleiben wir handlungsfähig, ohne auseinanderzufallen? Wie schaffen wir Strukturen, die Wandel nicht nur überstehen, sondern ihn ermöglichen?

Dieser neue Blick fängt mit einer anderen Perspektive an. Sicherheit ist längst keine reine Technikfrage mehr, kein Thema nur für die IT oder Werkschutz. Sie ist strategisch wichtig für alle Bereiche. Wer heute ein Unternehmen leitet, leitet auch ihre Sicherheit. Wer das nicht tut, führt im Blindflug. Denn Zukunftsfähigkeit ohne kluges Sicherheitsverständnis ist nur Wunschdenken.

Es ist ein alter Irrtum, Sicherheit nur als Einschränkung zu sehen. Als Bremse für Neues, als Bürokratie, als Kostenfaktor. Diese Sichtweise ist nicht nur falsch, sie ist gefährlich geworden. Denn in Wahrheit ermöglicht Sicherheit vieles. Sie ist der Boden, auf dem Sie Risiken eingehen können, weil Sie wissen, wie Sie Fehler auffangen. Sie ist der Raum, in dem Sie experimentieren dürfen, weil Sie lernen statt zu stürzen. Kurzum: Sicherheit nimmt Ihnen nicht die Freiheit. Sie schafft sie.

Ein Unternehmen, das Sicherheit strategisch denkt, bleibt handlungsfähig, auch wenn es schwierig wird. Es verfällt nicht in Panik, sondern navigiert mit einem klaren Kompass. Dieser Kompass heißt nicht Kontrolle, sondern Vertrauen. Und dieses Vertrauen entsteht nicht durch starre Regeln oder Hierarchien. Es wächst durch Klarheit, offene Kommunikation und eine Sicherheitskultur, die Verantwortung verteilt, statt sie zu zentralisieren.

Das heißt praktisch: Sicherheit muss überall mitgedacht werden. Sie ist kein Projekt für eine Abteilung, das mit einem Zertifikat endet. Sie ist ein Prinzip, das in alle Abläufe, jede Entscheidung, jede Beziehung gehört. Wer ein neues Produkt entwickelt, wer mit Partnern arbeitet, wer Mitarbeiter führt, muss sich fragen: Wie ermöglichen wir sicheres Ausprobieren, geschützte Innovation, gemeinsames Lernen? Wo setzen wir auf Vertrauen, aber bleiben realistisch? Wo schaffen wir Strukturen, die unterstützen, statt einzuengen?

Dabei geht es nicht darum, jedes Risiko zu vermeiden. Das wäre Unsinn in einer Welt, die ständig ungewiss ist. Es geht darum, gut mit Risiken umzugehen. Sie frühzeitig zu erkennen, zu bewerten und einzuordnen. Und die Bereitschaft zu haben, Verantwortung dafür zu übernehmen - auch wenn es unangenehm wird. Wer das kann, reagiert nicht nur schnell, sondern agiert klug. Wer Sicherheit nur als Versicherung gegen den Notfall sieht, hat den Notfall schon akzeptiert.

Die Zukunft fragt nicht, ob wir sie wollen. Sie fragt, ob wir bereit sind. Und genau hier wird Sicherheit zum Führungsprinzip. Es ist die Fähigkeit, Systeme zu gestalten, die sich anpassen, ohne sich selbst zu verlieren. Die Störungen aufnehmen, ohne gelähmt zu sein. Die auch unter Druck ihre Form behalten. Solche Systeme brauchen Menschen, die Sicherheit nicht mit Starrheit verwechseln. Sondern mit Haltung.

Gerade in Zeiten schneller digitaler Veränderungen und globaler Unsicherheit geben Organisationen, die resilient sind und gut mit Sicherheit umgehen können, Orientierung. Sie sind das Gegenteil von ständigem Reagieren, hektischem Umbruch-Management oder blindem Technik-Glauben. Sie sind nicht ängstlich, sondern überlegt. Nicht langsam, sondern nachhaltiger. Nicht risikoscheu, sondern klug im Umgang mit Risiken.

Damit schaffen sie etwas Wichtiges für die nächsten Jahre: Vertrauen. In einer Zeit, in der Institutionen schwächer werden, Fehlinformationen sich schneller verbreiten als Fakten und jede Entscheidung sofort öffentlich zerpflückt werden kann, ist Vertrauen nicht nur ein netter Bonus, sondern strategisch entscheidend. Und nichts schafft mehr Vertrauen als Sicherheit. Nicht als perfekte Lösung, sondern als glaubwürdige Verantwortung.

Was das konkret bedeutet? Wir müssen unsere Sicherheitsideen an Menschen ausrichten, nicht an Technik. Wir sollten nicht fragen: Welche Norm erfüllen wir? Sondern: Welches Verhalten wollen wir fördern? Welche Entscheidungen absichern? Welche Risiken wollen wir bewusst eingehen, um Neues zu schaffen? Denn nur wer Risiken gestaltet, gestaltet auch Zukunft.

Das erfordert Mut. Und eine andere Art von Führung. Eine Führung, die Sicherheit nicht nur bespricht, sondern lebt. Die Widersprüche aushält, statt sie zu ignorieren. Die Verantwortung übernimmt, statt sie abzuschieben. Die bereit ist, mit Unsicherheit zu arbeiten, statt sie bekämpfen zu wollen. Denn Sicherheit, das muss man klar sagen, ist kein fester Zustand. Sie ist ein Prozess. Und dieser Prozess ist nie vorbei. Aber er fängt immer mit einer Entscheidung an: der Entscheidung, sie ernst zu nehmen.

In einer Welt, die nicht ruhiger wird, ist das vielleicht unsere wichtigste Aufgabe. Nicht, die Welt zu kontrollieren. Sondern sie verständlich und gestaltbar zu halten. Sicherheit ist dabei keine Mauer gegen die Zeit. Sie ist das Werkzeug, um mit ihr zu arbeiten. Und sie ist der Unterschied zwischen bloßem Reagieren und echtem Gestalten.

Deshalb heißt Zukunft gestalten auch: Sicherheit neu denken. Nicht als lästige Pflicht, sondern als Chance. Nicht als Einschränkung, sondern als Stärkung. Nicht als Ende der Freiheit, sondern als ihr Anfang. Denn in der Unsicherheit der Welt liegt kein Untergang. Sondern die größte Einladung zur Verantwortung, die unsere Zeit uns gibt.

-v-

Holger KÖNNECKE

Neue Spannungsverhältnisse und Interdependenzen im Kontext der Cybersecurity und neuer regulatorischer Anforderungen

In unserer heutigen Welt sind die digitalen Systeme die Grundlage für Wirtschaft, Infrastruktur und Gesellschaft. Cybersecurity nimmt daher eine wachsende zentrale Rolle ein. Die zunehmende Vernetzung durch Cloud-Computing, Internet of Things (IoT) und globalen Lieferketten schafft Chancen als auch Risiken. Gleichzeitig drängen neue regulatorische Anforderungen, wie die EU-NIS-2-Richtlinie oder der Cyber Resilience Act, Unternehmen dazu, ihre Sicherheitsmaßnahmen zu verstärken. Die Komplexität dieser Vorgaben führt zu Spannungen zwischen technischen Möglichkeiten, organisatorischen Realitäten und rechtlichen Verpflichtungen.

Spannungsfeld Vernetzung: Effizienter, aber auch angreifbarer

Die moderne Wirtschaft basiert auf vernetzten Systemen, die von IoT-Geräten in der Produktion bis hin zu Cloud-Diensten für Datenverarbeitung reichen. Diese Interdependenzen erhöhen die Effizienz, machen Unternehmen jedoch anfälliger für Cyberangriffe. Der SolarWinds-Angriff von 2020 zeigte, wie ein kompromittierter Softwareanbieter Tausende Unternehmen und Behörden weltweit gefährden kann. Laut einer Bitkom-Studie von 2024 waren 81 % der deutschen Unternehmen in den letzten zwölf Monaten von Cyberangriffen betroffen, mit Schäden von 267 Milliarden Euro. Besonders kritische Infrastrukturen wie Energieversorger oder Krankenhäuser sind durch ihre Vernetzung gefährdet, da ein Ausfall weitreichende Kaskadeneffekte auslöst.

Die Abhängigkeit von globalen Lieferketten und Technologieanbietern verstärkt die Risiken. Ein Angriff auf einen einzelnen Anbieter, wie etwa ein Cloud-Dienstleister, kann ganze Branchen lahmlegen. Die Ransomware-as-a-service-Attacke auf die Colonial Pipeline 2021 führte zu Treibstoffknappheit in den USA und verdeutlichte die gesellschaftlichen Auswirkungen solcher Vorfälle. Endnutzer sind ebenfalls betroffen, da Datenschutzverletzungen das Vertrauen in digitale Dienste untergraben. Gleichzeitig fördern Interdependenzen Innovationen, etwa durch kollaborative Plattformen, was die Balance zwischen Sicherheit und Fortschritt zu einer zentralen Herausforderung macht.

Spannungsfeld Cybersecurity und Regulierung

Die EU hat mit der NIS-2-Richtlinie und dem Cyber Resilience Act ambitionierte Schritte unternommen, um die Cybersicherheit zu

stärken. NIS-2 erweitert die Anforderungen an Betreiber kritischer Infrastrukturen und verpflichtet Unternehmen zu strengeren Meldepflichten und Sicherheitsmaßnahmen. Der Cyber Resilience Act zielt darauf ab, die Sicherheit von Produkten mit digitalen Komponenten zu gewährleisten, etwa durch Sicherheitsupdates während des gesamten Produktlebenszyklus. In Deutschland ergänzt das IT-Sicherheitsgesetz 2.0 diese Vorgaben, indem es die Anforderungen an Betreiber kritischer Infrastrukturen verschärft. Ziel ist es, die Resilienz gegenüber Cyberbedrohungen zu erhöhen und einheitliche Standards zu schaffen.

Die Umsetzung dieser Regularien ist jedoch komplex. Besonders kleine und mittelständische Unternehmen (KMU) kämpfen mit den Kosten für Compliance, die laut Bitkom oft Millionenbeträge erreichen. Globale Unterschiede in der Regulierung – etwa zwischen der EU mit ihrer strengen Datenschutzgesetzgebung und den USA mit ihrem stärker marktorientierten Ansatz – erschweren die Harmonisierung für international tätige Unternehmen. Zudem fehlt es oft an einheitlichen technischen Standards, was die Einhaltung der Vorgaben zusätzlich erschwert.

Ein zentrales Spannungsfeld besteht zwischen technischen Innovationen und starren regulatorischen Vorgaben. Beispielsweise fördern flexible Cloud-Lösungen die Effizienz, können jedoch mit Meldepflichten oder Datenschutzanforderungen kollidieren. Ein weiteres Beispiel ist die Verschlüsselung: Während Unternehmen End-to-End-Verschlüsselung einsetzen, um Daten zu schützen, fordern einige Regierungen Hintertüren für Überwachungszwecke, was immer mit einer Schwachstelle für die Sicherheit einher geht. Diese Konflikte zwingen Unternehmen, Kompromisse zwischen Sicherheit und rechtlicher Konformität zu finden.

Die Vernetzung von Systemen wirft Fragen zur Haftung auf. Wer ist verantwortlich, wenn ein Angriff über einen Drittanbieter erfolgt? Der SolarWinds-Fall zeigte, dass die Haftung oft unklar bleibt, was rechtliche und finanzielle Unsicherheiten schafft. Zudem stehen Unternehmen im Spannungsfeld zwischen Autonomie und staatlicher Kontrolle. Regularien wie NIS-2 erhöhen die staatliche Aufsicht, was für einige Unternehmen als Eingriff in ihre Entscheidungsfreiheit wahrgenommen wird.

Der Mensch bleibt die größte Schwachstelle in der Cybersecurity. Laut dem Verizon Data Breach Investigations Report 2024 sind 74 % der Datenschutzverletzungen auf menschliches Fehlverhalten zurückzuführen, etwa durch Social Engineering oder unzureichende Schulungen. Regularien fordern zwar Awareness-Programme, doch die Umsetzung ist oft unzureichend. Zeit- und Kostendruck sind immer noch zu oft die Bewegungshebel für Unternehmen statt eines Sicherheitsstandards als Zielmarke.

Strategien zur Auflösung des Spannungsfelds

Um die Spannungsverhältnisse zu meistern, sind ganzheitliche Sicherheitskonzepte erforderlich. Diese integrieren IT-Sicherheit, physischen Schutz und organisatorische Maßnahmen. KI-gestützte Tools wie Intrusion Detection Systems oder Anomalieerkennung können helfen, Bedrohungen frühzeitig zu erkennen und gleichzeitig Compliance-Vorgaben zu erfüllen. Regelmäßige Sicherheitsaudits und Penetrationstests sind essenziell, um Schwachstellen zu identifizieren.

Die Komplexität der Bedrohungslage erfordert Zusammenarbeit. Public-Private-Partnerships, wie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) gefördert, können den Austausch von Bedrohungsinformationen verbessern. Globale Standards, etwa durch die ISO/IEC 27001, tragen zur Harmonisierung bei und erleichtern die Compliance für international tätige Unternehmen. Gleichzeitig müssen Unternehmen mit Lieferkettenpartnern kooperieren, um Schwachstellen in vernetzten Systemen zu minimieren.

Investitionen in Mitarbeiterschulungen sind unerlässlich, um die menschliche Schwachstelle zu stärken. Regelmäßige Simulationen von Phishing-Angriffen und Schulungen zur Erkennung von Social Engineering erhöhen die Widerstandsfähigkeit. Eine Sicherheitskultur, die von der Führungsebene vorgelebt wird, ist entscheidend, um die Einhaltung regulatorischer Vorgaben zu verankern.

Die Zukunft der Cybersecurity wird von Technologien wie Quantencomputing und zunehmender Automatisierung geprägt sein. Quantencomputing könnte bestehende Verschlüsselungssysteme obsolet machen, was neue regulatorische Anforderungen nach sich zieht. Gleichzeitig erfordern die Dynamik von Cyberbedrohungen flexible Regularien, die mit technologischen Entwicklungen Schritt halten. Unternehmen, Regierungen und internationale Organisationen müssen hier enger zusammenarbeiten, um globale Standards zu etablieren und die Resilienz zu stärken. -V-

Robert-P. PELIKAN

Kritische Infrastrukturen im Fadenkreuz: Wie sicher ist unsere Versorgung wirklich?

Cyberbedrohungen, Systemrisiken und die Lehren aus realen Vorfällen

Ob Energie, Gesundheit, Transport oder Kommunikation – die kritischen Infrastrukturen unserer Gesellschaft sind heute vernetzter denn je. Und damit auch anfälliger für gezielte Angriffe. Der Beitrag beleuchtet aktuelle Bedrohungen, reale Vorfälle – und was wir daraus lernen müssen.

Wenn Sicherheit zur Grundvoraussetzung wird

„Unsere Infrastruktur ist sicher" – eine Aussage, die zunehmend fragil wirkt. In einer Zeit, in der Strom, Wasser, digitale Kommunikation und Transportmittel miteinander verwoben sind, hat sich das Verständnis von Sicherheit fundamental verändert. Früher wurde Infrastruktur vor allem als physische Struktur gedacht – Brücken, Straßen, Kraftwerke. Heute umfasst sie zunehmend digitale Prozesse, datengetriebene Steuerungen und global vernetzte Systeme. Das macht sie nicht nur effizienter – sondern auch angreifbarer.

Cyberbedrohungen, Naturkatastrophen, politische Krisen – sie alle zeigen, dass kritische Infrastrukturen nicht mehr nur geschützt, sondern auch resilient sein müssen. Das bedeutet nicht nur technologische Absicherung, sondern auch organisatorische, rechtliche und gesellschaftliche Vorsorge. Ein Angriff auf eine kritische Infrastruktur ist längst nicht mehr nur ein „IT-Problem". Es ist ein Risiko für die Funktionsfähigkeit eines ganzen Landes – mit möglichen Auswirkungen auf die öffentliche Ordnung, die politische Stabilität und sogar das Vertrauen in demokratische Institutionen.

Darüber hinaus hat die Abhängigkeit von wenigen zentralen Anbietern – etwa bei Cloud-Diensten, Rechenzentren oder Energieübertragung – zu neuen Konzentrationsrisiken geführt. Viele kritische Prozesse hängen heute an sehr wenigen technischen Schnittstellen, die bei einer Störung kaskadierende Effekte auslösen können. In einer Welt zunehmender Vernetzung ist das Thema Sicherheit längst zur Chefsache geworden – es betrifft nicht mehr nur Technikabteilungen oder Spezialisten, sondern alle Entscheidungsebenen.

Was macht kritische Infrastrukturen so verletzlich?

Kritische Infrastrukturen sind hochkomplexe Systeme mit vielen interdependenten Komponenten. Ihre Verwundbarkeit ergibt sich nicht nur aus technischen Schwächen, sondern auch aus organisatorischen, ökonomischen und menschlichen Faktoren. Ein zentrales Problem: Die meisten dieser Systeme wurden nicht mit Blick auf IT-Sicherheit entwickelt. Sie sind oft jahrzehntelang gewachsen, modular erweitert und selten ganzheitlich neu gedacht worden. Der Begriff „Technologieschuld" beschreibt treffend, wie neue Funktionen auf alten Systemen aufbauen – ohne dass die Sicherheitsbasis je erneuert wurde.

Zudem sind viele Betreiber mit einem Dilemma konfrontiert: Modernisierung bedeutet Investitionen, die sich aus Sicht klassischer Betriebswirtschaft oft nicht direkt rechnen. Die Konsequenz: Sicherheitsupdates werden aufgeschoben, Migrationen verzögert, Personal eingespart. Das führt dazu, dass viele kritische Einrichtungen mit Systemen arbeiten, die über zehn Jahre alt sind – teilweise sogar mit Software, für die es keine Sicherheitsupdates mehr gibt.

Ein weiteres Problem ist die unklare Zuständigkeit: Wer ist verantwortlich, wenn ein externer IT-Dienstleister ein veraltetes Modul einsetzt? Wenn ein Subunternehmer Fernzugriff auf sicherheitsrelevante Systeme hat? In der Praxis gibt es oft keine klare Sicherheitsstrategie, keine einheitliche Sicherheitsarchitektur – und keine kontinuierliche Risikoanalyse. Damit bleiben viele Schwachstellen lange unentdeckt – bis ein Angreifer sie findet.

Sektor für Sektor: Wo die größten Risiken liegen

Energie
Die Energieversorgung gilt als das Nervensystem moderner Gesellschaften. Ein Stromausfall betrifft nicht nur Licht und Heizung, sondern auch Kommunikation, Verkehr, Handel und Gesundheitsversorgung. Besonders heikel ist die zunehmende Umstellung auf Smart Grids und dezentral organisierte Energieversorgung, die zwar effizienter, aber auch anfälliger für Angriffe sind. Die Zahl der digitalen Schnittstellen steigt rasant – von Smart-Metern bis hin zu intelligenten Lastverteilungen. Jede dieser Komponenten kann potenziell ein Angriffsziel sein.

Hinzu kommt die geopolitische Lage: Energieinfrastruktur ist ein strategisches Ziel staatlicher Akteure – etwa zur Destabilisierung, wirtschaftlichen Schwächung oder Demonstration von Macht. Auch Erpressungsszenarien sind denkbar: Ein Angriff auf ein Umspannwerk zur Heizsaison kann massiven politischen Druck erzeugen. Während viele Betreiber sich um Netzstabilität und Versorgungssicherheit bemühen, ist IT-Sicherheit nicht immer gleichwertig eingebettet – ein riskantes Ungleichgewicht.

Gesundheit
Das Gesundheitswesen ist in den letzten zehn Jahren rasant digitalisiert worden – jedoch häufig ohne gleichzeitige Erhöhung der Sicherheitsstandards. Elektronische Patientenakten, Medizingeräte mit Netzwerkanschluss, Krankenhausinformationssysteme (KIS), Apothekennetze – alles ist heute Teil einer kritischen digitalen Kette. Doch der technologische Fortschritt ist vielerorts nicht mit ausreichend IT-Fachpersonal abgesichert. In kleinen bis mittleren Spitälern gibt es teils nur eine einzige IT-Fachkraft, oft ohne Spezialisierung auf Sicherheit.

Erstaunlich ist auch, wie selten Notfallkonzepte geübt werden. Wie läuft die Aufnahme ohne IT-Systeme? Wie können Medikamente dokumentiert werden, wenn die Software ausfällt? Wie wird kommuniziert, wenn Telefon und Internet wegfallen? Viele Einrichtungen verlassen sich auf die Funktionsfähigkeit der Technik – und unterschätzen den Schaden bei einem längerfristigen Ausfall.

Verkehr und Logistik
Kaum ein Sektor ist so stark auf Just-in-Time-Logik und IT-gestützte Prozesse angewiesen wie der Transportsektor. Ob Flugpläne, Fahrgastinformationssysteme oder Containerverwaltung – nahezu alle Abläufe hängen an digitaler Infrastruktur. Besonders gefährlich sind Angriffe, die gezielt Schnittstellen stören: etwa das Zusammenspiel zwischen Warenwirtschaftssystemen, Trackinglösungen und Zahlungsabwicklung.

Ein weiteres Risiko liegt in der globalen Vernetzung: Viele Betreiber nutzen Softwarelösungen aus Drittstaaten oder lassen zentrale Komponenten von internationalen Dienstleistern warten. Dabei werden oft unbewusst rechtliche und technische Abhängigkeiten geschaffen, die im Krisenfall kaum kontrollierbar sind. Die Sicherstellung von Redundanz, Eigenkontrolle und Ausfallsicherheit ist daher nicht nur ein IT-, sondern auch ein geopolitisches Thema.

Kommunikation und IT
Die digitale Infrastruktur ist der Grundpfeiler fast aller anderen KRITIS-Bereiche. Der Ausfall eines großen DNS-Servers, eine gestörte Mobilfunkzelle oder ein Angriff auf ein Rechenzentrum kann massive Folgeschäden erzeugen – von Behördenausfällen bis zur wirtschaftlichen Lähmung. Besorgniserregend ist die wachsende Zentralisierung im Cloud-Bereich: Wenige große Anbieter betreiben den Großteil der europäischen Datenverarbeitung. Ein gezielter Angriff auf einen dieser Anbieter kann europaweit Auswirkungen haben.

Gleichzeitig zeigt sich, dass auch physische Angriffe zunehmen – etwa das Durchtrennen von Glasfaserleitungen oder Sabotage von 5G-Masten. Diese Angriffe sind vergleichsweise einfach durchzuführen, haben aber erhebliches Störpotenzial. Kritisch bleibt, dass viele Kommunikationssysteme keine echte Redundanz haben – fällt der Hauptkanal aus, steht alles still.

Weitere Bereiche: Wasser, Finanzen, Lebensmittelversorgung
Diese Bereiche werden in der öffentlichen Diskussion oft unterschätzt – dabei wären ihre Ausfälle besonders spürbar. In der Lebensmittelversorgung etwa hängt vieles an temperaturgeführten Lagerhäusern und automatisierten Logistiksystemen. Schon eine mehrstündige Störung kann zu Wegwurf, Preisanstieg und Versorgungslücken führen.

Im Finanzwesen wiederum sind Zahlungssysteme hochgradig automatisiert und stark von Netzwerken abhängig. Angriffe auf Clearingstellen, Online-Banking-Systeme oder Börsen könnten nicht nur wirtschaftlichen, sondern auch gesellschaftlichen Schaden anrichten – Stichwort Vertrauensverlust.

Täterprofile, Methoden, Motive

Die Bedrohungslage für kritische Infrastrukturen ist vielschichtig – denn auch die Angreifer sind divers. Während klassische Cyberkriminelle meist auf Profit aus sind, verfolgen staatlich unterstützte Gruppen oft strategische, politische oder militärische Ziele. Diese sogenannten Advanced Persistent Threats (APT) verfügen über große Ressourcen, Geduld und hochentwickelte Angriffstechniken. Sie operieren oft über Jahre hinweg, versteckt in Systemen, sammeln Daten oder manipulieren Prozesse – bis sie zuschlagen.

Ein wachsendes Risiko geht auch von „Hacktivisten" aus, also ideologisch motivierten Angreifern, die politische, gesellschaftliche oder ökologische Ziele verfolgen. In Zeiten zunehmender Polarisierung und geopolitischer Spannungen nutzen solche Gruppen Schwachstellen in kritischer Infrastruktur als Bühne. Ein Angriff auf eine Behörde, einen Energieversorger oder ein Gesundheitssystem wird zur symbolischen Aktion – oft mit weltweiter Aufmerksamkeit.

Nicht unterschätzt werden dürfen Insider-Bedrohungen: Mitarbeitende, Dienstleister oder Subunternehmer mit legitimem Zugriff, die unbeabsichtigt oder absichtlich Schaden verursachen. In manchen Fällen geschieht dies aus Nachlässigkeit – z. B. über veraltete Passwörter oder private

Geräte im Firmennetzwerk. In anderen Fällen steckt Sabotage, Erpressung oder Frust dahinter. Das Problem: Insider sind schwer zu erkennen, da sie Teil des Systems sind. Technische Kontrollen helfen – aber entscheidend ist eine Kultur der Aufmerksamkeit, der klaren Verantwortlichkeit und der Prävention.

Die Methoden werden immer raffinierter: KI-generierte Phishing-Mails, Deepfakes zur Identitätsmanipulation, gezielte Angriffe auf Firmware, kombinierte physisch-digitale Angriffe – die Liste wird länger. Wichtig ist: Viele Angreifer gehen arbeitsteilig vor. Die einen entwickeln Tools, andere nutzen sie – „Cybercrime-as-a-Service" macht Angriffe skalierbar und planbar. Gerade deshalb braucht es auf Seiten der Verteidiger mehr als nur Technik: Es braucht ein Verständnis für Motivlagen, Strukturen, Dynamiken.

Szenario: Wenn alles zusammenbricht

Stellen wir uns ein realistisch simuliertes Szenario vor, das auf Erkenntnissen aus Planspielen und realen Vorfällen basiert. Es zeigt, wie schnell sich eine technische Störung in eine gesellschaftliche Krise verwandeln kann.

Tag 1 – 16:40 Uhr: Ein gezielter Angriff auf mehrere Energieunternehmen in Zentraleuropa führt zu regionalen Stromausfällen. Wien, München und Prag sind betroffen. Erste Bahnen bleiben stehen. Der Mobilfunk funktioniert nur eingeschränkt. Der Notruf ist überlastet.

Tag 2 – 08:00 Uhr: Krankenhäuser melden Versorgungsengpässe. Apotheken können keine Rezepte mehr abrufen. Erste Supermärkte lassen nur noch Barzahlung zu. Behörden schalten auf Notbetrieb um. Social Media verbreitet Falschinformationen über einen „Krieg".

Tag 3 – 18:00 Uhr: Polizei und Feuerwehr kämpfen mit Koordinationsproblemen. In mehreren Stadtvierteln kommt es zu kleinen Plünderungen. Eine Klinik meldet drei Todesfälle aufgrund unterbrochener Beatmungssysteme. Die Bundesregierung ruft den Katastrophenfall aus.

Tag 4 – 12:00 Uhr: Internationale Hilfsorganisationen werden angefordert. Die Stromversorgung ist nur teilweise wiederhergestellt. Die politische Debatte beginnt: Warum war man nicht vorbereitet?

Dieses Szenario ist fiktiv – und dennoch realistisch. Es basiert auf Mustern, die wir aus der Ukraine, aus Frankreich, aus den USA kennen. Die Frage ist nicht ob ein solcher Vorfall eintritt – sondern wann. Und wie gut wir dann vorbereitet sind.

Was wir aus echten Vorfällen lernen müssen

Jeder reale Vorfall – ob Angriff, Panne oder Naturereignis – liefert wertvolle Lehren. Leider werden diese oft zu spät oder gar nicht analysiert. Dabei zeigen sie immer wieder ähnliche Schwächen:

Fehlende Vorbereitung: Viele Organisationen haben keinen strukturierten Notfallplan, keine klaren Eskalationsstufen, keine eingeübten Abläufe. Bei einem Angriff improvisiert man – und verliert wertvolle Zeit.

Technik ohne Prozesse: Firewalls und Monitoring sind gut – aber nutzlos, wenn niemand weiß, wie im Ernstfall gehandelt werden soll. Technik muss in Prozesse eingebettet sein.

Keine Übung: Viele Organisationen haben noch nie eine Cyberübung gemacht. Wer nicht unter Stress trainiert, wird im Ernstfall überfordert sein. Übungen sind kein Luxus, sondern Pflicht.

Kommunikationslücken: In vielen Vorfällen brach die interne Kommunikation zusammen – weil niemand wusste, wer zuständig ist. Auch externe Kommunikation (Presse, Kunden, Öffentlichkeit) war oft uneinheitlich oder unprofessionell.

Mangel an Transparenz: Viele Organisationen verschweigen Vorfälle aus Angst vor Reputationsverlust. Das ist verständlich – aber kurzsichtig. Nur durch Offenheit entsteht kollektive Lernfähigkeit.

Die wichtigste Lektion: Resilienz ist keine Technologie, sondern ein organisationaler Reifegrad. Wer sich vorbereitet, trainiert und vernetzt, kann auch im Ernstfall handlungsfähig bleiben.

Handlungsempfehlungen: Vom Schutz zur Widerstandsfähigkeit

Der klassische Ansatz „Schütze alles, was du kannst" funktioniert in der heutigen Risikolandschaft nicht mehr. Organisationen müssen davon wegkommen, Sicherheit nur als Abwehrmaßnahme zu sehen. Stattdessen geht es darum, Resilienz aufzubauen – also die Fähigkeit, trotz Störung funktionsfähig zu bleiben und sich schnell zu erholen. Dafür braucht es eine Kombination aus Technik, Prozessen, Kompetenzen und einer gelebten Sicherheitskultur.

Governance und Strategie

Sicherheit muss Chefsache sein – nicht delegierbar an die IT. Ein interdisziplinäres Krisen- und Resilienzboard sollte alle sicherheitsrelevanten Themen bündeln: IT, Betrieb, Kommunikation, Recht, Personal. Dazu gehört auch ein regelmäßiger Lagebericht an die Geschäftsführung sowie ein jährlicher Reifegrad-Check.

Technik

Technische Maßnahmen sind notwendig – aber nicht ausreichend. Zero-Trust-Architekturen, Härtung von OT-Systemen, Angriffserkennung durch KI-gestützte Systeme, getrennte Netze für kritische Anwendungen – all das gehört heute zum Standard. Entscheidend ist jedoch, dass diese Technik auch verantwortlich betrieben, dokumentiert und überwacht wird. Was nützt das beste SIEM-System, wenn es keine Reaktion gibt?

Organisation und Kultur

Sicherheitskultur entsteht durch Führung, Schulung und Vorleben. Regelmäßige Awareness-Trainings, klare Regeln für Zugriffsrechte, sinnvolle Passwortpolitik und ein Sicherheitskodex für alle Mitarbeitenden helfen enorm. Ein interner Meldeprozess für Sicherheitsvorfälle sollte niedrigschwellig und vertrauensvoll gestaltet sein – damit Probleme frühzeitig erkannt werden.

Kooperation

Niemand kann KRITIS-Schutz allein gewährleisten. Der Austausch mit Behörden (z. B. BSI, CERT.at), anderen Betreibern, Forschungseinrichtungen und Verbänden ist essenziell. Gemeinsame Übungen, tech-

nische Plattformen (z. B. MISP für Indicators of Compromise) und vertrauensvolle Zusammenarbeit im Ernstfall machen den Unterschied.

Investitionen
Resilienz kostet – aber sie spart im Ernstfall Millionen. Organisationen sollten Sicherheitsinvestitionen als Betriebssicherheit behandeln, nicht als Compliance-Posten. Dabei hilft eine Risikoanalyse mit Kosten-Nutzen-Szenarien. Förderprogramme auf nationaler und europäischer Ebene (z. B. KIRAS, Horizon Europe) können strategisch genutzt werden, um Projekte zu realisieren, die intern nicht vollständig finanzierbar sind.

Resilienz ist mehr als Verteidigung
Der Schutz kritischer Infrastrukturen ist kein Zustand – sondern ein Prozess. Er beginnt bei der Erkenntnis, dass Perfektion nicht erreichbar ist. Es wird immer Schwachstellen geben. Aber Organisationen können lernen, mit ihnen umzugehen. Sie können vorbereiten, üben, vernetzen und dadurch eine Kultur schaffen, in der Sicherheit nicht bremst – sondern schützt.

Resilienz ist auch Vertrauen: in die eigene Organisation, in Partner, in die Fähigkeit zur Reaktion. Wer in Übungen scheitert, kann im Ernstfall bestehen – wenn daraus gelernt wird. Der Weg zur Resilienz ist kein einmaliges Projekt, sondern ein Teil des strategischen Managements. Er betrifft den CEO genauso wie die Technikerin, den IT-Leiter ebenso wie die Sicherheitsbeauftragte.

Am Ende steht nicht nur die technische Sicherheit, sondern auch die gesellschaftliche Stabilität. Denn wenn kritische Infrastrukturen ausfallen, bricht Vertrauen. Und Vertrauen ist das wertvollste Kapital einer offenen, demokratischen Gesellschaft.

Ausblick: KI, Quanten und geopolitische Unsicherheiten

Die Sicherheitslage wird sich nicht entspannen – im Gegenteil. Neue Technologien und globale Machtverschiebungen erzeugen neue Bedrohungspotenziale.

Künstliche Intelligenz wird auf beiden Seiten zur Waffe. Sie kann helfen, Anomalien zu erkennen, Vorfälle zu priorisieren und Angriffe abzuwehren. Gleichzeitig wird KI genutzt, um Phishing-Mails zu perfektionieren, Fake-Stimmen zu erzeugen oder Social Engineering zu skalieren. Organisationen müssen ihre Schutzmaßnahmen KI-tauglich machen – sonst bleibt ihre Verteidigung analog in einer digitalen Welt.

Quantencomputer könnten binnen weniger Jahre konventionelle Verschlüsselung überflüssig machen. Wer heute nicht mit Post-Quantum-Verschlüsselung plant, riskiert in Zukunft kompromittierte Kommunikation – auch rückwirkend. Denn viele Angreifer speichern heute verschlüsselte Daten, in der Hoffnung, sie später mit neuen Technologien zu entschlüsseln („harvest now, decrypt later").

Geopolitisch sind kritische Infrastrukturen längst Teil hybrider Konflikte. Ob Pipeline, Glasfaserknoten, Rechenzentrum oder DNS-Infrastruktur – viele dieser Systeme sind heute nicht nur technisches, sondern auch strategisches Ziel. Autokratische Regime nutzen Cyberoperationen zur Destabilisierung, zur Einschüchterung und als Ersatz für offene Konfrontation.

Klimakrise und Extremwetter kommen als Stressfaktor hinzu. Trockenheit, Fluten, Stürme oder Brände setzen Infrastruktur auch physisch unter Druck – und erhöhen die Wahrscheinlichkeit für gleichzeitige (kombinierte) Ausfälle.

Der Weg in die Zukunft führt nicht über Angst – sondern über Vorbereitung. Wer in Szenarien denkt, in Partnerschaften investiert und Resilienz zur Strategie macht, wird auch die kommenden Herausforderungen bestehen. -v-

Prof. Dr. Ulrike LECHNER

Digitale Souveränität als strategische Herausforderung für Cybersicherheit und Unternehmensentscheidungen

In einer Ära zunehmender geopolitischer Spannungen und disruptiver digitaler Transformation gewinnt das Konzept der digitalen Souveränität in Europa stark an Bedeutung. Ziel ist es, die digitale Souveränität zu stärken – sowohl gegenüber internationalen Abhängigkeiten als auch hinsichtlich IT-sicherheitstechnischer Risiken. Der CIO des Bundes definiert in Deutschland digitale Souveränität als die Fähigkeit von Individuen und Institutionen, ihre Rolle in der digitalen Welt selbstbestimmt, sicher und unabhängig wahrzunehmen. Begriffe wie Autarkie und Selbstbestimmung werden in der Diskussion zu Digitaler Souveränität häufig als Schlüsselbegriffe genannt. Gleichzeitig zeigt die Realität: Eine vollständige europäische oder nationale Autarkie – sei es bei Hardware, Software oder digitalen Diensten – ist derzeit und auch in der Zukunft kaum praktikabel erreichbar. Wirtschaftliche Wertschöpfung lebt von Skaleneffekten und Vernetzung.

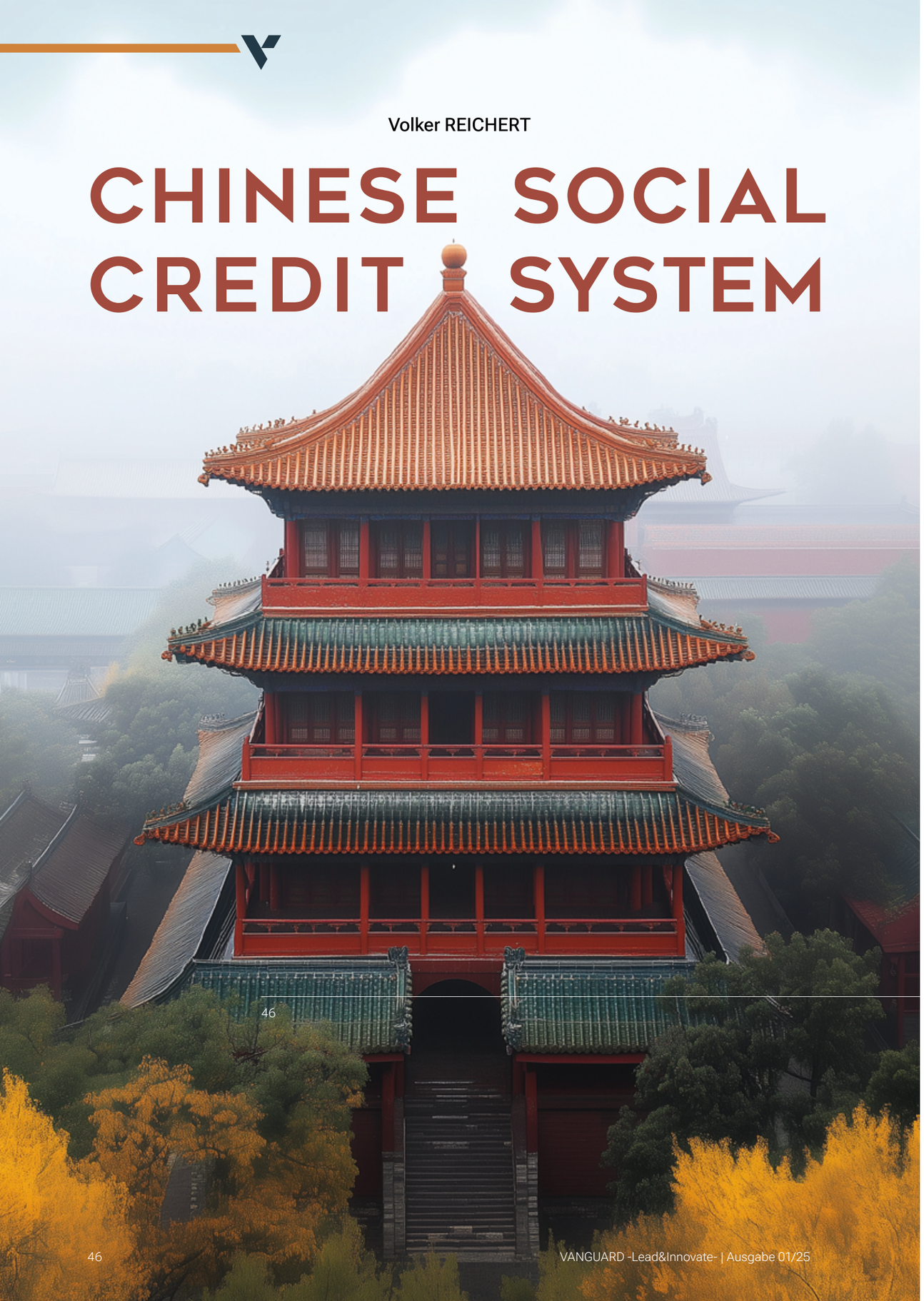
Trotzdem ist digitale Souveränität kein bloßes Ideal, sondern muss als Ausdruck eines strategischen Anspruchs gestaltet werden: Risiken erkennen, beherrschen und resiliente Strukturen schaffen. Für Unternehmen bedeutet dies, sich aktiv mit IT-Sicherheitsrisiken und Abhängigkeiten in der digitalen Lieferkette auseinanderzusetzen. Im Zentrum steht ein proaktives Risikomanagement, das über reine Compliance hinausgeht. Entscheider in Einkauf, IT-Strategie und Beratung müssen neue Maßstäbe anlegen – sowohl bei der Auswahl von Produkten und Dienstleistungen als auch bei der Bewertung langfristiger Abhängigkeiten und Sicherheitsversprechen, wenn Sie die Digitale Souveränität eines Unternehmens erhöhen sollen und möchten. Im der IT-Beratung rückt die Frage in den Vordergrund, welche Technologien, Architekturen und Partner dazu beitragen können, digitale Souveränität systematisch aufzubauen. Für Beschaffungsverantwortliche hingegen verändert sich das Anforderungsprofil grundlegend: Neben klassischen Kriterien wie Preis und Leistung müssen zukünftig Aspekte wie Update- und Patch-Fähigkeit, langfristige Lieferfähigkeit, regulatorische Anpassungsfähigkeit und Sicherheitsgarantien in die Bewertung einfließen. So lassen sich externe Angebote in souveräne, organisationseigene Lösungen und Mehrwerte für die Kunden überführen und die Souveränität der Kunden stärken.

Digitale Souveränität ist daher keine statische Eigenschaft, sondern ein kontinuierlich zu entwickelndes Unternehmensziel. Es erfordert Kompetenzen auf individueller und organisatorischer Ebene – von der strategischen Ausrichtung über die technische Umsetzung bis hin zur kontinuierlichen und in die Zukunft gerichteten, strategischen Risikobewertung. Die Fähigkeit, Veränderungen in der Bedrohungslage frühzeitig zu erkennen, Sicherheitslücken schnell zu schließen und regulatorischen Entwicklungen proaktiv zu begegnen, entscheidet zunehmend darüber, ob ein Unternehmen souverän handelt – oder abhängig bleibt. Die Fähigkeiten der Mitarbeiter und der Organisation und der Willen, digitale Souveränität umzusetzen und dafür jetzt zu investieren um in der Zukunft den Risiken selbstbestimmt entgegentreten zu können

Wie kann die Digitale Souveränität gelingen: Digitale Souveränität muss in spezifischen Rollen konkretisiert werden – im Einkauf, in der IT-Architektur, im CISO-Office wie auch im Produktmanagement. Wenn Unternehmen diese Fähigkeit aktiv gestalten, können sie ihren Kunden souveräne Produkte und Dienstleistungen anbieten und sich im digitalen Wettbewerb behaupten. -v-

Volker REICHERT

CHINESE SOCIAL CREDIT SYSTEM



Das Corporate Social Credit System (CSCS) ist ein staatliches Bewertungssystem in China, das das Verhalten von Unternehmen erfasst und bewertet. Es basiert auf einer Vielzahl von Daten – etwa zu Steuerzahlungen, Umweltauflagen, Produktsicherheit oder Vertragsverstößen – und soll sicherstellen, dass Unternehmen gesetzeskonform, ehrlich und zuverlässig agieren. Es wurde eingeführt, um Unternehmen, die sich an chinesische Gesetze halten, gezielt zu belohnen – und diejenigen, die gegen Vorschriften verstoßen, entsprechend zu sanktionieren. Die Einhaltung gesetzlicher Vorgaben wird dabei von den chinesischen Behörden anhand bestimmter Bewertungen und Listen überprüft. Je nachdem, wie ein Unternehmen eingestuft wird, können sich daraus entweder positive oder negative regulatorische Folgen ergeben.

Das CSCS integriert verschiedene Arten von Informationen aus mehreren Quellen. Zu den wichtigsten Informationsquellen zählen Entscheidungen chinesischer Behörden wie etwa der Marktaufsichtsbehörde (MSA), der Umweltbehörde (EPB), der Steuerbehörde oder dem Zoll. Darüber hinaus fließen auch gerichtliche Entscheidungen ein, allerdings nur in begrenztem Umfang. Eine weitere bedeutende Quelle sind Selbstberichtsinformationen, die Unternehmen gemäß den gesetzlichen Vorgaben an chinesische Behörden übermitteln. Schließlich werden auch Aufzeichnungen von sozialen Organisationen berücksichtigt, wie zum Beispiel von der China Real Estate Association oder der China Association of Warehousing and Distribution.

Eine beispielhafte Aufzählung von Verstößen und Einhaltungen, die zu dem jeweiligen Listing führen können, liefert folgende Abbildung:

Black-Listing

- Nichtzahlung oder verspätete Zahlung von Steuern und Sozialabgaben
- Umweltverschmutzung und Verstoß gegen Umweltauflagen
- Produktion und Verkauf von gefälschten oder unsicheren Produkten
- Verstoß gegen Arbeits- und Sozialschutzgesetze
- Vertragsbruch und schlechte Geschäftspraktiken
- Betrug und Falschangaben in Geschäftsdokumenten

Red-Listing

- Pünktliche und vollständige Zahlung von Steuern und Abgaben
- Einhaltung und sogar übertreffen von Umweltauflagen
- Hohe Produktsicherheit und Qualitätsstandards
- Zuverlässige und transparente Berichterstattung gegenüber Behörden
- Gute Arbeitsbedingungen und Einhaltung sozialer Standards
- Erfüllung von Vertragsverpflichtungen und fairer Umgang mit Geschäftspartnern
- Kooperation mit staatlichen Prüfungen und Kontrollen

Vgl. RMA Vortrag HEIDELBERG / CMS

Die Nachfolgende Abbildung gibt einen Überblick über mögliche Bestrafungen und Belohnungen, die aus den oben genannten Ursachen folgen können.

Black-Listing

- Risiko, Kunden zu verlieren, wenn gesetzliche Vorgaben, Vereinbarungen oder Unternehmensrichtlinien nicht eingehalten werden
- Strengere Anforderungen bei Genehmigungen (besonders, wenn Behörden einen großen Ermessensspielraum haben)
- Höhere Inspektionsraten
- Verbot der Teilnahme an öffentlichen Beschaffungsprojekten der Regierung
- Strengere Anforderungen beim Erwerb von Nutzungsrechten an Grundstücken vom Staat
- Verlust der „Roten Listen"-Einträge → Keine Verrechnung möglich

Red-Listing

- Beschleunigte Genehmigungsverfahren durch Behörden
- Niedrigere Inspektionsraten
- Einfacherer Zugang zu Krediten bei Banken
- Einfacherer Erwerb von Nutzungsrechten an Grundstücken vom Staat

Vgl. RMA Vortrag HEIDELBERG / CMS

Für ausländische Unternehmen, die in China aktiv sind oder mit chinesischen Partnern zusammenarbeiten, kann das CSCS ebenfalls große Auswirkungen entfalten. Neben der direkten Einhaltung chinesischer Gesetze sollten ausländische Unternehmen auch die Compliance ihrer Lieferanten, Kunden und Businesspartner im Blick behalten. Wenn beispielsweise ein chinesischer Zulieferer aufgrund schlechter CSCS-Bewertungen auf einer schwarzen Liste landet, könnte dies zu Lieferengpässen, Vertragsstrafen oder sogar zum Ausschluss von öffentlichen Ausschreibungen führen – was wiederum auch das ausländische Unternehmen beeinträchtigen dürfte. Zudem können negative Bewertungen von Partnerfirmen den Ruf und die Geschäftschancen ausländischer Firmen in China stark beeinträchtigen.

Herausforderungen können zudem durch die unterschiedlichen regionalen Anforderungen und die oft fehlende Transparenz des Systems entstehen, wodurch es schwierig wird, den Überblick über den Status von Partnern zu behalten. So kann sich auch der Umgang aufgrund der verschiedenen Bewertungsmatrizen („Ratings“) schwierig gestalten. Diese unterscheiden sich in den verschiedenen Bereichen wie Steuern, Umweltauflagen oder Produktsicherheit sowohl in der Form als auch in den Kriterien und Vorschriften. So könnte ein Unternehmen in einem Bereich, etwa der pünktlichen Steuerzahlung, sehr gut bewertet werden, während es in einem anderen Bereich, wie dem Umweltschutz, Probleme bekommt – was insgesamt den CSCS-Status beeinflusst. Diese unterschiedlichen Bewertungsmaßstäbe können von verschiedenen Behörden und auf regionaler Ebene durchaus unterschiedlich angewendet werden.

Ebenso stellt vor allem die Sprachbarriere (Webseite ist nur in chinesisch) und unterschiedliche rechtliche Standards eine große Herausforderung im Umgang mit dem CSCS dar. Viele der relevanten Informationen, Regularien und Behördenkommunikationen sind ausschließlich auf Chinesisch verfügbar, was die genaue Interpretation und Umsetzung der Anforderungen ohne entsprechende Sprachkenntnisse erschwert. Fachliche Nuancen könnten dabei oft verloren gehen, und ohne ausreichende Sprachkenntnisse könnte es schnell zu Missverständnissen kommen.

Diese Komplexität macht es für ausländische Unternehmen notwendig, nicht nur ihren eigenen CSCS-Status in den verschiedenen Bewertungsbereichen kontinuierlich selbst zu überprüfen, sondern auch die jeweiligen Businesspartner, Lieferanten und Kunden kontinuierlich im Blick zu behalten. Ohne dürfte daher ohne spezialisierte lokale Unterstützung schwierig werden und ein kontinuierliches Monitoring der einzelnen Ratings in den verschiedenen Bereichen sicherzustellen und den Überblick zu behalten. -V-

Thorsten JELINEK

5G-AI Integration is reshaping technology and digital sovereignty

AI is set to drive the next wave of productivity growth – but only if networks are ready

Fifth-generation networks, and the 6th generation currently under development and set for deployment around 2030, enable the uptake of advanced AI applications that require processing larger data volumes, higher data speeds, and real-time communication across diverse user experiences.

Such interactions demand the rapid transmission of data between device and network: consistently low latency (delay) and high uplink throughput. Standard 5G networks significantly reduce latency compared to 4G, typically achieving around 10ms and theoretically reaching as low as 1ms under optimal conditions (compared to 4G's 50-100ms). This latency improvement increases processing speed, including AI inference and data transmission, thereby enhancing responsiveness by 50–60%.

But current 5G architectures predominantly prioritize downlink (download) capacity, a legacy of earlier networks optimized for consumer activities like video streaming and gaming. Consequently, uplink bandwidth—essential for real-time, AI-driven use cases—often lags.

Therefore, fully realizing the consistently ultra-low latency and robust uplink capacity necessary for advanced AI applications will require further evolution of 5G networks into AI-centric infrastructures, integrating AI-driven management and operations directly into their architecture.

From infrastructure to value creation

Current networks won't be able to keep up. Some conventional 5G networks are already stretched by "network traffic waste," a term that refers to inefficient or unnecessary use of network resources caused by features such as auto play, infinite scroll, and prefetching of content – features incentivized by the business model of social media platforms. Vodafone's recent policy statement refer to this as a digital "tragedy of the commons."

While „Responsible use of Networks" is vital for addressing energy efficiency, the reality is that data traffic will continue to grow exponentially. This strain exposes a fundamental mismatch between traditional network architectures and emerging data-intensive AI applications. It makes a shift towards AI-centric network operations and management not just sensible, but indispensable if we are to manage rapidly growing data efficiently and enable highly flexible, real-time, high-bandwidth use cases. Such 5G-AI integration offers telecom operators a unique opportunity to accelerate 5G adoption by unlocking new use cases across various sectors.

However, this shift requires substantial investments in network infrastructure, in addition to already high investments in computing infrastructure and cloud services. As a result, while the AI-driven digital transformation offers tremendous productivity potential, it is also far more capital-intensive than the initial Internet revolution.

EU lags in network infrastructure buildout

As of 2024, the European Union had made substantial strides in expanding 5G coverage, which now reaches approximately 87% of the EU's population. However, it still lags behind the United States (98%) and South Korea (99%), both of which have achieved near-universal 5G availability. Despite the growing infrastructure, the actual 5G connection ratio in Europe remains relatively low at around 30%, compared to higher adoption rates in these leading markets.

Looking ahead, the EU is projected to reach 80% of mobile connections on 5G by 2030, indicating a slow but steady transition. This delay is largely attributed to the fragmented European telecom market, with varying regulatory environments and investment levels across member states. Moreover, many end-user applications are still adequately supported by 4G (e.g., video streaming, mobile gaming, and social media, as well as messaging and video calling, e-mail, web browsing, and cloud storage). All of this means that compelling consumer use cases for 5G have yet to materialize at scale.

Although Europe has achieved broad 5G coverage, its deployment of 5G Standalone (SA)—the architectural foundation needed to support AI-centric capabilities such as network slicing and ultra-low latency—remains minimal, with just 2% SA availability in Q4 2024, compared to 24% in the U.S., 52% in India, and 80% in China. This lag presents both a challenge and a strategic opening: by accelerating investment in 5G SA and embedding AI into network management and operations, telecom operators could shift from being a technology taker to a standard-setter in the AI-driven digital economy. This underscores the urgency of adopting an Infrastructure First approach. Rather than waiting for compelling applications to drive demand, the focus must shift to building AI-ready infrastructure proactively.

A paradigm shift to intelligent infrastructure

These capabilities signify a paradigm shift from static, hardware-centric networks to intelligent, software-driven infrastructure tailored for AI ecosystems. By adopting this transformation, telecom operators transcend their role as connectivity providers to become strategic enablers of AI innovation across industries.

Achieving this shift demands sustained investment in three pillars: a unified infrastructure layer that integrates edge-to-core networks to support low-latency AI data flows; an intelligent control layer that dynamically manages resources and resolves legacy 5G asymmetries, especially uplink limitations; and an autonomous operations layer that enables predictive optimization and real-time self-healing to ensure resilient, SLA-compliant performance for AI-driven applications. Through platforms like GSMA Open Gateway, operators can expose AI-optimized network capabilities—such as latency guarantees, bandwidth slicing, or reliability SLAs—to third parties, thereby generating new revenue streams (e.g., "network-as-a-service" models tailored to sector needs), establishing cross-sector ecosystems (e.g., partnerships with smart cities, manufacturers, healthcare providers), and driving policy innovation (e.g., developing secure, scalable access frameworks that balance open innovation with digital privacy and security regulations).

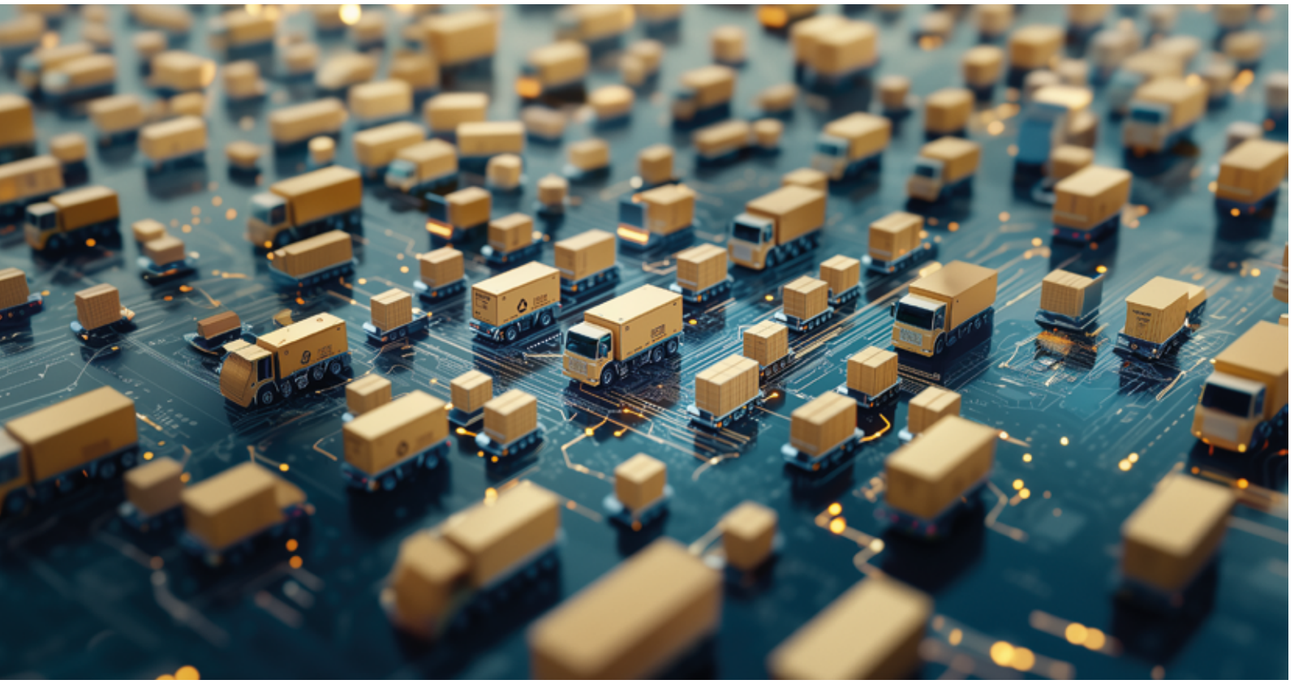
Unlocking this value, however, requires more than technical upgrades. It calls for systemic transformation. This evolution positions telecom networks as critical infrastructure for the AI economy, driving efficiency, safety, and economic growth while requiring collaboration between governments, industries, and regulators to standardize and scale. Yet despite this strategic evolution in the role of telecom networks, regional disparities in deployment and adoption remain significant.

A transformative leap

Looking ahead, 6G will mark a transformative leap by integrating AI directly into network architecture, evolving networks from connectivity platforms into intelligent

infrastructures capable of proactively managing themselves. Such "AI-native" design will enable networks to predict and autonomously adapt to demands, faults, and security threats, drastically enhancing efficiency and sustainability. Novel capabilities such as joint communication and sensing, semantic communication, and distributed AI will enable entirely new services, from hyper-accurate positioning to meaningful data exchange, while safeguarding privacy and minimizing energy consumption. This convergence means 6G will not just support digital economies—it will create them, necessitating forward-looking policies that balance innovation, regulation, and digital sovereignty.

For an economy to fully realize AI as a new driver of productivity, telecom operators must integrate AI into the operations and management of their 5G networks. This 5G-AI integration is critical—not only to deliver the connectivity and bandwidth needed for exponential data growth, but also to achieve the ultra-low latency required by advanced AI applications. -v-



DI Johannes GÖLLNER, *MSc*

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

Globalisierung, Digitalisierung und Automatisierung sind die Treiber für eine **holistischen Betrachtung der Verletzbarkeit der Supply Chain und seiner 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 Umweltereignissen, „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 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.

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 Lieferkettensorgfaltspflichten-gesetzes und 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. Zitat, S.55, link: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 und 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, link: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52023JC0020)

Im Wirtschaftsschutz 2024+, der sich als Ge¬meinschaftsleistung staatlicher und privatwirt-schaftlicher Akteure auf die Stärkung der Re¬silienz 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, die multiplen, sich wechselseitig verstärkenden 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 geprägt wird durch ein Größerwerden des Verantwortungsraums. Das Lieferkettensorgfaltspflichtengesetz fordert die Verantwortung für Risiken der gesamten Supply Chain. Das Spannungsfeld wird auch geprägt durch Wunsch und 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 (externe und interne) 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 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 Werkszeugen 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, um zur Strategie- und Produkt-Entwicklung positiv und wertschöpfend beitragen zu können.

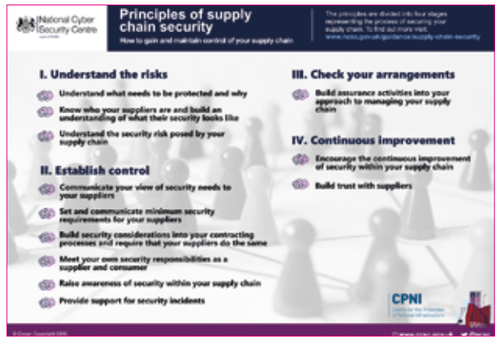
Das Erarbeiten eines umfassendes und ganzheitliches Cyber Security & Supply Chain Resilience (Security) Monitoring, -Rating und -Auditing Konzeptes, weil **Cyber Events** (weltweit: **34%**; AT: **40%**; GE: **40%**; CH: **57%**) und **Supply Chain Interruptions-Betriebsunterbrechungen** (weltweit: **34%**; AT: **32%**; GE: **46%**; CH: **41%**) zu den 10 weltweit größten Risiken gehören (siehe „Allianz Global Corporate & Specialty in Allianz Risk Barometer 2024 & 2023: Bsp.: Die 10 größten Geschäftsrisiken 2023, weltweit"), wird Unternehmen, KMU und auch öffentliche Verwaltung ab 2024 und in den Folgejahren massiv herausfordern.

Die internationale Standardisierung, vertreten durch ISO (International Organisation for Standardization, Genf), hat bereits **2007** mit der Herausgabe von Supply Chain Security-Standards (ISO 28000, ISO 28001, ISO 20858) 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 (siehe u.a. Bild).

Der supranationalen Gesetzgeber (EU) reagierte darauf mit der EU NIS2-Directive (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, Publications Office (europa.eu)), welche ab 18.10.2024 in Österreich und allen EU-Mitgliedschaften auch für spezifische KMU (wesentliche und wichtige Einrichtungen) gelten werden. 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 Anderen, daß zum Ersten Mal **Cyber Security mit Supply Chain Security, gemäß** Artikel 21 (Risikomanagementmaßnahmen im Bereich der Cybersicherheit und Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern) der NIS 2-Richtlinie verknüpft werden und welche bei der Auditierung nach ISO 27001 in Korrelation mit anderen Standards analysiert werden müssen..



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 auf einem mathematischen modell-basierten Cyber-Event und Bedrohungs-Monitoring sowie eines Risikoanalyse- und -bewertung-Modelles, 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 Strategische 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 nationalen zuständigen Aufsichtsbehörden zu begründen und um eine reduzierte Innovationsfreude -besonders bei KMU- oder Druck auf die digitale Transformation der KMU zu vermeiden.

Die Verfügbarkeit von qualitätsgesicherten modell-basierten Cyber-/Lieferketten Event und Bedrohungs-Monitoring-, Risikoanalyse- und Risikobewertungs-Werkzeugen sind fachlich nur eingeschränkt verfügbar.

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-Richlinie Vorgaben reduzieren zu können.

Die RMA-Risk Management und Rating Association e.V., München, Deutschland, entwickelt im Rahmen ihres Arbeitskreises: Supply Chain Risiko Management einen Leitfaden für Supply Chain (Resilience/Security) Management in Korrelation zur NIS 2-Richtlinie, welcher voraussichtlich im 3. Quartal/2025 veröffentlicht wird, und Unternehmen zur Verfügung stehen wird.

Initiierung einer Aus-, Fort- und Weiterbildung-Kampagne zur Bewältigung des existierenden facheinschlägigen IT/Cyber-Fachkräftemangels bei österreichischen Unternehmen sowie der Ausbildung aktuell in Österreich nicht in der entsprechenden Anzahl verfügbaren NIS 2-Zertifizierungsexperten, um die nach ISO 27001, etc. in großer Anzahl zu erwartenden zu auditierenden Unternehmen fachlich und zeitnah bedienen zu können.

Ein geeigneter Weg könnte hier 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.

Derzeit existiert noch kein verfügbares, inhaltlich qualitätsgesichertes Top-Management-Ausbildungskonzept für die die Zielgruppe: Top-Management (Geschäftsführer, Vorstände, Aufsichtsräte, Beiräte, etc.) im Sinne der Verantwortlichkeit des Top-Managements, gemäß NIS 2-Richtiinie.

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, link: https://a.storyblok.com/f/104752/x/bf5bd97da2/bme-leitfaden-logistikstudie-2024_final.pdf)

Das Zentrum für Risiko- und Krisenmanagement hat bereits im Dezember 2023 zum Thema: „NIS 2 – die neue Cybersecurity Richtlinie" der Europäischen Union ein ZRK-Positionspapier veröffentlicht. (siehe https://www.zfrk.org/bereich/publikationen/positionspapiere) -V-

DI Johannes GÖLLNER, *MSc* & Christian PAUL

STRATEGISCHE RESILIENZ

Resilienz, Organisatorische, Cyber, Supply Chain Resilienz haben sich in den letzten Jahren zu absoluten Schlagwörtern entwickelt. Zahlreiche Consultingfirmen 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 diese als Integriertes Management System (IMS) in Organisationen dienen.

Abbildung 1: RESILIENZ © Christian Paul, Johannes Göllner, Helmut Pisecky, Susanne Ludescher

Als Resilienz von Organisationen bezeichnet man die Fähigkeit einer Organisation, auf interne und externe Einschläge 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.

Seit COVID-19, der Energiekrise und dem Ukrainekrieg ist klar, dass Polykrisen kein fiktives Szenario, sondern die gelebte Realität sind - eine Realität, die Organisationen zwingt, resilient zu sein, um auf Einschläge durch Veränderungen der externen Rahmenbedingungen rasch und zielgerichtet reagieren zu können.

Außerdem stellt sich die Frage, ob es weitere relevante Faktoren gibt, die über die organisationale Resilienz als überlebenswichtiger und wettbewerbsentscheidender Faktor hinausgehen.

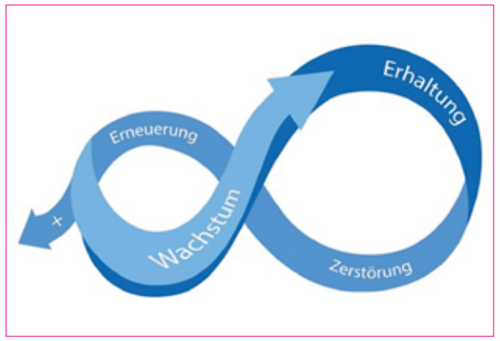


Abbildung 2: Phasen des Resilienzzyklus (Adaptive Zyklen nach Holling & Gunderson, 1986)

In den verschiedenen Phasen des Resilienz-Zyklus (Adaptive Zyklen nach Holling & Gunderson) hängt die erfolgreiche Umsetzung organisationaler Resilienz von der Ausprägung einzelner Fähigkeiten ab. Diese sind insbesondere die Agilität und Motivation der Mitarbeiter*innen und Führungskräfte sowie Antizipation, Flexibilität (kontinuierliche Lernfähigkeit), Adaptivität (Anpassungsfähigkeit) und Widerstandsfähigkeit. Die Resilienz der einzelnen Elemente des Systems und eine klare Strategie sind damit Grundvoraussetzungen für das Überleben der gesamten Organisation. Gerade einige Beispiele aus der Privatwirtschaft haben dies in den letzten Jahren gezeigt, z.B. Nokia, Siemens, Lufthansa und VW.

Angesichts der aktuellen geopolitischen Krisen wird aber auch die Frage nach der gesamtstaatlichen Resilienz immer dringlicher. Es darf bezweifelt werden, dass der Staat als allein zuständige Institution über die Ressourcen verfügt, um alle landesweiten oder grenzüberschreitenden Krisen meistern zu können.

Ein systemisches Denken in Bezug auf die Krisenbewältigung (Staat, Privat und Gesellschaft) erscheint daher zwingend notwendig, staatliche Resilienz- bzw. Krisenbewältigungsstrategien müssen privat rechtliche Körperschaften, wie Organisationen und Unternehmen, miteinschließen.

Dieser Ansatz geht über die organisationale Resilienz hinaus und eröffnet die Perspektive auf eine gesamtheitliche, strategische Resilienz. Hier gilt es, unter Berücksichtigung der Umfeldbedingungen und Potenziale neue Strategien zu entwickeln, die für alle Beteiligten einen konkreten Mehrwert bieten: Das System ist mehr als die Summe seiner Teile.

Alle verwendeten Begriffe finden sich auch in der gängigen Literatur zum Thema Strategisches Management (Malik, Drucker...) bzw. Integrierte Managementsysteme. Somit hat eine Kombination aus bestehenden Elementen und dem holistischen Ansatz des Resilienzmanagements das Potenzial, einen messbaren Mehrwert für Organisationen zu liefern, also sowohl Privat als auch Staat.

Insbesondere eine holistische Business Impact Analyse (BIA) bildet eine Grundlage für Entscheidungsprozesse, ergänzt durch passende Methoden des Risiko-, Security-, Safety-, Prozess-, Qualitätsmanagements sowie Strategieprozesse und -methoden (SWOT-Analyse, etc....). Das Ziel besteht darin, aus diesen einzelnen Elementen ein umfassendes Gesamtsystem der strategischen Resilienz zu formen.

Fazit und Ausblick

Aktuell ist der **Begriff „Strategische Resilienz" noch nicht definiert** und eröffnet daher die Möglichkeit, diesen zu prägen. Austrian Standards gibt die ÖNORM S 2412ff „Security Management Systeme" heraus, die auch in der ÖNORM 2414-3 das Resilienz Management definiert. Diese Norm wird voraussichtlich noch heuer (2025) evaluiert und zu einer Resilienz Management-Systeme-Norm umgebaut bzw. weiterentwickelt. Hierdurch und auch durch aktuelle Neuerungen (Krisensicherheitsgesetz, österreichischer Rechnungshofbericht zum Thema Blackout) ergibt sich ein Zeitfenster, um den Begriff zu definieren, zu besetzen, zu positionieren und zu disseminieren.

Die moderne Gesellschaft ist -unter anderem- stark von funktionierenden Infrastrukturen (Energie, Wasser, Informationstechnologie, Kommunikation, Transport, etc.) abhängig. **Die Stärkung der Resilienz einer modernen Gesellschaft ist unverzichtbar.**

Diesen Beitrag können Sie auch als Positionspapier von der ZRK-Homepage herunterladen (siehe https://www.zfrk.org/bereich/publikationen/positionspapiere).

Informationen:
Das KOMPETENZZENTRUM FÜR SICHERHEITSPOLITIK des Zentrums für Risiko- und Krisenmanagement wird 2025 als nächsten Schritt eine **Enquete zu „STRATEGISCHE RESILIENZ"** -mit Entscheidungsträgern und Vertretern aus den Bereichen Wirtschaft, Gesellschaft und Politik- organisieren und dazu einladen.

Ferner und derzeit initiiert das KOMPETENZZENTRUM FÜR SICHERHEITSPOLITIK des Zentrums für Risiko- und Krisenmanagement eine D-A-CH Arbeitsgruppe zur Herausgabe eines **„GRÜNBUCHES zu STRATEGISCHER RESILIENZ"**.

Darüber hinaus wird gerade ein **Kontaktstudium zum hochschulgeprüften „Resilienz Manager"** durch das Zentrum für Risiko- und Krisenmanagement- unter der Leitung von Christian Paul- entwickelt.

Wenn Sie an einer Mitwirkung und/oder Teilnahme an der Enquete zu „STRATEGISCHE RESILIENZ" Interesse haben, dann schreiben Sie uns bitte eine Email an: office@zfrk.org. -v-

Dr. Steffi RUDEL, *Prof. Dr.* Ulrike LECHNER, Judith STRUßENBERG *M.A.*

Gelebte IT-Sicherheit – Projekt CONTAIN verbindet Forschung und Praxis

Cyberangriffen effektiv begegnen

Ob Krankenhaus, Logistikdienstleister, Kunsthändler oder Handwerksbetrieb – Ransomware-Angriffe gehören inzwischen zum digitalen Alltag. Nur zu oft schieben insbesondere kleine und mittlere Unternehmen das Thema von sich weg – bis es dann zu spät ist. Daher steht für den deutsch-österreichischen Forschungsverbund CONTAIN die Frage „Was ist für eine gute Vorbereitung auf einen IT-Notfall zu tun?" im Mittelpunkt. Ziel des Projekts ist es, leicht umsetzbare Maßnahmen zu entwickeln, die die Widerstandsfähigkeit (Resilienz) von Organisationen gegenüber IT-Sicherheitsvorfällen stärken. Mit Methoden wie Serious Games, Referenzmodellen, Playbooks und einem umfassenden Reaktions-Framework arbeitet CONTAIN an einer praxisnahen Toolbox, die für Organisationen unter https://www.contain-projekt.de/toolbox/ öffentlich zugänglich ist.

Transnationale Sicherheit in Lieferketten

CONTAIN steht für „Effiziente Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten". Deshalb berücksichtigt CONTAIN bewusst unterschiedlichen Domänen von Logistik über Energie bis hin zu Zahlungsdienstleistungen. Um Ergebnisse zu erzielen, die in der Praxis anwendbar und gleichzeitig wissenschaftlich fundiert sind, forschen Universitäten, Unternehmen, Verbände und Behörden aus beiden Ländern gemeinsam an verschiedenen Aspekten des Themas.

„Das Ziel ist, dass Einzelpersonen und Unternehmen wissen, wie sie im Ernstfall handeln müssen – abgestimmt über die gesamte Lieferkette hinweg", erklärt Projektleiterin Prof. Dr. Ulrike Lechner von der Universität der Bundeswehr München. „Die Reaktionspläne müssen sitzen – im System und in den Köpfen."

Mit Spielen Kompetenzen stärken

Die Mitarbeitenden stellen einen wichtigen Baustein für die IT-Sicherheit der Organisation dar. Neben technischen und organisatorischen Maßnahmen ist daher die Weiterbildung der Mitarbeitenden ein ganz erheblicher Erfolgsfaktor. Hier passgenaue Maßnahmen zu entwickeln, die nicht nur bilden, sondern auch noch Spaß machen, ist ein Aspekt der deutsch-österreichischen Zusammenarbeit.

Unter anderem wurden folgende Serious Games im Projekt entwickelt:

Das Computerspiel CopyCat ist ein digitales Kartenspiel, das sich auf Verteidigungsmechanismen zum Schutz vor Angriffen auf die Software-Lieferkette konzentriert.
Ebenfalls online wird der DuckDebugger gespielt, ein Serious Game speziell für Softwareentwickler, das im Sicherheitsreview von Software schult.
Das Serious Game Hack dich nicht simuliert einen Ransomware-Angriff auf eine transnationale Lieferkette und fordert die Spieler heraus, logistische Abläufe trotz massiver Störungen aufrechtzuerhalten.
Operation Raven hilft IT-Security Profis, insbesondere mit dem Blick auf die technischen Herausforderungen den Ernstfall zu proben und Schwierigkeiten im eigenen Prozess zu erkennen.
Eine Frage der Sicherheit dagegen fokussiert sich auf den organisatorischen Umgang mit mobiler Ransomware und hilft, Kompetenzen für den Ernstfall aufzubauen. -v-

Mehr erfahren:

Auf Deutscher Seite wird das Projekt CONTAIN innerhalb des Programms Forschung für die zivile Sicherheit vom Bundesministerium für Bildung und Forschung (BMBF) gefördert (FKZ 13N16581-13N16587); auf Österreichischer Seite wird CONTAIN innerhalb des Sicherheitsforschungs- Förderprogramms KIRAS gefördert (FO999902707)

Aktuelle Neuigkeiten zu CONTAIN, Möglichkeiten zum Austausch und zu Terminen, auf denen Sie uns treffen, finden Sie in der öffentlichen Gruppe „CONTAIN - Research Project CONTAIN" auf LinkedIn: www.linkedin.com/groups/9549256 sowie auf den Webseiten www.contain-projekt.de und www.contain-projekt.at.

Philipp LADURNER

Von der digitalen Resilienz gemäß der DORA-VO (EU) 2022/2554 zur integrierten operationellen Resilienz im Banksektor

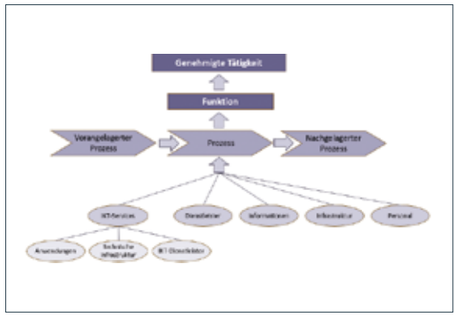
Ein aktueller Vorfall, der die Bedeutung robuster digitaler Resilienzstrategien eindrucksvoll verdeutlicht, ereignete sich am 27. Februar 2025, als das Zahlungssystem TARGET2 (T2) der Europäischen Zentralbank (EZB) von einer schwerwiegenden technischen Störung betroffen war. Diese führte zu erheblichen Verzögerungen bei Massenzahlungen wie Gehaltsüberweisungen, Rentenzahlungen und Sozialleistungen, wodurch die Abhängigkeit moderner Finanzsysteme von stabilen IT-Infrastrukturen deutlich wurde. Auch wenn die EZB betonte, dass es sich um ein technisches Problem und nicht um eine Cyberattacke handelte, zeigte der Zwischenfall, wie anfällig selbst kritische Finanzinfrastrukturen für technische Störungen sein können.

Dieser Vorfall unterstreicht die Notwendigkeit eines ganzheitlichen, integrierten Resilienzansatzes, der sowohl organisatorische als auch technologische Maßnahmen umfasst, um die Kontinuität kritischer Geschäftsprozesse selbst unter schwierigen Bedingungen sicherzustellen. Genau hier setzt die Digital Operational Resilience Act (DORA-VO) an, die gemeinsam mit den Principles for Operational Resilience (POR) des Basel Committee on Banking Supervision (BCBS) ein umfassendes regulatorisches Framework für den Bankensektor schafft.

Die digitale Transformation, der rasante Fortschritt in der Künstlichen Intelligenz (KI) und die zunehmende Abhängigkeit von Technologien stellen Finanzinstitute vor neue, komplexe Herausforderungen. Während die Chancen der Digitalisierung offensichtlich sind, wächst gleichzeitig die Anfälligkeit gegenüber Cyberbedrohungen, technischen Ausfällen und anderen unerwarteten Störungen, die die Kontinuität der Geschäftsprozesse gefährden können.

Angesichts dieser Risiken sind integrierte Managementsysteme zur effizienten Vorfallbewältigung – vom Incidentmanagement über Notfallmanagement bis hin zum Krisenmanagement – unerlässlich. Im Bankensektor bilden das Bankwesengesetz (BWG), das Zahlungsdienstegesetz (ZaDiG), die Kreditinstitute-Risikomanagementverordnung (KI-RMV) und diverse EBA-Guidelines den zentralen regulatorischen Rahmen. Eine wichtige Orientierung zur Umsetzung eines umfassenden operationellen Resilienzmanagements bieten die Principles for Operational Resilience (POR) des Basel Committee on Banking Supervision (BCBS) aus dem März 2021.

Ergänzend dazu trat am 16. Januar 2023 die Digital Operational Resilience Act (DORA-VO) in Kraft, die eine Übergangsfrist zur vollständigen Umsetzung der regulatorischen Anforderungen bis zum 17. Januar 2025 vorsieht. Diese Verordnung erweitert die regulatorischen Anforderungen an operationelle Resilienzsysteme um spezifische Anforderungen an die digitale operationelle Resilienz, mit einem besonderen Fokus auf IKT-Risikomanagement, IKT-Vorfallbewältigung, IKT-Drittdienstleistersteuerung und die Überprüfung der digitalen Resilienz durch regelmäßige Tests.



Integration der digitalen operationellen Resilienz in die operationelle Resilienz

Die DORA-VO ergänzt die POR, indem sie betont, dass Resilienz nicht nur organisatorisch, sondern auch technologisch verankert sein muss. Gemeinsam bilden sie ein umfassendes Framework, das die folgenden Kernbereiche abdeckt:

Governance und Verantwortung: Sowohl die DORA-VO als auch die POR fordern klare Verantwortlichkeiten auf Führungsebene und eine zentrale Steuerung der Resilienzstrategie. Diese muss in Übereinstimmung mit der Geschäftsstrategie entwickelt und mit Teilstrategien wie der Risikostrategie, IT-Strategie und Digitalisierungsstrategie abgestimmt sein.

Business Impact Analyse, Risikoanalyse und Bedrohungserkennung: Ein gemeinsames Ziel beider Regelwerke ist die Fähigkeit, Risiken frühzeitig zu erkennen und deren Auswirkungen präzise zu bewerten. Während die POR alle operationellen Risiken adressiert, konzentriert sich die DORA-VO auf IKT-Risiken und die Abhängigkeiten von IKT-Drittdienstleistern. Eine fundierte Business Impact Analyse (BIA) bildet dabei die Grundlage für die Kontinuitätsplanung im Business Continuity Management (BCM) und berücksichtigt kritische und wesentliche Funktionen und genehmigten Tätigkeiten (abgeleitet von den Konzessionen) des Finanzinstitutes, die Abhängigkeiten, Wechselwirkungen der Geschäfts- und Unterstützungsprozesse sowie die notwendigen Ressourcen.

Geschäftsfortführungsplanung, IKT-Geschäftsfortführungsplanung, Krisenmanagement: Im Fokus des BCM steht die Erstellung von Geschäftsfortführungsplänen für kritisch identifizierte Prozesse sowie risikoszenario-basierter Notfallpläne.

Ergänzend zu den allgemeinen regulatorischen Anforderungen für das BCM legt die DORA-VO sehr detailliert die Anforderungen an die IKT-Geschäftsfortführungsplanung fest. Hierbei müssen die Analysen aus dem BCM berücksichtigt werden, sodass die ermittelten Anforderungen bei den Wiederherstellungszielen der IKT-Assets eingehalten werden können. Der technische Regulierungsstandard (EU) 2024/1774 zur DORA-VO verlangt zusätzlich, dass IKT-Geschäftsfortführungspläne nach einem risikobasierten Ansatz erstellt und auch IKT-Reaktions- und Wiederherstellungspläne für relevante Risikoszenarien wie Cyberangriffe, Insiderbedrohungen, Stromausfälle, Personalausfall oder Naturkatastrophen entwickelt werden.

Für ein zielgerichtetes, effizientes Vorgehen empfiehlt es sich, die bestehenden Notfallpläne aus dem BCM zu prüfen und bei Bedarf um die IKT-Geschäfts-, Reaktions- und Wiederherstellungspläne zu ergänzen bzw. darauf zu verweisen. Als Ergebnisdokument der erstellten und gesammelten Pläne eignet sich ein um die IKT-Pläne erweitertes Notfallhandbuch oder auch ein separates IKT-Notfallhandbuch.

Ergänzend zu der im BCM vorbereiteten Notfall- und IKT-Notfallstruktur kann es auch sinnvoll sein, ein reaktives Krisenmanagementsystem im Unternehmen zu etablieren. Dies ermöglicht es, nicht identifizierte Risiken mit Auswirkungen auf den Geschäftsbetrieb, andere disruptive Ereignisse oder eskalierte Notfälle situativ und flexibel zu bewältigen. In der DORA-VO selbst wird zwar lediglich die Etablierung einer Krisenmanagementfunktion zur Aktivierung der Krisenkommunikation bei IKT-bezogenen Vorfällen gefordert, doch eine breitere, proaktive Ausrichtung kann die Resilienz erheblich stärken.

Incident Management und Krisenkommunikation: Die DORA-VO fordert detaillierte Maßnahmen zur Bewältigung IKT-bezogener Vorfälle und zur effektiven Krisenkommunikation. Unternehmen sollten bestehende Notfall- und Krisenkommunikationspläne evaluieren und bei Bedarf an die spezifischen Anforderungen der DORA-VO anpassen, um eine nahtlose Kommunikation im Krisenfall sicherzustellen.

Testing und kontinuierliche Verbesserung: Sowohl die POR als auch die DORA-VO verlangen regelmäßige Tests und Übungen, um die Resilienz kontinuierlich zu prüfen und zu verbessern. Diese Maßnahmen sollten eng mit der bestehenden BCM-Planung abgestimmt und durch spezifische IKT-Tests ergänzt werden. Zur Erzeugung weiterer Synergieeffekte kann auch die Testplanung aus dem Informationssicherheitsmanagementsystem (ISMS) integriert werden, um die Effektivität der technischen und organisatorischen Schutzmaßnahmen ganzheitlich zu prüfen.

Externe Abhängigkeiten und Drittparteimanagement: Die Einbindung externer Dienstleister und IKT-Dienstleister, insbesondere solcher, die kritische oder wesentliche Funktionen unterstützen, stellt einen kritischen Faktor für die Gesamtresilienz dar. Sowohl DORA als auch die POR fordern die Integration dieser Dienstleister und IKT-Drittanbieter, die kritische oder wesentliche Funktionen unterstützen, in die Notfall- und IKT-Notfallplanung sowie in die regelmäßigen Tests, um

eine konsistente und belastbare Resilienzstrategie zu gewährleisten. Hierbei ist sicherzustellen, dass die Anforderungen an Ausfallsicherheit und Wiederherstellungsfähigkeit auch bei diesen externen Partnern erfüllt werden.

Fazit: Die Anforderungen der DORA-VO erweitern die klassische operationelle Resilienz um eine dringend notwendige digitale Dimension. Für Finanzinstitute bedeutet dies, dass ein ganzheitlicher, integrierter Resilienzansatz notwendig ist, um den wachsenden technologischen Herausforderungen gerecht zu werden und gleichzeitig regulatorische Anforderungen effizient zu erfüllen. Nur durch die enge Verzahnung organisatorischer und technologischer Resilienz können Unternehmen die kontinuierliche Betriebsfähigkeit auch in kritischen Situationen sicherstellen.

Angesichts der ständig steigenden regulatorischen Anforderungen kann es sich für Finanzinstitute lohnen, sich an etablierten Normen wie der ISO 22316 (Organizational Resilience), ISO 22361 (Crisis Management), den BSI-Standards für Notfall- und Krisenmanagement sowie der österreichischen ÖNORME S 2414-3 (Resilienzmanagement) zu orientieren. Diese Normen bieten praxisnahe Leitlinien und Best Practices für die Entwicklung eines robusten und umfassenden Resilienzmanagements, das über die regulatorischen Mindestanforderungen hinausgeht. -v-

Zentrum für Risiko- & Krisenmanagement

Mag. Manfred OSCHOUNIG

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.

Wissen, das wirkt: Studien, Projekte, Forschung

Das Zentrum für Risiko- und Krisenmanagement (ZRK) steht für wissenschaftlich fundierte Forschung mit direkter Praxisrelevanz. In enger Zusammenarbeit mit Hochschulen, Unternehmen, Ministerien, Städten, Gemeinden und NPO werden wissenschaftliche Grundlagen erarbeitet und in anwendbare Lösungen übersetzt. Ein Schwerpunkt liegt auf der innovativen Weiterentwicklung von Notfall- und Krisenprozessen – insbesondere durch die Analyse realer Ereignisse, den Aufbau belastbarer Führungskulturen und -strukturen und die Standardisierung von Abläufen.

Zu den abgeschlossenen Projekten zählt ASGARD (Analysis System for Gathered Raw Data), das im Rahmen des EU-Forschungsprogramms Horizon 2020 entwickelt wurde. Ziel war es, Strafverfolgungsbehörden und EUROPOL durch die Entwicklung eines offenen, modularen Analysewerkzeugs für große Datenmengen zu unterstützen. Dabei lag der Fokus auf der Verarbeitung beschlagnahmter Daten, der Anwendung von Big-Data-Technologien und der Entwicklung von Visual-Analytics-Tools, um die technologische Autonomie der Behörden zu stärken. Um die Verbreitung, Weiterentwicklung und den Betrieb dieses Tools sicherzustellen, wurde im Jahr 2020 die EUROPEAN ANTI-CYBERCRIME TECHNOLOGY DEVELOPMENT ASSOCIATION (EACTDA) durch ehemalige ASGARD-Projektpartner gegründet. ZRK ist ein Gründungsmitglied der EACTDA.

Das deutsch-österreichische Forschungsprojekt NutriSafe beschäftigte sich mit der Resilienz von Lebensmittelversorgungsketten. Im Fokus stand die Anwendung von Distributed-Ledger-Technologien (DLT), insbesondere Blockchain, um die Rückverfolgbarkeit und Sicherheit in der Lebensmittelproduktion und -logistik zu erhöhen. Durch die Entwicklung eines modularen Toolkits wurden Technologien, Datenmodelle und Geschäftsprozesse bereitgestellt, die primär kleinen und mittleren Unternehmen helfen sollen, ihre Versorgungsketten gegen Störungen und Cyberangriffe abzusichern.

Ein weiteres bedeutendes Projekt ist SHELTER (Sustainable Historic Environments hoListic reconstruction through Technological Enhancement and community-based Resilience). Dieses EU-finanzierte Projekt zielte darauf ab, die Resilienz historischer Stadtgebiete gegenüber den Auswirkungen des Klimawandels zu verbessern. Durch die Entwicklung eines datenbasierten und gemeinschaftsorientierten Wissensrahmens wurden Werkzeuge und Strategien entwickelt, um den Schutz und die nachhaltige Wiederherstellung des kulturellen Erbes zu fördern.

Diese Projekte verdeutlichen das Engagement des ZRK, Forschungsergebnisse nicht nur theoretisch zu erarbeiten, sondern sie in praktischen Anwendungen umzusetzen. Die gewonnenen Erkenntnisse fließen in Weiterbildungen, Veranstaltungen und standardisierte Zertifizierungsverfahren ein, um die Resilienz und Sicherheit in verschiedenen Sektoren nachhaltig zu stärken.

Weitere Informationen zu aktuellen Projekten, Kooperationen und Forschungsclustern finden Sie unter: www.zfrk.org

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, Circular Economy, Wirtschaftsmediation, Gesundheitswesen und Sicherheitspolitik. Hier wird Wissen nicht nur vermittelt, sondern konkret angewendet – etwa in der Standardisierung und Entwicklung von sektorübergreifender Leitlinien oder der systemischen Krisenvorbereitung für Institutionen.

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
- Praxisnaher 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-

Ralph A. HUBER

Ist der Leitfaden für Compliance-Management-Systeme in kleinen und mittleren Unternehmen ein Lichtblick?

Disclaimer: Deser Artikel wurde mit Hilfe einer KI verfasst.

Die Kelten haben Ihr Regelwerk vor tausenden von Jahren in 8 Worte gefasst: „Verehre die Natur! Thue nichts Böses! Beweise Muth!" (Buch „Die Houbirg oder Geschichte der Nürnberger Schweiz, Johann Wolfgang Woerlein, 1838, Seite 27)

Warum gelingt uns das heute nicht mehr? Die Zehn Gebote, wie sie in der Bibel (2. Mose 20, 2-17) stehen, haben ca. 80 Wörter. Die EU-Richtlinie NIS2 (Richtlinie (EU) 2022/2555) hat ca. 30.000 Wörter! Was bringen uns Regeln, die nicht mehr klar, leicht zu verstehen, eindeutig und ohne Einschränkung anzuwenden sind?

EU-Richtlinien gelten branchen-, umsatz- oder mitarbeiterbezogen, sind also nicht durchgängig anwendbar. Die nicht betroffenen Unternehmen z.B. bei der Corporate Sustainability (CSRD (Richtlinie (EU) 2022/2464) und CSDDD (Richtlinie (EU) 2024/1760)), werden über die Kundenanforderungen der betroffenen Unternehmen einbezogen! Das heißt, dass trotz aller Limits die gesetzt werden, am Ende doch alle eingebunden sind. Und das erfolgt dann mit eigenen, abgeleiteten und angereicherten Regelwerken, dem sog. Code of Conduct für Geschäftspartner. Es gibt zwar ein gesetzliches Regelwerk, aber so macht jeder Kunde sein eigenes Regelwerk daraus und erhöht den Aufwand in der Lieferkette und die Komplexität. Das ginge wirklich einfacher! Ein Mindest-Standard für alle! Und dann kann die EU ja in einigen Jahre die Mindest-Anforderungen langsam erweitern. So wie es jetzt läuft, bekommen auch die kleinen und mittleren Unternehmen über die Kundenanforderungen die gesetzlichen Vorgaben aufgestülpt.

Die Veröffentlichung der DIN SPEC 91524 **„Leitfaden für Compliance-Management-Systeme in kleinen und mittleren Unternehmen"** (https://www.dinmedia.de/de/technische-regel/din-spec-91524/390496185) im Mai 2025 als kostenloses PDF zum Download stellt hier einen einfachen umzusetzenden Mindestansatz nicht nur für kleine und mittlere Unternehmen dar.

Kleine und mittelständische Unternehmen (KMUs) stehen vor der Herausforderung, Compliance-Management-Systeme (CMS) zu implementieren, die ihren begrenzten Ressourcen und spezifischen Bedürfnissen gerecht werden. Der Leitfaden DIN SPEC 91524:2025-05, bietet eine praxisorientierte Anleitung für KMUs, um ein effektives CMS aufzubauen. Dieser Artikel fasst die zentralen Inhalte des Leitfadens zusammen, beleuchtet die Bedeutung von Compliance für KMUs und stellt die wichtigsten Handlungsempfehlungen vor.

Der Leitfaden richtet sich an KMUs, die oft inhabergeführt sind, durch eine familiäre Geschäftsführung vertreten werden oder der Eigenkapitalhaftung unterliegen. Diese Unternehmen verfügen häufig über begrenzte Ressourcen – sowohl zeitlich als auch finanziell – und haben oft nur eingeschränktes Compliance-Wissen. Ziel des Dokuments ist es, KMUs dabei zu unterstützen, ein CMS zu implementieren, das ihre spezifischen Bedürfnisse berücksichtigt und gleichzeitig die Einhaltung gesetzlicher und freiwilliger Verpflichtungen sicherstellt.

Der Leitfaden wurde nach dem PAS-Verfahren (Publicly Available Specification) erstellt und ist kein Teil des Deutschen Normenwerks. Er entstand unter Mitwirkung von Experten wie DIKOIN GmbH, dem Expertenrat Mittelstands-Compliance e.V. und PARK Compliance Services GmbH. Er ergänzt bestehende Normen wie DIN ISO 37301 (Compliance-Managementsysteme), DIN ISO 37001 (Korruptionsbekämpfung) und DIN ISO 37002 (Hinweismanagementsysteme), die jedoch primär auf größere Unternehmen ausgerichtet sind.

Das Dokument definiert zentrale Begriffe, die für das Verständnis eines CMS in KMUs essenziell sind:

Compliance: Die Erfüllung aller gesetzlichen, regulatorischen und freiwillig eingegangenen Verpflichtungen einer Organisation.
Compliance-Risiko: Die Wahrscheinlichkeit und die Folgen von Verstößen gegen diese Verpflichtungen.
KMU: Unternehmen mit bis zu 250 Mitarbeitenden, einem Jahresumsatz von maximal 50 Millionen Euro oder einer Bilanzsumme von maximal 43 Millionen Euro, bei denen Eigentum und Leitung eng verknüpft sind.
Compliance-Managementsystem (CMS): Ein System von Prozessen, Richtlinien und Maßnahmen, das regelkonformes Verhalten fördert und Haftungsrisiken minimiert.

Diese Definitionen bilden die Grundlage für die weitere Struktur des Leitfadens, der sich auf die Identifikation und Steuerung von Compliance-Risiken konzentriert.

Der Leitfaden gliedert sich in mehrere Abschnitte, die KMUs durch den Prozess der Implementierung eines CMS führen:

Anwendungsbereich: Das Dokument dient als Leitfaden für KMUs, um den aktuellen Stand ihres CMS zu bewerten, Risikobereiche zu identifizieren und Handlungsempfehlungen umzusetzen.
Normative Verweisungen: Es verweist auf relevante Normen wie DIN ISO 37301 und andere, die als Orientierung für die Entwicklung eines CMS dienen.
Selbst-Check: Ein zentrales Element des Leitfadens ist der Selbst-Check, der Unternehmen hilft, ihren Ist-Zustand zu analysieren und Schwachstellen zu erkennen.
Prozessanalyse: Der Leitfaden beschreibt die Identifikation und Bewertung von Geschäftsprozessen, die für die Compliance relevant sind.
Handlungsempfehlungen: Konkrete Maßnahmen zur Risikominimierung und zur Förderung eines regelkonformen Verhaltens.

Der Selbst-Check ist ein praktisches Instrument, das KMUs dabei unterstützt, ihren Compliance-Status zu bewerten. Die zentralen Ziele des Selbst-Checks sind:

Sensibilisierung: Unternehmensverantwortliche und Mitarbeitende sollen für Compliance-Risiken sensibilisiert werden.
Ist-Zustand-Erhebung: Bestehende Compliance-Strukturen und -Maßnahmen werden identifiziert.
Risikoidentifikation: Die größten Compliance-Risiken in verschiedenen Unternehmensbereichen werden ermittelt.
Handlungsempfehlungen: Konkrete Maßnahmen zur Verbesserung des CMS werden vorgeschlagen.

Ein zentraler Aspekt des Leitfadens ist die Analyse von Geschäftsprozessen, die in drei Kategorien unterteilt werden:

Steuerungsprozesse: Diese umfassen Planung, Organisation, Personaleinsatz, Führung und Kontrolle sowie Themen wie Risikomanagement und Compliance.
Wertschöpfungsprozesse: Dazu gehören Kernprozesse wie Produktion, Einkauf, Vertrieb und Logistik, die direkt zur Wertschöpfung beitragen.
Unterstützungsprozesse: Diese Prozesse, wie Personal- oder IT-Prozesse, unterstützen die Kernprozesse und sind für die Betriebsbereitschaft essenziell.

Der Leitfaden bietet eine detaillierte Analyse dieser Prozesse und identifiziert spezifische Compliance-Risiken, die in den folgenden Abschnitten näher beleuchtet werden.

Vertriebsprozesse

Vertriebsprozesse sind besonders risikobehaftet, da sie oft Zielkonflikte zwischen Umsatzsteigerung und gesetzlicher Einhaltung aufweisen. Typische Risiken umfassen:

Kartellverstöße: Illegale Absprachen mit Wettbewerbern, z.B. über Preise oder Kundenaufteilung.
Korruption: Das Anbieten oder Gewähren von Vorteilen an Kundenmitarbeitende.

Handlungsempfehlungen:
Regelmäßige Schulungen zum Kartellrecht und zur Korruptionsbekämpfung
Entwicklung von Richtlinien zu Kartellrecht und Antikorruption
Einführung eines Hinweisgebersystems
Funktionstrennung und Vier-Augen-Prinzip

Wertschöpfungsprozesse

In Produktions- und Dienstleistungsprozessen stehen Arbeitsschutz, Arbeitssicherheit und Umweltvorschriften im Fokus. Risiken umfassen:

Arbeitsschutzverstöße: Besonders in produzierenden Gewerben bestehen Risiken für Unfälle durch mangelnde Sicherheitsmaßnahmen.
Umweltverstöße: Verstöße gegen Umweltauflagen, z.B. durch unsachgemäße Entsorgung oder Anlagenbetrieb.

Handlungsempfehlungen:
Schulungen zu Arbeitsschutz und Umweltschutz
Erarbeitung von Richtlinien zu Arbeitssicherheit und Umweltschutz
Regelmäßige Kontrollen und Festlegung klarer Zuständigkeiten

Personalprozesse

Personalprozesse bergen Risiken in Bereichen wie Datenschutz, Arbeitsrecht und Diskriminierung. Typische Risiken sind:

Datenschutzverstöße: Unsachgemäßer Umgang mit personenbezogenen Daten, z.B. durch unzureichende IT-Sicherheit.
Arbeitsrechtsverstöße: Nichteinhaltung von Arbeitszeiten, Mindestlohn oder Betriebsratsrechten.

Handlungsempfehlungen:
Datenschutzschulungen und Erarbeitung von Datenschutzrichtlinien
Implementierung technischer und organisatorischer Maßnahmen (TOMs)
Einführung eines Hinweisgebersystems

IT-Prozesse

IT-Prozesse sind bereichsübergreifend und bergen Risiken in den Bereichen Datenschutz und IT-Sicherheit. Risiken umfassen:

Unbefugte Zugriffe: Mangelhafte Schutzmaßnahmen gegen interne oder externe Angriffe.
Offenlegung von Geschäftsgeheimnissen: Unsachgemäßer Umgang mit sensiblen Daten.

Handlungsempfehlungen:
Entwicklung eines IT-Sicherheitskonzepts
Regelmäßige IT-Sicherheitsschulungen und Kontrollen
Schutzmaßnahmen für Geschäftsgeheimnisse

Logistikprozesse

Logistikprozesse sind anfällig für Vermögensdelikte und Arbeitsschutzverstöße. Risiken umfassen:

Vermögensstraftaten: Diebstahl oder Unterschlagung im Logistikprozess.
Arbeitsschutzverstöße: Verstöße gegen Sicherheitsvorschriften bei Transport oder Lagerung.

Handlungsempfehlungen:
Implementierung von Schutzmaßnahmen und regelmäßige Kontrollen
Schulungen zu Arbeitsschutz und Einrichtung eines Hinweisgebersystems

Finanzprozesse

Finanzprozesse sind besonders anfällig für Steuerstraftaten und Vermögensdelikte. Risiken umfassen:

Steuerstraftaten: Missachtung steuerlicher Vorgaben, z.B. durch fehlende Dokumentation.
Vermögensdelikte: Unterschlagung oder Betrug durch mangelnde Kontrollen.

Handlungsempfehlungen:
Regelmäßige Tax-Compliance-Schulungen
Erarbeitung von Richtlinien und Festlegung von Zuständigkeiten
Implementierung von Budgetkontrollen und Schutzmaßnahmen

Rechtliche Rahmenbedingungen

Der Leitfaden verweist auf zahlreiche gesetzliche Regelungen, die für KMUs relevant sind, darunter:

Arbeitsschutzgesetz (ArbSchG): Regelt Maßnahmen zur Verbesserung der Sicherheit und Gesundheit der Beschäftigten.
Datenschutz-Grundverordnung (DSGVO): Stellt Anforderungen an den Umgang mit personenbezogenen Daten.
Lieferkettensorgfaltspflichtengesetz (LkSG): Verpflichtet Unternehmen zur Einhaltung von Menschenrechtsstandards in der Lieferkette.
Geldwäschegesetz (GWG): Regelt Maßnahmen zur Verhinderung von Geldwäsche.

Diese Regelungen bilden die Grundlage für die Identifikation von Compliance-Verpflichtungen und die Entwicklung entsprechender Maßnahmen.

Die kostenlose, von der Technischen Universität Dortmund entwickelten und von der Funk Stiftung geförderten, APP „MyRiskGov" soll als nächstes um die Compliance-Selbstauskunft des Leitfadens erweitert werden. In den letzten 10 Jahren würden ca. 160 Projekte gefördert, davon gingen die Fördergelder zum überwiegenden Teil an die Risikomanagementprojekte. Es lohnt sich also sich mal die jeweils kostenlosen Risikomanagementprojekte und -tools auf der Website (www.funk-stiftung.org) anzusehen.

Hilfreich ist es auch, als nächsten Schritt, die 33 Compliancefelder des Deutschen Institut für Compliance e.V. (DICO e.V.), in den sieben Gruppen: Criminal-, Competition-, Production- IP/IT-, HR-, Financial- und Sustainability Compliance in einer Risikoanalyse (Eintrittswahrscheinlichkeit, Schadenshöhe, Reputation und Haftung) zu bewerten und auf das eigenen Unternehmen anzupassen. Für eine detaillierte Anwendung ist der DICO Risikokatalog 3.0 auf der Homepage (www.dico-ev.de) für Mitglieder kostenfrei und für Nicht-Mitglieder gegen Gebühr verfügbar.

Zu den Complaincefeldern gibt es jeweils eine Erläuterung/Beschreibung, Compliance-Risiko-Bereiche mit beispielhaften Ausprägungen, den typischen Auswirkungen bei Compliance-Verstößen und eine Auswahl der wesentlichen Gesetze. Dies ist beim Aufbau eines Compliance Management Systems eine hervorragende Basis.

Das Institut der Wirtschaftsprüfer (www.idw.de) hat mit dem Prüfungsstandard 980 (09.2022) die Prüfung von Compliance Management Systemen mit sieben Elementen eines Compliance-Management-Systems: Compliance-Kultur, Compliance-Ziele, Compliance-Risiken, Compliance-Programm, Compliance-Organisation, Compliance-Kommunikation und Compliance-Überwachung und -Verbesserung, vorgegeben. Jedes Element umfasst spezifische Unterelemente, wie z. B. „Tone at the Top" und Mitarbeiterakzeptanz (Kultur), Identifikation relevanter Rechtsgebiete (Ziele), Risikoanalyse (Risiken), Richtlinien und Schulungen (Programm), Ernennung eines Compliance-Beauftragten (Organisation), Hinweisgebersystem (Kommunikation) sowie regelmäßige Audits und Feedback-Schleifen (Überwachung). Dies wäre dann die Möglichkeit zum Nachweis eines angemessenen und wirksamen Compliance Management Systems.

Wenn mir mit diesem Artikel zwei Punkte gelungen sind, bin ich mehr als zufrieden.

Zum Einen wollte ich Sie auf einen interessanten Mindestansatz für Compliance Management Systeme mit der Möglichkeit der Selbstauskunft aufmerksam machen und zum Anderen auf die immer weiter ausufernden Regelwerke der EU. Es sollten nicht immer nur neue Regelwerke dazukommen, sondern ein nicht unerheblicher Teil der Gremien sollte sich auch mit der Vereinfachung und dem Weglassen von Regelwerken beschäftigen. Wie dies auch schon Prof. Dr. Fredmund Malik in seinem Buch „Führen Leisten Leben" mit der „systematischen Müllabfuhr im Unternehmen" als Werkzeug wirksamer Führung vorgibt. -v-

Tit.-Univ.-Prof. Dr.habil. DDr. Thomas BENESCH

Quantitatives und qualitatives strategisches und operatives Risikomanagement in Unternehmen in Relation zu NIS-2

Die NIS-2-Richtlinie (Network and Information Security Directive 2), die am 16. Januar 2023 in Kraft trat, verschärft die Cybersicherheitsanforderungen für Unternehmen in kritischen Sektoren, um Schwächen der Vorgängerrichtlinie NIS1 – wie unklare Definitionen kritischer Infrastrukturen – zu beheben (Schmitz-Berndt & Chiara, 2022). Sie erweitert den Geltungsbereich und klassifiziert Unternehmen nach ihrer Größe als „wichtige" oder „wesentliche" Einrichtungen, wodurch die Cybersicherheitsvorgaben in der EU harmonisiert werden (Noack, 2023; Vogel & Ziegler, 2023).

Um den Anforderungen gerecht zu werden, müssen Unternehmen sowohl quantitative als auch qualitative Methoden des Risikomanagements einsetzen. Diese sind strategisch (z. B. langfristige Sicherheitsziele, Ressourcenplanung) und operativ (z. B. Incident-Response, kontinuierliche Überwachung) umzusetzen. Zudem etabliert die Richtlinie detaillierte Maßnahmen für ein umfassendes Risikomanagement, um die Resilienz kritischer Infrastrukturen zu stärken.

Beim quantitativen Risikomanagement werden mathematische Modelle und statistische Methoden eingesetzt, um Risiken zu bewerten. Dazu gehören die Berechnung der finanziellen Auswirkungen von Cyberangriffen, die Modellierung von Ausfallwahrscheinlichkeiten mithilfe von Simulationen sowie die Bewertung von Sicherheitsinvestitionen durch Kosten-Nutzen-Analysen.

Im Zusammenhang mit der NIS-2 Richtlinie ist das quantitative Risikomanagement wichtig, weil Unternehmen verpflichtet sind, Sicherheitsvorfälle mit konkreten Zahlen zu melden. Außerdem müssen Unternehmen nachweisen können, dass sie ausreichend in Sicherheitsmaßnahmen investieren.

Das qualitative Risikomanagement stützt sich auf Expert*innenwissen und scenario-basierte Analysen. Typische Anwendungsbereiche sind die Erstellung von Risikomatrizen, die Bewertung der Sicherheitskultur im Unternehmen sowie die Identifikation kritischer Geschäftsprozesse gemäß NIS-2-Vorgaben.

Für die NIS-2-Compliance ist das qualitative Risikomanagement unverzichtbar, weil es hilft, Sicherheitsrichtlinien zu dokumentieren und Mitarbeiter*innen durch Schulungen für Cybersicherheit zu sensibilisieren.

Das strategische Risikomanagement legt den Grundstein für eine nachhaltige Cybersicherheitsstrategie. Zu den Maßnahmen gehören die Integration der NIS-2-Anforderungen in die Unternehmensstrategie, die Definition klarer Sicherheitsrichtlinien sowie Investitionen in moderne Sicherheitstechnologien wie KI-basierte Bedrohungserkennung. Im Kontext der NIS-2-Richtlinie müssen Unternehmen nachweisen, dass sie über ein ganzheitliches Sicherheitskonzept verfügen. So können sie langfristig resilient gegen Cyberbedrohungen bleiben.

Das operative Risikomanagement kümmert sich um die praktische Umsetzung der Sicherheitsstrategie. Dazu gehören regelmäßige Sicherheitsaudits, die Überwachung der IT-Systeme in Echtzeit sowie schnelle Reaktionsprozesse bei Sicherheitsvorfällen. Die NIS-2-Richtlinie verlangt von Unternehmen, dass sie Sicherheitsvorfälle innerhalb von 24 Stunden melden. Zudem müssen sie ihre Sicherheitsprozesse kontinuierlich verbessern.

Um die Anforderungen der NIS-2-Richtlinie zu erfüllen, sollten Unternehmen die folgenden Schritte befolgen:
müssen sie Risiken identifizieren und bewerten. Dabei sollten sie sowohl quantitative Methoden wie finanzielle Risikomodelle als auch qualitative Methoden wie Experteninterviews einsetzen.
müssen sie die regulatorischen Anforderungen erfüllen. Dazu gehört die Dokumentation aller Sicherheitsmaßnahmen sowie die regelmäßige Berichterstattung an die Aufsichtsbehörden.
sollten sie ein Krisenmanagement etablieren. Dazu gehören ein Incident-Response-Plan und regelmäßige Notfallübungen.
müssen sie technische und organisatorische Maßnahmen umsetzen. Beispiele sind die Einführung von Zero-Trust-Architekturen und Schulungen zur Erhöhung der Sicherheitsawareness.

Die NIS-2-Richtlinie erfordert ein ganzheitliches Risikomanagement, das quantitative und qualitative Methoden kombiniert. Unternehmen, die diese Ansätze auf strategischer und operativer Ebene umsetzen, sind nicht nur regulatorisch abgesichert, sondern auch besser gegen Cyberbedrohungen gewappnet. Um dies zu erreichen, sollten Unternehmen regelmäßige Risiko-Assessments durchführen, Sicherheitsbudgets datenbasiert planen, ihre Mitarbeiter*innen sensibilisieren und ihre Sicherheitsstrategie kontinuierlich anpassen. Durch eine proaktive Herangehensweise können Unternehmen Cyberrisiken minimieren und gleichzeitig die Anforderungen der NIS-2-Richtlinie effizient erfüllen. -v-

Literaturverzeichnis

Noack, A. (2023). Mehr Cybersicherheit in einer vernetzten Welt. ENTSORGA-Magazin, 42(4), 28-30.
Schmitz-Berndt, S., & Chiara, P. G. (2022). One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. International Cybersecurity Law Review, 3(2), 289-311.
Vogel, V., & Ziegler, N. (2023). Kritikalität: Von der BSI-KritisV zur NIS2-Richtlinie. International Cybersecurity Law Review, 4(1), 1-19.

Robert-P. PELIKAN

Cybersicherheit 2025: Resilient. Intelligent. Vernetzt.

Warum Resilienz, KI und Lieferketten zentrale Herausforderungen für Führungskräfte sind

Cybersicherheit ist 2025 mehr denn je eine Führungsaufgabe. Resilienz, künstliche Intelligenz und vernetzte Lieferketten erfordern neue Denkweisen. Der Beitrag zeigt, warum Organisationen strategisch umdenken müssen – und was Entscheider konkret tun können.

Die neue Cyberrealität – eine Frage der Führung

Die digitale Welt von 2025 ist ein hochgradig vernetztes Ökosystem. Datenströme, Plattformen, Partnernetzwerke und automatisierte Prozesse durchdringen nahezu alle Lebens- und Wirtschaftsbereiche. Diese Entwicklung bringt Chancen – aber auch Risiken. Cyberbedrohungen sind heute nicht mehr isolierte technische Probleme, sondern systemische Herausforderungen, die Organisationen in ihrer Gesamtheit betreffen.

Gleichzeitig steigt der Druck auf Führungskräfte: Kunden, Märkte, Aufsichtsbehörden und Partner erwarten, dass Unternehmen nicht nur über Cybersicherheit sprechen, sondern auch belastbare Strukturen schaffen – mit klaren Verantwortlichkeiten und messbarer Wirksamkeit.

Veranstaltungen wie die IKT-Sicherheitskonferenz, das Cybersecurity Forum Europe, die Munich Cyber Security Conference oder auch branchenspezifische Fachkongresse spiegeln diese Realität wider: Cybersecurity wird nicht mehr in den Technik-Workshops am Rande diskutiert – sie ist zur Chefinnensache geworden.

Resilienz: Mehr als ein Buzzword

Resilienz ist kein neues Konzept, aber es gewinnt in der digitalen Sicherheitslandschaft neue Bedeutung. Während sich viele Unternehmen auf die Vermeidung von Angriffen konzentrieren, zeigt die Realität, dass kein Schutz hundertprozentig wirkt. Die entscheidende Frage ist also: Was passiert, wenn der Angriff erfolgreich war?

Cyberresilienz meint die Fähigkeit, trotz eines Vorfalls weiterzuarbeiten, den Schaden zu begrenzen, Abläufe schnell wiederherzustellen und aus dem Ereignis zu lernen. Technische Redundanzen sind ein Teil davon – aber entscheidend sind auch organisatorische Faktoren:

- Gibt es einen trainierten Notfallplan?
- Sind Kommunikationswege definiert?
- Weiß die Führung, wann sie welche Entscheidungen treffen muss?

Eine resiliente Organisation denkt in Szenarien – nicht in Idealen. Sie testet ihre Krisenreaktion regelmäßig, integriert Lessons Learned in laufende Prozesse und versteht Sicherheit als kontinuierlichen Prozess. Besonders in stark regulierten Branchen wie der Energieversorgung, im Gesundheitswesen oder in der öffentlichen Verwaltung ist das nicht nur Best Practice – es ist Pflicht.

Künstliche Intelligenz: Gamechanger mit Doppelgesicht

Kaum ein Thema polarisiert derzeit so stark wie der Einsatz von künstlicher Intelligenz (KI) in der Cybersicherheit. Einerseits eröff-
f
net sie enorme Möglichkeiten für die Verteidigung:

- **Threat Detection:** KI-Systeme erkennen Abweichungen im Nutzerverhalten oder Netzwerkverkehr frühzeitig – auch dort, wo herkömmliche Signatur-basierte Systeme scheitern.
- **Automatisierte Reaktionen:** In definierten Fällen kann eine KI automatisch Prozesse blockieren, Systeme isolieren oder Administratoren benachrichtigen.
- **Predictive Analytics:** KI kann historische Daten auswerten und potenzielle Angriffsvektoren vorausschauend identifizieren – bevor es zu einem Vorfall kommt.

Andererseits nutzen auch Cyberkriminelle zunehmend KI – und das mit wachsender Professionalität. Dazu zählen:

- Automatisierte Phishing-Kampagnen, die personalisierte Mails in der Sprache des Opfers generieren.
- Deepfake-Videos und -Anrufe, die Stimmen und Gesichter täuschend echt simulieren, um Autorisierungen zu erzwingen oder Überweisungen auszulösen.

Malware-Optimierung durch KI, bei der Schadsoftware laufend angepasst wird, um signaturbasierte Erkennung zu umgehen.

Ein beunruhigendes Beispiel war 2024 ein Vorfall in Südkorea, bei dem ein CEO durch einen Deepfake-Anruf vermeintlich seine Finanzabteilung anwies, eine sechsstellige Summe zu überweisen. Der Betrug wurde erst durch Zufall entdeckt – die Stimme im Anruf war künstlich erzeugt, das Gesprächsverhalten täuschend echt simuliert.

Für Führungskräfte bedeutet das:

- KI ist nicht nur ein Tool der IT – sie wird Teil strategischer Entscheidungsfindung.
- Die Einführung von KI in Sicherheitsstrukturen muss ethisch, nachvollziehbar und reguliert erfolgen.
- Es braucht klare Governance-Strukturen, um Missbrauch und Fehlentscheidungen zu verhindern.

Die Lieferkette als Angriffsziel – und Schwachstelle

Kaum ein Bereich wurde in den letzten Jahren so häufig übersehen wie die digitale Verwundbarkeit durch Dritte. Dabei zeigt sich in nahezu jedem größeren Cybervorfall: Der Weg ins Zielsystem führt oft über einen vermeintlich harmlosen Partner.

Supply-Chain-Attacken zielen genau auf

diese Schwachstelle. Dabei geht es nicht nur um IT-Dienstleister – betroffen sind auch:

- Externe Entwicklerteams,
- Anbieter von Cloud-Diensten,
- Hardwarezulieferer mit versteckten Hintertüren,
- Subunternehmen im Facility Management mit Zugriff auf interne Netze.

Das Dilemma: Viele Unternehmen kennen nicht einmal die vollständige Liste ihrer digitalen Abhängigkeiten. Risikobewertungen beschränken sich häufig auf finanzielle oder vertragliche Kriterien – nicht auf sicherheitsrelevante.

Ein besonders dramatischer Fall war der SolarWinds-Hack, bei dem Angreifer über manipulierte Software-Updates Zugang zu Netzwerken von US-Behörden, Technologieunternehmen und Militärorganisationen erhielten. Der Ursprung: ein Angriff auf die Update-Infrastruktur eines Drittanbieters.

Für Unternehmen heißt das:

- Sicherheitsstandards müssen entlang der gesamten Lieferkette gelten – nicht nur intern.
- Verträge mit Dienstleistern sollten Sicherheitsverpflichtungen, Auditrechte und Meldepflichten enthalten.
- Es braucht ein strukturiertes Third-Party Risk Management (TPRM) mit kontinuierlicher Überprüfung.

Ein zukunftsweisender Ansatz sind digitale Lieferkettentransparenzsysteme, die automatisiert überwachen, welche Datenflüsse, Schnittstellen und Zugriffspfade über Partner laufen – und wie diese abgesichert sind.

Was Führungskräfte jetzt tun können – Handlungsempfehlungen

Cybersicherheit ist keine rein technische Disziplin mehr – sie ist ein integraler Bestandteil moderner Unternehmensführung. Wer Verantwortung trägt, muss auch Verantwortung für digitale Resilienz übernehmen.

Konkret empfehlen sich folgende Schritte:

1. Cyberresilienz zur Führungspriorität machen
   - Strategische Risikoanalyse auf C-Level-Ebene
   - Integration in Notfallpläne, Business Continuity Management und Kommunikation
   - Regelmäßige Planspiele und Simulationen
2. KI-Kompetenz aufbauen und steuern
   - Interdisziplinäre KI-Governance etablieren (IT, Recht, Ethik, Kommunikation)
   - Einführung nur bei nachvollziehbaren Entscheidungsprozessen (Explainable AI)
   - Schulung von Schlüsselpersonen in KI-Potenzial und -Grenzen
3. Lieferkettensicherheit systematisch managen
   - Kritische Drittanbieter identifizieren und bewerten
   - Sicherheitsanforderungen in Verträgen verankern
   - Kontinuierliches TPRM einführen – nicht nur bei Vertragsabschluss
4. Kommunikation vorbereiten
   - Kommunikationsstrategie für Cybervorfälle vorab definieren
   - Medien-, Kunden- und Behördenkommunikation abstimmen
   - Interne und externe Transparenz als Vertrauensfaktor verstehen
5. Kulturwandel anstoßen
   - Sicherheitskultur aktiv fördern – vom Vorstand bis zur Werkstatt
   - Fehlertoleranz für gemeldete Vorfälle schaffen
   - Sicherheit als Teil von Innovationsprozessen denken

Checkliste: 5 Schritte zur Cyber-Resilienz

1. Vorbereitung durch Szenarienplanung

- Identifizieren Sie kritische Systeme und Prozesse.
- Entwickeln Sie realistische Angriffsszenarien.
- Integrieren Sie diese in bestehende Notfall- und Krisenpläne.

2. Klare Rollen und Entscheidungswege

- Definieren Sie ein zentrales Incident Response Team (IRT).
- Stellen Sie Eskalationsstufen und Entscheidungskompetenzen schriftlich dar.
- Benennen Sie Vertreter:innen für alle Schlüsselpositionen.

3. Simulation und Training

- Führen Sie regelmäßige Notfallübungen durch (mind. 1x jährlich).
- Simulieren Sie Worst-Case-Szenarien wie Ransomware oder Systemausfall.
- Beziehen Sie auch Geschäftsführung und Kommunikation mit ein.

4. Wiederanlauf & Wiederherstellung sicherstellen

- Prüfen Sie Backups auf Wiederherstellbarkeit und Integrität.
- Halten Sie Notfall-IT-Infrastruktur (z. B. Offline-Systeme) bereit.
- Planen Sie für Teilwiederanläufe priorisierter Systeme.

5. Lernen & verbessern

- Dokumentieren Sie jeden Vorfall umfassend.
- Analysieren Sie Schwachstellen und Reaktionszeiten.
- Überarbeiten Sie Pläne und Schulungen auf Basis der Erkenntnisse.

Wer führen will, muss absichern

Cybersicherheit im Jahr 2025 verlangt Verantwortung, Vernetzung und vorausschauendes Handeln. Wer glaubt, mit punktuellen Maßnahmen oder reaktiver Technik sei es getan, irrt. Die Zukunft gehört Organisationen, die ihre Systeme verstehen, ihre Partner prüfen, ihre Risiken beherrschen – und sich nicht scheuen, digitale Sicherheit zur Chefsache zu erklären.

Veranstaltungen wie die IKT-Sicherheitskonferenz oder die European Cybersecurity Month Events zeigen: Das Wissen ist da. Jetzt ist die Zeit, es anzuwenden. -v-

Zuschriften:
ZRK Beteiligungs-, Service und Management GmbH
Reisnerstrasse 5/20a, A-1030 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