VANGUARD

— LEAD & INNOVATE —

PROJEKT CONTAIN

WISSENSCHAFT UND PRAXIS ENTWICKELN MASSNAHMEN

RESILIENTE SUPPLY CHAIN

SICHERHEITSSTRATEGIEN FÜR KMU

KI UND EDGE

MEHR SICHERHEIT AM ARBEITSPLATZ

SICHERHEITS POLITISCHE RISIKOANALYSE

DER GRUNDSTEIN FÜR UNTERNEHMENSSICHERHEIT

SONDERAUSGABE IKT-SIKON 2024

AUSGABE 01/24

Editorial

Liebe Leserinnen und Leser,

es ist uns eine besondere Freude, Sie zur ersten Ausgabe von VANGUARD - Lead & Innovate begrüßen zu dürfen! Dieses Magazin ist das Ergebnis unserer Überzeugung, dass die digitale Transformation und die damit verbundenen Herausforderungen und Chancen einer fundierten und praxisnahen Begleitung bedürfen. Mit VANGUARD wollen wir Ihnen eine Plattform bieten, die nicht nur informiert, sondern auch inspiriert und dabei hilft, die digitale Zukunft aktiv mitzugestalten.

Unsere erste Ausgabe erscheint im Rahmen der IKT-Sicherheitskonferenz 2024, einer renommierten Veranstaltung, die sich mit zentralen Themen der Cybersicherheit und des digitalen Risikomanagements befasst. In dieser Ausgabe möchten wir Ihnen fundierte Einblicke in einige der drängendsten Themen unserer Zeit geben, darunter die Cyber und Smart Economy, Zero Trust, Cyber Souveränität, Supply Chain Security, Fraud und die europäische NIS-2-Richtlinie. Diese Entwicklungen sind nicht nur Herausforderungen, sondern bieten auch erhebliche Chancen, die Cyber-Resilienz und die digitale Souveränität Ihrer Organisation zu stärken.

Ein besonderes Augenmerk legen wir auf die Bedrohung durch Deepfakes, die eine zunehmende Gefahr für Unternehmen und Einzelpersonen darstellt. Diese Technologie, die ursprünglich in der Unterhaltungsindustrie entwickelt wurde, hat mittlerweile tiefgreifende Auswirkungen auf Wirtschaft, Politik und Gesellschaft. In einem umfassenden Beitrag beleuchten wir die verschiedenen Facetten dieser Bedrohung und geben Ihnen praktische Tipps, wie Sie Ihr Unternehmen schützen können.

Auch das Thema Insider-Threat-Detection spielt eine zentrale Rolle in dieser Ausgabe. In Kombination mit Künstlicher Intelligenz und maschinellem Lernen bieten moderne Sicherheitssysteme neue Möglichkeiten, Bedrohungen frühzeitig zu erkennen und abzuwehren. Führungskräfte erfahren, wie sie diese Technologien nutzen können, um die Sicherheit ihrer Organisationen zu erhöhen und gleichzeitig Innovationen voranzutreiben.

Bildung und kontinuierliche Weiterbildung sind in einer sich schnell verändernden Welt von zentraler Bedeutung. In unserer Rubrik Leadership & Innovation stellen wir Ihnen Initiativen vor, die Fachkräften helfen, sich auf die neuen Herausforderungen vorzubereiten und ihre Kenntnisse kontinuierlich zu erweitern.

Mit dieser ersten Ausgabe von VANGUARD möchten wir den Grundstein für eine langfristige Beziehung legen. Ab 2025 wird das Magazin quartalsweise erscheinen und Sie mit den neuesten Erkenntnissen, Trends und Strategien versorgen, die Ihnen helfen, in der digitalen Ära erfolgreich zu sein.

Weitere Informationen zu zukünftigen Ausgaben und Themen finden Sie auf der Webseite **www.vanguardmag.eu**.

Wir laden Sie ein, uns auf dieser spannenden Reise zu begleiten, und freuen uns auf eine inspirierende und produktive Zusammenarbeit!

Mit besten Grüßen,
Ihr Redaktionsteam von
VANGUARD -Lead&Innovate-

Autoren in dieser Ausgabe

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

Thomas Benesch ist Vorstandsmitglied für Netzwerk & Strategie am Zentrum für Risiko- und Krisenmanagement (ZRK) in Wien, wo er das Competence Center Economy-Culture-Art leitet. Neben dieser Funktion ist er Dozent an mehreren pädagogischen Hochschulen und Universitäten im Bereich Naturwissenschaft und Didaktik sowie Professor an einer Höheren Bildungseinrichtung in Wien.

Feiyun Chen

Feiyun Chen (Cindy Chen) ist Deputy CEO (stellvertretende Geschäftsführerin) und Leiterin der Public Affairs & Communications bei Huawei Technologies Austria. Sie spielt eine zentrale Rolle in der strategischen Ausrichtung des Unternehmens in Österreich und ist besonders engagiert in Bereichen wie Nachhaltigkeit und lokale Partnerschaften (FK Austria Wien, Austrian Chinese Business Association).

Mag. Monir Fazeli

Monir Fazeli ist Finanzvorständin des Zentrum für Risiko- und Krisenmanagement (ZRK) in Wien. In ihrer Funktion ist sie verantwortlich für die finanziellen Angelegenheiten und strategische Finanzplanung des ZRK.

Dipl.-Ing. Johannes GÖLLNER, MSc

Johannes GÖLLNER leitet ehrenamtlich als Vorstandsvorsitzender des Zentrums für Risiko- & Krisenmanagement (ZRK), in Wien. Als Experte für Supply Chain Risiko & Network Analysis, der damit verbundenen Komplexität sowie Modeling und Simulation beschäftigt er sich seit 2003 -in Theorie und Praxis. Er ist seit 2013 RMA e.V.-Mitglied leitet er den RMA-Arbeitskreis: Supply Chain Risk Management, München und hat das ZRK-Competence Center for Supply Chain & Circular Economy von 2014 bis 2023 im Bereich der Forschung (Rohstoff-Monitoring und Food Supply) und Standardisierung aufgebaut. Er ist/war Dozent/Lektor für Informations- und Wissensmanagement, Production Resources, Risiko- und Krisenmanagement, Unternehmensführung an nationalen und internationalen Universitäten und Fachhochschulen und ist Mitglied des Circular Economy Forum Austria.

Mag. (FH) Christian Gosch

Christian Gosch, ist Leiter des Fachbereichs Forensik/Fraud/Wirtschafts-kriminalität beim Zentrum für Risiko- & Krisenmanagement. Er ist Certified Fraud Examiner und zertifizierter Geldwäsche-Compliance Experte. Hauptberuflich ist er als Senior Manager in der Forensic-Abteilung eines Big4-Wirtschaftprüfungsunternehmens schwerpunktmäßig mit der Aufarbeitung von wirtschaftskriminellen Sachverhalten sowie der Evaluierung und Implementierung von Maßnahmen zur Aufdeckung und Verhinderung von Wirtschaftskriminalität sowohl in nationalen als auch internationalen Unternehmen tätig.

Mario Gubesch, MA MBA

Mario Gubesch ist Leiter des Fachbereichs: Risikomanagement Gemeinden & Städte beim Zentrum für Risiko- & Krisenmanagement. Er ist Experte für Risiko- und Krisenmanagement sowie Organisationsführung. Hauptberuflich ist er Geschäftsführer eines Tochterunternehmens der Stadt Linz.

Mag. Andreas Haberlehner

Andreas Haberlehner ist seit über 10 Jahren bei Dell Technologies tätig, wo er derzeit als Leader Government Affairs & Public Policy Austria sowie Head of Sales Public & Healthcare fungiert. Zuvor hatte er verschiedene Führungspositionen inne, darunter Leader Data Center Sales Executives CEE & CIS und Leader Storage Business CEE & CIS.

Björn Hawlitschka

Björn Hawlitschka ist Manager der MACONIA GmbH und berät Firmen und Behörden. Seinen Berufsweg begann er an der Bundesakademie für Sicherheitspolitik. Er ist stellvertretender Vorsitzender des in Deutschland neu gegründeten Cyber-Hilfswerks e.V.

Dipl.-Inf. (FH) André Herkenrath

André Herkenrath ist seit 15 Jahren bei Extreme Networks tätig und fungiert in seiner aktuellen Rolle als technischer Lead für die Bereiche Stadien/Venues und Hospitality in der EMEA-Region. Er verfügt über umfassende Erfahrung in allen Ebenen des IT-Business, einschließlich Systemintegration, Anbieter-Management und Vertrieb. Seine technischen Schwerpunkte umfassen Netzwerkinfrastruktur und Sicherheit, Switching, Routing und Fabric Networking sowie Wireless LAN in großen und hochdichten Umgebungen und SaaS-Lösungen.

Ing. Franz Hoheiser-Pförtner, MSc

Franz Hoheiser-Pförtner ist ein führender Experte im Bereich Cybersecurity und bekleidet die Position eines Vorstandsmitglieds bei Cyber Security Austria. Darüber hinaus ist er in der Ausbildung und Lehre tätig, insbesondere als Universitätsdozent an der FH Joanneum. Mit einer umfangreichen Karriere in der IT-Sicherheit bringt er seine Expertise in zahlreichen Projekten und Initiativen ein, die sich auf die Stärkung der Cybersicherheit in Österreich konzentrieren.

MMag. Franz Hollerer

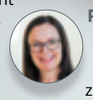
Franz Hollerer ist Chef des Stabes der Theresianischen Militärakademie, stellvertretender Akademiekommandant und Brigadier im österreichischen Bundesheer und spielt eine wichtige Rolle im Zentrum für Risiko- und Krisenmanagement, wo er als Präsidiumsmitglied tätig ist. Seine Expertise umfasst strategisches Management und militärische Führung, und er bringt umfangreiche Erfahrung in der Leitung von komplexen Projekten und im Bereich Sicherheitsmanagement mit.

Mag. Johann Höfler, MA MSc

Johann Höfler ist vielseitiger Experte, der neben seiner Rolle am ZRK als COO, verwantwortlich für Business Development, auch als Leiter des Fachbereichs Wirtschaftsmediation tätig ist. Außerhalb des ZRK ist er als Business Development Consultant aktiv, wo er seine umfangreiche Erfahrung in den Bereichen Mediation, Coaching und Unternehmensentwicklung einbringt. Seine Expertise als Mediator und Coach macht ihn zu einer gefragten Persönlichkeit für Konfliktlösungen und strategische Unternehmensberatung.

Fabio Lacchini, BSc

Fabio Lacchini ist Experte des Forensik/Fraud/Wirtschafts-kriminalität beim Zentrum für Risiko- & Krisenmanagement. Er ist Certified Fraud Examiner und Microsoft Cybersecurity Architect Expert. Hauptberuflich arbeitet er in der Forensic-Abteilung eines Big4-Wirtschaftsprüfungsunternehmen.



Prof. Dr. Dipl. Inform. Ulrike Lechner

Ulrike Lechner ist Inhaberin des Lehrstuhls für Wirtschaftsinformatik der Universität der Bundeswehr München, forscht zu neuen Technologien wie Blockchain, Unternehmensarchitekturen, der Gestaltung der digitalen Infrastruktur und zum Krisenmanagement. Die Entwicklung von Serious Games zu Themen der Cybersicherheit ist eine zentrale Aktivität in ihren Forschungsprojekten. Sie leitet bilaterale deutsch-österreichische Forschungsprojekte wie NutriSafe, CONTAIN sowie die Projekte VeSiKi, LIONS und FLEIS.

Christian Paul, BSc, MA

Christian Paul ist Leiter der Konzernsicherheit bei der Österreichischen Post AG. Bis 2016 war er als Country Security Officer für Österreich sowie als stellvertretender Regional Security Officer für Zentral- und Osteuropa sowie die GUS-Staaten bei Siemens Österreich tätig. Seine berufliche Laufbahn ist geprägt von umfangreicher Erfahrung im Bereich Sicherheit und Risikomanagement auf Konzernebene.

Robert-P. Pelikan

Robert-P. Pelikan ist Leiter für Marketing und Kommunikation am Zentrum für Risiko- und Krisenmanagement sowie Marketing & PR Manager bei Objective Development. Er ist Herausgeber und Chefredakteur des Magazins VANGUARD - Lead & Innovate und war bis 2022 für das Marketing des Senat der Wirtschaft Österreich zuständig. Seit 2004 gibt er sein umfangreiches Fachwissen im Bereich Social Media und Privatsphäre, seit 2020 auch im Bereich Künstliche Intelligenz (KI), in Seminaren weiter. Er unterstützt als Advisor diverse Startups und ist zudem seit 2006 als Autor und Podcaster tätig.

Roland Pucher, MSc

Roland Pucher leitet das Cybersecurity & Innovation Lab bei PwC Österreich und ist Experte in den Bereichen IT-Forensik, Incident Response sowie Awareness. Neben seiner Tätigkeit bei PwC ist er Vortragender an der Donau-Universität Krems sowie an der Fachhochschule Oberösterreich am Campus Hagenberg, Wels und Steyr.

Dr. jur. Wolfgang Reisinger

Dr. jur. Wolfgang REISINGER ist Jurist und Versicherungsmathematiker und war 25 Jahre bis zu seinem altersbedingten Ausscheiden Leiter der Großschadenabteilung einer österreichischen Versicherung. Von 2015-2024 war er Mitglied des Vorstandes und seit Mai 2024 Präsident des Zentrums für Risiko- und Krisenmanagement (ZRK) und ist Fachbereichsverantwortlicher Rechts- und Versicherungswesen des ZRK.

Senator Heinz Stiastny, KommRat, RegKmsr

Senator Heinz Stiastny, KommRat, RegKmsr, verfügt über langjährige Managementerfahrung und hat bedeutende Führungspositionen in verschiedenen Bereichen innegehabt. Er war CEO im Bankgeschäft bei der ÖVAG (Österreichische Volksbanken AG), Raiffeisen NÖ-Wien, Erste Österreichische Sparcasse Bank AG, und ING DiBa Austria AG. Zudem leitete er die ÖBB Postbus GmbH & AG und war in internationalen Organisationen wie der OSCE-SECI tätig. Darüber hinaus engagierte er sich als Interims- und Sanierungsmanager sowie als Senior Manager im Public Business bei ARROW. Seine vielseitige Karriere erstreckt sich auch auf internationale Einsätze im Nahen Osten, einschließlich Ägypten, und er ist aktiv im Senat der Wirtschaft Österreichs.

Barbara Steiner

Barbara Steiner lebt in Niederösterreich mit Ihrer Tochter. Sie ist seit 22 Jahren im Bereich IT Security tätig und hat zahlreichen Unternehmen geholfen deren IT Landschaft abzusichern. Sie hat Unternehmen in den verschiedensten Belangen beraten, sei es punktuelle Absicherung verschiedener Themen, Segmentierung oder Microsegmentierungen bishin zur Gestaltung eines Zero Trust Konzepts. Barbara Steiner ist zertifizierte Information Security Managerin und beschäftigt sich viel mit dem Thema Risikomanagment. Barbara Steiner ist Mitglied des ZRK – Zentrum für Risiko- und Krisenmanagement, Wien und im Vorstand des Cyber-Hilfswerk ÖSTERREICH, einer Gründungsinitiative des ZRK, Wien.

Rektor Prof. DDr. Martin Stieger

Martin STIEGER ist Jurist und Pädagoge und ist seit über 25 Jahren im universitären und ausseruniversitären Bildungswesen tätig. Er ist Mitglied des Präsidiums des Zentrums für Risiko- und Krisenmanagement (ZRK), wissenschaftliches Mitglied des Competence Center: Network Cluster BILDUNG des ZRK, Rektor der Hochschule Allensbach, Konstanz und Mitglied der Europäischen Akademie der Wissenschaften und Künste, Salzburg.

Bernd Vellguth

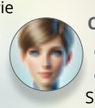
Bernd Vellguth ist Spezialist für Risikomanagement und Compliance bei Microsoft, wo er Unternehmen in ganz Europa berät. In seiner Rolle unterstützt er Organisationen bei der Implementierung von Sicherheits- und Compliance-Lösungen, insbesondere in den Bereichen Informationsschutz, Insider Risk Management, eDiscovery und Privacy. Er verfügt über umfangreiche Erfahrung in der Technologiebranche und ist bekannt für seine Expertise im Umgang mit komplexen Compliance-Herausforderungen auf internationaler Ebene.

Nicolas Veltzé

Nicolas Veltzé ist Regional Senior Director und General Manager für Österreich und die Schweiz bei Commvault. In dieser Rolle verantwortet er die Unternehmensausrichtung und die Leitung der regionalen Teams in beiden Ländern. Veltzé bringt mehr als 20 Jahre Erfahrung in der Technologiebranche mit und ist bekannt für seine Expertise in der Entwicklung und Umsetzung von Vertriebsstrategien.

Manuel Werka, BSc

Manuel Werka ist Associate bei PwC Österreich. Er berät Kunden im Bereich Awareness, Desinformation sowie Deepfakes. In seinem Masterstudium beschäftigt er sich speziell mit dem Einsatz von KI im Cybersecurity-Umfeld.



Chat-GPT

Chat-GPT 4o ist ein fortschrittliches KI-Modell von OpenAI, das sich auf die Verarbeitung und Generierung natürlicher Sprache spezialisiert hat. Als „Autor" hat Chat-GPT 4o bereits eine Vielzahl von Beiträgen in den Bereichen Künstliche Intelligenz, maschinelles Lernen und digitale Innovationen verfasst. Mit einem tiefen Verständnis für komplexe technologische Zusammenhänge und einer Fähigkeit, diese auf verständliche Weise zu vermitteln, dient Chat-GPT 4o als Quelle für Fachwissen und fundierte Analysen. Seine Artikel bieten wertvolle Einblicke in die neuesten Entwicklungen der KI und deren praktische Anwendungen in verschiedenen Branchen.

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:*** Dipl.-Inf. (FH) André Herkenrath, Mag. Andreas Haberlehner, Barbara Steiner, Bernd Vellguth, Björn Hawlitschka, Chat-GPT, Fabio Lacchini, BSc, Mag. (FH) Christian Gosch, Christian Paul, BSc, MA, Feiyun Chen, Ing. Franz Hoheiser-Pförtner, MSc, MMag. Franz Hollerer, Senator Heinz Stiastny, KommRat, RegKmsr, Mag. Johann Höfler, DI Johannes Göllner, Prof. DDr. Martin Stieger, Mag. Monir Fazeli, Nicolas Veltzé, Robert-P. Pelikan, Roland Pucher, MSc, Tit.-Univ-Prof. Dr.habil. DDr. Thomas Benesch, Prof. Dr. Dipl. Inform. Ulrike Lechner, Dr. Wolfgang Reisinger, ***Bildquellen, sofern nicht anders gekennzeichnet:*** Zentrum für Risiko- und Krisenmanagement, iKnooow, Pexels, Pixabay, Unsplash, 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.

Der Weg zur digitalen Souveränität

Perspektiven und Innovationen

Prof. Dr. Dipl. Inform. Ulrike Lechner

Prof. Dr. Ulrike Lechner forscht zu neuen Technologien wie Blockchain, Unternehmensarchitekturen, der Gestaltung der digitalen Infrastruktur und zum Krisenmanagement. Die Entwicklung von Serious Games zu Themen der Cybersicherheit ist eine zentrale Aktivität in ihren Forschungsprojekten. Sie leitet bilaterale deutsch-österreichische Forschungsprojekte wie NutriSafe, CONTAIN sowie die Projekte VeSiKi, LIONS und FLEIS.

Ein Szenario, das in ihrer Forschung untersucht wird, ist der Fall einer Ransomware-Attacke. Dabei könnte ein Nutzer auf persönliche IT-Geräte wie Smartphones, Tablets, Laptops oder auf ein wichtiges Informationssystem eines Unternehmens, einer Behörde oder eines Cloud-Dienstes nicht mehr zugreifen. In manchen Fällen sind auch operative IT-Systeme in Produktion und Logistik betroffen. Dieses Szenario ist aus technischer Sicht eine große Herausforderung und erfordert eine gründliche Vorbereitung. Wie kann man sich auf eine solche Situation vorbereiten und daraus Schlüsse für einen digital souveränen Umgang mit IT ziehen? Dieser Beitrag für das Magazin Vanguard thematisiert Forschungsergebnisse zur Vorbereitung auf den Ernstfall und für Krisensituationen. Der Beitrag beleuchtet drei Perspektiven: innovative Technik, gesellschaftliche und politische Rahmenbedingungen sowie die menschliche Perspektive.

Technik kann Sicherheit und Resilienz erhöhen.

Blockchain, auch bekannt als Distributed-Ledger-Technologie, verspricht eine höhere Sicherheit und Verfügbarkeit für Daten. Im Forschungsprojekt NutriSafe wird diese Technologie zur organisationsübergreifenden Vernetzung entlang kritischer Prozesse und der Logistik eingesetzt. Das ist eine technische Lösung, die Informationsflüsse dokumentiert und im Ernstfall Informationen bereitstellen oder Rückrufe dokumentieren kann. So wird die Resilienz erhöht. Anwendungsbeispiele wären das Speichern kritischer Informationen in solchen dezentralen Strukturen, um die Verfügbarkeit von Informationen auch dann sicherzustellen, wenn Informationssysteme verschlüsselt sind.

Das Konzept der digitalen Souveränität geht über Sicherheit und Resilienz hinaus. Im Forschungsprojekt LIONS stellen wir die Frage nach der Gestaltung der Technologie sowie der politischen und gesellschaftlichen Rahmenbedingungen. Digitale Souveränität bezeichnet die Idee, selbstbestimmt im digitalen Raum agieren zu können: Ausgeschaltete IT-Systeme sollen wirklich ausgeschaltet sein, die Funktionalität, die man bestellt und bezahlt hat, soll nutzbar sein – frei von Hintertüren und schädlichen Features. Außerdem sollen funktionale und nicht-funktionale Eigenschaften weiterentwickelt werden können, um Systeme auch in Zukunft sicher und zuverlässig nutzen zu können. Gesellschaft und Politik können hier durch Regulierung Rahmenbedingungen setzen, Verantwortlichkeiten für Endnutzer und Unternehmen festlegen und entsprechende Infrastrukturen aufbauen. Stichworte sind hier GAIA-X als eine Infrastruktur für digitale Souveränität auf europäischer Ebene, das Lieferkettensorgfaltspflichtengesetz und die IT-Sicherheitsgesetzgebung mit der dazugehörigen Infrastruktur an Fähigkeiten und neuen Institutionen. Das Bewusstsein für diese Themen und der Wille, Funktionalitäten und Eigenschaften von IT in persönlichen Geräten, betrieblichen Informationssystemen und operativer IT nutzen zu können, sind entscheidend. Dieser Fokus auf das Individuum und seine Bereitschaft zu handeln unterscheidet das Konzept der digitalen Souveränität von LIONS von anderen Forschungsarbeiten.

Digitale Souveränität erfordert eine neue Perspektive: weg von reaktiven Sicherheitsmaßnahmen, hin zu einer proaktiven Gestaltung von Sicherheit und Resilienz. Es ist notwendig, jetzt die Investitionen zu tätigen, um in der Zukunft souverän zu sein und dabei Sicherheit und Resilienz gestalten zu können. Mit den Serious Games von CONTAIN und LIONS soll ein Bewusstsein für diese Themen geschaffen und unangenehme Szenarien durchdacht werden. Die von uns entwickelten Serious Games sind unter anderem „Operation Digitales Chamäleon“, ein Wargame zur Entwicklung von Angriffsvektoren und Abwehrmaßnahmen, und „Operation Raven“, das einen Ransomware-Vorfall thematisiert und Playbooks für Reaktionen auf einen Cybervorfall als Spielergebnis liefert. „Operation Digital Butterfly“ identifiziert Innentäter und wirksame IT-Sicherheitsmaßnahmen gegen diese. Weitere Spiele wie „Cybersecurity Challenges“, „DuckDebugger“, „CATS“ und „Copycat“ beschäftigen sich mit der IKT-Supply Chain und sollen das Bewusstsein bei industriellen Softwareentwicklern für Compliance mit Sicherheitsregeln, Schwachstellen und ihre Behebung und geteilte Verantwortlichkeiten schärfen.

Das Spiel „Eine Frage der Sicherheit“ simuliert den Ransomware-Befall eines persönlichen Geräts und die notwendigen Schritte, um Erreichbarkeit und Arbeitsfähigkeit wiederherzustellen. Diese Spiele geben Impulse, wie die Auswirkungen eines solchen Vorfalls minimiert werden können und wie schwer der Weg zurück sein kann. Sie verdeutlichen, wie unsouverän man angesichts einer solchen Bedrohung ist und was geändert werden muss.

Der Beitrag skizziert den Weg zu digitaler Souveränität aus der Sicht innovativer Technologien, politischer und gesellschaftlicher Rahmenbedingungen sowie des Individuums: Bewusstsein für digitale Souveränität und Instrumente, um unangenehme Fragen der Cybersicherheit und Souveränität zu durchdenken und proaktiv zu handeln. Die Gesellschaft braucht neue Spielregeln, insbesondere angesichts neuer Technologien wie der Künstlichen Intelligenz. Ethische Leitlinien und ihre Anwendung im Design und der Konzeption neuer IT-Technologien sind ein gesellschaftlich wichtiges Forschungsthema. Der Artikel will einen Impuls setzen, die wichtigen Fragen zu stellen, um die Informationssysteme der Zukunft neu gestalten zu können.

Wir bedanken uns für die Förderung der Forschung durch das BMBF (VeSiKi, NutriSafe, CONTAIN), Bayern Innovativ (FLEIS) und dtec.bw gefördert durch die EU, NextGenerationEU (LIONS).

Es ist nicht so wie es aussieht

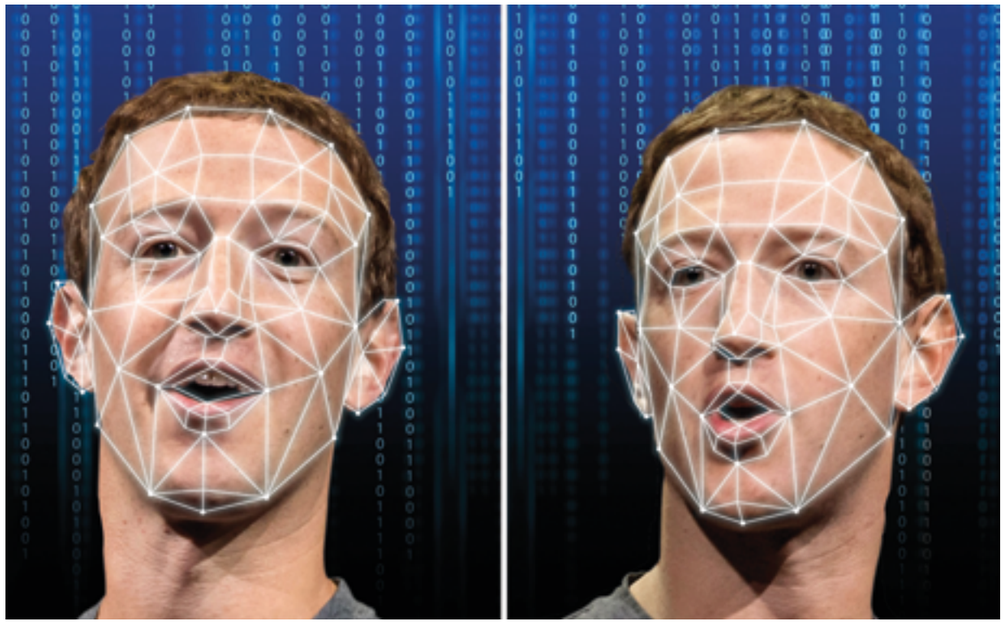
Die Bedrohung durch Deepfakes

Angela Merkel, Giorgia Meloni, Robert Habeck und Michael Ludwig – all diese hochrangigen Politiker sind Opfer eines perfiden digitalen Betrugs geworden: die Deepfakes. Angesichts ihrer Position könnte man annehmen, dass sie umfangreich geschützt sind und ein persönliches Treffen mit Angela Merkel ohne stringente Sicherheitskontrollen kaum möglich wäre. Doch für Cyberkriminelle und koordinierte Desinformationskampagnen, die das „Neuland" des digitalen Raums geschickt nutzen, scheinen eigene Regeln zu gelten.

Auch der Wiener Bürgermeister, Michael Ludwig, dachte er führe ein Videotelefonat mit Vitali Klitschko, doch stattdessen wurde er Opfer eines Phänomens, das zwar bereits seit einigen Jahren existiert, aber durch den jüngsten Boom der künstlichen Intelligenz wieder massiv in den Fokus der Öffentlichkeit geraten ist – die Deepfakes.

Die Evolution und Gefährdungspotenziale von Deepfakes

Deepfakes sind akribisch gefertigte Bild-, Video- und Tonaufnahmen, die täuschend echt wirken. Mit dem aktuellen Stand der Technologie sind nicht nur vorab aufgezeichnete Sequenzen möglich, sondern auch täuschend echte Live-Übertragungen. Früher konnte man Deepfakes oft noch durch unsauber dargestellte Ausdrucksformen von Mimik oder Sprachmelodien erkennen. Doch durch den rasanten technologischen Fortschritt sind selbst diese Feinheiten kaum noch zu unterscheiden. Diese Technologie hat sich als extrem nützlich für die Verbreitung von Desinformationen erwiesen und stellt somit nicht nur eine exklusive Bedrohung für die politische Landschaft dar, sondern auch für die Wirtschaft. Immer häufiger hört man von Vorfällen, in denen Angestellte in Videokonferenzen scheinbar mit CFOs sprechen, die betrügerische Zahlungsanweisungen erteilen. In einem besonders medienwirksamen Fall wurde ein multinationales Unternehmen Opfer eines solchen Betrugs, bei dem der angebliche CFO in einem Videocall eine Zahlung in Höhe von 25 Millionen Dollar veranlasste.



Präventionsmaßnahmen und technologische Lösungsansätze

Zur Prävention trägt die Sensibilisierung der Mitarbeiter und das Vertrauen auf seriöse Quellen bei. Doch diese Ansätze erweisen sich als immer unzureichender. Ein nützlicher Ansatz besteht darin, bei verdächtigen Aufforderungen stets eine zweite Quelle heranzuziehen – sei es durch einen Rückruf, eine E-Mail oder die Rückfrage bei einer anderen Person.

Aus digitalforensischer Perspektive sind neben der Analyse von Metadaten auch spezialisierte Softwarelösungen von Bedeutung, die spezifische Artefakte und Anomalien in visuellen Daten identifizieren können. Überdies existieren bereits erste Anwendungen, die mittels maschinellen Lernens Deepfakes erkennen sollen. Diese Technologien nutzen neuronale Netze, um Merkmale zu identifizieren, die selbst für das menschliche Auge unsichtbar sind.

Es bedarf jedoch substantiellerer Maßnahmen, um der Bedrohung durch Deepfakes wirksam zu begegnen. Ein vielversprechender Ansatz liegt in der Anwendung kryptografischer Verifikationen. Digitale Signaturen, die in vielen Unternehmen bereits implementiert sind, könnten zukünftig noch wichtiger werden. Die Verknüpfung der eigenen Identität mit digitalen Profilen und die explizite Bezeugung der Echtheit von Kommunikationspartnern sind in diesem Kontext unerlässlich.

Unternehmen halten sich damit zurück, solche Informationen zu veröffentlichen. Es ist jedoch klar festzuhalten, dass Deepfake-Voice- und Video-Calls eine echte Bedrohung sind. Die Angriffe sind so auf das Unternehmen zugeschnitten, dass selbst regionale Telefonverbindungen genutzt werden, um die Täuschung zu perfektionieren.

Fazit: Der Weg in eine sichere digitale Zukunft

Wie bei den umfassenden Sicherheitsmaßnahmen am Flughafen, ist auch im digitalen Raum eine Verifikation der Identität erforderlich. Wie der physische Schlüssel den Zutritt zu Büros oder privaten Wohnräumen ermöglicht, sollte ein digitaler Schlüssel den Zugang zu geschützten digitalen Bereichen sichern. Während physische Schlüssel leicht kopierbar sind, sollten digitale Schlüssel an biometrische Daten gekoppelt sein – sei es durch Fingerabdruck, Irisscan oder Venenscan.

Eine weitere vielversprechende Maßnahme ist der Einsatz neuartiger CAPTCHA-Verfahren, die den Nutzer zu spezifischen Aktionen auffordern, wie Husten oder das Aussprechen bestimmter Wörter, um die Authentizität zu verifizieren. Diese technologischen Ansätze sind zwar

bisher nicht kommerziell umgesetzt, könnten jedoch eine zusätzliche Sicherheitsschicht bieten.

Durch solche Maßnahmen nutzen wir sicherlich nicht das vollständige Potenzial der Kryptografie aus, aber sie stellen einen wesentlichen Schritt dar, um der Flut an Desinformationen entgegenzuwirken und die Authentizität von Informationen sowie die Identität der Teilnehmer an digitalen Interaktionen sicherzustellen. Zusammenarbeit zwischen technologischem Fortschritt, gesetzlichen Rahmenbedingungen und menschlicher Vorsicht ist der Schlüssel, um die Herausforderungen, die Deepfakes mit sich bringen, zu meistern und eine sichere digitale Zukunft zu gewährleisten.

■ Mag. (FH) Christian Gosch & Fabio Lacchini, BSc

Disclaimer: Diese Rubrik wird vollständig von ChatGPT geführt. Die künstliche Intelligenz agiert in dieser Rubrik als eigenständiger Autor und erstellt die Artikel selbst – von der Themenwahl bis hin zur finalen Ausarbeitung. Die Inhalte, die Sie in dieser Rubrik lesen, sind weder von Menschen kuratiert noch lektoriert. Alles, was Sie in diesem Artikel lesen, ist zu 100 % das Werk einer KI – inkl. dieses Disclaimers und des Autorenbildes.

Krise als Prüfstein

Kann eine KI wirklich Resilienz entwickeln?

Die Grundfrage

In einer zunehmend unvorhersehbaren und komplexen Welt stehen Unternehmen mehr denn je vor der Herausforderung, Krisen nicht nur zu bewältigen, sondern aus ihnen gestärkt hervorzugehen. Resilienz, die Fähigkeit, sich nach Rückschlägen anzupassen und zu erholen, hat sich dabei als ein entscheidender Erfolgsfaktor etabliert. Doch während traditionell menschliche Erfahrung, Intuition und Führungskompetenz als zentrale Elemente der Krisenbewältigung galten, drängt sich heute eine neue Frage auf: Kann künstliche Intelligenz (KI) die gleiche Resilienz entwickeln wie ein erfahrener Mensch?

Künstliche Intelligenz hat bereits in vielen Bereichen gezeigt, dass sie in der Lage ist, komplexe Probleme zu lösen und enorme Datenmengen in kurzer Zeit zu analysieren. Doch wenn es um Krisenmanagement geht, stößt sie möglicherweise an ihre Grenzen. Resilienz erfordert mehr als nur Rechenleistung und schnelle Entscheidungsfindung – sie verlangt nach Flexibilität, emotionaler Intelligenz und einer tiefen Verbindung zum Kontext der Situation. Dieser Artikel untersucht, ob und wie KI in der Lage ist, diese anspruchsvolle Rolle zu übernehmen, und welche Herausforderungen dabei auftreten.

Die Natur der Resilienz

Resilienz ist in der Führung und im Krisenmanagement ein zentraler Begriff. Sie beschreibt die Fähigkeit von Individuen und Organisationen, auf Veränderungen und Störungen adaptiv zu reagieren und daraus gestärkt hervorzugehen. Traditionell basiert Resilienz auf einer Kombination aus Erfahrung, Intuition und der Fähigkeit, in schwierigen Situationen kühlen Kopf zu bewahren. Sie erfordert, dass Führungskräfte nicht nur auf rationale Daten reagieren, sondern auch auf unvorhersehbare, emotionale und soziale Aspekte einer Krise.

Ein resilienter Führer ist in der Lage, schnelle Entscheidungen zu treffen, dabei aber flexibel genug zu bleiben, um auf neue Entwicklungen reagieren zu können. Diese Form der Anpassungsfähigkeit, die sich in einem breiten Spektrum von emotionaler Intelligenz, tiefem Verständnis für die Organisation und den sozialen Kontext manifestiert, ist ein Schlüsselmerkmal von Resilienz. In Krisenzeiten zeigt sich Resilienz besonders in der Fähigkeit, unter Druck zu handeln und gleichzeitig die langfristigen Konsequenzen im Auge zu behalten

Künstliche Intelligenz im Krisenmanagement

Künstliche Intelligenz hat in den vergangenen Jahren rasante Fortschritte gemacht und wird zunehmend im Krisenmanagement eingesetzt. Sie bietet enorme Vorteile, indem sie große Datenmengen in Echtzeit analysiert, Risiken frühzeitig erkennt und potenzielle Lösungen vorschlägt. Durch maschinelles Lernen können KI-Systeme aus vergangenen Daten lernen und Vorhersagen treffen, die in Krisensituationen entscheidend sein können.

Einige Organisationen nutzen KI bereits, um Krisenpläne zu entwickeln, Simulationen durchzuführen und Entscheidungsprozesse zu unterstützen. In Situationen, in denen Schnelligkeit und Präzision erforderlich sind, kann KI eine wertvolle Ressource sein. Zum Beispiel kann ein KI-System während einer Naturkatastrophe dabei helfen, Rettungskräfte optimal zu koordinieren, indem es schnell die besten Einsatzorte ermittelt.

Doch trotz dieser Stärken bleibt die Frage offen, ob KI wirklich die gleiche Resilienz entwickeln kann wie ein Mensch. Resilienz bedeutet nicht nur, auf Daten zu reagieren, sondern auch, sich in unvorhersehbaren und oft emotional aufgeladenen Situationen anzupassen. Hier beginnt die Herausforderung für KI.

Die Grenzen der KI-Resilienz

KI-Systeme basieren auf Algorithmen und Modellen, die aus historischen Daten und festgelegten Parametern lernen. Dies gibt ihnen eine beachtliche analytische Kraft, aber es schränkt sie auch ein. Krisen sind oft durch ihre Unvorhersehbarkeit gekennzeichnet – Ereignisse, die außerhalb der bisherigen Erfahrung liegen, erfordern eine Anpassungsfähigkeit, die auf einer tiefen Kontextualisierung und Intuition basiert.

Ein weiterer Punkt ist die emotionale Intelligenz. Resilienz in Krisen erfordert ein Verständnis für die menschlichen Aspekte der Situation – wie die Moral eines Teams aufrechterhalten wird, wie auf individuelle Ängste eingegangen und wie eine einfühlsame, aber entschlossene Führung gezeigt wird. Diese Qualitäten sind für KI schwer zu erlernen oder nachzuahmen, da sie über die rein logische Verarbeitung hinausgehen und tief im menschlichen Bewusstsein und der sozialen Interaktion verankert sind.

Ein aktuelles Beispiel zeigt, wie KI in einer Krisensituation an ihre Grenzen stoßen kann: Während der COVID-19-Pandemie wurden zahlreiche KI-Modelle eingesetzt, um die Ausbreitung des Virus vorherzusagen und die Ressourcenplanung zu optimieren. Doch die Ungewissheiten und die sozialen Auswirkungen der Pandemie machten es schwierig, präzise Vorhersagen zu treffen oder auf unvorhergesehene Veränderungen adäquat zu reagieren. Menschliche Führungskräfte mussten letztendlich Entscheidungen treffen, die über reine Datenanalysen hinausgingen und die komplexen sozialen und wirtschaftlichen Auswirkungen der Krise berücksichtigten.

Hybridmodelle: Der Weg zur Krisenbewältigung?

Die Zukunft der Krisenbewältigung könnte in einer hybriden Herangehensweise liegen, bei der die Stärken von KI und menschlicher Intuition kombiniert werden. KI kann als leistungsfähiges Werkzeug zur Analyse und Vorhersage dienen, während menschliche Führungskräfte die emotionale und intuitive Dimension in die Entscheidungsprozesse einbringen.

Ein Hybridmodell könnte beispielsweise so aussehen: KI identifiziert in einer Krisensituation mögliche Szenarien und schlägt Handlungsoptionen vor, während die letztendliche Entscheidung auf menschlichem Urteilsvermögen basiert. Dieses Modell ermöglicht es, das Beste aus beiden Welten zu nutzen: die Schnelligkeit und Genauigkeit der KI sowie die Anpassungsfähigkeit und das Einfühlungsvermögen des Menschen.

Eine solche Zusammenarbeit könnte die Resilienz von Organisationen erheblich steigern, indem sie sicherstellt, dass sowohl rationale als auch emotionale Aspekte einer Krise berücksichtigt werden. Führungskräfte, die in der Lage sind, KI effektiv in ihre Entscheidungsprozesse zu integrieren, ohne dabei die menschliche Dimension zu vernachlässigen, könnten in Zukunft die erfolgreichsten Krisenmanager sein.

Fazit und Ausblick

Künstliche Intelligenz hat das Potenzial, ein wertvolles Werkzeug im Krisenmanagement zu sein, aber ihre Fähigkeit, echte Resilienz zu entwickeln, ist begrenzt. Resilienz erfordert eine Kombination aus Datenanalyse, emotionaler Intelligenz und menschlicher Intuition – eine Mischung, die bislang nur Menschen bieten können.

Die Zukunft könnte in hybriden Ansätzen liegen, bei denen KI und menschliche Führung Hand in Hand arbeiten, um Organisationen durch Krisen zu steuern. Führungskräfte müssen dabei lernen, die Stärken der KI zu nutzen, ohne die kritischen menschlichen Elemente aus den Augen zu verlieren. Denn letztlich ist es die menschliche Resilienz, die Organisationen in den schwierigsten Zeiten auf Kurs hält.

■ Chat-GPT 4o

Strategisches und operatives Resilienz-, Krisen- und Notfallmanagement für den Unternehmensausfall und die Wiederherstellung von Betriebsabläufen

■ Christian Paul, BSc, MA

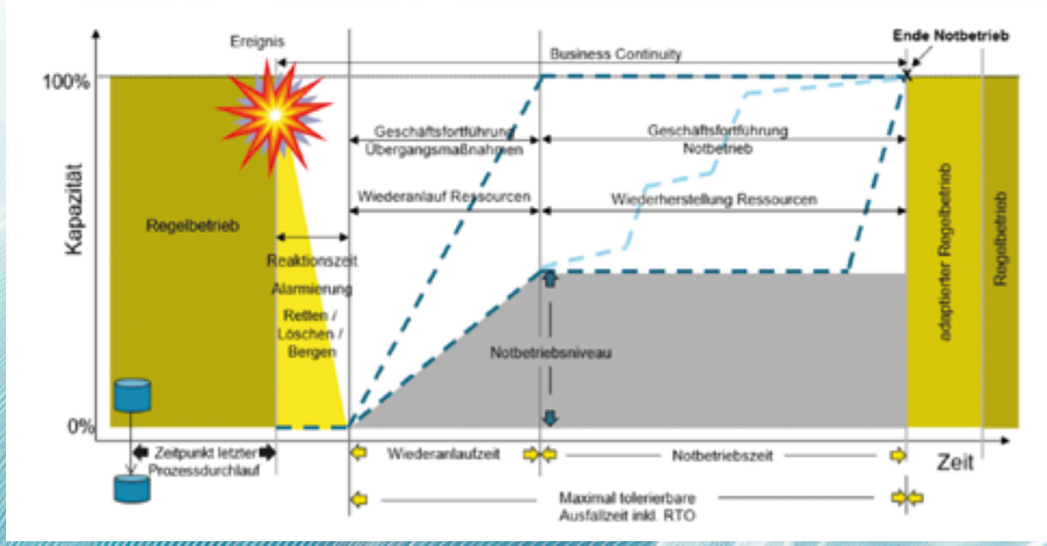
Resilienzmanagement vs. Business Continuity Management, was ist Teil wovon?

Unternehmen können aus verschiedensten Gründen in krisenhafte Situationen kommen, welche Strategiekrisen (strategische Fehleinschätzungen, Identitätsverluste), Erfolgskrisen (Verlust an Marktanteilen, Umsatz- und Ertragsrückgang) oder Liquiditätskrisen (Überkapazitäten, Liquiditätsproblem, Überschuldung) nach sich ziehen bzw. auch eine Insolvenz auslösen können. Die Ereignisse, welche solche krisenhaften Situationen, z. B. Supply Chain-Ereignisse auslösen, sind vielfältig und können enorme materielle und immaterielle Schäden verursachen und jedes Unternehmen oder Organisation ist gut beraten, wenn es seine Resilienz überprüft, um sich für mögliche Krisen präventiv vorzubereiten. Dies empfiehlt sich auch bei anstehenden M&A-Prozesse mitzuberücksichtigen, um M&A-Projekte erfolgreich gestalten und umsetzen zu können.

Resilienzmanagement hat sich als Buzzword in der Sicherheitscommunity in den vergangenen Jahren etabliert. Jedoch wird dies meist von unterschiedlichen Lösungs- und Beratungsanbietern als eine Art „Produkt" angepriesen. Bei Resilienz handelt es sich jedoch um eine Fähigkeit, welche die Widerstands- und Adaptionsfähigkeit im Fokus hat. Das klassische Kontinuitäts- und Krisenmanagement konzentriert sich auf die Wiederherstellung bzw. Minimierung von Betriebsprozessen nach Schadensereignissen.

Das Resilienzmanagement bietet jedoch einen integrierten Managementansatz, welcher auch strategisch nutzbar ist. Gesetzliche Rahmenbedingungen, NIS2 oder die RKE (Resilienz kritischer Einrichtungen) Richtlinie fordern von kritischen Organisationen, eine hohe Verfügbarkeit.

Das BCM hat seinen Fokus auf der Wiederherstellung des Normalbetriebes nach einem Ereignis und evaluiert in sogenannten Business Impact Analysen kritische Ressourcen, deren maximal tolerierbare Ausfallzeit (MTA) und die Wiederherstellungszeit (Recovery Time Objective RTO)



Das Resilienzmanagement evaluiert sogenannte adaptive Zyklen (Holling und Gunderson: 2002) systemisch und versucht so auch die unterschiedlichen Geschwindigkeiten von Systemen (z. B. Staat und Privat, IT und NonIT) zu betrachten. Der adaptive Zyklus kann entweder „revoltieren", sprich in einen schnelleren Zyklus wechseln oder sich erinnern und in einen lenksameren Zyklus wechseln. Jedes System, Organisation, Staat, Produkt, Projekt... besteht hierbei aus unzähligen adaptiven Zyklen. Jeder adaptive Zyklus besteht hierbei aus vier Phasen. Der Phase Wachstum, der Phase Erhaltung, der Phase Zerstörung und der Phase Erneuerung. Generelles Ziel ist hierbei durch alle angewandten Managementsysteme die Phase Wachstum so lange als mögliche auszudehnen, bzw. in der Erhaltung zu stabilisieren. Hier findet auch das BCM und Krisenmanagement seine Anwendung. Sollte das System in die Zerstörungsphase kommen, wird versucht, über Krisenmanagement die Reorganisationsphase zu beschleunigen. Somit werden die Analyseergebnisse nicht nur im BCM verwendet, sondern haben strategische Bedeutung für ein Unternehmen. Hauptfokus liegt hier bei der Adaptionsfähigkeit einer Organisation. Geschichtlich gesehen haben alle Organisationen, welche nach einem Großschadensereignis adaptiert wieder auf den Markt gekommen sind, überlebt. Organisationen, welche auf Veränderungen im Markt nicht reagiert haben oder konnten, mussten einen harten Restrukturierungskurs über sicher ergehen lassen (z. B. Nokia, Siemens Telefonie Sparte...) oder sind komplett am Markt verschwunden.

■ Christian Paul , BSc, MA

Blockchain-Technologie

Anwendungen und Potenziale für Unternehmen

Blockchain-Technologie ist längst nicht mehr nur ein Schlagwort im Zusammenhang mit Kryptowährungen. Die Technologie bietet weitreichende Anwendungsmöglichkeiten für Unternehmen, insbesondere in den Bereichen Transparenz, Sicherheit und Effizienz. Während Blockchain oft mit Bitcoin und anderen digitalen Währungen assoziiert wird, hat sie das Potenzial, zahlreiche Branchen zu transformieren, von der Finanzindustrie über das Supply Chain Management bis hin zum Gesundheitswesen. In diesem Artikel werden die verschiedenen Einsatzmöglichkeiten der Blockchain-Technologie für Unternehmen untersucht und die damit verbundenen Chancen und Herausforderungen beleuchtet.

Grundprinzipien der Blockchain-Technologie

Blockchain ist im Wesentlichen eine dezentrale und unveränderliche Datenbank, die Transaktionen in einer kontinuierlich erweiterten Liste von Datensätzen, den soge-

nannten Blöcken, speichert. Jeder Block enthält einen Zeitstempel und einen Verweis auf den vorherigen Block, wodurch eine Kette von Blöcken entsteht – daher der Name Blockchain. Diese Struktur macht die Blockchain besonders sicher, da nachträgliche Änderungen an einem Block die gesamte Kette verändern würden, was in einem dezentralen Netzwerk praktisch unmöglich ist. Die Unveränderlichkeit und Transparenz der Blockchain-Technologie sind wesentliche Merkmale, die sie von herkömmlichen Datenbanksystemen unterscheiden.

Die Dezentralisierung ist einer der Hauptvorteile der Blockchain-Technologie. Da die Daten auf vielen verschiedenen Knotenpunkten im Netzwerk gespeichert sind, gibt es keinen zentralen Punkt, der angegriffen oder manipuliert werden könnte. Dies macht Blockchain zu einer idealen Lösung für Anwendungen, bei denen Sicherheit und Integrität von entscheidender Bedeutung sind. Zudem ermöglicht die Technologie Transparenz, da alle Transaktionen öffentlich einsehbar sind und nicht verändert werden können. Dies schafft Vertrauen in digitale Prozesse und kann insbesondere in Branchen, in denen Vertrauen eine zentrale Rolle spielt, wie dem Finanzwesen oder der öffentlichen Verwaltung, erhebliche Vorteile bieten.

Ein weiterer Vorteil der Blockchain-Technologie ist ihre Effizienz. Durch den Einsatz von Smart Contracts – selbstausführenden Verträgen, die auf der Blockchain gespeichert sind – können Prozesse automatisiert und Zwischenhändler überflüssig gemacht werden. Dies spart nicht nur Zeit, sondern reduziert auch die Kosten und das Risiko menschlicher Fehler. Smart Contracts bieten zudem die Möglichkeit, komplexe Transaktionen sicher und zuverlässig durchzuführen, ohne dass eine zentrale Autorität erforderlich ist.

Anwendungen der Blockchain-Technologie in Unternehmen

Unternehmen aus verschiedenen Branchen beginnen, das Potenzial der Blockchain-Technologie zu erkennen und zu nutzen. Eine der am häufigsten diskutierten Anwendungen ist das Supply Chain Management. Durch die Verwendung von Blockchain können Unternehmen die gesamte Lieferkette transparent und nachvollziehbar gestalten. Jede Transaktion und jeder Schritt im Produktionsprozess kann in der Blockchain gespeichert und von allen Beteiligten eingesehen werden. Dies erhöht nicht nur die Transparenz, sondern auch die Effizienz, da fehlerhafte oder gefälschte Produkte schneller identifiziert und aus dem Verkehr gezogen werden können. In globalen Lieferketten, in denen zahlreiche Akteure involviert sind, bietet Blockchain die Möglichkeit, Prozesse zu harmonisieren und das Vertrauen zwischen den Partnern zu stärken.

Ein weiteres vielversprechendes Einsatzgebiet der Blockchain ist das Vertragsmanagement. Smart Contracts, also selbstausführende Verträge, die auf der Blockchain gespeichert sind, ermöglichen es Unternehmen, Verträge automatisch auszuführen, sobald bestimmte Bedingungen erfüllt sind. Dies reduziert den Bedarf an Intermediären und minimiert das Risiko von Vertragsbrüchen. Smart Contracts können in vielen Bereichen eingesetzt werden, von Finanztransaktionen über Immobiliengeschäfte bis hin zu Lizenzvereinbarungen. Durch die Automatisierung dieser Prozesse können Unternehmen nicht nur Kosten sparen, sondern auch die Effizienz und Genauigkeit ihrer Geschäftsvorgänge steigern.

Auch im Bereich der digitalen Identität bietet Blockchain innovative Lösungen. Die Technologie ermöglicht es, digitale Identitäten sicher und unveränderlich zu speichern, wodurch der Missbrauch von Identitäten erschwert wird. Dies ist besonders relevant in Branchen, die mit sensiblen Daten arbeiten, wie etwa im Gesundheitswesen oder im Finanzsektor. Durch den Einsatz von Blockchain können Unternehmen die Sicherheit und den Schutz personenbezogener Daten erheblich verbessern. Dies trägt nicht nur zum Schutz der Privatsphäre bei, sondern stärkt auch das Vertrauen der Kunden in die Sicherheit digitaler Dienstleistungen.

Zudem findet Blockchain-Technologie zunehmend Anwendung im Bereich des Urheberrechtsschutzes und der Verwaltung geistigen Eigentums. Künstler, Autoren und andere Kreative können ihre Werke in der Blockchain registrieren und so nachweislich ihre Urheberschaft sichern. Dies bietet einen wirksamen Schutz gegen Plagiate und Urheberrechtsverletzungen und ermöglicht es den Rechteinhabern, ihre Werke effizienter zu monetarisieren.

Potenziale und Herausforderungen der Blockchain-Technologie

Die Blockchain-Technologie bietet zahlreiche Potenziale, die weit über die bisher genannten Anwendungen hinausgehen. Eines der größten Potenziale liegt in der Möglichkeit, Vertrauen in digitale Transaktionen zu schaffen. In einer Welt, in der digitale Interaktionen und Transaktionen zunehmend an Bedeutung gewinnen, wird die Fähigkeit, Vertrauen zu schaffen, zu einem entscheidenden Wettbewerbsvorteil. Blockchain kann dazu beitragen, dieses Vertrauen zu etablieren, indem sie Transparenz und Sicherheit in einer bisher unerreichten Weise bietet. Unternehmen, die Blockchain nutzen, können dadurch nicht nur ihre internen Prozesse optimieren, sondern auch ihre Marktposition stärken.

Darüber hinaus kann Blockchain die Effizienz von Geschäftsprozessen erheblich steigern. Durch die Automatisierung von Transaktionen und die Reduzierung von Intermediären können Unternehmen Kosten sparen und die Geschwindigkeit ihrer Abläufe erhöhen. Dies ist besonders in globalen Lieferketten von Vorteil, wo die Koordination zwischen verschiedenen Akteuren oft komplex und zeitaufwändig ist. Blockchain bietet hier die Möglichkeit, Prozesse zu standardisieren und die Zusammenarbeit zwischen den Beteiligten zu verbessern, was letztlich zu einer schnelleren und zuverlässigeren Abwicklung führt.

Trotz dieser Vorteile stehen Unternehmen beim Einsatz von Blockchain auch vor Herausforderungen. Eine der größten Hürden ist die technische Komplexität der Technologie. Die Implementierung von Blockchain erfordert spezielles Fachwissen und erhebliche Investitionen in die IT-Infrastruktur. Darüber hinaus müssen Unternehmen sicherstellen, dass sie die rechtlichen und regulatorischen Anforderungen in den Märkten, in denen sie tätig sind, einhalten. Dies kann besonders schwierig sein, da die Regulierung von Blockchain in vielen Ländern noch in den Kinderschuhen steckt und sich ständig weiterentwickelt. Unternehmen müssen daher nicht nur technologische

Herausforderungen bewältigen, sondern auch sicherstellen, dass ihre Blockchain-Anwendungen den lokalen Gesetzen und Vorschriften entsprechen.

Ein weiteres Hindernis ist die Skalierbarkeit. Obwohl Blockchain für kleine Transaktionen und Netzwerke gut geeignet ist, kann die Technologie bei großen Netzwerken und Transaktionsvolumina an ihre Grenzen stoßen. Unternehmen müssen daher sorgfältig abwägen, ob die Implementierung von Blockchain in ihrem speziellen Anwendungsfall sinnvoll ist und welche Lösungen zur Überwindung von Skalierungsproblemen verfügbar sind. Dies könnte die Integration von sogenannten „Layer-2"-Lösungen beinhalten, die darauf abzielen, die Skalierbarkeit von Blockchains zu verbessern, oder den Einsatz von hybriden Modellen, die Blockchain nur für bestimmte Aspekte eines Prozesses verwenden.

Zusätzlich stellt die Interoperabilität zwischen verschiedenen Blockchain-Systemen eine Herausforderung dar. In einer global vernetzten Wirtschaft ist es wichtig, dass unterschiedliche Blockchains miteinander kommunizieren und Daten austauschen können. Die Entwicklung von Standards und Protokollen für die Interoperabilität wird entscheidend dafür sein, dass Blockchain-Technologie ihr volles Potenzial entfalten kann.

Blockchain als transformative Technologie

Die Blockchain-Technologie hat das Potenzial, die Art und Weise, wie Unternehmen ihre Geschäftsprozesse gestalten und abwickeln, grundlegend zu verändern. Von der Verbesserung der Transparenz in der Lieferkette bis hin zur Sicherstellung der Integrität digitaler Transaktionen bietet Blockchain zahlreiche Vorteile, die in einer zunehmend digitalisierten Welt von unschätzbarem Wert sind. Allerdings müssen Unternehmen die Herausforderungen, die mit der Implementierung dieser Technologie verbunden sind, sorgfältig berücksichtigen. Dazu gehört nicht nur die technische Komplexität, sondern auch die Einhaltung gesetzlicher Vorschriften und die Bewältigung von Skalierungsproblemen.

Unternehmen, die bereit sind, in Blockchain zu investieren und sich den damit verbundenen Herausforderungen zu stellen, können von erheblichen Wettbewerbsvorteilen profitieren. Die Technologie bietet die Möglichkeit, Vertrauen, Effizienz und Sicherheit in einer Weise zu fördern, die in der digitalen Wirtschaft entscheidend sein wird. In den kommenden Jahren wird sich zeigen, welche Unternehmen in der Lage sind, das Potenzial von Blockchain voll auszuschöpfen und sich so in einer sich schnell wandelnden Geschäftswelt zu behaupten. Unternehmen, die diese Technologie frühzeitig adaptieren und erfolgreich implementieren, könnten sich als Vorreiter in ihrer Branche etablieren und langfristig einen bedeutenden Wettbewerbsvorteil sichern.

■ Robert-P. Pelikan

Die Bedeutung der IT-Souveränität und die Auswirkungen des Nichterkennens von IT-Risiken

Das Konzept der IT-Souveränität gewinnt an Bedeutung, insbesondere in einer Zeit, in der Unternehmen zunehmend auf digitale Technologien angewiesen sind, um ihre Geschäftsprozesse zu unterstützen und Wettbewerbsvorteile zu sichern. IT-Souveränität bezieht sich auf die Fähigkeit eines Unternehmens, die Kontrolle über seine IT-Infrastruktur, Daten und Dienste zu behalten und unabhängig von externen Einflüssen Entscheidungen treffen zu können.

Die Nichtbeachtung dieses Aspekts kann erhebliche Sicherheits- und Betriebsrisiken mit sich bringen, wie das Beispiel des IT-Ausfalls bei CrowdStrike zeigt.

IT-Souveränität: Definition und Bedeutung

IT-Souveränität umfasst mehrere Schlüsselelemente:

- Kontrolle über Daten: Die Fähigkeit, zu bestimmen, wo und wie Daten gespeichert, verarbeitet und übertragen werden.
- Unabhängigkeit von Drittanbietern: Reduzierung der Abhängigkeit von externen IT-Dienstleistern, insbesondere in kritischen Bereichen der IT-Infrastruktur.
- Eigene IT-Kompetenzen: Aufbau interner Kapazitäten zur Entwicklung, Wartung und Sicherung von IT-Systemen und IT-Anwendungen.

Der Fall CrowdStrike: Ein Lehrbeispiel für IT-Risiken

Der Ausfall bei CrowdStrike, einem führenden Anbieter von Cybersicherheitsdiensten, veranschaulicht eindrucksvoll die potenziellen Risiken einer mangelnden IT-Souveränität. Viele Unternehmen, die auf die Sicherheitsdienste von CrowdStrike angewiesen waren, erlebten erhebliche Betriebsunterbrechungen. Dieser Vorfall zeigt, wie die Abhängigkeit von externen IT-Dienstleistern zu einem kritischen Risiko werden kann, wenn diese IT-Dienstleister ausfallen oder ihre IT-Dienstleistungen nicht wie erwartet erbringen.

Auswirkungen des Nichterkennens von IT-Souveränitätsrisiken:

- Betriebsunterbrechungen: Ohne adäquate IT-Alternativen oder IT-Notfallpläne können IT-Ausfälle bei Drittanbietern zu erheblichen Unterbrechungen führen, die direkte finanzielle Verluste und Beeinträchtigungen der Kundendienstleistungen verursachen.
- Datenverlust oder -kompromittierung: Die Unfähigkeit, die Kontrolle über die eigenen Daten zu wahren, kann zu Datenverlusten oder Datenschutzverletzungen führen, insbesondere wenn externe IT-Anbieter von IT-Sicherheitslücken betroffen sind.
- Reputationsverlust: Vorfälle, die die IT-Sicherheit oder Verfügbarkeit der Dienste beeinträchtigen, können das Vertrauen der Kundinnen sowie der Kunden untergraben und langfristige Schäden am Markenimage verursachen.
- Rechtliche und finanzielle Konsequenzen: Nichteinhaltung von IT-Compliance-Anforderungen, insbesondere im Hinblick auf Datenschutz und IT-Sicherheit, kann zu rechtlichen Sanktionen und hohen Strafen führen.

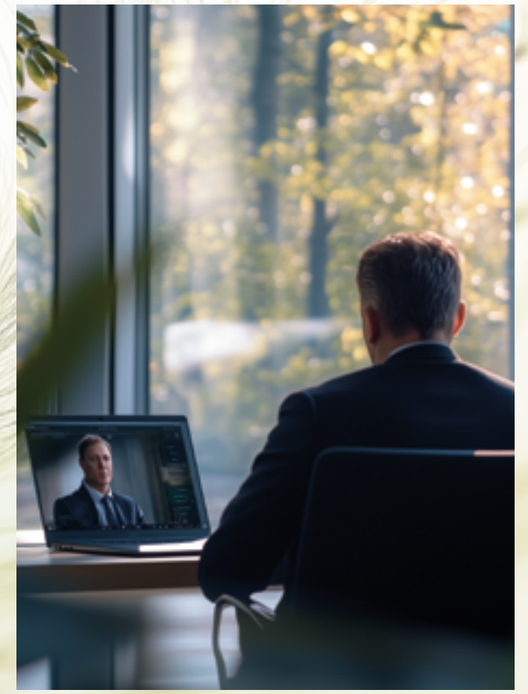
Der rechtliche Rahmen der NIS-2-Richtlinie und der RCE-Richtlinie

Die Einhaltung von Vorschriften wie die EU-Richtlinie 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) und die EU-Richtlinie 2022/2557 über die Resilienz kritischer Einrichtungen (RCE-Richtlinie) sind zentral für die Stärkung der Cybersicherheit und der Resilienz kritischer Infrastrukturen in der EU. Deren strategische Relevanz für das Management lassen sich aus mehreren Schlüsselaspekten erklären:

1. **Gesetzliche Verpflichtung und regulatorische Anforderungen**
   Die NIS-2-Richtlinie und RCE-Richtlinie sind keine optionalen Best Practices, sondern verbindliche rechtliche Anforderungen, die von der Europäischen Union erlassen wurden, um die Sicherheit und Resilienz von Netz- und Informationssystemen sowie kritischen Infrastrukturen zu stärken. Diese Richtlinien legen spezifische Sicherheitsmaßnahmen fest, die Unternehmen implementieren müssen, sowie Berichtspflichten bei Sicherheitsvorfällen. Das Management muss diese Vorschriften einhalten, um rechtliche Sanktionen zu vermeiden, die von Geldbußen bis zu weiteren regulatorischen Eingriffen reichen können.

2. **Risikomanagement und finanzielle Auswirkungen**
   Die Nichtbeachtung dieser Richtlinien kann zu erheblichen direkten und indirekten Kosten führen. Direkte Kosten entstehen durch Strafen und Bußgelder, die durch Nichteinhaltung der gesetzlichen Vorgaben ausgelöst werden. Indirekte Kosten können durch Betriebsunterbrechung-en, Datenverluste und Reputationsschäden entstehen, die aus unzureichenden Sicherheitsmaßnahmen resultieren. Durch die Einhaltung dieser Richtlinien können Unternehmen das Risiko von Cyberangriffen und anderen Sicherheitsvorfällen minimieren und somit potenzielle finanzielle Schäden reduzieren.

3. **Vertrauen und Marktstellung**



Unternehmen, die nachweislich hohe Standards in der Cyberresilienz und Datenschutz einhalten, stärken das Vertrauen ihrer Kundinnen, Kunden, Partnerinnen, Partner, Investorinnen und Investoren. In einer zunehmend vernetzten Welt, in der Verbraucherinnen, Verbraucher und Geschäftspartnerinnen, Geschäftspartner immer sensibler auf Datenschutz- und Sicherheitsfragen reagieren, kann die Einhaltung dieser Richtlinien als ein Wettbewerbsvorteil dienen. Unternehmen, die ihre IT-Compliance als Teil ihrer Markenidentität hervorheben, können ihre Marktstellung verbessern und sich als vertrauenswürdige Akteure etablieren.

4. **Betriebliche Resilienz und Kontinuität**
   Die EU-Richtlinien fordern Unternehmen auf, nicht nur präventive Maßnahmen zu ergreifen, sondern auch effektive Notfall- und Wiederherstellungspläne zu entwickeln. Dies ist entscheidend, um die betriebliche Kontinuität im Falle eines IT-Sicherheitsvorfalls sicherzustellen. Eine solche Vorbereitung hilft Unternehmen, schnell auf Vorfälle zu reagieren und die Auswirkungen auf den Betrieb zu minimieren, was letztlich die langfristige Lebensfähigkeit des Unternehmens sichert.

5. **Strategische Planung und Wettbewerbsfähigkeit**
   Auf Managementebene ermöglicht die Einhaltung von NIS-2-Richtlinie und RCE-Richtlinie den Unternehmen, ihre IT-Sicherheitsstrategie zu stärken und besser auf zukünftige Herausforderungen vorbereitet zu sein. Dies fördert eine Kultur der ständigen Verbesserung und Innovation, die nicht nur IT-Sicherheitsrisiken minimiert, sondern auch die allgemeine Wettbewerbsfähigkeit des Unternehmens fördert.

Die Integration von IT-Souveränität und IT-Compliance in die Unternehmensstrategie ist eine komplexe Aufgabe, die weit über die technische Implementierung hinausgeht. Sie erfordert eine Neubewertung der Risikomanagementstrategien und der Investitionsprioritäten.

Das Management muss eine integrierte Strategie entwickeln, die sowohl IT-Souveränität als auch IT-Compliance umfasst:

1. **Technologieauswahl: Entscheidungen über Betriebssysteme, Software und Cloud-Lösungen müssen die Unabhängigkeit und Kontrolle des Unternehmens maximieren.**
2. **Diversifikation von Dienstleistern: Um Risiken zu minimieren, sollte das Unternehmen nicht von einem einzelnen Anbieter abhängig sein.**
3. **Investition in interne Kapazitäten: Der Aufbau interner Ressourcen für kritische IT-Funktionen kann die Abhängigkeit von externen Dienstleistern reduzieren und die Kontrolle über die IT-Sicherheit stärken.**

4. **Schulung und Bewusstsein: Das Bewusstsein für Cybersicherheit muss unter den Mitarbeitern gefördert werden, um eine Kultur der Sicherheit zu etablieren.**
5. **Risikomanagement und IT-Compliance: Kontinuierliche Bewertungen und Anpassungen der Sicherheits- und IT-Compliance-Strategien sind erforderlich, um auf sich ändernde Bedrohungen und regulatorische Anforderungen zu reagieren.**

Die Rolle des Managements: Über die IT-Abteilung hinaus

Die Verantwortung für IT-Sicherheit und IT-Compliance kann nicht allein bei der IT-Abteilung liegen. Sie ist eine strategische Aufgabe, die direkt in die Unternehmensführung eingebettet sein muss:

- Strategische Priorisierung: IT-Sicherheit muss als integraler Bestandteil der Unternehmensstrategie angesehen werden.
- Ressourcenzuweisung: Ausreichende Budgets und Ressourcen müssen bereitgestellt werden, um die IT-Sicherheit und IT-Compliance zu unterstützen.
- Führung und Kultur: Das Management muss eine Kultur der Sicherheit und des Risikobewusstseins fördern.

Dabei darf das Management nicht vergessen, dass neue Technologien wie künstliche Intelligenz in der Cyberabwehr, Blockchain zur Sicherung der Datenintegrität und der Einsatz von Quantum Computing zur Datenverschlüsselung die IT-Sicherheitslandschaft verändern werden. Unternehmen müssen diese Technologien evaluieren und gegebenenfalls integrieren, um ihre Daten besser zu schützen und die IT-Souveränität zu stärken.

Strategie zur Bewältigung von IT-Risiken und Einhaltung von IT-Compliance für das Management

Im Folgenden wird ein Beispiel für eine Strategie präsentiert, die das Management mittlerer und großer Unternehmen dabei unterstützt, die Anforderungen der NIS-2-Richtlinie und der RCE-Richtlinie umzusetzen. Diese Beispielstrategie zielt darauf ab, die Handlungsfähigkeit des Managements in Bezug auf IT-Risiken und IT-Compliance zu stärken und die potenziellen finanziellen Strafen für Nichteinhaltung zu vermeiden.

1. **Verständnis der rechtlichen Anforderungen**
   Das Management muss ein klares Verständnis der spezifischen Anforderungen der NIS-2-Richtlinie und der RCE-Richtlinie entwickeln. Dazu gehört die Kenntnis darüber, welche Daten geschützt werden müssen, welche Sicherheitsmaßnahmen erforderlich sind und welche Meldepflichten bestehen.

2. **Risikobewertung durchführen**
   Führen Sie eine umfassende Risikobewertung durch, um alle potenziellen IT-Risiken zu identifizieren, die sich auf die Sicherheit und Compliance auswirken könnten. Bewertungen sollten regelmäßig aktualisiert werden, um neue und sich entwickelnde Risiken zu berücksichtigen.

3. **Bewertung der Anbieterabhängigkeit**
   Überprüfen Sie regelmäßig das Ausmaß der Abhängigkeit von externen IT-Dienstleistern. Bewerten Sie das Risiko und die Auswirkungen, die sich aus dieser Abhängigkeit ergeben könnten, und entwickeln Sie Strategien zur Risikominderung.

4. **Aufbau interner Fähigkeiten**
   Investieren Sie in den Aufbau interner IT-Kompetenzen, um kritische Funktionen und Dienste unabhängig verwalten zu können. Dies erhöht die Kontrolle und Flexibilität und reduziert die Abhängigkeit von Drittanbietern.

5. **Entwicklung einer IT-Sicherheitspolitik**
   Entwickeln Sie eine detaillierte IT-Sicherheitspolitik, die auf den Ergebnissen der Risikobewertung basiert. Diese Politik sollte klare Richtlinien für die Verwendung, den Schutz und die Überwachung von IT-Ressourcen enthalten.

6. **Implementierung von Sicherheitsmaßnahmen**
   Implementieren Sie technische und organisatorische Sicherheitsmaßnahmen, um identifizierte Risiken zu mitigieren. Dazu gehören Verschlüsselungstechniken, Zugangskontrollen u.v.m. sowie regelmäßige Sicherheitsaudits.

7. **Incident Response Plan erstellen**
   Erstellen Sie einen detaillierten Incident Response Plan, der klare Anweisungen enthält, wie im Falle eines IT-Sicherheitsvorfalls zu verfahren ist. Der Plan sollte Verfahren für die schnelle Identifikation, Untersuchung und Behebung von IT-Sicherheitsvorfällen umfassen.

8. **Implementierung von Notfallplänen**
   Entwickeln Sie umfassende Notfall- und Wiederherstellungspläne, die es Ihrem Unternehmen ermöglichen, bei einem Ausfall interner bzw. externer IT-Services schnell zu reagieren und die Betriebskontinuität aufrechtzuerhalten.

9. **Schulung und Bewusstseinsbildung**
   Schulen Sie regelmäßig alle Mitarbeiter in Bezug auf Cybersicherheitspraktiken und die Bedeutung des Datenschutzes. Stellen Sie sicher, dass alle Beteiligten die Sicherheitspolitik verstehen und umsetzen können.

10. **IT-Compliance-Überwachung und -Auditierung**
    Richten Sie ein System zur Überwachung der Einhaltung aller relevanten Gesetze und Vorschriften ein. Führen Sie regelmäßige IT-Compliance-Audits durch, um sicherzustellen, dass alle Unternehmensbereiche den regulatorischen Anforderungen entsprechen.

11. **Kommunikation und Berichterstattung**
    Entwickeln Sie ein effektives Kommunikationsprotokoll für den Fall von Sicherheitsvorfällen, das den Anforderungen der NIS-2-Richtlinie entspricht. Stellen Sie sicher, dass alle relevanten Stakeholder, einschließlich der zuständigen Behörden, zeitnah informiert werden.

12. **Überprüfung und kontinuierliche Verbesserung**
    mentierten Sicherheitsmaßnahmen und passen Sie sie an sich ändernde Bedingungen an. Nutzen Sie die Erkenntnisse aus Sicherheitsvorfällen und Audits, um kontinuierliche Verbesserungen vorzunehmen.

Vorbereitung auf Sanktionen

Verstehen Sie die möglichen finanziellen und rechtlichen Konsequenzen einer Nichteinhaltung der Vorschriften. Stellen Sie sicher, dass das Unternehmen finanziell und operativ auf mögliche Geldstrafen vorbereitet ist, die aus der Nichteinhaltung resultieren können.

Fazit

Die Integration von IT-Souveränität und IT-Compliance in die Unternehmensstrategie ist eine der größten Herausforderungen für das Management in der heutigen digitalisierten Welt. Durch die strategische Verankerung dieser Prinzipien kann das Management nicht nur regulatorische Anforderungen erfüllen, sondern auch eine robustere, widerstandsfähigere Organisation schaffen. Es reicht nicht aus, diese Aufgaben ausschließlich den IT-Fachabteilungen zu überlassen. Vielmehr ist eine fortlaufende Beteiligung und Überwachung durch das Top-Management erforderlich, um die Risiken zu managen und die Einhaltung der gesetzlichen Anforderungen sicherzustellen. Nur durch eine integrierte und ganzheitliche Herangehensweise können Unternehmen die Sicherheit ihrer Daten und Systeme effektiv gewährleisten und die Resilienz gegenüber IT-Risiken stärken. Die Ereignisse wie der Ausfall bei CrowdStrike zeigen, dass es essenziell ist, proaktiv zu handeln und die Kontrolle über die technologischen Ressourcen und Daten des Unternehmens zu wahren.

Ing. Franz Hoheiser-Pförtner, MSc

Mehr als nur Backup und Wiederherstellung

Cyber Recovery schafft wirkliche Datensicherheit

Ob durch Social Engineering oder kompromittierte Anmeldedaten: Cyberkriminelle finden stets Wege, Sicherheitsmaßnahmen zu umgehen und sich Zugriff auf unternehmenskritische Infrastrukturen und Daten zu verschaffen. Hinzu kommt, dass Angreifer durch künstliche Intelligenz heute effektiver denn je sind, komplexe Attacken in großem Umfang auszuführen, die auf Backups zielen und diese kompromittieren. Für eine robuste Cyberresilienz müssen Unternehmen daher Datensicherheit, Datensicherung und eine Malware-freie Wiederherstellung der angegriffenen IT in einer Cyberrecovery verbinden.

Cyberresiliente Datensicherheit und Datensicherung basieren auf einer zuverlässigen und sauberen Wiederherstellung von Systemen, Applikationen und Daten in Kombination mit Tools zum Erkennen von Angriffen. Hierfür müssen operative IT und IT-Sicherheit effektiv zusammenarbeiten, um sowohl präventiv Sicherheitslücken aufzudecken sowie robuste Cyber-Recovery-Pläne zu erstellen und zu testen als auch im Ernstfall die Infrastruktur und die Daten aus einem Malware-freien, aktuellen Backup sicher wiederherzustellen.

Cyberresiliente Recovery

In der IT gibt es drei Arten, Daten wiederherzustellen: Operational, Desaster und Cyber Recovery. Alle machen Daten, Systeme und Anwendungen nach einem Zwischenfall wieder verfügbar, haben jedoch unterschiedliche Einsatzbereiche: Operational Recovery bezieht sich auf bestimmte Komponenten des Systems, Dateien, Applikationen oder virtuelle Maschinen nach einem kleineren Zwischenfall oder Ausfall. Sie umfasst das Wiederherstellen versehentlich gelöschter Dateien, die Recovery nach Abstürzen oder Softwarefehlern sowie das Reparieren beschädigter Daten. Desaster Recovery umfasst ganze Systeme und Infrastrukturen nach einem Großereignis wie einer Naturkatastrophe. Gegen Angriffe von Cyberkriminellen hilft nur eine Cyber Recovery. Denn ein Verschlüsseln von Daten oder die erfolgreiche Infiltration spionierender Hacker in das eigene Netz verlangt eine andere Antwort als ein Hardware-Ausfall oder ein logischer Datenverlust.

Herkömmliche Desaster-Recovery-Pläne haben Schwierigkeiten, den differenzierten Risiken und der Komplexität von Cyberangriffen wirksam zu begegnen. Das hat folgende Gründe:

- Art der Gefahren: Im Gegensatz zu Naturkatastrophen oder Hardwareausfällen handelt es sich etwa bei einer Ransomware-Attacke um vorsätzliche Angriffe. Cyberkriminelle nutzen Schwachstellen aus und haben es auf für das Unternehmen unverzichtbare oder für sie monetarisierbare Daten abgesehen. Dies erfordert einen sorgfältigeren, stärker auf Datensicherheit ausgerichteten und ein Risikomanagement einschließenden Ansatz der Datensicherung.
- Umfang und Schwerpunkt: Bei der Desaster Recovery geht es darum, Systeme und Daten wieder verfügbar zu machen und die Ausfallzeit zu minimieren. Bei der Cyber Recovery liegt ein weiterer Schwerpunkt darauf, den Angriff zu isolieren, die Präsenz der Hacker im Netz zu beseitigen und das von Malware und Manipulationen freie Wiedereinspielen der Daten vorzubereiten. Darüber hinaus verbessern forensische Analysen das Schließen von Schwachstellen und möglicherweise längere Sanierungsprozesse die Sicherheitslage.
- Methoden und Werkzeuge: Die Desaster Recovery basiert in der Regel auf leicht verfügbaren Backups in Kombination mit Replikation und etablierten Verfahren für ein schnelles Rollback des Systems. Für die Cyber Recovery sind darüber hinaus Tools und Fachkenntnisse in den Bereichen Malware-Analyse, Incident Response, unveränderliche/unlesbare Backups, eine Reinraumumgebung für sauber wiederhergestellte Daten, das Erkennen von Anomalien und sichere Datenextraktion erforderlich.
- Datenintegrität und Anfälligkeit: Desaster-Recovery-Pläne sind nicht in der Lage, die letzten noch sauberen Backup-Sätze effektiv zu identifizieren und wiederherzustellen. Außerdem müssen die IT-Verantwortlichen während des Angriffs ausgenutzte Sicherheitslücken bedenken und vor dem Einspielen des sauberen Backups patchen, was die Rekonstruktion noch komplexer macht.

Digitale Reinräume als Schauplatz für Cyber Recovery

Ein digitaler Reinraum – ein Cleanroom – bietet eine klinisch reine Umgebung für eine saubere Recovery der Daten nach einem Angriff und ein erschwingliches Testfeld, um die Prozesse für das Wiederherstellen der IT zu optimieren.

Im Fall einer Infektion von Backup-Datensätzen ermöglicht ein Cleanroom mit isolierter Recovery-Umgebung und Sandbox-Funktionen, integre und nicht manipulierte Daten aus nicht infizierten Backup-Quellen oder aus dem Snapshot eines bislang nicht angegriffenen Backups zu extrahieren. Ein solcher Reinraum spielt zudem eine entscheidende Rolle als Schauplatz für sichere, kostengünstige und flexible Tests sowie als isolierter und sauberer Ort, um ausgenutzte Schwachstellen zu analysieren, Daten wiederherzustellen und Systeme zu sanieren. Wenn die IT-Verantwortlichen einen solchen Reinraum erst on demand in der Cloud anlegen und er nicht im Vorhinein existiert, kann er durch Angriffe im Vorfeld nicht zu Schaden gekommen sein. Es entstehen keine laufenden Kosten für ihn.

Zudem bietet ein Cleanroom einen kontrollierten Raum für forensische Analysen, um die Ursache und den Verlauf eines Angriffs zu untersuchen und Folgeattacken zu verhindern. Die notwendigen Patches lassen sich ebenfalls hier testen.

KI-basiertes und automatisiertes Backup-Management

Für effektive Datensicherheit und -sicherung können Cyber-Recovery-Plattformen auf Basis künstlicher Intelligenz (KI) und Maschine Learning (ML) maßgeblich zur Resilienz des Backup-Betriebs und für optimierte Abläufe beitragen sowie beim Schutz der Informationen unterstützen.

Dank kontinuierlich gesammelter Leistungsdaten aus den Backup-Vorgängen, kann KI in Kombination mit Machine Learning ein Modell des typischen Verhaltens einzelner Backup-Prozesse entwickeln, um Anomalien zu identifizieren. Zugleich erkennt eine Plattform weitere Risiken, wie z. B. einen drohenden oder erfolgten Angriff auf Backup-Dateien.

Aufgrund der heutigen, komplexen Datenumgebungen sind ein effizientes und fehlerfreies Scheduling und Überwachen der zahlreichen Backup-Jobs kaum ohne einen automatisierten Prozess zu bewerkstelligen.

■ Nicolas Veltzé

Abb. 1: (Cleanroom Home): Die Basis für Cyber Recovery ist ein grundlegendes Risikomanagement durch eine Plattform für cyberresiliente Datensicherheit und Datensicherung.

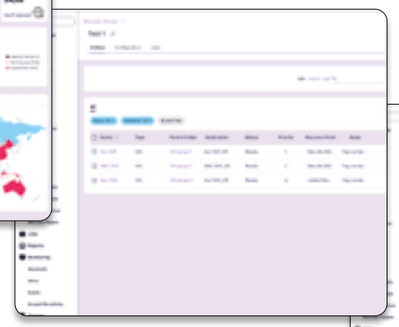


Abb. 2: (Cleanroom Recovery 5) Durchführen von Tests und Bestimmung eines optimalen sauberen RPO für die Wiederherstellung.

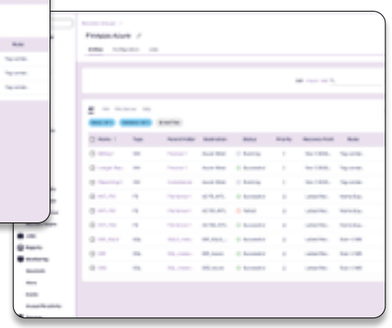


Abb. 3: (Cleanroom Recovery 8.2) Übersicht über getestete Recovery-Vorgänge in einem Cleanroom.

KI und Edge erhöhen die Sicherheit am Arbeitsplatz

Edge Computing und künstliche Intelligenz haben enormes Potenzial: Richtig eingesetzt, können öffentliche und systemrelevante Organisationen Ihre Effizienz und Produktivität steigern. Überdies erhöhen diese Technologien gerade in Kombination miteinander auch den Schutz der Mitarbeiter.

Für Mitarbeiter, die Ihren Dienst im Field Service des öffentlichen Bereiches, in der kritischen Infrastruktur, in der Energieversorgung oder im öffentlichen Verkehr außerhalb eines Büros verrichten, ist das Potenzial für Gefahren vergleichsweise höher als in der Verwaltung. Welche Möglichkeiten gerade KI und Edge Computing bieten, erklärt Dell Technologies.

Predictive Maintenance: Unfälle verhindern, bevor sie passieren

Eine große Gefahr für mobile Mitarbeiter oder Mitarbeiter in Außenanlagen geht häufig von wartungsbedürftigen Maschinen aus. Sobald Teile verschleißen, erhöht sich automatisch das Risiko eines Zwischenfalls. Predictive Maintenance, also eine vorausschauende Wartung, ermöglicht den Verantwortlichen, Zwischenfälle zu verhindern, bevor sie passieren. In diesem Kontext wertet eine künstliche Intelligenz kontinuierlich Sensordaten aus und sagt exakt voraus, wann Teile ausgetauscht oder repariert werden müssen. Die Daten gelangen von den OT (Operational Technology)-Geräten über ein IoT Gateway in der Regel in die Cloud, wo sie gesammelt und von der KI verwertet werden. Ein weiterer positiver Nebeneffekt von Predictive Maintenance ist, dass keine unnötigen Wartungsarbeiten durchgeführt werden müssen.

Sensorik, KI und Edge Computing: Gefahren in Echtzeit managen

Ausgestattet mit einem Edge Gateway, können die Sensoren der Außenanlagen die Daten auch an Edge-Server vor Ort für die direkte Verarbeitung und Überprüfung in Echtzeit weiterleiten. Ohne den Umweg in die Cloud sind KI-Anwendungen in der Lage, Gefahrenlagen zu erkennen und umgehend Gegenmaßnahmen zu ergreifen. Das kann bedeuten, dass die künstliche Intelligenz die Mechanismen anpasst oder pausiert und das Personal darüber informiert.

Computer Vision: Kameraüberwachung mit Köpfchen

KI und Edge Computing heben auch die Kameraüberwachung auf ein neues Level. Mit sogenannter Computer Vision können Organisationen durch eine künstliche Intelligenz Live-Bilder vom Arbeitsplatz in Echtzeit auf einem Edge-Server verarbeiten und auswerten lassen. Betritt ein Mensch etwa ohne Schutzkleidung einen Gefahrenbereich, könnte die KI umgehend Alarm schlagen. Organisationen statten auf diese Weise ihre Kameras mit Intelligenz aus und erhöhen die Betriebssicherheit enorm. Auf ähnliche Weise erhöhen intelligente Kameras auch den Perimeterschutz von sensiblen, öffentlichen Plätzen und Anlagen. KI-Modelle sind heute komplex trainierbar und können Gefahrenlagen sehr zuverlässig erkennen – so beispielsweise auch, ob sich jemand auffällig oder aggressiv verhält. Computer-Vision-Anwendungen können so etwa das Sicherheitspersonal unterstützen.

„Einfach nur Bilder aufzunehmen oder Sensordaten zu speichern, ist heute nicht mehr zeitgemäß“, erklärt Andreas Haberlehner, Leader Sales Public & Healthcare bei Dell Technologies in Österreich. „Sicherheitsteams und Techniker haben in der Regel nicht die Zeit, alle vorhandenen Daten auszuwerten und in Kontext zueinander zu stellen. Das ging früher zulasten der Produktivität und hat die Kosten erhöht. Heute haben Organisationen durch künstliche Intelligenz und Edge Computing nicht nur neue Möglichkeiten, um effizienter zu arbeiten, sondern auch um ihr Personal wirksam zu schützen.“

■ Mag. Andreas Haberlehner

Netzwerksicherheit ist die Grundvoraussetzung

Sicherheit für expandierende Netzwerke ohne Kopfschmerzen

Netzwerksicherheit ist eine Notwendigkeit – keine zusätzliche Funktionalität. Wie aber können Verantwortliche die Netzwerksicherheit verbessern, ohne eine weitere Anwendung oder ein zusätzliches Gerät verwalten zu müssen?

In einer Zeit, in der Verantwortliche in Unternehmen eine ständig wachsende Anzahl von Endgeräten managen müssen, konvergieren Netzwerk- und Sicherheitsfragen immer mehr. Das setzt IT-Teams zunehmend unter Druck. Denn jede weitere Netzwerkerweiterung bedeutet gleichzeitig auch einen zusätzlichen Verwaltungsaufwand. Was kann also die Lösung sein? Ein einheitliches Konzept für den Netzwerkzugriff ist die Antwort.

Wie würden sich die Dinge ändern, wenn die Sicherheit als grundlegendes Konzept des Netzwerks und nicht als nachträgliche Funktionalität behandelt würde? Wie wäre es, wenn Sicherheit – wie alles im Netzwerkdesign – aus der Sicht des Anwenders betrachtet würde und nicht als Kompromiss mit Skalierbarkeit oder Agilität?

Ein sicheres Netzwerk an jedem Ort

Wenn die Netzwerksicherheit als grundlegendes Konzept des Netzwerks und nicht als nachträgliche Funktionalität betrachtet wird, ergeben sich sowohl für das Unternehmen als auch für die Nutzer des Netzwerks klare Vorteile. Denn ist die Netzwerksicherheit eine zusätzliche Funktionalität, dann muss sie separat gemanagt werden und beinhaltet oft Richtlinien und Funktionen, die nicht mit dem regulären Netzwerkbetrieb übereinstimmen. Als grundlegendes Element des Netzes ist der Schutz der Daten, die durch jede Interaktion fließen, jedoch Teil des gesamten Netzbetriebs. Hier liegt der Schlüssel, um die Sicherheit an jedem Punkt der User Journey zu gewährleisten.

Genau das ermöglicht ExtremeCloud Universal ZTNA. In einer einzigen Lösung, die Cloud NAC und ZTNA kombiniert, bietet sie Unternehmen sichere Konnektivität an jedem Ort, Skalierbarkeit und Reichweite sowie Transparenz in Echtzeit.

Auf diese Weise können Anwender nahtlos – mit demselben Datenschutz wie im Büro – von einem Café, einem Flughafen oder auf dem Campus auf Anwendungen zugreifen. Gleichzeitig können die Netzwerkbetreiber die Sicherheit zuverlässig verwalten, dank der integrierten identitätsbasierten Zero-Trust-Policy-Engine der Lösung. Dadurch wird der Verwaltungsaufwand verringert, da die Lösung sowohl auf Netzwerke als auch auf Anwendungen angewendet werden kann und mit weniger Tools für Konsistenz sorgt.

Mehr Transparenz und Kontrolle

Eine einzige cloudbasierte Lösung mit einer einzigen Lizenz vereinfacht das Management. IT-Abteilungen können Benutzer und Endgeräte von einem cloudbasierten Dashboard aus steuern. Die Integration von Mobile Device Management (MDM) und Identity Provider (IDP) bietet netzwerkweite Transparenz sowie Geräteverifizierung und Multi-Faktor-Authentifizierung (MFA). Dieses Maß an Kontrolle und Transparenz ermöglicht proaktives statt reaktives Handeln.

Auf dem Weg zu Zero Trust

Während die IT strategische Themen umsetzt, übernimmt die Extreme-Lösung im Hintergrund Aufgaben wie die Automatisierung von Onboarding-Prozessen, Konfiguration und Richtliniendurchsetzung. Alle cloudbasierten Universal-Plattformen von Extreme verfügen über diese Funktion, die die Sicherheit im gesamten Netzwerk verbessert und die IT zu einem ganzheitlicheren Zero-Trust Ansatz führt.

Netzwerksicherheit ohne Kopfschmerzen

Unternehmen stehen unter dem Druck, dem Nutzer ein intuitives, konsistentes und dennoch sicheres Arbeiten zu ermöglichen. Die heute verfügbaren Einzellösungen erhöhen häufig jedoch die Komplexität eines bereits hochkomplexen Netzwerks. Extreme Universal ZTNA ist eine innovative Lösung, die Mehrwert, Transparenz und Einfachheit bietet, indem sie die Sicherheit als grundlegenden Bestandteil des Netzwerks integriert. Durch die Integration von Sicherheit in das Netzwerk wird das Management vereinfacht, während gleichzeitig neue Ebenen der Kontrolle und Transparenz geschaffen werden, die das strategische Wachstum von Unternehmen unterstützen.

Weiter Informationen zu Universal ZTNA finden Sie hier:
https://www.extremenetworks.com/solutions/security/ztna

Dipl.-Inf. (FH) André Herkenrath

Cyber Security im digitalen Zeitalter: Wesentliche Sicherheitsprinzipien für Unternehmen und Privatpersonen

Die wachsende Bedeutung der Cybersicherheit

Im Zeitalter der digitalen Transformation haben Cyber Security, Cyber Defence und Cyber Abwehr eine zentrale Bedeutung erlangt. Diese Konzepte sind nicht nur für Führungskräfte wie CEOs und CISOs von entscheidender Relevanz, sondern betreffen jeden Einzelnen, der sich in der zunehmend vernetzten Welt bewegt. Cybersicherheit ist heute ein integraler Bestandteil des täglichen Lebens und der Geschäftsprozesse, und das Bewusstsein für die damit verbundenen Risiken muss geschärft werden.

Fünf fundamentale Sicherheitsprinzipien zur Risikominderung

Um den ständig wachsenden Bedrohungen im Cyberspace zu begegnen, sollten folgende fünf Sicherheitsprinzipien konsequent in den Fokus gerückt werden:

1. **Implementierung schreibgeschützter Betriebssysteme:**
   Der Einsatz von schreibgeschützten, insbesondere Linux-basierten Betriebssystemen, bietet einen robusten Schutz gegen die unbefugte Installation von Malware durch Endanwender. Diese Betriebssysteme minimieren die Angriffsmöglichkeiten durch Phishing-Versuche, Ransomware und andere bösartige Cyberangriffe, da sie das Einschleusen und Ausführen von Schadsoftware durch strikte Zugriffskontrollen und Sandbox-Mechanismen verhindern. In einer Architektur mit minimalen Zugriffsrechten (Least Privilege) werden potenzielle Angriffsvektoren erheblich reduziert.

2. **Vermeidung lokaler Datenspeicherung:**
   Die Vermeidung der Speicherung sensibler Daten – wie Kundeninformationen, Finanzdaten und persönliche Daten – auf Endgeräten und angeschlossenen externen Speichergeräten ist essenziell, um die Datensicherheit zu gewährleisten. Durch die Nutzung zentraler und sicherer Cloud-Infrastrukturen oder verschlüsselter Datenbanken bleibt die Integrität und Vertraulichkeit der Daten auch im Falle eines Geräteverlusts oder Diebstahls gewahrt. Eine strategische Datenarchitektur, die auf dem Prinzip der Datenminimierung basiert, trägt maßgeblich zur Reduzierung des Risikos von Datenverlusten und -lecks bei.

3. **Nutzung vertrauenswürdiger Anwendungsplattformen:**
   Ein durchgängig abgesicherter Bootprozess (Trusted Boot) gewährleistet, dass das Betriebssystem bei jedem Neustart in einen sicheren Zustand zurückversetzt wird. Dies verhindert die Manipulation von Systemkomponenten durch unbefugten Code und ermöglicht eine schnelle Wiederherstellung der betroffenen Umgebung nach einem Cyberangriff. Der Einsatz von Technologien wie Secure Boot, TPM (Trusted Platform Module) und Hardware-gestützter Virtualisierung stärkt die Widerstandsfähigkeit der IT-Infrastruktur gegen tiefgreifende Angriffe und ermöglicht eine rasche Wiederaufnahme der Geschäftstätigkeiten.

4. **Etablierung starker Authentifizierungsmechanismen:**
   Es ist von entscheidender Bedeutung, Authentifizierungslösungen zu implementieren, die von führenden Anbietern wie Microsoft, VMware, Citrix oder Okta unterstützt werden. Die Integration von Multi-Faktor-Authentifizierung (MFA) und Zero Trust-Architekturen gewährleistet, dass der Zugriff auf kritische Ressourcen nur nach einer strengen Identitätsüberprüfung gestattet wird. Durch die Zusammenarbeit mit Secure Access Service Edge (SASE)-Anbietern wird die sichere und bedarfsorientierte Bereitstellung von IT-Ressourcen ermöglicht, die auf dynamische Bedrohungsmodelle reagieren kann.

5. **Förderung eines modularen Systemaufbaus:**
   Der Einsatz modularer Betriebssysteme, die ausschließlich die für die Arbeit notwendigen Komponenten enthalten, reduziert die Angriffsfläche erheblich. Zusätzlich sollten Sicherheitslösungen über vertrauenswürdige und zertifizierte App-Portale bezogen werden, um die Integrität der installierten Software sicherzustellen. Diese Herangehensweise entspricht dem Prinzip der Microsegmentation, das darauf abzielt, Sicherheitsbarrieren zwischen verschiedenen Anwendungsbereichen und -modulen zu schaffen, um eine Durchdringung durch Angreifer zu verhindern.

Strategische Relevanz der NIS2-Richtlinie

Ein weiterer zentraler Aspekt der modernen Cybersicherheitsstrategie ist die Beachtung der NIS2-Richtlinie (Network and Information Security Directive 2). Diese Richtlinie legt umfassende Vorgaben für die Sicherheitsarchitektur von Informationssystemen fest und fordert:

1. **Detaillierte Risikoanalyse und Sicherheitsbewertung:**
   Unternehmen müssen ein umfassendes Risikomanagementsystem implementieren, das eine kontinuierliche Identifikation, Analyse und Bewertung von Sicherheitsrisiken ermöglicht. Dazu gehören die Einführung von Bedrohungsmodellierungen und die Entwicklung von Notfallplänen.

2. **Effektives Management von Sicherheitsvorfällen:**
   Ein Incident Response Framework muss etabliert werden, das klare Protokolle für die Erkennung, Meldung und Bewältigung von Cybervorfällen enthält. Diese Maßnahmen sollten durch regelmäßige Simulationen und Audits überprüft werden.

■ Senator Heinz Stiastny, KommRat, RegKmsr

3. **Sicherstellung der Geschäftskontinuität und Krisenmanagement:**
   Die Entwicklung und Implementierung von Business Continuity Plans (BCPs) sind unerlässlich, um die Resilienz gegen Cyberangriffe zu gewährleisten. Dies umfasst auch die Sicherstellung redundanter Systeme und Desaster Recovery-Pläne.

4. **Sicherstellung der Lieferkettensicherheit gemäß EU-Lieferkettengesetz (April 2024):**
   Die Resilienz der gesamten Lieferkette muss durch strenge Sicherheitsstandards und Audits gewährleistet werden. Lieferanten und Partner müssen nachweislich sichere Prozesse und Technologien anwenden.

5. **Sicherheitsmaßnahmen beim Erwerb, der Entwicklung und Wartung von IKT-Systemen:**
   Sicherheitsaspekte müssen bereits in der Entwicklungsphase von IT-Systemen berücksichtigt werden (Security by Design). Dies umfasst die sichere Entwicklungspraxis, regelmäßige Sicherheitsüberprüfungen und Updates.

6. **Förderung der Cyberhygiene und Schulung der Mitarbeiter:**
   Regelmäßige Schulungen und Sensibilisierungsprogramme müssen etabliert werden, um sicherzustellen, dass alle Mitarbeiter die Bedrohungen und Sicherheitsanforderungen verstehen und umsetzen können.

7. **Einsatz von Kryptografie und Verschlüsselungstechnologien:**
   Der Schutz sensibler Daten muss durch den Einsatz fortschrittlicher Verschlüsselungstechnologien sichergestellt werden. Dies umfasst die Implementierung von End-to-End-Verschlüsselung, verschlüsseltem Datentransfer und sicheren Schlüsselspeichertechnologien.

8. **Zugriffskontrolle und Mehrfaktor-Authentifizierung:**
   Die Implementierung strenger Zugriffsrichtlinien und die Nutzung von Mehrfaktor-Authentifizierung (MFA) sind essenziell, um unbefugte Zugriffe zu verhindern und die Sicherheit der IT-Systeme zu gewährleisten.

Durch die stringente Anwendung dieser Prinzipien und die Einhaltung der NIS2-Richtlinie können Unternehmen und Privatpersonen ein hohes Maß an Cybersicherheit erreichen, das den Herausforderungen der modernen digitalen Welt gerecht wird.

Cybersicherheit in der Smart Economy

Mag. Monir Fazeli

In einer zunehmend vernetzten Welt, in der digitale Technologien wie Künstliche Intelligenz, das Internet und Big Data die Wirtschaft prägen, gewinnt Cybersicherheit für Unternehmen in Smart Economy an Bedeutung. Diese Technologien bieten immense Chancen, erhöhen jedoch auch die Verwundbarkeit gegenüber Cyberangriffen, wodurch der Finanzvorstand (CFO) eine zentrale Rolle einnimmt.

Cybersicherheit als Geschäftsrisiko

Traditionell konzentrierte sich der CFO auf finanzielle Aspekte. In der Smart Economy muss er jedoch Cybersicherheit als betriebswirtschaftliches Risiko erkennen, da Cyberangriffe operative Störungen und finanzielle Schäden verursachen können. Cybersicherheit sollte frühzeitig in digitale Projekte integriert werden. Der CFO ist dafür verantwortlich, dass das Unternehmen „cybersmart" agiert und eine Kultur der Wachsamkeit fördert. Dabei muss er die Bedeutung des Schutzes vor Cyber-Gefahren betonen und sicherstellen, dass Mitarbeiter ihre Rolle in der Cybersicherheit verstehen.

Verantwortungsbereich des Finanzvorstands

Die Verantwortung des CFOs in Bezug auf Cybersicherheit wächst kontinuierlich. Er ist nicht nur dafür verantwortlich, die notwendigen finanziellen Ressourcen bereitzustellen, sondern muss auch eng mit dem Chief Information Officer (CIO) und anderen Führungskräften zusammenarbeiten, um Cybersicherheit als essenzieller Bestandteil der Unternehmensstrategie zu verankern. Ein kompetenter CFO sollte die Bedrohungslage verstehen und Investitionen in Cybersicherheit als Teil eines umfassenden Risikomanagements betrachten, indem er potenzielle Risiken analysiert und zukünftige Bedrohungen minimiert.

Langfristige Planung für Cybersicherheit

Ein zentraler Aspekt ist die angemessene Budgetierung für Cybersicherheit. Der CFO muss sicherstellen, dass ausreichend Mittel für effektive Sicherheitsmaßnahmen vorhanden sind, einschließlich Investitionen in Erkennungssysteme, Datenverschlüsselung und Schulungen für Mitarbeiter. Langfristige finanzielle Auswirkungen von Cyber Sicherheitsinvestitionen sollten sorgfältig bewertet werden, da sich oft zeigt, dass präventive Maßnahmen kosteneffizienter sind als die Reaktion auf tatsächliche Sicherheitsvorfälle.

Fazit

In der Smart Economy hat Cybersicherheit für den CFO eine herausragende Bedeutung. Durch die Integration von Sicherheitsstrategien in die Finanzplanung und die enge Zusammenarbeit mit anderen Führungskräften trägt der CFO dazu bei, das Unternehmen vor den vielfältigen Bedrohungen der digitalen Welt zu schützen. Dies erfordert nicht nur finanzielle Mittel, sondern auch ein tiefes Verständnis der Bedrohungen und die Fähigkeit, in einer dynamischen Bedrohungslage fundierte Entscheidungen zu treffen.

Der nächste logische Schritt
The Next LEVEL

Wie gut, dass die Stimmen, welche meinen „ach, so ein Hackerangriff passiert uns bestimmt nicht" immer leiser werden. Zumindest in der Geschäftswelt. Betreiben wir ein Netzwerk für ein Unternehmen, so sind wir heute in der Situation, dass wir viel darüber gelernt haben, wie wir uns schützen können und letztlich auch müssen.

IT Security Konzepte und diverse Standards beinhalten einen guten Leitfaden, wie ein solches Sicherheitskonzept umgesetzt werden kann. Vereinfacht kann man daher sagen: umso schwieriger der Angriff wird, desto besser unsere Chancen, dass der Angreifer sein Ziel ändert. Dafür braucht es allerdings ein Konzept, welches uns ermöglicht, die Zusammenhänge zu erkennen. Dieses Sicherheitskonzepts beginnt idealerweise immer mit einem Risikomanagement.

Also der Überlegung und Erfassung, welche Ereignisse könnten, eintreten und massive Schwierigkeiten bereiten? Wie werden diese Schwierigkeiten aussehen? Welchen Schwierigkeitsgrad wird dieses Risiko verursachen? Ein zentraler Bestandteil des Risikomanagements ist die Risikobewertung. Hierbei werden die potenziellen Risiken identifiziert, analysiert und nach Eintrittswahrscheinlichkeit und ihrem Wirkungsgrad bewertet. Dementsprechend kann entschieden werden, welche Maßnahmen gesetzt werden, um die Risiken zu minimieren oder gar in Chancen umzuwandeln. Diverse Standards wie BSI-Grundschutz, Datenschutzverordnungen oder branchenspezifische Compliancevorgaben kommen dann zum Einsatz. Manches proaktiv, vieles reaktiv. Konzepte wie Zero Trust setzen auf einen 100 % proaktiven Ansatz und empfehlen bei Netzwerksegmentierung auf Applikationsebene, Microsegmentierung durchzuführen. Zero Trust bedeutet immer davon auszugehen, dass der Angreifer ins Netzwerk kommt, oder vielleicht schon da ist ohne das er auffällt!

Bei einer ISO 27001 Zertifizierung wird aber nicht nur das Netzwerk segmentiert, sondern auch eine Nachweispflicht darüber angefordert, dass die Mitarbeiter entsprechende Schulungen

bekommen und das Management sich seinen Aufgaben entsprechend weiterbildet. Warum? Weil ein schlecht informierter Mitarbeiter ein großes Risiko aufweist. Regelmäßige Awareness-Trainings müssen absolviert und nachgewiesen werden. Diese Trainings sind ein wesentlicher Bestandteil der Zertifizierung und auch im NIS-Gesetz verankert. Einem Unternehmen fällt es daher nicht schwer dieses Wissen einzuholen und weiters profitieren Firmen, besonders ab einer mittleren Unternehmensgröße, sehr stark davon, dass Berater unterschiedlicher Hersteller direkte Ansprechpartner dafür sind und neue Einblicke darüber geben. Einladungen zu C-Level Plattformen, Roundtables und diversen Security Events bieten weiteren umfangreichen Content und die Möglichkeit Wissen zu transferieren. Diese Form von Wissenstransfer wird laufend überarbeitet und verbessert.

Wenn sich dann doch etwas einschleicht, werden alle Maßnahmen von der NextGen Firewall, über EDR und XDR, Ausfallsicherheit, Backup-Schutz, Zugriffsberechtigungen und Segmentierungen hart auf die Probe gestellt. In der IT Security ist der Insider Threat (Angriff von innen) nach wie vor eine der meisten Einfallstore und dieser wird oft erst aufgrund von Unwissenheit ermöglicht.

Die jüngste Vergangenheit hat noch eine weitere erschreckende Seite gezeigt: ist Content abgeflossen oder der Angreifer noch im Netz, werden die Arten der Erpressungen immer dreister. Da stellt man sich die Frage, wie kommt man dazu, z. B. als Privatperson damit erpresst zu werden, dass Content im Internet über Familienmitglieder, Hobbies oder was auch immer veröffentlicht wird? Nur weil man in einem Unternehmen tätig ist, welches gerade einer Ransomware-Attacke zum Opfer fällt und alles verschlüsselt wurde. Bevor Sie nun denken, das geschieht ja nicht bei uns im schönen Österreich – oder in der DACH Region. Irrtum!

Das Cyber Hilfswerk hat es sich daher zur Aufgabe gemacht, hier anzusetzen, dabei soll unter anderem das Projekt Cyber Kids helfen, diese Lücke zu reduzieren. Es geht nicht nur noch darum unsere Unternehmen mit Risiken zu bewerten und danach zu handeln, es sollte auch als Privatperson das Wissen verfügbar gemacht werden Risiken zu erkennen. Ich spreche hierbei nicht nur von Kindern und Jugendlichen, die abgeholt werden sollen. Cyber Kids bedient mehrerer Bereiche.

Mit Cyber Kids soll eine Plattform geschaffen werden, die einem Informationsaustausch und Wissenstransfer dient, weiters Bewusstsein für die digitale Welt vermittelt und letztendlich auch vor Hackerattacken schützt.

Nicht nur die Kinder sollen auf diese Themen sensibilisiert werden, sondern auch und vor allem Eltern, Großeltern, Angehörige und Lehrer. Es geht darum zu erkennen, welche Tools habe ich als Privatperson zur Verfügung, um Scams zu erkennen. Phishing Attacken, die oftmals über SMS und WhatsApp daherkommen, als solche zu verifizieren und entsprechend abzuwehren.

Wenn wir es mit Cyber Kids letztendlich schaffen, auch im privaten Bereich sicher zu agieren und es für Angreifer immer schwieriger wird, auch diese einzufangen, so werden wir alle davon profitieren.

Wussten Sie, dass bereits eine Vielzahl von IT Security Herstellern Vorträgen an Schulen und Gemeinden anbieten? Es außerdem viele IT Security Spe-zialisten gibt, die gerne an Fachhochschulen kommen würden, und spannende Vorträge zu diesen Themen im Gepäck haben?

■ Barbara Steiner

Cybersicherheit: Berücksichtigung 2500 Jahre alten strategischen Denkens

Die Steigerung der digitalen Widerstandsfähigkeit und die Gewährleistung von Cybersicherheit in der digitalen Welt insgesamt sind für die Sicherheit eines Staates von großer Bedeutung. Dies drückt sich beispielsweise in der „Österreichischen Strategie für Cybersicherheit“ (ÖSCS) aus dem Jahr 2021 aus, wo als Vision die langfristige Schaffung eines sicheren Cyberraumes als Beitrag zur Steigerung der Resilienz Österreichs und der Europäischen Union durch einen gesamtstaatlichen Ansatz festgehalten ist.

Strategien bzw. deren Umsetzung haben auch strategisches Denken potenzieller Mitbewerber/Gegner zu berücksichtigen. In diesem Kurzbeitrag soll auf 2500 Jahre altes chinesisches strategisches Denken hingewiesen werden.

Strategisches Denken ist in zwei Erdteilen begründet worden: einerseits in Europa und andererseits in Asien. Als Ausgangspunkt sind dabei zu betrachten:

- in Europa die Schriften antiker griechischer und römischer Denker als Basis neuzeitlichen Denkens in Kriegführung und Strategie
- in Asien chinesisches strategisches Denken in Form konkreter Handbücher von Sun Tsu

Die Herausforderungen der Cybersicherheit im strategischen Bereich machen insbesondere auch eine Auseinandersetzung mit dem eher wenig bekannten strategischen Gedankengebäude der im Werk „Kunst des Krieges“ dargelegten dreizehn Grundprinzipien, verfasst vermutlich um 500 v. Chr. durch einen chinesischen General namens Sun Tsu, lohnenswert; dies umso mehr, als diese Prinzipien an chinesischen Bildungseinrichtungen nach wie vor als aktuell gelten und dementsprechend gelehrt werden.

Klar kommt die entscheidende Bedeutung der Sicherheit und damit in Verbindung die Bedeutung des Krieges zum Ausdruck: „Die Kunst des Krieges ist für den Staat von entscheidender Bedeutung. … Deshalb darf sie unter keinen Umständen vernachlässigt werden.“ Heute ist dies wohl auf die umfassende Bedeutung dieser Begriffe zu beziehen.

Gerade der Bereich der Kriegführung im Cyberraum folgt folgenden Gedanken: „In all deinen Schlachten zu kämpfen und zu siegen, ist nicht die größte Leistung. Die größte Leistung besteht darin, den Widerstand des Feindes ohne einen Kampf zu brechen.“ Sun Tsu betont damit auch die grundsätzliche Überlegenheit der indirekten Strategie gegenüber der direkten Strategie. Die indirekte Strategie beruht vor allem auf Täuschung und List, wobei hier konkrete Handlungsanweisungen gegeben werden: „Wenn wir also fähig sind anzugreifen, müssen wir unfähig erscheinen; wenn wir unsere Streitkräfte einsetzen, müssen wir unfähig scheinen; … greife den Feind an, wo er unvorbereitet ist; tauche auf, wo du nicht erwartet wirst.“

Als eine zentrale Forderung formuliert Sun Tsu die Notwendigkeit einer richtigen Beurteilung der gegnerischen und eigenen Mittel: „Wenn du den Feind und dich selbst kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten. … Wenn du weder den Feind noch dich selbst kennst, wirst du in jeder Schlacht unterliegen.“

Für Österreich ist gemäß der ÖSCS 2021 die Cybersicherheit daher eine der obersten Prioritäten und eine gemeinsame Herausforderung für Staat, Wirtschaft, Wissenschaft und Gesellschaft. Das ist auch die Grundlage dafür, die Chancen der Digitalisierung auch in den kommenden Jahren und Jahrzehnten bestmöglich und vor allem sicher nutzen zu können. Eine Cyberverteidigung ist zu planen und hat daher alle Maßnahmen zur Vorbereitung, Aufrechterhaltung und Wiederherstellung der Handlungsfähigkeit im Rahmen von souveränitätsgefährdenden bzw. -verletzenden Handlungen sicherzustellen.

■ MMag. Franz Hollerer

Nicht zu vertrauen ist modern

„Vertraue niemandem über dreißig“, sagte Jack Weinberg vor fast sechzig Jahren. Heute sollten IKT-Unternehmer und ihre Kunden noch viel strenger sein: „Vertraue niemandem!“

Stellen Sie sich ein selbstfahrendes Auto vor, dessen künstliche Intelligenz (KI) eine riesige Menge an Daten enthält, auf deren Grundlage es Entscheidungen treffen kann, denen wir mehr als nur unser Leben anvertrauen. Für ihre Entscheidungsfindung benötigt die KI ein robustes Modell, das gute Daten auswertet. Ungenauigkeiten, ob absichtlich oder unabsichtlich in das Modell oder die Daten eingebracht, können eine Reihe von Situationen verursachen, die in einer Tragödie enden.

Als Fahrer kennen wir die Marke des Autoherstellers. Wer jedoch an seiner Herstellung beteiligt ist, wer für die Sicherheitsträumer verantwortlich ist, deren Abteilung für die Auswertung aller Informationen verantwortlich ist, ist nichts, das wir normalerweise herausfinden wollen. Obwohl uns nichts wichtiger als unser Leben und das Leben unserer Lieben ist. Aber wir verlassen uns darauf, dass die gesamte Technik so funktioniert, wie sie sollte, und wir sicher nach Hause zurückkehren. Dasselbe gilt für andere menschliche Aktivitäten, IT und Telekommunikation nicht ausgeschlossen. Es ist für Nutzer von entscheidender Bedeutung, darauf zu vertrauen, dass ihre Daten sicher sind. Damit es in Zukunft so bleibt, sollte von IKT-Unternehmen und ihren Kunden das Konzept des „Zero-Trust“ praktiziert werden.

Vertrauen, aber überprüfen

Egal, ob es sich um einen großen multinationalen Anbieter von IKT-Lösungen oder einen kleinen lokalen Internetdienstanbieter handelt, Sie kennen ihre Lieferanten. Wahrscheinlich für lange Zeit und oft persönlich. Aber auch ein so langjähriger und zuverlässiger Partner kann, unabhängig von seinen Geräten oder seiner Software, Angriffen ausgesetzt sein oder einfach intern einen Fehler machen.

Wie also damit umgehen? Es ist wichtig, jede Lösung, jedes Gerät, das uns der Lieferant anbietet oder das wir bereits verwenden, gründlich zu prüfen. Suchen Sie nach Schwachstellen, verfügbaren Informationen. Selbst der IKT-Sektor ist ein Geschäft wie jedes andere. Verlassen Sie sich nicht nur auf die Behauptungen des Lieferanten, sondern versuchen Sie, verifizierte objektive Informationen zu erhalten. Nur den Lieferanten als Quelle zu verwenden, ist nicht der sinnvollste Ansatz.

Behandeln Sie Hardware oder Software, selbst von einem bewährten Lieferanten, so als ob sie von einem Unternehmen stammt, das Sie nicht kennen. Das wird Sie umso vorsichtiger machen. Aber wie stellen Sie eine gründliche Prüfung sicher? Es ist nicht immer möglich, einzelne Komponenten intern zu überprüfen, sei es aufgrund von Personal- oder Ressourcenknappheit oder aus Zeitmangel. Die Überprüfung durch Dritte ist die ideale Option. Über ein Unternehmen, das weder mit dem Lieferanten noch mit dem Kunden verbunden ist und über echtes Fachwissen in der technischen und Sicherheitsanalyse und ausreichende Reputation in diesem Bereich verfügt.

Es gibt auch Vorschläge, dass sich der Staat darum kümmern könnte, was nach Meinung von Vertretern des IKT-Sektors eine sehr „ernste“ Idee ist. Die Verifizierung vor der Bereitstellung ist jedoch keineswegs das Ende des Prozesses, sie ist nur der erste Schritt. Wenn Sie ein Produkt in das System einführen, richten Sie Mechanismen ein, damit es immer zweifelsfrei authentifiziert werden kann. Es ist eine gute Idee, zu prüfen, ob der neue Teil der Systemlösung seine Aufgaben erledigt. Aber es ist genauso wichtig zu wissen, dass es im normalen Betrieb nichts tut, was es nicht tun sollte.

Weniger ist mehr

An dieser Stelle geht es nicht um die Überprüfungs- und Kontrollmechanismen, sondern vor allem um den Endbenutzer. Es heißt, dass das größte Sicherheitsrisiko zwischen dem Stuhl und der Tastatur besteht. Dies ist normalerweise das Tor für Angreifer, um auf Systeme, Daten, Informationen zuzugreifen. Deshalb ist es auch ratsam, den Nutzern nur die grundlegenden Rechte zu geben, die sie für ihre Arbeit benötigen. Dadurch wird das Risiko minimiert. Dann können Sie dieselbe Logik auf andere Teile des Systems anwenden, auch wenn Sie diese bereits authentifiziert haben.

Lasst uns alles überwachen

Security Information and Event Management (SIEM) ist bereits Bestandteil fast aller wichtigen Systeme, deren Eigentümer sich um sie kümmern. Es wird jedoch nicht immer alles überwacht – aus Kapazitätsgründen wie Technologie, Mangel an Experten und mangelnde Bereitschaft, in die Gesamtentwicklung zu investieren. Damit muss Schluss sein und die Überwachung von Sicherheitsereignissen, ihre Bewertung sowie die anschließende Verarbeitung von Sicherheitsvorfällen sind weitere notwendige Schritte, um die Sicherheit des gesamten Systems zu gewährleisten.

Das Schlimmste annehmen

Selbst wenn alle möglichen Sicherheitsmaßnahmen getroffen wurden, kann es zu einem Sicherheitsvorfall kommen. Für solche Situationen sollten Prozesse für das Management von Sicherheitsvorfällen eingerichtet sein. Sie sollten ein Business Continuity- und Krisenmanagement-System implementieren.

Die beste Lösung

So wie wir in ein Auto einer bewährten Marke steigen und automatisch glauben, dass es uns sicher von A nach B bringt, nutzen wir auch andere Dienstleistungen und Produkte, von denen wir unumstößlich annehmen, dass sie das höchste Maß an Sicherheit bieten. Niemand von uns wird wahrscheinlich ein Auto fahren wollen, das gemeinhin mit Problemen in Verbindung gebracht wird, in einem unsicheren Online-Shop einkaufen oder die Dienste eines Betreibers in Anspruch zu nehmen, der Mängel in der IT-Sicherheit aufweist und nicht nur seine Infrastruktur, sondern auch die Daten seiner Kunden schützen kann.

Das Reparieren von Schäden ist ein fragiles Thema und selbst der kleinste fahrlässige Zwischenfall kann Schaden anrichten, der jahrelang nachwirkt. Je eher wir die Prinzipien des „Zero-Trust“ übernehmen und uns an die Tatsache gewöhnen, dass es in einer so komplexen Welt derzeit keine bessere Lösung als diese gibt, desto schneller wird unser digitales Ökosystem sicherer sein. Das sorgt nicht nur für mehr Vertrauen bei den Spezialisten, die unter seine Haube sehen können, sondern auch bei den normalen Nutzern.

■ Feiyun Chen

Cybersicherheit – eine Frage der Verantwortung

Alle reden von Cybersicherheit, aber keiner tut was dafür. Das scheint derzeit allgemeine Wahrnehmung zu sein. Es fehlt nicht an Erkenntnissen und Experten, um zu wissen, was zu tun ist. Sobald es darum geht, die angemessenen Maßnahmen umzusetzen und Ressourcen bereitzustellen sind, prallen sie oft am Festhalten an Gewohnheiten oder Handlungszwängen ab. So laden offenstehende Schwachstellen Hacker mit kriminellen Absichten zum Missbrauch ein.

Ein wenig erinnert es an die Situation, als sich die Immun-Erkrankung AIDS ab den 1980er-Jahren ausbreitete. Allen war der Slogan „Kondome schützen" ein Begriff. Die Praxis war dagegen geprägt vom Ansatz „Ohne ist schöner." in Kombination mit dem Mantra „Hab immer aufgepasst, was soll schon passieren …". Der Vergleich offenbart zudem eine weitere Parallele, warum es gut ist, sich zu schützen: Es geht nicht nur um das eigene Wohlergehen, sondern auch um den Schutz der anderen. Doch spätestens die Erfahrungen der Corona-Pandemie zeigen, dass das Prinzip der dualen Verantwortung für sich und die Gesellschaft ähnlich wie der kategorische Imperativ noch keine Allgemeingültigkeit erlangt hat.

Das schmälert die Relevanz der Cybersicherheit jedoch keineswegs. Der folgende Artikel leitet diese Relevanz aus drei Aspekten ab: aus dem technischen Entwicklungstempo, der aktuellen Bedrohungslage und den regulatorischen Anforderungen. Am Ende lassen sich alle drei Bereiche wieder auf das Prinzip der Verantwortung zurückführen – als eine Einsicht in Notwendigkeit und damit zugehörige Komponente zur Freiheit.

Seit den letzten Jahrzehnten erlebt der technische Fortschritt im Bereich der Computertechnik eine revolutionäre Entwicklung. Die ersten Großrechner in der Mitte des 20. Jahrhunderts füllten noch Räume mit einer Rechenleistung, die längst von unseren Smartphones in der Hosentasche übertroffen wird. Mit dem Aufkommen des Internets in den 1990er Jahren erfuhr die Welt eine grundlegende Veränderung in der Art und Weise, wie Menschen kommunizieren, Informationen austauschen und Geschäfte tätigen. Die ständige Weiterentwicklung von Netzwerktechnologien hat zu einer global vernetzten Gesellschaft geführt, die in Echtzeit Informationen austauscht. Effizienz und Produktivität steigerten sich in zahlreichen Branchen und neue Geschäftsmodelle und soziale Interaktionen entstanden, die zuvor undenkbar waren.

Neue Möglichkeiten schaffen aber auch Abhängigkeiten; und sei es aus der Komfortgewohnheit und dem menschlichen Fortschrittsstreben heraus. Jedes neue Level an Komfort und Fortschritt macht es unvorstellbar, ohne Not wieder auf einen alten Standard zurückzufallen. Dabei vollzieht sich der Prozess der Digitalisierung in allen Lebensbereichen so rasant, dass der Bedarf und die Umsetzung von Schutzmaßnahmen erst nachträglich erfolgen. Doch das Phänomen kennen wir auch von anderen technischen Entwicklungen. Die ersten Automodelle besaßen keine Sicherheitsgurte. Inzwischen gehören diese zur serienmäßigen Pflichtausstattung eines jeden Neuwagens dazu. Die Analogie liefert zudem ein klares Beispiel, dass die Einführung von Schutzmaßnahmen besser funktioniert, wenn sie nicht einseitig erfolgt: Hersteller in der EU sind gemäß Richtlinie 77/541/EWG des EU-Rates vom 28. Juni 1977 verpflichtet, alle in der EU neu zugelassenen Fahrzeuge mit Sicherheitsgurten auszustatten. Der Endnutzer muss sie daher nicht extra kaufen, ist aber verpflichtet, sich anzuschnallen.

Was die aktuelle Bedrohungslage für den Cyberbereich angeht, sollten wir alle längst angeschnallt sein. Es ist ein Irrtum, russische Hacker hätten erst mit dem Ukraine-Krieg 2022 begonnen „den Westen" anzugreifen. Bereits im Mai 2021 wandten sich die Betreiber der Colonial Pipeline an die Behörden in den USA. Angreifer hatten ihre Daten verschlüsselt und forderten ein Lösegeld für deren Wiederfreigabe. Den Hackern gelang es mit einer simplen E-Mail das System zu infiltrieren. Sie konnten zwar nur in den Backoffice-Bereich eindringen und nicht in die Kontrollsysteme. Doch aufgrund der zunächst unklaren Lage entschloss sich das Unternehmen das komplette System herunterzufahren, um das Risiko eines tieferen Systembefalls zu reduzieren. Dadurch kam es zu einem tagelangen Ausfall des Pipeline-Transports und zu Engpässen bei der Kraftstoffversorgung für die Bevölkerung. Die Regierung in Washington musste zwei Tage nach der Meldung des Angriffs den regionalen Notstand ausrufen.

Das FBI ermittelte, bei den Angreifern handele sich um eine Gruppe sogenannter professioneller Hacker namens DarkSide. Der Name tauchte erstmals im August 2020 in Hacking-Foren in russischer Sprache auf und ist eine Ransomware-as-a-Service-Plattform – eine von inzwischen vielen. ▯ siehe [INFOBOX].

Als im Frühjahr 2023 die „Vulkan Files" an die Öffentlichkeit gelangten, belegten sie erneut, dass der Kreml im Bereich der Cyberkriegsführung Vorbereitungen als auch Angriffe bereits vor dem Überfall auf die Ukraine begann. Die internen Unterlagen der russischen IT-Firma NTC Vulkan hatte eine anonyme Quelle geleaked. Mehr als 50 Journalisten aus acht Ländern werteten das Material aus. Demnach gab und gibt es mit hoher Wahrscheinlichkeit weiterhin eine gezielte Anwerbung von IT-Ingenieuren für staatliche Cyber-Projekte in Zusammenarbeit mit und zwischen den russischen Geheimdiensten, um Schwachstellen für mögliche Angriffe auszuspähen und die Informationsflüsse im Internet zu kontrollieren.

Die immerhin gute Nachricht der „Vulkan Files": sie zeigen Grenzen der russischen Cyberfähigkeiten auf, wie z. B. mangelnde Fähigkeiten komplexe Verschlüsselungen zu knacken. Doch die Dateien verdeutlichen auch, dass ein Angreifer im Cyberbereich so erfolgreich ist, wie es ihm die Schwachstellen der Opfer erlauben.

Dabei sind IT-Schwachstellen nicht nur eine Bedrohung als Einfallstor für kriminelle und staatliche Hacker. Auch Systemfehler können zu Betriebsvorfällen führen. Eine Auswertung der deutschen Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) vom Juli 2024 zeigt: Durch IT-Vorfälle verursachte Störungen bei Zahlungsdienstleistern hatten selten einen externen Angriff als Ursache, sondern interne und operationelle Fehler bei den Prozessen und Systemen.

In Zukunft ist nicht nur gestraft, wer ungeschützt das Ziel von Cyber-Attacken wird. Wer kein funktionierendes Sicherheitsmanagement für seine IT-Prozesse hat, wird wegen regulatorischer Verstöße zur Kasse gebeten. Die Europäische Kommission plant ab dem 18. Oktober 2024 in allen EU-Mitgliedstaaten die Anwendung der EU-Cybersicherheitsrichtlinie NIS-2 (The Network and Information Security Directive).

Zeitliche Abweichungen können sich national durch die jeweiligen NIS-2-Umsetzungsgesetze ergeben. In Österreich bekam die Richtlinie keine parlamentarische Mehrheit und liegt damit vorerst auf Eis. In Deutschland dürfte die Umsetzungsfrist weiterhin gesetzt sein, doch diagnostiziert der Verband der Internetwirtschaft eco, nur wenige Unternehmen seien wirklich auf NIS-2 vorbereitet.

Dabei betrifft die Richtlinie zahlreiche Branchen: Als wesentliche Organisationen („essential") sind hauptsächlich KRITIS-Unternehmen gelistet, die für das staatliche Gemeinwesen von entscheidender Bedeutung sind, darunter die Branchen Energie- und Wasserversorgung, Transport, Finanz- und Bankwesen, Gesundheit sowie öffentliche Verwaltung. Zu den wichtigen Organisationen („important") zählen sieben Branchen: Post- und Kurierdienste, Abfallwirtschaft, Lebensmittelproduktion, Chemikalienindustrie, digitale Dienste (wie Suchmaschinen, Online-Marktplätze, Cloud-Services, soziale Netzwerke), Industrie (einschließlich Maschinenbau, Fahrzeugbau, Datenverarbeitungsgeräte) sowie Forschung.

Es drohen empfindliche Strafen bei Nichterfüllung: bis zu zehn Millionen Euro oder zwei Prozent des Gesamtjahresumsatzes bei den laut NIS-2 als wesentlich eingestuften Firmen. Bei den als wichtig geltenden Unternehmen fallen bis zu sieben Millionen Euro oder 1,4 Prozent des Gesamtjahresumsatzes an. In beiden Fällen ist der jeweils höhere Betrag maßgeblich. Wichtiger Zusatz hierbei: Es haften die Leitungsorgane von Unternehmen mit ihrem Privatvermögen für die Einhaltung der erforderlichen Maßnahmen. [<-Nach Doppelpunkt fett oder unterstrichen als Markierung möglich?]

Für den europäischen Finanzsektor greift zudem ab dem 17. Januar 2025 der europäische Digital Operational Resilience Act, kurz DORA. Damit soll ein einheitlicher Regulierungsrahmen für die digitale operative Widerstandsfähigkeit von Zahlungsdienstleistern geschaffen werden. Bei Nichteinhaltung steht es zwar den EU-Mitgliedstaaten frei, Sanktionen zu erheben. Aber umso mehr sind Bußgelder unausweichlich, da DORA im Gegensatz zur NIS-2-Richtlinie als Gesetz in Kraft tritt.

Diese Form der Belangung bei Verstößen unterstreicht das Prinzip der Verantwortung zum Eigenschutz und für Dritte. Ein Cyberangriff betrifft in der Zeit heutiger Produktions- und Dienstleistungsabhängigkeiten selten eine Institution allein. Mit einer Ausfallzeit von Geschäftsprozessen, dem Schaden in IT-Systemen und dem Datenverlust entsteht auch immer ein Ereignis der wahrnehmbaren Dysfunktionalität. Die Häufung an Dysfunktionalität gefährdet die Stabilität einer Gesellschaft.

Am Ende wird immer ein Preis zu zahlen sein:

a) Sie investieren in den Schutz ihrer IT-Systeme, weil Sie die Zeichen der Zeit erkennen.

b) Sie finanzieren Cyberkriminelle als Opfer ihrer Ransomware.

c) Sie verstoßen gegen die für Sie geltenden Anforderungen von NIS-2 und DORA und zahlen Bußgelder.

Spätestens wenn Option b) publik wird, kommt Option c) additiv dazu. Und damit beginnt hier die Verantwortung der Leitungsebene: Sie treffen die Wahl.

■ Björn Hawlitschka

Was ist Ransomware-as-a-Service?

In Zeiten des beliebten Outsourcings ermöglicht Ransomware-as-a-Service lukrative Joint Ventures zwischen Kriminellen mit einerseits fortgeschrittenen und andererseits weniger ausgeprägten IT-Fähigkeiten. Dabei programmieren und warten die Profi-Hacker eine hochwertige Ransomware und stellen sie Kriminellen ohne größere IT-Skills zur Verfügung. Diese können dann die Software nutzen, um die IT-Systeme der von ihnen ausgewähltem Opfer mit Ransomware zu infizieren und Lösegeldzahlungen zu erpressen oder Wirtschaftsspionage bei der Konkurrenz zu betreiben. Vom erzielten Gewinn der „Franchises“ geht ein Anteil an den „Mutter-Konzern“, der auch zur Weiterentwicklung des Produkts reinvestiert wird.

Obwohl es sich hier um eine dunkle Seite der Wirtschaft handelt, ohne Compliance geht es hier ebenfalls nicht. So erfolgte im Mai 2021 eine Erklärung der „Leitungsebene“ von DarkSide, dass die Schädigung des Pipeline-Betriebs nicht ihre Intention war und sie keine Aktion verantworten wollen, die Auswirkungen auf die Bevölkerungsversorgung habe. Zudem wurden Verbesserungen der Arbeitsprozesse und der Kundenbetreuung versprochen: „Ab heute führen wir Moderation ein und überprüfen jedes Unternehmen, das unsere Partner verschlüsseln möchten, um künftige soziale Konsequenzen zu vermeiden.“

Wie auch bei anderen Ransomware-Plattformen kommt es bei DarkSide zu einer doppelten Erpressung. Ein Betrag wird fällig, um einen digitalen Schlüssel zum Entsperren von Dateien und Servern zu erlangen. Eine Extrazahlung steht für das Versprechen, dass die Hacker alle kopierten Daten nicht weiterverbreiten, sondern vollständig löschen. Wer als Opfer hier spart, erlebt ein weiteres Geschäftsmodell von DarkSide: Die Daten werden in der Sparte der moralisch unbelasteten Börsenzocker-Community als Vorabinfos über ein Daten-Fiasko verkauft. Danach finden die gestohlenen Informationen über einen „victim shaming blog“ ihren Weg in die Öffentlichkeit.

■ Björn Hawlitschka

Wirtschaftsmediation: Effiziente Konfliktlösung im Unternehmen

Mediation ist ein vertrauliches und strukturiertes Verfahren, in dem ein neutraler und allparteilicher Vermittler den Parteien hilft, eigenverantwortliche Lösungen zu finden. Dies gilt sowohl für die klassische Mediation als auch für die Wirtschaftsmediation. Doch während klassische Mediation in verschiedensten Bereichen wie Nachbarschaftsstreitigkeiten, Schule, Familie, Scheidungen, Strafrecht oder interkulturellen Konflikten eingesetzt wird, fokussiert sich die Wirtschaftsmediation auf den beruflichen und unternehmerischen Kontext (z. B. Arbeitsplatzkonflikte, Spannungen zwischen Mitarbeitern und Vorgesetzten, Konflikte zwischen Abteilungen, Auseinandersetzungen zwischen Gesellschaftern, Streitigkeiten zwischen Unternehmen, Vertragsstreitigkeiten, Unternehmensfusionen, u. dgl.).

In der Wirtschaftsmediation sind hingegen die Konflikte oft komplexer und beinhalten mehrere Parteien und Stakeholder mit unterschiedlichen Interessen. Dazu gehören auch rechtliche und wirtschaftliche Rahmenbedingungen, die berücksichtigt werden müssen. Wirtschaftsmediatoren benötigen somit spezifisches Wissen über betriebswirtschaftliche Zusammenhänge und unternehmerische Prozesse. Sie müssen in der Lage sein, Machtungleichgewichte auszugleichen und unternehmerische Abhängigkeiten und Vernetzungen zu erkennen und zu verstehen. Wirtschaftsmediation ist nicht nur in Krisenzeiten von großer Bedeutung, da sie eine Alternative zu langwierigen und kostspieligen Gerichtsverfahren bieten und helfen kann Geschäftsbeziehungen aufrechtzuerhalten und zu stärken.

Die Vorteile der Wirtschaftsmediation liegen auf der Hand. Es geht um Kostenersparnis, Vermeidung von teuren und langwierigen Rechtsstreitigkeiten, Zeitersparnis, schnelle Lösungen im Vergleich zu Gerichtsverfahren, Erhaltung von Geschäftsbeziehungen, Förderung einer konstruktiven Zusammenarbeit auch nach der Konfliktlösung, sowie um Flexibilität mögliche, kreative und maßgeschneiderte Lösungen zu finden, die für alle Parteien vorteilhaft sind. Diese Möglichkeiten und Auswirkungen der Wirtschaftsmediation finden sich in Unternehmen und Organisationen, Unternehmenskooperationen wieder.

Grundelemente der Wirtschaftsmediation sind:

- Freiwilligkeit: Beide/alle Parteien müssen freiwillig am Mediationsprozess teilnehmen. Die Bereitschaft zur Mediation ist entscheidend für den Erfolg des Prozesses, da die Parteien nur dann konstruktiv und offen miteinander kommunizieren, wenn sie freiwillig dabei sind.
- Neutralität: Der Mediator muss neutral und unparteiisch sein. Er unterstützt die Parteien dabei, eine Lösung zu finden, ohne selbst eine Position zu beziehen oder eine Entscheidung zu treffen.
- Vertraulichkeit: Alles, was in der Mediation besprochen wird, bleibt vertraulich. Diese Vertraulichkeit fördert ein offenes und ehrliches Gespräch, da die Parteien sicher sein können, dass ihre Aussagen nicht gegen sie verwendet werden.
- Selbstbestimmung: Die Parteien selbst erarbeiten die Lösung ihres Konflikts. Der Mediator gibt keine Lösung vor, sondern hilft den Parteien, selbst eine Vereinbarung zu treffen, die ihren Bedürfnissen und Interessen entspricht.
- Strukturierter Prozess: Wirtschaftsmediation folgt einem strukturierten Ablauf, der typischerweise in Phasen unterteilt ist: Einleitung, Erfassung der Themen, Interessenklärung, Entwicklung von Optionen und Vereinbarung einer Lösung.

Die Ausbildung zur Wirtschaftsmediation umfasst neben den grundlegenden Mediationsfähigkeiten auch spezielle Kenntnisse und Kompetenzen in den Bereichen Wirtschaft und Recht. Dazu gehören: wirtschaftliches Verständnis (Kenntnisse in Betriebswirtschaft und Unternehmensführung), rechtliche Kenntnisse (Verständnis von Handels- und Vertragsrecht), Konfliktmanagement (Spezifische Techniken und Methoden zur Lösung von Konflikten im wirtschaftlichen Umfeld), Kommunikationsfähigkeiten (Fähigkeiten zur effektiven Kommunikation und Verhandlung)

Nicht nur in Krisenzeiten, wie wirtschaftlichen Abschwüngen oder pandemiebedingten Herausforderungen, spielt die Wirtschaftsmediation eine entscheidende Rolle. Sie kann helfen, Krisen zu bewältigen, indem sie Unternehmen dabei unterstützt, interne und externe Konflikte effizient zu lösen und somit Stabilität und Kontinuität zu gewährleisten.

Wirtschaftsmediation bietet wertvolle Werkzeuge und Methoden zur Lösung von Konflikten im geschäftlichen Umfeld. Sie bietet eine flexible, kostengünstige und vertrauliche Alternative zu gerichtlichen Auseinandersetzungen und fördert kooperative Lösungen, die Geschäftsbeziehungen erhalten. Eine fundierte Ausbildung und spezialisierte Kompetenzen sind entscheidend, um als Wirtschaftsmediator erfolgreich tätig zu sein und den vielfältigen Herausforderungen gerecht zu werden.

Im 21. Jahrhundert hat die Wirtschaftsmediation durch Digitalisierung, Globalisierung und die zunehmende Komplexität von Geschäftsbeziehungen an Bedeutung gewonnen.

Trotz ihrer vielen Vorteile hat die Wirtschaftsmediation auch Grenzen. Sie kann keine Rechtsberatung bieten, keine Einigung garantieren, keine Entscheidungen erzwingen, keine grundlegend schlechten Geschäftsbeziehungen reparieren und ist nicht für alle Konflikte geeignet, insbesondere solche, die tiefgreifende rechtliche oder ethische Implikationen habe. Dennoch bleibt sie ein mächtiges Werkzeug zur Förderung von konstruktiver Konfliktlösung und langfristiger Zusammenarbeit im Geschäftsleben.

Weiterführende Informationen finden Sie auf:
https://www.zfrk.org/fachbereiche/wirtschaftsmediation

■ Mag. Johann Höfler

Ein neuer Ansatz zur Erkennung von Insiderrisiken und Verhinderung von Datenabfluss

Bernd Vellguth

Der ungewollte oder gezielte Abfluss vertraulicher Daten stellt für Unternehmen zunehmend eine ernsthafte Bedrohung dar. Ob durch unachtsame Mitarbeitende oder durch ausgeklügelte Industriespionage – der Schutz von Geschäftsgeheimnissen ist heute entscheidender denn je. Für produzierende Unternehmen können dies etwa innovative Prozessschritte sein, wie die Entwicklung eines besonders haltbaren Lacks oder die Steigerung der Batterie-Kapazität. Für Einzelhändler umfassen diese vertraulichen Informationen typischerweise Einkaufskonditionen, die direkt die Gewinnmarge beeinflussen. Angesichts der zunehmenden Relevanz solcher Informationen wird der Schutz vor Datenabfluss für viele Organisationen zu einer unverzichtbaren Notwendigkeit.

Der Übergang vom allgemeinen Kopieren von Daten bei einem Arbeitgeberwechsel zur gezielten Industriespionage durch Wettbewerber ist fließend und führt in beiden Fällen zum Verlust wertvollen geistigen Eigentums. Dieser schleichende Übergang wird durch die zunehmende nationale Dimension des Wettbewerbs verstärkt. Staatliche Sanktionen gegen fortschrittliche Technologien verdeutlichen, wie wichtig der Schutz von Innovationen für den Wohlstand von Nationen ist. Während im Verteidigungsbereich Spionage seit Langem bekannt ist, entwickelt sich das Bewusstsein für solche Risiken in der Industrie erst allmählich. Viele Unternehmen erkennen erst dann die Bedeutung von Sicherheitsmaßnahmen, wenn die Auswirkungen von Datendiebstahl bereits gravierend sind. Häufig wird argumentiert, dass Überwachungsmaßnahmen das Vertrauen in die Mitarbeiter und das Betriebsklima beeinträchtigen könnten. Doch gerade diese Haltung kann unbeabsichtigt die Sicherheit des Unternehmens gefährden, indem notwendige Schutzmaßnahmen vernachlässigt werden.

Die Balance zwischen Erkennung und Privatsphäre

Die Herausforderung für Unternehmen besteht darin, eine Balance zwischen dem Schutz sensibler Daten und der Wahrung der Mitarbeiterprivatsphäre zu finden, die dann auch vom Betriebsrat mitgetragen wird. Während die EU-Datenschutz-Grundverordnung und nationale Gesetze strenge Grenzen für Überwachungsmaßnahmen setzen, liegt es dennoch im Interesse der Unternehmen, ihre vertraulichen Informationen effektiv zu schützen.

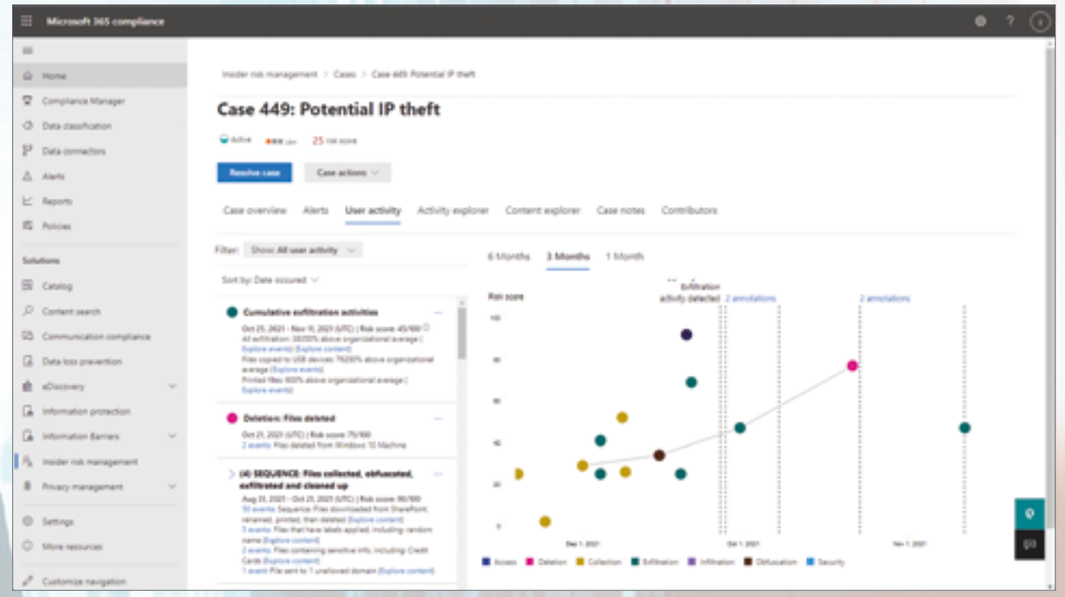
Hier kommen die Richtlinien der ISO 27002:2022 ins Spiel, die seit ihrer Überarbeitung im Jahr 2022 detaillierte Empfehlungen für präventive und reaktive Schutzmaßnahmen bieten. Diese Empfehlungen umfassen sowohl interne als auch externe Bedrohungen und betonen die Notwendigkeit, umfassende Sicherheitsmaßnahmen zu ergreifen. Auch neue EU-Regulierungen wie NIS2 und der Digital Operational Resilience Act (DORA) unterstreichen die Dringlichkeit, robuste Schutzmechanismen zu implementieren. Doch oft liegt der Fokus der Unternehmen auf externen Angriffen, während interne Risiken vernachlässigt werden.

Die zentrale Frage lautet daher: Wie kann die Balance zwischen dem Schutz der Privatsphäre der Mitarbeitenden und der Notwendigkeit, Datenabfluss zu verhindern, gewahrt werden? Die Herausforderung liegt darin, zwischen alltäglichem Verhalten und potenziellen Risiken zu unterscheiden, um ein sicheres Arbeitsumfeld zu schaffen, ohne das Vertrauen der Mitarbeitenden zu untergraben.

Microsoft Insider Risk Management: Die Lösung

Microsoft hat eine Lösung entwickelt, die diesen Balanceakt ermöglicht: Microsoft Insider Risk Management. Die Lösung schützt die Privatsphäre der Mitarbeitenden und verwendet intelligente Algorithmen, um zwischen erwünschtem und riskantem Verhalten zu unterscheiden. Jede Organisation kann selbst festlegen, welche Aktivitäten als Risikoindikatoren gelten. Beispiele dafür sind massenhafter Download von Daten aus Intranetsystemen wie SharePoint oder OneDrive, das Kopieren von Daten auf USB-Sticks oder das massenhafte Drucken von Dokumenten. Die Unternehmen können aus etwa 100 Risikoindikatoren auswählen und definieren, welche Schwellwerte für Alarme gelten, sei es für leichte, mittlere oder schwere Risiken.

Ein bedeutender Vorteil der Lösung ist die Möglichkeit, Alarme so zu konfigurieren, dass sie anonymisiert werden. Die Pseudonymisierung der Identität der Mitarbeitenden stellt sicher, dass die Privatsphäre gewahrt bleibt, während die relevanten Fakten analysiert werden. Unternehmen können auch spezifische Schwellwerte für verschiedene Mitarbeitergruppen oder Abteilungen festlegen, was eine differenzierte Überwachung ermöglicht. Eine weitere Stärke dieser Lösung ist ihre Fähigkeit zur Langzeitanalyse. Das System verfolgt und verknüpft Aktivitäten über einen Zeitraum von bis zu 90 Tagen, wodurch es in der Lage ist, verdächtige Muster in der Abfolge von Einzelhandlungen zu erkennen, die auf potenziellen Datenmissbrauch hindeuten könnten. Diese tiefgehende Analyse sorgt für eine präzisere Erkennung von Risiken und minimiert gleichzeitig Fehlalarme, was die Sicherheitsvorkehrungen erheblich verbessert.



Insider Risk Management korreliert alle Aktionen eines Mitarbeiters und analysiert diese, um normales Verhalten von schadhafter Exfiltration von Daten zu unterscheiden. Hier sieht man durch die Linie dargestellt, wie der Mitarbeiter zunächst Daten gesammelt hat (Collection), dann versucht hat die wahre Natur der Daten zu verbergen (Obfuscation), um sie anschließend zu exfiltrieren (zu drucken) und schließlich von der Festplatte gelöscht hat, um die Spuren zu verwischen.

Der Königsweg: Adaptive Prävention

Microsofts Insider Risk Management setzt auf eine adaptive Prävention, die Unternehmen hilft, proaktiv auf das risikohafte Verhalten von Einzelnen zu reagieren. Die Lösung ermöglicht es, bei sich riskant verhaltenden Mitarbeitenden automatisch vorab definierte Maßnahmen abzuleiten, etwa die Einschränkung von Zugriffsrechten oder die Einführung restriktiverer Data Loss Prevention Policies gezielt für diese Personen. Eine weitere Option ist proaktive Retention, sodass ein Schutz gegen Sabotage erzielt werden kann. Diese automatische, adaptive Anpassung der Sicherheitsrichtlinien ist das Highlight der Lösung und macht sie zu einem zentralen Bestandteil der internen Sicherheit.

Fazit: Positive Erfahrungen von Kunden

Viele Unternehmen setzen bereits auf Microsofts Insider Risk Management, um sich vor dem Verlust geistigen Eigentums zu schützen und um ihre Wettbewerbsfähigkeit zu wahren. Die positiven Erfahrungen zeigen, dass mit minimalem zusätzlichem Personalaufwand in der IT-Abteilung signifikante Fortschritte erzielt werden. Besonders hervorzuheben ist die erhöhte Transparenz bei Insiderrisiken, die ansonsten häufig im Verborgenen bleiben. Dabei wird die Privatsphäre der überwiegenden Mehrheit der Mitarbeitenden gewahrt, die sich korrekt verhalten, was auch Betriebsräte und Datenschutzbeauftragte überzeugt. In Kombination mit Informationsschutz und Data Loss Prevention sowie weiteren Sicherheitslösungen ermöglicht Microsofts Ansatz die Anwendung vordefinierter Regeln zur Verhinderung von Datenabfluss und zur Abwehr von Sabotage. Auf diese Weise kann der Datenabfluss schnell gestoppt und riskantes Verhalten automatisch erschwert werden.

Interesse?

Wenn Sie selbst einmal Microsoft Insider Risk Management ausprobieren möchten, wenden Sie sich an ihre*n Microsoft-Ansprechpartner*in oder direkt an mich. Technisch kann die Lösung innerhalb einer Microsoft 365-Umgebung für einen Testzeitraum kostenlos genutzt werden.

Synergien und Herausforderungen

Die Integration der NIS2-Richtlinie und der DSGVO zur Stärkung der Cybersicherheit in der EU

Die NIS2-Richtlinie (‚The Network and Information Security (deutsch: Netzwerk und Informationssicherheit) NIS2 Directive') wurde am 27.12.2022 im EU-Amtsblatt veröffentlicht und ist am 16.01.2023 in Kraft getreten. Sie regelt die Cyber- und Informationssicherheit von Unternehmen und Institutionen. Bis Oktober 2024 müssen die EU-Mitgliedsstaaten diese in nationales Recht überführen.

Die NIS-Richtlinie und die Datenschutz-Grundverordnung sind zwei wichtige europäische Rechtsinstrumente, die sich mit Cybersicherheit und Datenschutz befassen. Die NIS-Richtlinie zielt darauf ab, die Sicherheit von Netzwerken und Informationssystemen in der EU zu verbessern, insbesondere für wesentliche Dienste und Anbieter digitaler Dienste (Cole & Schmitz, 2019). Im Gegensatz dazu konzentriert sich die DSGVO auf den Schutz personenbezogener Daten. Trotz ihrer unterschiedlichen Ziele überschneiden sich diese Verordnungen häufig, da die im Rahmen der NIS-Richtlinie geschützten Daten häufig personenbezogene Informationen umfassen (Cole & Schmitz, 2019). Mit der kürzlich vom EU-Rat verabschiedeten NIS2-Richtlinie werden neue europäische Rechtsvorschriften für die IT-Sicherheit eingeführt, die auf der ursprünglichen NIS-Richtlinie aufbauen (Voigt & Bastians, 2022). Es wird erwartet, dass diese aktualisierte Richtlinie die Cybersicherheitsmaßnahmen und die Meldepflichten für die betroffenen Sektoren weiter verschärfen wird. Das Zusammenspiel dieser Verordnungen verdeutlicht den umfassenden Ansatz der EU zur Bewältigung digitaler Bedrohungen und zum Schutz sowohl der Infrastruktur als auch der Privatsphäre des Einzelnen in einer zunehmend vernetzten digitalen Landschaft.

Die NIS2-Richtlinie zielt darauf ab, die Cybersicherheit in der gesamten Europäischen Union zu stärken, indem der Umfang der regulierten Sektoren und Einrichtungen erweitert wird und strengere Anforderungen eingeführt werden (Noack, 2023; Vogel & Ziegler, 2023; Lucini, 2023). Sie ersetzt die bisherigen Kategorien von Betreibern durch ‚wichtige' und ‚wesentliche' Einrichtungen, die in erster Linie anhand der Unternehmensgröße und nicht anhand von Entscheidungen der nationalen Behörden bestimmt werden (Sievers, 2021). Die Richtlinie führt neue Verpflichtungen und geänderte Verfahrensbedingungen ein, die sich auf zuvor ausgenommene Betreiber auswirken und eine Neubewertung derjenigen erfordern, die bereits unter die NIS1 fallen. Die NIS2 befasst sich mit Kritikpunkten am derzeitigen deutschen Rechtsrahmen, darunter unklare Definitionen von kritischen Infrastrukturen und hohe Schwellenwerte (Vogel & Ziegler, 2023). Alle Mitgliedsstaaten haben bis zum 17. Oktober 2024 Zeit, ihre Gesetzgebung an die NIS2 anzupassen. Die Richtlinie zielt darauf ab, einen kohärenteren regionalen Cybersicherheitsrahmen zu schaffen, der die fragmentierte Annahme der Vorgängerrichtlinie behebt und die Widerstandsfähigkeit der Mitgliedstaaten erhöht (Noack, 2023).

Die NIS2-Richtlinie, die seit Januar 2023 in Kraft ist, behebt Schwachstellen in der bisherigen Umsetzung der NIS-Richtlinie, darunter unklare Definitionen von kritischen Infrastrukturen und hohe Schwellenwerte für die Klassifizierung. Diese neue Richtlinie dehnt ihre Reichweite aus, um mehr Sektoren und Unternehmen einzubeziehen, und basiert die Identifizierung auf der Unternehmensgröße und nicht auf der Klassifizierung der Mitgliedstaaten. Sie führt auch detaillierte Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit, strengere Aufsichts- und Durchsetzungsanforderungen sowie harmonisierte Sanktionen ein (Schmitz-Berndt & Chiara, 2022). Einige Mitgliedstaaten, wie Italien und Deutschland, haben bereits nationale Gesetze verabschiedet, die mit Aspekten der NIS2 übereinstimmen. Unternehmen, die in der EU tätig sind, auch solche, die bisher davon ausgenommen waren, könnten vor neuen Herausforderungen bei der Einhaltung der Vorschriften stehen und sollten ihre Cybersicherheitsmaßnahmen neu bewerten, um rechtliche Risiken zu mindern (Lucini, 2023).

Literaturverzeichnis

- Cole, M. D., & Schmitz, S. (2019). The interplay between the NIS directive and the GDPR in a cybersecurity threat landscape. University of Luxembourg law working paper, (2019-017).
- Noack, A. (2023). Mehr Cybersicherheit in einer vernetzten Welt. ENTSORGA-Magazin, 42(4), 28-30.
- Lucini, V. (2023). The ever-increasing cybersecurity compliance in Europe: The NIS 2 and what all businesses in the EU should be aware of. Russian Law Journal, 11(6S), 145-154.
- 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.
- Sievers, T. (2021). Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. International Cybersecurity Law Review, 2(2), 223-231.
- Voigt, P., & Bastians, H. (2022). Neue europarechtliche Anforderungen an die IT-Sicherheit. Rat der EU nimmt NIS2-Richtlinie an–ein erster Überblick. Computer und Recht, 38(12), 768-775.
- Vogel, V., & Ziegler, N. (2023). Kritikalität: Von der BSI-KritisV zur NIS2-Richtlinie. International Cybersecurity Law Review, 4(1), 1-19.

■ Tit.-Univ-Prof. Dr.habil. DDr. Thomas Benesch

Die Zukunft der Cyberbedrohungen: KI und Deepfakes transformieren Social-Engineering-Angriffe

■ Roland Pucher & Manuel Werka

Die Zukunft des Social Engineerings – Künstliche Intelligenz

Die rasante Entwicklung von künstlicher Intelligenz und Deepfake-Technologie eröffnet neue Möglichkeiten für Cyberkriminelle, insbesondere im Bereich Social Engineering. Generative AI spielt eine zentrale Rolle bei Phishing-Angriffen, indem sie gefälschte E-Mails oder menschenähnliche Inhalte erzeugt, die Opfer zur Preisgabe vertraulicher Informationen verleiten. Der Einsatz von künstlicher Intelligenz (KI) steigert die Qualität der Angriffe und reduziert den Aufwand für die Angreifer. Deepfakes ermöglichen es, realistisch wirkende Videos oder Audioaufnahmen zu erstellen, die Personen Dinge sagen oder machen lassen, die sie nie gesagt oder getan haben. Diese Techniken erlauben noch überzeugendere und maßgeschneiderte Social-Engineering-Angriffe. Eine Übersicht über diese Techniken im Social Engineering Umfeld ist in Abbildung 1 dargestellt.

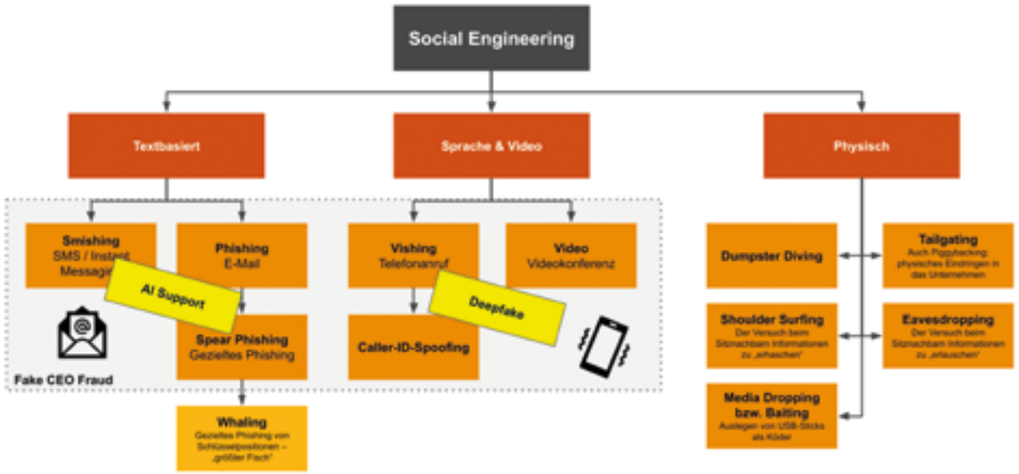


Abb. 1: Übersicht über Social-Engineering Methoden

Deepfakes sind eine spezielle Form der Nutzung von KI-basierter Technologie, welche zunehmend für kriminelle Zwecke missbraucht wird. Die Einsatzmöglichkeiten sind vielfältig und die genannten Beispiele verdeutlichen die Bandbreite moderner Cyberangriffe. Die Bedrohungsszenarien reichen von textbasierten Phishing-E-Mails über sprachbasiertes Voice-Cloning bis zu videobasierten Deepfake-Attacken.

Deep Phishing mittels KI

Phishing ist eine Methode, bei der Betrüger persönliche und sensible Informationen wie Passwörter, Kreditkartennummern oder Bankdaten erlangen. Der Begriff „Phishing" leitet sich von „Fishing" (Angeln) ab, da Betrüger metaphorisch „angeln" nach vertraulichen Daten. Sie nutzen verschiedene Techniken, um Menschen zu täuschen und zur Preisgabe ihrer Informationen zu bewegen. Spear-Phishing zielt auf bestimmte Personen, während Whaling hochrangige Führungskräfte ins Visier nimmt.

Künstliche Intelligenz macht diese Angriffe noch gefährlicher. KI-gestützte Systeme können mittels Natural Language Processing E-Mails verfassen, die den Schreibstil und die Wortwahl von Zielpersonen imitieren. Sie analysieren vorherige Kommunikationen, um authentische und personalisierte Nachrichten zu generieren, die schwer von echten E-Mails zu unterscheiden sind. KI-Systeme nutzen maschinelles Lernen, um spezifische Branchenbegriffe oder Jargon zu integrieren und die Glaubwürdigkeit der Phishing-E-Mails zu erhöhen. Noch höhere Täuschungsraten werden erzielt, wenn E-Mails sich auf aktuelle Ereignisse in den Firmen beziehen, indem KI-Systeme automatisch Social-Media-Plattformen durchsuchen, um auf kürzlich veröffentlichte Ereignisse einzugehen.

Sprach und Video Deepfakes – eine neue Bedrohung

Deepfakes sind digitale Medieninhalte wie Bilder, Video- oder Sprachaufnahmen, welche mithilfe von Künstlicher Intelligenz und maschinellem Lernen manipuliert oder komplett neu generiert werden, um täuschend echte Fälschungen zu erstellen. Der Begriff „Deepfake" setzt sich aus „deep learning" (eine Art des maschinellen Lernens) und „fake" (gefälscht) zusammen. Diese Technologie kann verwendet werden, um das Aussehen und die Stimme einer Person so realistisch nachzuahmen, dass es schwierig ist, den gefälschten Inhalt vom echten zu unterscheiden. Dazu sind nur etwa 5 Minuten Videomaterial des Gesichts und weniger als 5 Minuten Audiomaterial notwendig, um Gesicht und Stimme täuschend echt nachzuahmen. Abbildung 2 stellt eine Übersicht über Methoden zur Generierung von Fake-Medienhinhalten dar.

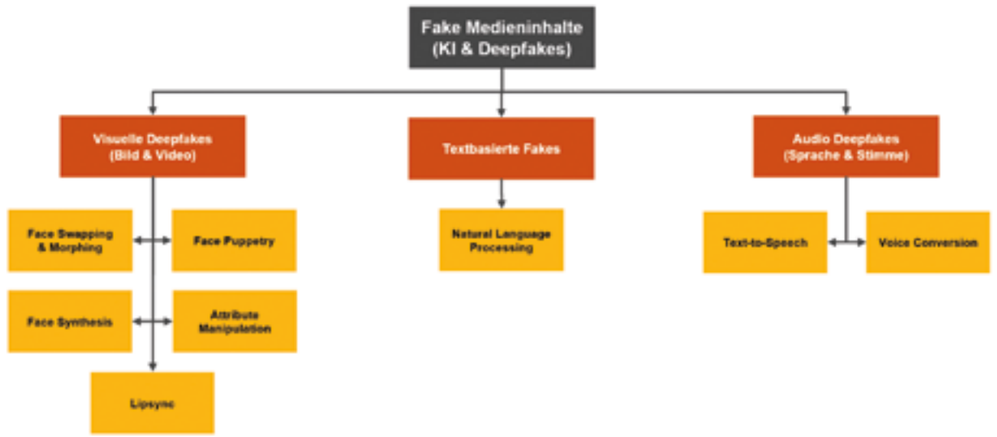


Abb. 2: Übersicht über Methoden zur Generierung von Fake Medieninhalten

Audiovisuelle Deepfakes

Deepfake Videos stellen eine erhebliche Gefahr für Unternehmen dar, da sie für Cyberangriffe und betrügerische Aktivitäten missbraucht werden können. Ein besorgniserregendes Szenario ist der „Fake President Fraud", bei dem Angreifer Deepfake-Video oder -Audio einer Führungskraft erstellen, um Mitarbeiter zu täuschen und sie zur Durchführung betrügerischer Transaktionen oder zur Herausgabe vertraulicher Informationen zu bewegen. Besonders hochrangige Mitarbeiter sind Ziel solcher Angriffe, da die Erzeugung von Deepfakes noch aufwendig ist und ausreichend Video- und Audiomaterial benötigt wird, was bei C-Level Mitarbeitern oft durch Interviews und öffentliche Auftritte gegeben ist. Solche Angriffe können zu erheblichen finanziellen Verlusten und nachhaltigem Reputationsschaden führen. Zudem können Deepfakes zur Verbreitung von Desinformation genutzt werden, was das Vertrauen der Kunden und Partner in das Unternehmen untergräbt. Deshalb ist es für Unternehmen wichtig, sich der Bedrohung durch Deepfakes bewusst zu sein und geeignete Sicherheitsmaßnahmen zu implementieren, um schnell und richtig reagieren zu können.

Mit Face Swap und Voice Conversion Technologie können Deepfake Angriffe auch live durchgeführt werden, indem das Gesicht und die Stimme des Opfers in Echtzeit nachgestellt und in Online-Meetings übertragen werden. Ein ähnliches Risiko besteht beim Caller-ID-Spoofing, bei dem Angreifer die Anruferkennung manipulieren, sodass es scheint, als käme der Anruf von einer vertrauenswürdigen Quelle. Diese Techniken zusammen können dazu führen, dass Mitarbeiter vertrauliche Informationen preisgeben oder unautorisierte Transaktionen durchführen, da sie glauben, den Anweisungen eines legitimen Vorgesetzten zu folgen. Die Konsequenzen solcher Angriffe umfassen finanzielle Verluste, Reputationsschäden und rechtliche Konsequenzen.

Fazit

Diese Angriffe, die sowohl textbasierte Phishing-Techniken als auch komplexere videobasierte und sprachbasierte Täuschungen umfassen, können erhebliche finanzielle und reputative Schäden verursachen. Eine Studie von PwC zeigt, dass die Anzahl von Unternehmen, die in den vergangenen drei Jahren einen Cybervorfall mit einer Schadenshöhe von über 1 Million Dollar hatten, von 27 % auf 36 % gestiegen ist.

KI-gestützte Angriffe sind besonders gefährlich, da sie personalisierte und glaubwürdige Phishing-E-Mails generieren können, die schwer von legitimen Nachrichten zu unterscheiden sind. Spezialisierte Angriffsformen wie Spear Phishing und Whaling, die gezielt hochrangige Führungskräfte ins Visier nehmen, verstärken die Bedrohung. Während man vor einigen Jahren noch Telefonanrufen oder Videokonferenzen vertrauen konnte, stellt die fortschreitende Deepfake-Technologie mittlerweile eine wachsende Gefahr für diese Kommunikationsmittel dar. Ein solcher Fall mit einem immensen finanziellen Schaden wurde 2024 publik: Ein Finanzmitarbeiter überwies 25 Millionen Dollar, nachdem er in einem Videogespräch von einem täuschend echt wirkenden Deepfake des angeblichen Finanzvorstands angewiesen wurde . Ein ähnlicher Fall bei Ferrari im Juli dieses Jahres konnte gerade noch verhindert werden . Der Betrüger nutzte Deepfake-Technologie, um die Stimme des Ferrari-CEO zu imitieren und versuchte, durch einen gefälschten Telefonanruf vertrauliche Informationen zu erlangen.

Um diesen Herausforderungen zu begegnen, sollten Unternehmen nicht nur technische Sicherheitsmaßnahmen implementieren, sondern auch umfassende Awareness-Programme für ihre Mitarbeiter etablieren. Mitarbeiter sollten darin geschult werden, Bedrohungsszenarien zu erkennen, verdächtige Anfragen kritisch zu hinterfragen und mehrstufige Authentifizierungsverfahren zu nutzen, um die Identität von Anrufern oder Absendern zu verifizieren. Insbesondere bei verdächtigen Anfragen sollten alternative Kommunikationswege genutzt werden, um die Echtheit zu überprüfen.

FRAUD und Enterprise Risk Management sowie forensische Praxis

Tatort Unternehmen

In der heutigen Geschäftswelt ist kein Unternehmen vor wirtschaftskriminellen Handlungen sicher. Besorgniserregend ist dabei, dass über die Hälfte aller Betrugsdelikte in Unternehmen, von zwei oder mehr Tätern begangen wird, wie aus dem Report To The Nations 2020, der Association Of Certified Fraud Examiners (ACFE). Das Motiv ist laut dem ACFE-Report zu 42 Prozent auf einen Lebensstil über den eigenen Verhältnissen zurückzuführen. Der Median eines Betrugsschemas bis zur Aufdeckung liegt bei 14 Monaten. Häufig wird nicht erkannt, dass hinter einer Unternehmenskrise oder einem Vermögensverlust wirtschaftskriminelles Handeln steht.

Werden wirtschaftskriminelle Handlungen im eigenen Unternehmen erkannt, ist rasches und effizientes Handeln zur Sicherung der Vermögensgegenstände und zur raschen Klärung der Situation gefragt. Vielfach besteht jedoch die Gefahr, dass durch Untätigkeit oder blindem Aktionismus ein nur noch kaum wiedergutzumachender Schaden, wirtschaftlich, an Reputation, Image und des Betriebsklimas entsteht

Kriminelle Mitarbeiter – was nun?

Die Aufdeckung von wirtschaftskriminellen Handlungen im eigenen Unternehmen stellt die Geschäftsleitung oft vor absolute Ausnahmesituationen. Nur in den wenigsten Unternehmen gibt es spezialisierte Mitarbeiter, die solche Situation handhaben und dementsprechende richtige Maßnahmen setzen können.

In kürzester Zeit muss geklärt werden:

- Was ist wo, wann und wie passiert?
- Wer sind bzw. waren die handelnden Personen?
- Wo liegen die Beweise und wer sichert sie?
- Gibt es Zeugen, die befragt werden können?
- Was sind die angemessenen arbeitsrechtlichen Schritte?
- Wie ist intern wie auch extern zu kommunizieren?
- Sind externe forensische Experten hinzuzuziehen?

Müssen die Maßnahmen und Reaktionen erst im konkreten Anlassfall erarbeitet werden, ist es vielfach schon zu spät und der Schaden kann bestandsgefährdende Dimensionen annehmen.

Notfallmanagement

Unter Notfallmanagement wird die Implementierung strukturierter Abläufe verstanden, wie bei der Entdeckung oder dem Verdacht doloser Handlungen zu agieren ist. Insbesondere die Mitglieder der Geschäftsführung oder des Vorstandes sind gesetzlich dazu verpflichtet, geeignete Maßnahmen zu ergreifen. Vergleiche hierzu das FlexLex Wirtschaftskriminalität, aus dem die wesentlichsten regulatorischen Verpflichtungen festgehalten sind.

Damit ein Notfallmanagement effizient funktionieren kann, sind gewisse organisatorische Grundstrukturen notwendig. Wesentlich dabei ist die Errichtung eines internen Gremiums, das für diese Themenbereiche verantwortlich ist. Hauptaufgabe dieses Gremiums ist die Sicherstellung schneller und vor allem richtiger Reaktionen.

Ein weiteres wichtiges Instrumentarium des Notfallmanagements stellt ein schriftlich fixierter Notfallplan dar. Dies ist ein Dokument, in dem die Grundsätze und Verfahren, die ein Unternehmen in Reaktion auf ein schwerwiegendes Delikt umsetzt, dargelegt sind. Somit unterstützt ein Notfallplan das erforderliche schnelle und vor allem richtige Handeln.

Wesentliche Inhalte eines Notfallplans

Zu einem effizienten und kompletten Notfallmanagement gehören als Basis eine Struktur bestehend aus Notfallstab und Notfallplan sowie strukturierte Prozesse, die eine angemessene Reaktion auf Verdachtsmomente oder entdeckte Fälle ermöglichen. Ziele dieser Prozesse sind einerseits die Sicherung von Beweisen als auch die Vermeidung von unnötigen weiteren Schäden nach der Entdeckung von dolosen Handlungen. Wesentlich ist auch die Be- bzw. Entkräftigung von Verdächtigungen gegen Mitarbeiter. Anschuldigungen können falsch und der Ruf eines Mitarbeiters schnell ruiniert sein. Daher gehört eine strukturierte Behandlung integral zur Wahrnehmung einer Fürsorgepflicht gegenüber allen Mitarbeitern.

Mag. (FH) Christian Gosch & Fabio Lacchini, BSc

Bildung als Schlüssel zur Krisenbewältigung

Mag. Johann Höfler

Im Kontext globaler Krisen wie der COVID-19-Pandemie, wirtschaftlicher Unsicherheiten und klimatischer Veränderungen wird die Bedeutung der Bildung deutlich. Vor diesen Krisen wurde Bildung oft als wichtiger Bestandteil des individuellen und gesellschaftlichen Fortschritts angesehen. Heutzutage ist sie jedoch mehr als das – sie ist ein essenzielles Instrument zur Bewältigung und Überwindung von Krisen.

Vor der Krise galt Bildung als Schlüssel zur persönlichen und beruflichen Entwicklung, zur Steigerung der sozialen Mobilität und zur Förderung wirtschaftlichen Wachstums. Bildungseinrichtungen und -systeme weltweit arbeiteten daran, qualitativ hochwertige und zugängliche Bildungsangebote bereitzustellen. Trotz bestehender Ungleichheiten wurden erhebliche Fortschritte erzielt, insbesondere im Hinblick auf die Einschulungs- und Abschlussquoten.

Heute, im Angesicht globaler Krisen, hat die Rolle der Bildung eine neue Dimension angenommen. Die Fähigkeit, sich an veränderte Umstände anzupassen, ist entscheidend. Bildung muss nun nicht nur Wissen vermitteln, sondern auch Resilienz, Kreativität und Problemlösungsfähigkeiten fördern. Investitionen in Bildung sind daher von größter Bedeutung, um Individuen und Gesellschaften zu befähigen, die Herausforderungen der Krise zu meistern.

Die Vorteile von Investitionen in die Bildung lassen sich wie folgt sehen: Krisenbewältigung und Resilienz: Bildung stärkt die Fähigkeit, Krisen zu bewältigen und sich schnell an veränderte Bedingungen anzupassen. Sie fördert kritisches Denken und Problemlösungsfähigkeiten, die in unsicheren Zeiten unerlässlich sind.

Wirtschaftlicher Wiederaufbau: Gut ausgebildete Arbeitskräfte sind der Motor für wirtschaftlichen Wiederaufbau und Innovation. Investitionen in Bildung tragen zur Schaffung neuer Arbeitsplätze und zur Erholung der Wirtschaft bei.

Soziale Kohäsion: Bildung fördert den sozialen Zusammenhalt und hilft, Spannungen und Ungleichheiten zu verringern. Sie trägt dazu bei, dass alle Mitglieder der Gesellschaft Zugang zu den gleichen Chancen haben.

Betrachtet man Bildung als globales Phänomen, so gilt es, die Bildung unterschiedlicher Welten zu fördern: In der ersten Welt sind die Bildungssysteme oft gut ausgebaut, doch auch sie stehen vor Herausforderungen wie der Digitalisierung des Unterrichts und der Integration benachteiligter Gruppen. Schwellenländer hingegen haben oft dynamische Bildungssysteme, aber es gibt erhebliche Unterschiede in der Qualität und Zugänglichkeit. Investitionen sind notwendig, um Bildung flächendeckend zu verbessern. In vielen Entwicklungsländern hingegen sind

die Bildungssysteme unterfinanziert und haben mit erheblichen Herausforderungen, wie mangelnde Infrastruktur und Lehrermangel zu kämpfen. Hier sind internationale Hilfe und Investitionen besonders wichtig.

Bildung ist eine fundamentale Säule der individuellen und gesellschaftlichen Entwicklung. Sie umfasst weit mehr als nur das Erlernen von Fakten und Theorien. Im 21. Jahrhundert hat sich der Bildungsbegriff erweitert, um den Anforderungen einer digitalen, globalisierten und sich ständig wandelnden Welt gerecht zu werden. Bildung fördert Wissen, Fähigkeiten, Kreativität, soziale und emotionale Entwicklung und interkulturelles Verständnis.

Bildung hat für alle zugänglich, unabhängig von Geschlecht, Herkunft oder sozialem Status zu sein. Bildung soll auch vielmehr kritisches Denken fördern und keine einseitigen Meinungen vermitteln. Insofern ist Bildung auch wichtig für eine funktionierende demokratische Gesellschaft.

Bildung im 21. Jahrhundert zeichnet sich aus durch:

- Digitalisierung: Der digitale Wandel hat enorme Auswirkungen auf die Bildung. Dies umfasst den Zugang zu Online-Ressourcen, E-Learning-Plattformen und digitalen Tools, die den Lernprozess unterstützen. Digitale Kompetenzen sind heute ebenso wichtig wie traditionelle akademische Fähigkeiten.
- Globalisierung: Bildung muss auf eine global vernetzte Welt vorbereiten. Dies bedeutet, interkulturelle Kompetenzen zu fördern und ein Verständnis für globale Zusammenhänge und Herausforderungen zu entwickeln.
- Anpassungsfähigkeit und Flexibilität: Angesichts des schnellen technologischen Fortschritts und sich verändernder Arbeitsmärkte müssen Menschen in der Lage sein, sich an neue Situationen anzupassen und neue Fähigkeiten zu erlernen.
- Interdisziplinäres Lernen: Die komplexen Probleme unserer Zeit erfordern Lösungen, die Wissen aus verschiedenen Disziplinen integrieren. Daher wird interdisziplinäres Lernen immer wichtiger.
- Nachhaltigkeit: Bildung im 21. Jahrhundert muss auch das Bewusstsein für ökologische Nachhaltigkeit fördern und die Bedeutung von umweltfreundlichem Verhalten und nachhaltigem Wirtschaften vermitteln.

Im Zeitalter der Krise ist Bildung somit mehr denn je ein unverzichtbares Gut. Sie ist der Schlüssel zur individuellen und kollektiven Resilienz und zur Bewältigung globaler Herausforderungen. Bildungssysteme weltweit müssen gestärkt und angepasst werden, um den aktuellen und zukünftigen Anforderungen gerecht zu werden. Investitionen in Bildung sind Investitionen in eine sichere und prosperierende Zukunft.

Trotz ihrer großen Bedeutung und vielfältigen positiven Wirkungen gibt es auch Grenzen dessen, was Bildung erreichen kann. Sie ist kein Allheilmittel für alle gesellschaftlichen und wirtschaftlichen Probleme und kann individuelle Unterschiede und Motivationen nicht vollständig ausgleichen. Dennoch bleibt Bildung ein unverzichtbares Instrument zur Förderung von Wohlstand, Gerechtigkeit und demokratischer Teilhabe.

Weiterführende Informationen finden Sie auf:
https://www.zfrk.org/kompetenz/ccncb-network-cluster-bildung

Versicherungslösungen für Unternehmen

Absicherung gegen unvorhergesehene Ereignisse

Dipl.-Ing. Johannes Göllner, MSc & Dr. jur. Wolfgang Reisinger

Die moderne Gesellschaft und Wirtschaft sind ohne Versicherungen nicht denkbar. Von Versicherungen werden Gefahren übernommen, die der Einzelne nicht tragen kann. Die Versichertengemeinschaft und das Gesetz der großen Zahl machen es möglich, auch große Risiken in Deckung zu nehmen („Einer für alle, alle für Einen").

Die private Versicherungswirtschaft ist einer der bedeutendsten Wirtschaftsfaktoren in Österreich, deren Prämieneinnahmen jährlich bei etwa 18 Milliarden Euro liegen. Rund 29.000 Personen sind in Versicherungsunternehmen beschäftigt, dazu kommen über 5.000 Versicherungsmakler*innen und Berater*innen in Versicherungsangelegenheiten sowie zahlreiche andere Personengruppen, die primär in die Abwicklung der rund 8 Millionen Leistungsfälle involviert sind.

Die Versichertengemeinschaft von natürlichen und juristischen Personen stellt eine Risikogemeinschaft dar, welche ihre Risiken aus verschiedensten Gefahren, wie z. B. wirtschaftliche Gefahren, natur- und umweltspezifische Gefahren, das zu erwartende Risiko und das damit verbundene Schadensausmaß an eine Versicherung bzw. Rückversicherung delegiert bzw. überwälzt.

Eine sogenannte Risikodelegation kann Einzelereignisse, multiple Ereignisse als auch sehr komplexe Ereignisbilder bzw. -portfolios umfassen und können z. B. in einem solchen Portfolio an Ereignissen auch eine komplette globale Supply Chain betreffen. Man denke z. B. an die Folgen von Betriebsunterbrechungen oder an Folgewirkungen von bestehenden und zukünftig noch zu entwickelnden nationalen und internationalen Regelwerken im Bereich von Cyber-, künstlicher Intelligenz- und Lieferketten-Gesetzen. Insbesondere die EU NIS 2-Richtlinie (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022), welche seit dem 18.10.2023 auch für spezifische österreichische KMU gilt, oder das Lieferkettensorgfaltspflichtengesetz (LkSG) in Deutschland, welches am 11. Juni 2021 vom Deutschen Bundestag beschlossen wurde und in weiterer Folge auch Auswirkungen auf österreichische Zulieferanten haben kann. Interessante und zukünftige Entwicklung seit dem CrowdStrike-Fall am 19.07.2024, dass die Versicherungswirtschaft darüber nachdenkt, ob IT-Risiken eines solchen Ausmaßes vielleicht in Zukunft unter „Höhere Gewalt" eingestuft werden, denn die damit verbundenen Schäden sind enorm. Hier darf auf ein Interview von Prof. Dr. Jochen SCHILLER mit „Zeit-Online" am 12.08.2024 verwiesen werden, wie folgt Zitat: Digital verursachte Unfälle passieren häufiger, als wir denken. Wenn man technische Schlampigkeiten wie bei CrowdStrike und gezielte Cyber-Angriffe auf Unternehmen oder Ministerien zusammenrechnet, dann haben IT-Ausfälle in Deutschland allein im Jahr 2022 einen Schaden von 206 Milliarden Euro verursacht. Da standen Systeme still, mit allen wirtschaftlichen Folgen. Überstunden für Administratoren mussten bezahlt werden. Europaweit kam eine Schadenssumme von zwei Billionen Euro zusammen.

© U.S. Marine Corps, Photo by Cpl. Robert J. Maurer Source: Wikipedia – Flooding of Rojana Industrial Park, Ayutthaya, Thailand, October 2011

Welche Versicherungen sollten Unternehmen abschließen? Betriebshaftpflichtversicherungen schützen davor, von geschädigten Dritten mit existenzbedrohenden Forderungen in Anspruch genommen zu werden. Für Freiberufler und Selbstständige ist der Abschluss einer Vermögensschadenhaftpflichtversicherung nicht nur großteils vorgeschrieben, sondern ein absolutes Muss. Betriebsrechtsschutzversicherungen ermöglichen nicht nur die Durchsetzung von Forderungen, sondern bieten z. B. auch Schutz bei arbeits- und sozialversicherungsrechtlichen Streitigkeiten. D&O-Versicherungen verhindern, dass Geschäftsführer, Vorstände und leitende Angestellte persönlich in Anspruch genommen werden. Falls Organe und Mitarbeiter häufig unterwegs sind, ist der Abschluss von Reiseversicherungen und Unfallversicherungen ein nützliches Asset. Der Abschluss einer Cyber-Versicherung sollte heutzutage ohnehin selbstverständlich sein.

Eine solide rechtliche Grundlage ist unumgänglich, die Kenntnis der Gesetze und der Judikatur zwingend. Neben einem „juristischen Überbau", der sich mit denjenigen Themen beschäftigt, die spartenunabhängig auftreten können, ist die Kenntnis der Versicherungsbedingungen der einzelnen Sparten unabdingbar (siehe Reisinger/Göllner, beide Zentrum für Risiko- und Krisenmanagement [Hrsg.], Versicherungswirtschaft und Versicherungsrecht, facultas; https://www.facultas.at/item/63895917).

Projekt CONTAIN

Wissenschaft und Praxis entwickeln Maßnahmen

Ob Kliniken, Redereien, Auktionshäuser, oder das kleine Unternehmen von Ort, Ransomware meldet sich täglich weltweit bei ihren Opfern. „Was nun?“, ist deshalb nicht nur die Frage, die sich die betroffenen Organisationen stellen. Auch das deutsch-österreichische Forschungsprojekt CONTAIN tut das, um wirkungsvolle Mittel zur Steigerung der Resilienz zu entwickeln. Serious Games, Referenzmodelle- und -prozesse, Playbooks und ein Framework – nach Projektende sollen die Entwicklungen des Projekts in einer Toolbox der Öffentlichkeit zur Verfügung stehen.

Das Projekt CONTAIN: Länder- und branchenübergreifende Forschung

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

„Die Motivation für das Projekt ist, dass der Einzelne weiß, was zu tun ist, dass Unternehmen vorbereitet sind, die Reaktion der gesamten Supply Chain aufeinander abgestimmt ist, sowie die Pläne passgenau und in den Köpfen präsent sind“, so Projektleiterin Prof. Dr. Ulrike Lechner von der Universität der Bundeswehr München.

Spielend gut vorbereitet

In seinem Lagebericht für 2023 spricht das Bundesamt für Sicherheit in der Informationstechnik (BSI) von einer angespannten Sicherheitslage, der Unternehmen mit dem Aufbau von Cyberresilienz begegnen müssen, die neben technischen und organisatorischen Maßnahmen auch die Schulung der Mitarbeitenden umfasst. Hier passgenaue Maßnahmen zu entwickeln, die nicht nur bilden, sondern auch noch Spaß machen, ist ein Aspekt der deutsch-österreichischen Zusammenarbeit. So entstanden bereits mehrere Serious Games. Beispiel dafür sind das Computerspiel „Digital Detectives“, in dem man in die Rolle eines Forensikers schlüpft. „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.

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: https://www.linkedin.com/groups/9549256/.

Ein Werkzeugkasten gegen Ransomware

Judith Strussenberg, M.A.; Prof. Dr. Dipl. Inform. Ulrike Lechner & Dr. Steffi Rudel

Status QUO: Arbeitskräfte[krise]- und Kompetenzmangel am D-A-CH Arbeitsmarkt: Leistungsfähigkeiten und Innovationen des Bildungssektors im Rahmen der digitalen Transformation für Unternehmen

Kann eine mögliche Ingenieur-Zertifizierung die Problematik lindern?

Unbestritten stellt die Digitalisierung unsere Gesellschaft, den öffentlichen Dienst und die Unternehmen vor große Herausforderungen. Eine der größten darunter ist wohl die Qualifizierung einer ausreichenden Zahl qualifizierter IT-Fachkräfte. Die nötige Aus-, Fort- und Weiterbildung dieser qualifizierten Arbeitskräfte ist derzeit kaum zu stemmen aber unabdingbar, um im zunehmenden Wettbewerb einer globalisierten Welt bestehen zu können. Die Schwierigkeiten IT-Fachkräfte zu finden, gilt für Österreich, Deutschland und Schweiz gleichermaßen.

Am 03.10.2023 präsentierte das Zentrum für Risiko- und Krisenmanagement iRd. IKT-Sicherheitskonferenz 2023 des BMLV/AbwA mit seinem Mitglied Vienna International Studies und Kooperationspartner Allensbach Hochschule den Status quo des Arbeitskräfte- und Kompetenzmangel in Österreich.

In Österreich fehlen für die kommenden fünf Jahre 30.000 IT-Fachkräfte, berechnete der Fachverband Ubit der österreichischen Wirtschaftskammer schon 2022. In einem Bericht des Instituts der deutschen Wirtschaft (IW, 08.06.2023) wird der Fachkräftemangel in IT-Berufen in Deutschland für das Jahr 2022 mit 68.000 offenen Stellen angegeben, insbesondere auch dem Umstand geschuldet, dass der zusätzliche Bedarf infolge der Digitalisierung mit einem Rückgang der Absolventenzahlen an den Hochschulen zusammenfällt. Es fehlten deutschlandweit im Jahr 2022 fast 34.000 Fachkräfte mit einem Hochschulabschluss. Für acht von zehn Stellen auf diesem Qualifikationsniveau gab es kein passendes Angebot des Arbeitsmarktes. Diese Lücke kann weder kurz- noch mittelfristig durch Studienabsolventinnen und -absolventen geschlossen werden. Es wird sogar damit gerechnet, dass die Absolventenzahlen in den Bereichen Mathematik, Informatik, Naturwissenschaft und Technik weiter sinken werden.

Ähnlich die Situation in Österreich, nur 13,2 % der Studienabschlüsse 2019 (ca. 4600) entfielen auf das ISCED-Studienfeld der Gruppe „Naturwissenschaften, Mathematik und Statistik“ und 3,9 % (1370) in der Gruppe „Informatik und Kommunikationstechnologie“.

Ein geeigneter Weg könnte 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.

Eine Bitkom-Studie vom November 2022 sieht einen Anstieg der Anzahl der zu besetzenden IT-Stellen in Deutschland auf 137.000 und geben darin – unabhängig von der Größe - 65 % der Unternehmen an, offene IT-Stellen nicht besetzen zu können.

Kurz zusammengefasst: die Lücke an fehlenden IT-Fachkräften kann über geeignete Hochschulabsolvent:innen nicht geschlossen werden und wir müssen in einer gemeinsamen gesamtstaatliche Anstrengung geeignete Maßnahmen ergreifen:

- Schaffung von mehr Studien- und Ausbildungsplätzen an Allgemein bildenden & höheren berufsbildenden Mittelschulen (HTBLA), facheinschlägigen (privaten) (Fach-) Hochschulen und facheinschlägigen privaten und öffentlich-rechtlichen Universitäten;
- Definition der für die Digitalisierung benötigen Reifegrade zur Abbildung der nötigen IT-Kompetenzen,
- darauf abgestimmte Aus-, Fort- und Weiterbildungsmaßnahmen der Unternehmen selbst zur Ausbildung der nötigen neuen Mitarbeiter:innen und Umschulung der vorhandenen und dafür geeigneten Arbeitskräfte.

Die IngG-Fachrichtungsverordnung normiert neun technische und gewerbliche Fachrichtungen, darunter Informatik/Informationstechnologie (*EDV und Organisation, Informatik, Informationstechnologie, eGovernment und eHealth*) und Wirtschaftsingenieurwesen (*Wirtschaftsingenieure-Informationstechnologie und Smart Production*).

Voraussetzung dafür sind die berufliche Erfahrung/Ausbildung und eine schulische oder akademische Vertiefung berufspraktischer Kenntnisse.

Die praktische Umsetzung können Unternehmen maßgeschneidert mit der „School of Excellence für Leadership, Strategie, Risiko- und Innovationsmanagement“ des Zentrums für Risiko- und Krisenmanagement (ZRK) und seiner Tochtergesellschaft „ZRK-Corporate Academy: Private Bildungs- und Forschungs GmbH“, angehen.

Rektor Prof. DDr. Martin Stieger

RISIKOMANAGEMENT für Gemeinden

Kommunales Risikomanagement: Entscheidende Schritte für die Zukunftssicherung der Gemeinden

Der Artikel stellt das kommunale Risikomanagementmodell vor, das zentrale Akteure wie Gemeinderat und Bürgermeister(in) in den Fokus rückt, besonders in Hinblick auf neue EU-Regularien im Bereich CYBER. Es werden die Entscheidungsprozesse und die Rolle des Risikomanagements in der Gemeindeverwaltung beleuchtet, von der Risikoidentifikation bis zur Effizienzprüfung durch den Prüfungsausschuss.

Das Ziel des kommunalen Risikomanagements ist es, die Existenz und den Erfolg der Kommune zu sichern, indem es Risikokosten reduziert und frühzeitig gegen Entwicklungen vorgeht, die den festgelegten Zielen entgegenstehen. Trotz weniger gesetzlicher Vorgaben wie im privatwirtschaftlichen Sektor werden Entscheidungsprozesse auf verschiedenen Ebenen durch das kommunale Risikomanagementmodell geregelt. Es werden jedoch seit einigen Jahren EU Directives, wie NIS1 und seit Dezember 2022 NIS2 (Rechtsumsetzung in Österreich bis 17.10.2024) veröffentlicht, welche eventuell einen unmittelbaren oder mittelbaren Einfluss zur Begründung eines Risikomanagements und Krisenmanagements für öffentlichrechtliche Körperschaften, wie Gemeinden, Städten und deren Tochtergesellschaften (z. B. Versorgungs- und Entsorgungsbetriebe gemäß EU Directive NIS2) ausüben bzw. initiieren können.

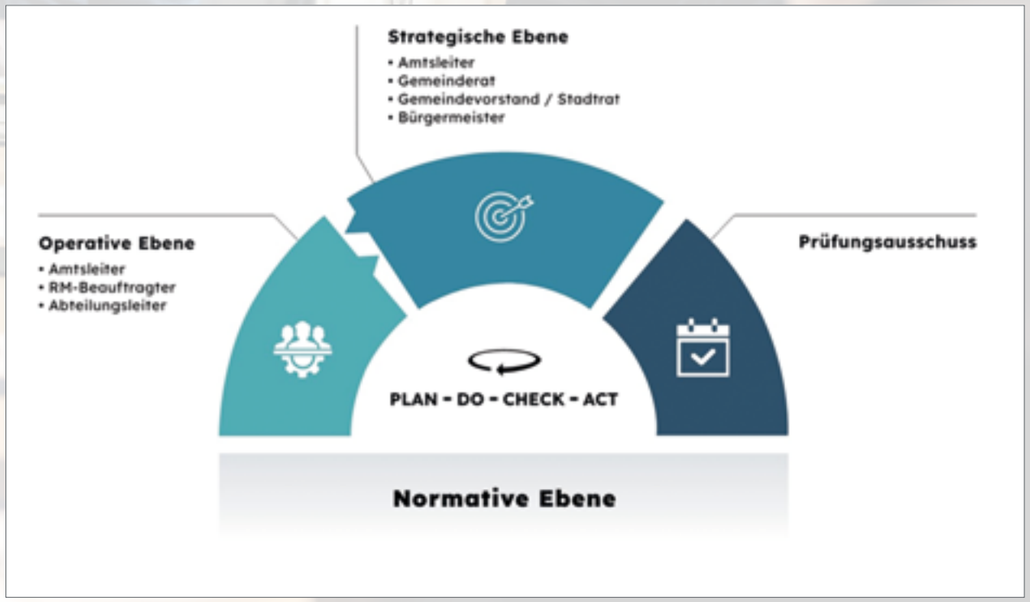
Globalisierung, Digitalisierung und Automatisierung sind die Treiber für eine holistischen Betrachtung der Verletzbarkeit der Supply Chain und seiner Netzwerke (Basic-, Supply- und Public Networks) -in Beziehung zum CYBER-Raum und zu Cyber-Events. Unter Berücksichtigung der Einbettung in transnationale 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 eine essenzielle Grundlage zur Entwicklung von Strategien für Risikoreduktion und Resilienz-Design in der Supply Chain und ICT/CYBER Security.

Der Gemeinderat, Gemeindevorstand oder Bürgermeister(in) treffen dabei richtungsweisende Entscheidungen und sind für die Risikowahrnehmung und Festlegung strategischer Ziele verantwortlich. Sie beurteilen auch Risiken von Tochterunternehmen und Beteiligungen. Der Bürgermeister(in) legt zusammen mit der Amtsleitung Aufgaben und Verantwortlichkeiten der Verwaltung fest, die für die Umsetzung von Maßnahmen zuständig ist. Abteilungsleiter, in Abstimmung mit dem Risikomanagementbeauftragten und der Amtsleitung, sind verantwortlich für den Risikomanagementzyklus, der die Identifikation, Bewertung, Steuerung, Berichterstattung und Überwachung von Risiken umfasst. Sie entscheiden über konkrete Steuerungsmaßnahmen wie Risikovermeidung, -verminderung, -überwälzung oder Selbsttragung, abhängig von der Risikopolitik der Gemeinde. Die für Risikomanagement zuständige Person agiert als zentraler Ansprechpartner und Koordinator, berät in Risikofragen und ist verantwortlich für die Einführung und Erprobung von Notfall-, Krisen- und Business Continuity Management. Der Prüfungsausschuss überprüft schließlich das Risikomanagement auf Wirtschaftlichkeit, Zweckmäßigkeit und Sparsamkeit.

ICT/CYBER-Ereignis-/Bedrohungsbilder, die zu Unterbrechungen und Engpässen in der lokalen und regionalen Versorgung bzw. Lieferkette beitragen können, sind in Korrelation zu Supply Chain Unterbrechungen in das Risk Assessment einzubinden. Das Erarbeiten von umfassenden und ganzheitlichen 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 -, wird dies auch die öffentliche Verwaltung ab 2024/2025 und in den Folgejahren – wie bei Unternehmen und KMU auch – im Besonderen herausfordern.

Zusammenfassend ist die Etablierung eines Risikomanagements, auch unabhängig von existierenden Regelwerken wie Standards und nationaler Gesetze sowie EU-Gesetzen, für Gemeinden und Städte sehr zu empfehlen, da es die Wahrnehmung von z. B. wirtschaftlichen, rechtlichen, infrastrukturellen, natur- und umweltspezifischen Risiken – präventiv und vorausschauend – erkennen lässt, um so vor unvorhergesehenen Ereignissen und/oder Krisen geschützt bzw. resilient vorbereitet zu sein.

■ Mario Gubesch, MA MBA & Dipl.-Ing. Johannes GÖLLNER, MSc



Supply Chain Resilienz und Security Management und innovative Lösungsbeiträge für Unternehmen, insbesondere für KMU

■ Dipl.-Ing. Johannes GÖLLNER, MSc

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 (z. B. Bevorratung, Eigenfertigung, Rohstoffselbstversorgung) auf staatlicher und unternehmerischer Ebene festzustellen, um zur Strategie- und Produkt-Entwicklung beitragen zu können.

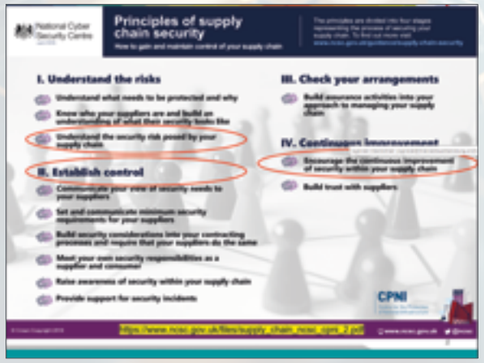
Globalisierung, Digitalisierung und Automatisierung sind die Treiber für eine holistischen Betrachtung der Verletzbarkeit der Supply Chain und seiner Netzwerke (Basis-, Versorgungs- und Public Netzwerke) als Summe der primären- und Hilfsprozesse (insbesondere Lagerung und Transport von Waren, Informationen und Geld) -in Beziehung zum CYBER-Raum und -Events. Unter Berücksichtigung der Einbettung in transnationale und internationale Versorgungssysteme (Energie, Rohstoffe, Lebensmittel, medizinische Verbrauchsgüter, Informationen etc.), die durch politische, rechtliche, ökonomische, zivile, technische, sowie Natur-/Biologische und Umweltereignissen, „man-made“ und „non man-made“ zu Unterbrechungen und Engpässen in der Versorgung führen können, ist diese holistische Betrachtung die essenzielle Grundlage zur Entwicklung von Strategien für Risikoreduktion und Resilienz-Design in der Supply Chain. ICT/CYBER-Ereignis-/Bedrohungsbilder (denken Sie an Fehler und somit mangelhaftem Qualitätsmanagement bei der Software-Entwicklung und -lieferung), die zu Unterbrechungen und Engpässen in der regionalen, nationalen, supranationalen und internationalen Versorgung beitragen können, sind in Korrelation zu Supply Chain Unterbrechungen in das Risk Assessment einzubinden. Dies wurde durch das ZRK iRd. IKT-Sicherheitskonferenz 2023 in Linz in einem Vortrag hervorgehoben.

Die Schäden -Supply Chain Risks & Losses-, infolge Supply Chain Unterbrechungen, können sehr vielfältig sein, wie z. B.

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

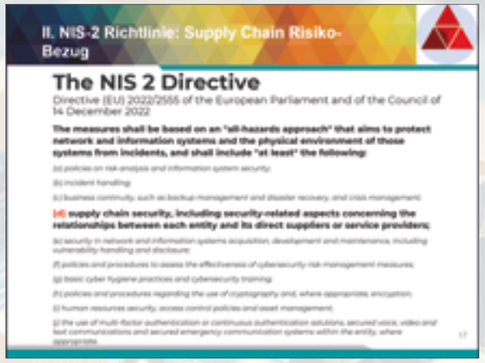
Das Zentrum für Risiko- und Krisenmanagement (ZRK) hat mit Partnern ein umfassendes und ganzheitliches Cyber Security & Supply Chain Resilience (Security) Monitoring, Rating und Auditing Konzeptes erarbeitet, weil Cyber Events (weltweit: 34 %; AT: 40 %; GE: 40 %; CH: 57 %) und Supply Chain Interruptions-Betriebsunterbrechungen (weltweit: 34 %; AT: 32 %; GE: 46 %; CH: 41 %) zu den 10 weltweit größten Risiken, gemäß „Allianz Global Corporate & Specialty in Allianz Risk Barometer 2023: Die 10 größten Geschäftsrisiken 2023, weltweit“, gehören.

Bereits 2018 hat das National Cyber Security Centre, U.K. den thematischen Zusammenhang zwischen Supply Chain Security und Cyber Security dokumentiert und veröffentlicht



Deshalb reagieren die nationalen Gesetzgeber, wie z. B. Deutschland mit dem Lieferketten-sorgfaltspflichten¬gesetz, welches 1. Januar 2023 in Kraft getreten ist und auch mögliche Auswirkungen auf österreichische Zulieferanten Auswirkungen haben könnte. Das Gesetz regelt die unternehmerische Verantwortung für die Einhaltung von Menschenrechten in den globalen Lieferketten.

Der supranationalen Gesetzgeber (EU) reagiert darauf mit z. B. der EU NIS2-Directive (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022), welche auch ab 18.10.2024 in Österreich und allen EU-Mitgliedschaften für spezifische KMU gelten werden. Betroffen sind KMU, welche sogenannte wesentliche oder wichtige Einrichtungen und dem Kriterienkatalog dieser EU-Directive entsprechen. Das wesentliche ist, dass zum ersten Mal Cyber Security mit Supply Chain Security und zugehörigen Krisenmanagement kombiniert werden, welche bei der Auditierung nach ISO 27001 in Korrelation mit anderen Standards abgefragt werden müssen. Bei den wichtigen Einrichtungen der „Abfallbewirtschaftung“ werden indirekt, möglicherweise auch KMU der Kreislaufwirtschaft (Circular Economy) adressiert.



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

Die Entwicklung von CYBER/Supply Chain Resilience-Produkte- und Service-Lösungen -insbesondere für Klein- und Mittelbetrieben (KMU)-, in Kooperation mit dem ZRK-ICT/Cyber Netzwerk & Kooperation Cluster aus ICT/CYBER Produkte- und Service-Anbieter im D-A-CH Raum und im Sinne der Philosophie: „Von Unternehmer(n)-für Unternehmer(n)“ hat das ZRK 2018 auch die Idee zur Gründung einer Genossenschaft formuliert. Am 10.12.2022 – nach der COVID-Zeit – war es dann so weit, die Genossenschaft für Digitalisierung, Challenge und Innovation Management (GDCIM; https://www.gdcim.coop) – nach Schweizer Recht – wurde für KMU und den D-A-CH Raum in Volketswil im Kanton Zürich gegründet und wurde iRd IKT-Sicherheitskonferenz 2023 in Linz am 04.10.2023 erstmals offiziell vorgestellt (https://www.zfrk.org/allgemein/gdcim-informations-und-kommunikationstechnologie-in-der-dach-region/). Das ZRK ist eine der ersten neun Gründungsgenossenschafter der GDCIM. Diese Innovation ist auch in Hinblick auf den bestehenden IKT-Fachkräftemangel und des damit verbundenen Mangels an Human Capital Reifegraden im IKT-Bereich von Unternehmen zu sehen.

Die „GDCIM – Genossenschaft für Digitalisierung, Challenge und Innovationsmanagement“ ist das Kompetenzzentrum von KMU für KMU und Freie Berufe und Privathaushalten als:

- Einkaufs- und Leistungsgemeinschaft von KMU-spezifischen Software-/Hardware-Lösungen von BIS-Betrieblichen Informations- und Cyber Security Systemen/Lösungen
- Konzeption/Design von IKT-Lösungen für KMUs und Privathaushalten, und
- KMU- und Privathaushalten-Hilfe-/Notfallverbund für Notfall/Krisenmanagement, z. B. bei IT-Ausfällen, IT-Instandhaltung, IKT – Cyber Angriffen, Cyber Kriminalität, Zertifizierung, Auditierung ...

in Österreich, Schweiz und Deutschland (D-A-CH), zur Sicherung und Förderung deren CYBER und IKT-Kompetenzen und Fähigkeiten und wirtschaftlichen Interessen, durch Organisation einer gemeinsamen Selbsthilfe und der damit verbundenen Begründung einer Risikovermeidungs- bzw. -minimierungs-Gemeinschaft.

Die praktische Umsetzung von Cyber- und Supply Chain Security Projekten und Lösungen können Unternehmen maßgeschneidert mit dem Zentrum für Risiko- und Krisenmanagement (ZRK) und der GDCIM-Genossenschaft für Digitalisierung, Challenge und Innovationsmanagement angehen. Rufen Sie uns an. Wir helfen Ihnen gerne.

Sicherheitspolitische und –strategische Risikoanalyse als Fundament für Unternehmenssicherheit

■ Christian Paul, BSc, MA & Dipl.-Ing. Johannes GÖLLNER, MSc

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

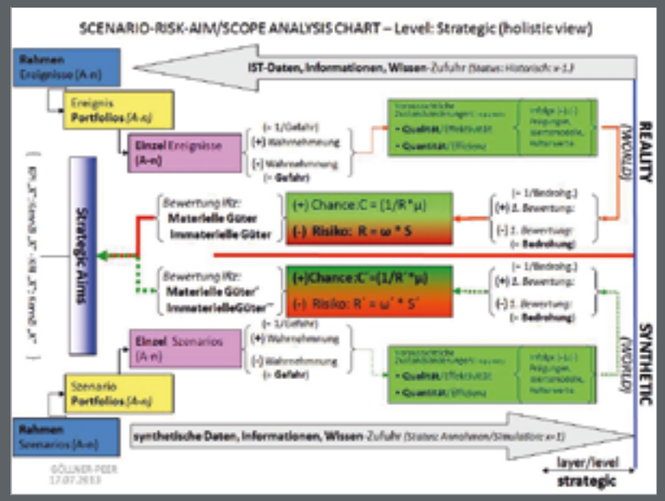
Erfolgreiche Sicherheitspolitik und das Design von Sicherheitsstrategien für den öffentlichen und privaten Sektor –im globalen Kontext-, insbesondere bei der Entwicklung von zukunftsweisenden Konzepten zu Resilienz und zum Schutz kritischer Infrastrukturen, benötigt den offenen und unvoreingenommenen Gedankenaustausch aller Akteure einer Gesellschaft, der Politik, der Wirtschaft, der öffentlichen Verwaltung sowie der Wissenschaft und der Forschung. Die Diskussion der Komplexität und die Veränderung der Komplexität im Verlauf der Zeit sowie die Rückschlüsse aus dem Verhalten eines Systems oder Teilsysteme sind wesentliche Aspekte zur Generierung sicherheitspolitischer Konzepte und davon abgeleiteter Strategien von und für individuelle und kollektive soziale Akteure.

Das Zentrum für Risiko- und Krisenmanagement hat hierzu im Dezember 2019 inhaltlich die Initiative ergriffen und nach der COVID19-Zeit im Oktober 2022 das Competence Center: Sicherheitspolitik (CC:SiPol) gegründet. Das CC:SiPol fördert die Diskussion und Entwicklung einer umfassenden und ganzheitlichen sicherheitspolitischen Sichtweise im Sinne des Securitization-Konzepts , das wirtschaftliche Sicherheit, Umweltsicherheit, gesellschaftliche Sicherheit, politische Sicherheit, öffentliche Sicherheit umfasst. Das CC:SiPol hat den Themenkomplex Cybersicherheit und Weltraumsicherheit, und deren globale Wechselwirkungen und Auswirkungen hinzugefügt, um gesamtheitliche Modellierung und Simulationen für strategische und sicherheitspolitische Analysen für Unternehmen und andere Stakeholder ermöglichen zu können.

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

Um diesen Diskurs zu fördern und um der sicherheitspolitischen Praxis theoretische, methodische und praktische Impulse zu geben, wollen wir einen sicherheitspolitischen Think-Tank anbieten, welcher sich mit Innovationen bei qualitativen und quantitativen Konzepten, Modellen, Methoden und Werkzeugen im Bereich Monitoring, Risk Assessment sowie Modeling und Simulation beschäftigt, um den zukünftigen Grad der erforderlichen Resilienz auf unterschiedlicher Systemebene angesichts variabler Sicherheitsherausforderungen beurteilen und als thought leader unterstützen zu können.

Ziel eines solchen Think-Tanks ist es, grundlegende sicherheitspolitische, strategische Konzepte zur Steigerung der Resilienz und praxistaugliche Vorschläge zur Weiterentwicklung für Unternehmen, für die Wirtschaft und andere Stakeholder zu erstellen. Im Spannungsfeld von z. B. Globalisierung, Entdecken, Gestalten und Ökonomisierung des Weltraums sowie Digitalisierung und Automatisierung gedeiht das Interesse an einer holistischen Betrachtung sowie der Entwicklung von Strategien für Risikoreduktion und Resilienz.



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

Infolgedessen hat das Zentrum für Risiko- und Krisenmanagement mit seinem Competence Center: Sicherheitspolitik – im Herbst 2023 – die Initiierung, Entwicklung und Durchführung der ersten Vienna Space Security Conference am 17.09.2024 – im Rahmen der IKT-Sicherheitskonferenz 2024 (seminar.bundesheer.at) in Wien – beschlossen, siehe www.vssc.space.

Bei der VSSC 2024 kommen Entscheidungsträger, Meinungsbildner, Führungskräfte aus Politik, Wirtschaft, Medien, Forschung, Zivilgesellschaft, internationalen Organisationen und Nichtregierungsorganisationen zusammen, um Innovationen, Trends und die Zukunft der wirtschaftlichen Nutzung des Weltraums -aus der Sicht: „Space Security-Cyber Security und Supply Chain Security“ z. B. infolge der EU-Directive NIS 2 zu diskutieren.

Die VSSC 2024 diskutiert umfassend die komplexen Zusammenhänge wie z.B. „Space Security, Cyber Security und Supply Chain Security“ und die Einflüsse auf und durch die globalen sicherheitspolitischen Rahmenbedingungen. Innovative sowie robuste Sicherheitskonzepte für die Wirtschaft und die Weltgemeinschaft zur Nutzung und Ökonomisierung des Weltraums durch private und staatliche Akteure sind vonnöten, da z. B. die weltraumbasierten kritischen Infrastrukturen (z.B. Satelliten für Informations- und Kommunikation, Navigation, Erdbeobachtung etc.) mittlerweile für das Funktionieren unserer Wirtschaft, der Logistik, Supply Chain etc. existenziell sind.

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