Jahrestagung Handelsblatt Cybersecurity 2024

Angespannte Lage, entschiedene Antworten: Cybersicherheit in Deutschland 2024 – Claudia Plattner

Die aktuelle Cybersicherheitslage in Deutschland ist angespannt und geprägt von zunehmenden Bedrohungen durch Ransomware, DDoS-Attacken und eine wachsende Zahl von Sicherheitslücken. Laut Bitkom belaufen sich die Schäden durch Cyberangriffe auf deutsche Unternehmen im Jahr 2024 auf geschätzte 179 Milliarden Euro. Dabei werden täglich etwa 309.000 Schadprogrammvarianten und 78 neue Schwachstellen identifiziert – ein Volumen, das manuell nicht mehr handhabbar ist. Die Zahl der gemeldeten Vorfälle beim Bundesamt für Sicherheit in der Informationstechnik (BSI) ist um 33 % gestiegen, wobei die Dunkelziffer potenzieller Angriffe in Netzwerken noch unbekannt bleibt.

Angesichts der zunehmenden Digitalisierung wächst die Angriffsfläche erheblich, was nicht nur den Wohlstand bedroht, sondern auch die demokratische Stabilität gefährdet. Die geopolitische Lage erschwert die Situation zusätzlich, da zwischen Spionage und Sabotage oft nur ein schmaler Grat liegt. Das BSI, das nun für rund 29.000 Einrichtungen, darunter KRITIS-Betreiber, als Aufsichtsbehörde fungiert, fordert entschiedene Maßnahmen, wie die Einführung von Melde-, Registrierungs- und Nachweispflichten.

Ein zentraler Lösungsansatz ist eine stärkere Zusammenarbeit zwischen Behörden, Wirtschaft und Forschung. Es braucht eine „Cybernation Deutschland“, bei der alle Akteure miteinander verbunden arbeiten. Universitäten und Unternehmen zeigen Interesse an gemeinsamen Initiativen, wie der Allianz für Cybersicherheit, und streben eine höhere Automatisierung bei der Verarbeitung von Bedrohungs- und Schwachstellenmeldungen an. Das Ziel: Effektive Resilienzmaßnahmen entwickeln und Cybersicherheit auf die Agenda setzen.

Zudem wird die Authentizität von Informationen als entscheidend erachtet, um Vertrauen in die Arbeit des BSI sicherzustellen. Ansätze wie Zertifizierungen und geschlossene Benutzergruppen könnten hier Abhilfe schaffen. Trotz der Herausforderungen gibt es eine klare Botschaft: Es besteht keine Lust mehr auf Resignation, sondern auf entschlossene Antworten. Deutschland will sich der Cyberbedrohung aktiv stellen und innovative Lösungen vorantreiben – die Cybernation!

Cybersicherheit in erhöhter Bedrohungslage – Szenarien und Herausforderungen für die wehrhafte Demokratie - Sinan Selen

Die aktuelle Bedrohungslage für deutsche Unternehmen zeigt, dass Cyberangriffe zunehmend mit realweltlichen Bedrohungen verknüpft sind. Nachrichtendienstliche Akteure, insbesondere aus Russland und China, entwickeln sich kontinuierlich weiter und greifen gezielt KRITIS-Unternehmen sowie Organisationen an, die im Kontext des Ukraine-Krieges stehen. Ziele sind dabei Logistik, Luft- und Raumfahrt, IT-Dienstleister sowie politische Stiftungen und Verbände. Die Angriffe werden immer ausgefeilter: Neben direkten Cyberangriffen setzen Angreifer auf gefälschte Nachrichtenartikel, die über Bots und soziale Netzwerke verteilt werden, um gezielt

Meinungsbildung und politische Destabilisierung zu betreiben. Auch niederschwellige Akteure, salop gesgat „Useful Idiots“, werden über Plattformen wie Telegram angeworben und oft mit Kryptowährungen entlohnt, um Spionage- und Sabotageaktionen durchzuführen. Solche Methoden erschweren die Aufklärung und Abwehr erheblich.
China zeigt eine zunehmende Industrialisierung der Cyberspionage, unterstützt durch Unternehmen, die verpflichtet sind, Schwachstellen an die Regierung zu melden. Russland hingegen agiert aggressiver im Informationsraum, insbesondere seit Beginn des Ukraine-Krieges, und testet durch Angriffe die Reaktionsfähigkeit von Ländern und Behörden. Dabei werden sowohl digitale als auch physische Angriffsmethoden genutzt, beispielsweise durch Einheiten wie die GRU oder prorussische Aktivistengruppen wie „Noname 57“.
Die Zukunft der Cybersicherheit wird durch eine stärkere Verknüpfung von Cyber- und realweltlichen Bedrohungen geprägt sein. Gleichzeitig wird erwartet, dass Nachrichtendienste einerseits ihre „Show-of-force“-Strategien ausbauen und andererseits verdeckte Aktivitäten fortsetzen. Angriffe werden eng mit geopolitischen Entwicklungen und Konflikten verknüpft bleiben.
Um dem zu begegnen, bedarf es eines zeitgemäßen Werkzeugkastens und intensiver nationaler und internationaler Zusammenarbeit, etwa mit Partnern wie dem FBI. Der Austausch von Informationen und eine klare öffentliche Kommunikation sind essenziell, um Handlungsfähigkeit sicherzustellen und Bedrohungen effektiv zu begegnen. Cybersicherheit wird somit zu einem internationalen Teamsport, der ein abgestimmtes Vorgehen und den Einsatz nachrichtendienstlicher Mittel erfordert.

Militärische Herausforderungen im Cyber- und Informationsraum - Generalleutnant Michael Vetter

Die sicherheitspolitische Lage ist komplexer denn je, insbesondere durch den Krieg in der Ukraine, der zeigt, wie stark der Cyberraum als strategisches Mittel genutzt wird. Angriffe betreffen nicht nur direkte Ziele, sondern auch Partner und Bündnisse, um Unsicherheit zu schüren und Allianzen zu schwächen. Hacktivisten und gezielte Desinformation spielen dabei eine zentrale Rolle. NATO-Strategien wie "Persistent, Simultaneous, Boundless" betonen, dass klassische Grenzen zwischen Frieden und Krieg zunehmend verschwimmen. Technologien wie Künstliche Intelligenz und Quantentechnologie werden in Zukunft massive Auswirkungen auf militärische Strategien haben.
Für die Bundeswehr ist Cybersicherheit ein integraler Bestandteil der Gesamtsicherheit. Ziel ist es, eine „Software-defined Defense“ zu etablieren, bei der digitale Technologien, modulare Architekturen und Schnittstellen eine zentrale Rolle spielen. Eine engere Zusammenarbeit mit der Rüstungsindustrie und Start-ups soll Innovationsprozesse fördern. Prototypen und frühzeitige Diskussionen über neue Technologien sind essenziell, um Resilienz und Überlegenheit im Cyberraum zu gewährleisten.

Die Bundeswehr setzt dabei auf aktive Cyberabwehr, die auch gezielte Einwirkungen auf Gegner umfasst. Eine effektive Verteidigung ist nur durch die gemeinsame Anstrengung von Militär, Wirtschaft und Gesellschaft möglich. Gleichzeitig betont Herr Vetter, dass der Mensch weiterhin eine wichtige Rolle spielt, insbesondere bei der Abschätzung von „akzeptablen Risiken" im Einsatz von Technologien und KI (wie es aktuell auch schon in anderen Kontexten gemacht wird). Initiativen wie die Cyberreserve, bei der ehemalige Soldaten eingebunden werden, sollen dazu beitragen, IT-Expertise zu sichern.
Das Fazit lautet: Wer nicht digitalisiert, verliert – wer konsequent digitalisiert, gewinnt. Cybersicherheit ist ein essenzieller Teil der integrierten Sicherheit, und nur durch gemeinsame Anstrengungen kann die Bundeswehr ihre Ziele erreichen.

Vor die Welle kommen: Strategien zur Stärkung der Cyberabwehr in einer komplexen Bedrohungslandschaft – Naby Diaw, Sabine Griebsch, Claudia Plattner

Die Diskussion beleuchtete aktuelle Herausforderungen in der Cybersecurity, insbesondere im Zusammenhang mit KRITIS und großen Unternehmen wie Lufthansa. Der Vorfall mit Crowdstrike zeigte, wie stark Organisationen in einem operativen Ökosystem voneinander abhängen. Trotz schnellem Reagieren und der Bereitstellung von Workarounds wurde deutlich, dass Ausfallsysteme oft unzureichend vorbereitet sind. Ein zentraler Punkt war die Frage der Haftung bei solchen Vorfällen, wobei eine Klagekultur als kontraproduktiv angesehen wurde. Stattdessen müsse aus Fehlern gelernt und die Zusammenarbeit gestärkt werden, um die Resilienz zu erhöhen.
Die Abhängigkeit von ausländischen Cybersecurity-Produkten, insbesondere aus den USA, wurde kritisch betrachtet. Es besteht ein Bedarf, strategisch Nischen zu besetzen und langfristig unabhängigere Lösungen zu schaffen. Allerdings sei vollständige Autarkie unrealistisch, und bestehende Systeme müssten effektiv genutzt werden. Für Kommunen wurde hervorgehoben, dass die empfohlenen 20 % des IT-Budgets für Cybersecurity selten erreicht werden und die Priorisierung oft fehlt.
Künstliche Intelligenz spielt zunehmend eine Rolle, sowohl als Unterstützung im Fachkräftemangel als auch als Werkzeug der Angreifer. Die Geschwindigkeit, mit der Schwachstellen erkannt und behoben werden können, wird zum entscheidenden Faktor. Dennoch sei nicht alles automatisierbar; menschliche Entscheidungen und Sensibilität bleiben essenziell. KI müsse gezielt eingesetzt und abgesichert werden, während gleichzeitig die Bevölkerung stärker für Manipulationen sensibilisiert werden soll, etwa im Kontext von Bundestagswahlen oder Desinformationskampagnen.
Abschließend wurde die Notwendigkeit betont, von einer „Shaming-Kultur" wegzukommen und gemeinsam an besseren Lösungen zu arbeiten. Vertrauen in IT-Systeme, strategische Investitionen und Backup-Pläne sind Schlüsselfaktoren für eine resilientere Zukunft.

Die Bedrohungslage in Deutschland: Ein Überblick über Sicherheitsherausforderungen - Prof. Haya Schulmann

Deutschland wird zunehmend digitaler, doch die hybride Infrastruktur vieler Organisationen bringt neue Herausforderungen mit sich. Universitäten stellen durch ihre zahlreichen IT-Systeme und geringen Sicherheitsstandards eine besonders große Angriffsfläche dar. Ebenso weisen Parteien, Medien und Länderregierungen die meisten Schwachstellen auf. Früher lag IT-Infrastruktur häufig On-Premise, heute ist sie zunehmend verteilt, mit einem wachsenden Anteil in der Cloud.

Im internationalen Vergleich ist Deutschland jedoch zurückhaltend beim Einsatz von Cloud-Lösungen, wobei hyper-skalierte Cloud-Anbieter oft höhere Sicherheitsstandards und Service-Level-Agreements (SLAs) bieten als On-Premise-Systeme. Dennoch bleibt die Cloud keine Allheilmittel: Auch dort sind Wartung und Sicherheitsmaßnahmen erforderlich.

Angriffe erfolgen zunehmend über Lieferketten, da keine Organisation mehr vollständig On-Premise arbeitet. Der Umstieg auf Zero-Trust-Architekturen wird daher als notwendige Maßnahme gesehen, um der wachsenden Bedrohungslage gerecht zu werden. Die Umsetzung von NIS2 in Deutschland verdeutlicht zudem die Herausforderungen, die mit stark verteilten Ressourcen einhergehen.

Ein zentraler Kritikpunkt ist, dass viele Lageberichte vor allem die Perspektive der Angreifer einnehmen, während ein stärkerer Fokus auf resiliente Strukturen und Abwehrmaßnahmen erforderlich wäre. Das Fazit lautet: Die Forschung steht besonders schlecht da, und Digitalisierung bringt nur dann Sicherheit, wenn sie konsequent umgesetzt wird. Cloud-Lösungen können ein wichtiger Bestandteil sein, erfordern jedoch weiterhin sorgfältige Verwaltung und Kontrolle.

Hybride Bedrohungen im digitalen Zeitalter - Stephan J. Kramer

Hybride Bedrohungen stellen eine zentrale Herausforderung dar, da sie sowohl konventionelle als auch unkonventionelle Angriffsformen kombinieren, um Schwachstellen in Gesellschaften auszunutzen. Dabei geht es nicht nur um technische Angriffe, sondern auch um Strategien wie "Teile und herrsche", die Zwiespalt und Misstrauen säen. Besonders kritisch sind Desinformation und Wahlmanipulation, bei denen Informationen gezielt als Waffe eingesetzt werden. Staaten wie Russland und China werden hier als die gefährlichsten Akteure genannt.

Die zunehmende Digitalisierung ist ein zweischneidiges Schwert: Einerseits ermöglicht sie Fortschritt und Konnektivität, andererseits schafft sie mehr Schwachstellen und Angriffsflächen. Besonders kleinere und mittlere Unternehmen (KMU) sowie Kommunen, Ärzte und Handwerker haben großen Nachholbedarf in Sachen Cybersicherheit. Maßnahmen wie regelmäßige Backups, Reaktionsfähigkeit durch KI sowie gezielte Trainings und Schulungen werden als essenziell erachtet.

Auch soziale Medien spielen eine zentrale Rolle, sowohl als Plattform für Desinformation als auch für faktenbasierte Gegenstrategien. Es reicht jedoch nicht aus, lediglich auf Missstände hinzuweisen; es muss aktiv gehandelt werden. So könnten Bots gezielt genutzt werden, um Desinformationen „just in time“ zu begegnen. Gleichzeitig wird die Frage gestellt, wer die Moderation von Inhalten übernimmt und wie man wahre Informationen gezielt verbreitet, etwa auf Plattformen wie TikTok.

Die Stärkung der Cybersicherheit erfordert jedoch Ressourcen und eine klare Verantwortungsteilung, insbesondere zwischen Ländern, Kommunen und der Wirtschaft. Im

Ergebnis geht es nicht nur um Schutz vor Krieg und Gewalt, sondern um die Sicherung von Lebensgrundlagen, Wohlstand und Resilienz. Deutschland muss lernen, Angriffe nicht nur abzuwehren, sondern auch selbst aktiv zu reagieren und Rückschläge auszuhalten. Fazit: Cybersicherheit ist eine gesamtgesellschaftliche Aufgabe, bei der langfristige Wehrhaftigkeit und Nachhaltigkeit entscheidend sind.

Interview mit der Handelsblatt Korrespondentin für Russland, Ukraine und Osteuropa - Mareike Müller, Moderation: Christof Kerkmann

Russland:
Die öffentliche Wahrnehmung in Russland oszilliert zwischen einer gezielten Ignoranz und einer intensiven Dauerbeschallung durch staatliche Propaganda. Der Krieg wird weiterhin als „militärische Spezialoperation“ dargestellt, begleitet vom Narrativ, Russland rette die Welt vor dem Faschismus. Mobilisierungskampagnen laufen intensiv, da die Armee neue Soldaten benötigt. Gleichzeitig schränkt der Staat alternative Informationsquellen immer weiter ein: VPN-Dienste funktionieren zwar noch, sind jedoch zunehmend eingeschränkt, und soziale Medien werden blockiert. Die Nutzung solcher Dienste birgt zudem wachsende Risiken für die persönliche Sicherheit.
Eine allgemeine Kriegsmüdigkeit in der russischen Bevölkerung ist nur teilweise zu vernehmen. Proteste werden konsequent unterdrückt, und Verhaftungen sind an der Tagesordnung. Personen, die früher noch Hoffnung auf Veränderungen hatten, ziehen sich zunehmend zurück. Für die Korrespondenten wird der Alltag durch Bürokratie, Überwachung und Einschüchterung erschwert. Deutschland wird in der russischen Propaganda als direkter Feind dargestellt, was auch das Arbeiten deutscher Journalisten in Russland erschwert.
Für Journalisten ist der Schutz ihrer Quellen und Daten von höchster Priorität. Geräte wie Laptops und Handys werden erst vor Ort eingerichtet und niemals unbeaufsichtigt gelassen. Reisen zu kritischen Standorten werden vermieden oder nur mit höchster Vorsicht durchgeführt. Die Bereitschaft der Russ:innen, mit deutschen Journalisten zu sprechen, ist vor allem in wirtschaftlichen Themen höher, während Interviews mit pro-russischen Personen äußerst schwierig bleiben.

Ukraine:
In der Ukraine hat sich die Stimmung seit Beginn des Krieges deutlich verändert. Vor einem Jahr gab es noch Hoffnung auf erfolgreiche Gegenoffensiven, doch mittlerweile sind viele Menschen erschöpft und zermürbt von der anhaltenden Gewalt. Luftalarme gehören fast jede Nacht zum Alltag, was die Resilienz der Bevölkerung zusätzlich belastet.

Fazit:

Der Krieg in der Ukraine prägt sowohl die russische als auch die ukrainische Gesellschaft auf tiefgreifende Weise. Während Russland eine propagandistische Erzählung aufrechterhält und den Zugang zu unabhängigen Informationen systematisch erschwert, kämpft die Ukraine mit den psychischen und physischen Belastungen eines zermürbenden Krieges. Beide Länder zeigen, wie entscheidend Informationskontrolle und Schutz in solchen Konflikten sind – sei es durch staatliche Repression oder persönliche Sicherheitsmaßnahmen.

Schau genau hin! Mit Logik und Spürsinn KI-Fakes entlarven - Stefan Voß, Moderation: Christof Kerkmann

Die Deutsche Presse-Agentur (dpa) beschäftigt sich intensiv mit der Verifikation von Nachrichteninhalten und der Entlarvung von KI-generierten Medien. Dabei zeigt sich, dass KI in der Erzeugung von täuschend echten News-Inhalten noch nicht ausgereift ist. Um gefälschte Bilder oder Videos zu erkennen, hat die dpa zwei zentrale Regeln entwickelt (zutreffend auf Situationen im öffentlichen Raum): Erstens, echte Ereignisse werden typischerweise durch mehrere unabhängige Fotos und Videos dokumentiert. Zweitens, die Reaktionen von Personen im Umfeld sollten realistisch und angemessen zur Situation erscheinen.
Insgesamt veröffentlicht die dpa rund 2000 Faktenchecks pro Jahr, von denen weniger als 5 % KI-generierte Inhalte betreffen. Trotz zahlreicher KI-Detection-Tools bleibt die Herausforderung groß, da es auch zukünftig kein Tool geben wird, das KI-Inhalte zuverlässig identifizieren kann (persönliche Einschätzung von Herrn Voß). Modelle, die solche Inhalte generieren, haben fundamentale Verständnisprobleme, beispielsweise bei physikalischen Gesetzmäßigkeiten wie der Schwerkraft oder der Objektpermanenz. Dies führt zu offensichtlichen Fehlern, wie Objekten, die verschwinden. Das macht es für Menschen aktuell noch möglich visuellen generierten Content zu erkennen. Dennoch ist zu sagen, dass sogenannte „Cheap Fakes“ häufig aus, um Zielgruppen zu täuschen, da sie oft nur oberflächlich überzeugen müssen.
Herr Voß betont die Bedeutung von Aufklärung und Schulungen, etwa für Journalistinnen und Schülerinnen, um die Funktionsweise von Sprachmodellen und deren Trainingsdaten besser zu verstehen. Diese Maßnahmen zielen darauf ab, kritisches Denken und den logischen Umgang mit KI-generierten Inhalten zu fördern. Gleichzeitig ist die dpa in sozialen Netzwerken aktiv eingebunden, was die prozessuale Nutzung ihrer Verifikationsarbeit unterstreicht.
Auf eine Nachfrage aus dem Auditorium, ob Audio auch noch als Fake erkannt werden sollte, reagierte Herr Voß mit einem Seufzen und erklärte, dass dies mittlerweile so gut wie nicht mehr unterscheidbar ist.

KI & Automatisierung: Chance oder Bedrohung? - Jörg Peine-Paulsen, Moderation: Christof Kerkmann

Unternehmen stehen vor vielfältigen Herausforderungen im Bereich der IT-Sicherheit. Eine zentrale Frage ist, wie Sicherheit effektiv produziert werden kann. Frameworks wie die ISO

27001 bieten ideale Leitlinien, doch in der Praxis fehlen oft Zeit, Geld und Kompetenz, um diese konsequent umzusetzen. Wichtig ist, dass IT-Abteilungen und Security-Bereiche getrennt betrachtet werden, da eine Zusammenlegung organisatorische Fehler begünstigen kann. Sicherheit erfordert spezialisierte Verantwortung, um sowohl technische als auch organisatorische Schwachstellen zu vermeiden.
Phishing-Mails und Innentäter stellen dabei besondere Gefahren dar. Während die Qualität von Phishing-Angriffen stetig steigt, machen interne Bedrohungen wie Korruption und Ransomware-Erpressung mittlerweile 63 % der Schäden aus. Unternehmen müssen realistisch einschätzen, wie lange sie Ausfälle ihrer IT-Systeme überbrücken können, und entsprechende Maßnahmen planen. Gleichzeitig beschleunigt KI die Dynamik von Netzwerkangriffen, beispielsweise durch schnellere Scans nach offenen Ports, was maßgeschneiderte Verteidigungsstrategien erfordert.
Ein blindes Vertrauen in KI-Tools oder externe Lösungen ist nicht angebracht. Vielmehr sind regelmäßige Code-Analysen essenziell, denn sicherer Code bietet die Grundlage für IT-Sicherheit. Hier zeigt sich auch das Potenzial der KI, etwa in der Code-Optimierung. Dennoch bleibt der Umgang mit KI ein sensibles Thema: Angst vor technologischen Fortschritten kann nur durch Kompetenz und schnelle Anpassungsfähigkeit überwunden werden.
Abschließend betont Christof Kerkmann die Bedeutung motivierter Talente, wie etwa durch duale Studiengänge. Unternehmen sollten gezielt junge, kompetente Mitarbeitende einbinden, um die Herausforderungen der Zukunft erfolgreich zu bewältigen.

Wie verändert KI die Cybersicherheitslandschaft? - Andreas Maack, Jörg Peine-Paulsen, Stefan Voß, Christof Kerkmann

Die Diskussion drehte sich um aktuelle Herausforderungen durch Cyberangriffe und den Einfluss von KI. Ein Hauptproblem sind DDos-Attacken und Phishing, wobei Deep Fakes eine zunehmend größere Rolle spielen. Insbesondere gefälschte Audioaufnahmen und gezielte Angriffe durch Social Engineering, wie der CEO-Fraud, stellen große Gefahren dar. Es wurde betont, dass die menschliche Komponente oft der Schwachpunkt ist, da Opfer von Täuschungen ungern Fehler eingestehen.
KI wird zunehmend für die Verbreitung von Fehlinformationen genutzt, insbesondere durch manipulative Inhalte, die gezielt auf emotionale und kognitive Schwächen der Zielgruppe abzielen. Trends werden analysiert und genutzt, um Meinungen zu beeinflussen oder um Falschnachrichten durch scheinbar glaubwürdige Kanäle, wie gefälschte News-Outlets, zu verbreiten. Dabei verliert Wissen an Bedeutung, und Überzeugungen gewinnen die Oberhand, was das Problem weiter verschärft.
Ein Lösungsansatz ist „Prebunking“ – das frühzeitige Erkennen und Entlarven von Fehlinformationen. Zudem wurden technische Lösungen wie zertifizierte und auditierte Medienquellen diskutiert, um „Source of Truth“-Systeme zu schaffen. Zwischenmenschlich könnten Codewörter oder persönliche Fragen helfen, um Täuschungen zu verhindern. Es wurde angemerkt, dass Menschen heutzutage weniger kritisch hinterfragen und oft einem „Zero Trust“-Ansatz auf technischer Ebene mehr vertrauen als der eigenen Einschätzung. Schließlich wurde

Emotionalität als eine Stärke hervorgehoben, die Menschen nutzen sollten, um Sensibilität und Vertrauen aufzubauen.

Cybersecurity, Darknet, Konflikte und KI: Herausforderungen und Lösungen der IT-Security im Journalismus Bereich - Walter Bühner

Die Sicherung sensibler Informationen und der Schutz vor Angriffen stehen im Fokus moderner IT-Sicherheitsstrategien. Unternehmen müssen die aktuelle Bedrohungslage genau verstehen und sich proaktiv mit möglichen Gefahrenquellen auseinandersetzen. Dazu gehört das Monitoring von Plattformen wie Telegram, auf denen potenzielle Bedrohungen, beispielsweise durch extremistische Gruppen, frühzeitig erkannt werden können. Ein Beispiel dafür ist die Analyse von Drohungen gegen Verlagsgebäude, die gezielt über solche Kanäle verbreitet werden.
Um Sicherheitslücken zu schließen, setzen Unternehmen zunehmend auf proaktive Gefahrensuche. Dies beinhaltet, potenzielle Risiken an Standorten, die durch journalistische Korrespondenzen betroffen sein könnten, frühzeitig zu identifizieren. Insbesondere in Krisen- und Kriegsgebieten ist es entscheidend, den Schutz von Mitarbeitenden sicherzustellen. Die Bedrohung durch APT-Gruppen (Advanced Persistent Threats) erfordert dabei ein tiefes Verständnis der Angreifer, ihrer Motive und ihrer eingesetzten Systeme.
Neben traditionellen Bedrohungen nimmt die Herausforderung durch KI-basierte Angriffe zu. Immer besser gemachte Fälschungen von Bildern, Videos oder Texten erschweren die Verifikation von Inhalten. Gleichzeitig birgt KI Potenziale, etwa in der Transkription oder der Identifikation von Geschäftsabläufen, die jedoch auch für Angreifer nutzbar sind. Unternehmen sollten daher Tools selbst entwickeln, um auf diese Herausforderungen schnell reagieren zu können, wie beispielsweise eigene Fake-Checker für Medieninhalte.
Eine umfassende Sicherheitsstrategie erfordert eine Kombination aus Technologie, Prozessanpassung und tiefem Verständnis der Angreiferwelt, um Gefahren effektiv abzuwehren und Daten sowie Mitarbeitende zu schützen.

Tabuthema: Insider Threats - Thomas Franke

Innentäter stellen eine erhebliche Bedrohung für Unternehmen dar und können aus verschiedenen Personengruppen stammen: Bewerber*innen, Partner, externe Dienstleister oder Mitarbeitende, die Zugriff auf sensible Daten haben. Sie sind verantwortlich für 63 % der sicherheitsbezogenen Vorfälle in Unternehmen. Die Risiken reichen von der unbefugten Weitergabe von Daten über Betrug und Korruption bis hin zu Insidergeschäften oder Sabotage, die häufig zur Vertuschung von eigenem Versagen dient.
Die Gründe, warum Menschen zu Innentätern werden, sind vielfältig. Neben vorsätzlichen Motiven wie persönlicher Bereicherung, Gründung eines Konkurrenzunternehmens oder dem Erwerb von Know-how für eine neue Anstellung, spielen auch unbewusste Faktoren eine Rolle, etwa soziale Ängste, Unsicherheit oder mangelnde Identifikation mit der Unternehmenskultur.

Ein Mangel an Unrechtsbewusstsein oder die Verfügbarkeit krimineller Angebote im Darknet fördern zusätzlich die Wahrscheinlichkeit solcher Handlungen.

Fehlende interne Kontrollen, unzureichende Awareness-Schulungen sowie der Einsatz privater Geräte am Arbeitsplatz verschärfen das Problem. Auch der Offboarding-Prozess von Mitarbeitenden birgt Risiken, da ehemalige Mitarbeitende oft kritisches Wissen behalten. Wirtschaftsspionage durch Geheimdienste ist ebenfalls eine reale Bedrohung und erfordert besondere Aufmerksamkeit.
Die Prävention, Detektion und Reaktion auf Innentäter muss ein ganzheitlicher Ansatz sein, der Technik, Prozesse und den menschlichen Faktor gleichermaßen berücksichtigt. Technische Lösungen allein sind nicht ausreichend, da viele Aspekte auf menschlichem Verhalten und zwischenmenschlichen Dynamiken basieren. Unternehmen benötigen daher ein Mindestmaß an Fähigkeiten und Werkzeugen, um effektive Maßnahmen zu entwickeln. Eine Unternehmenskultur, die Vertrauen und Identifikation fördert, sowie regelmäßige Schulungen und strikte interne Kontrollen können das Risiko deutlich reduzieren.

Digitale Selbstverteidigung im Volkswagen Konzern – Wer sind die Crash-Test-Dummies in der digitalen Welt? - Andreas Maack

Die IT-Sicherheitslandschaft befindet sich in einer zunehmend prekären Lage, geprägt durch schnelle technologische Entwicklungen und steigende Bedrohungen durch Cyberkriminalität. Die Herausforderungen sind vielschichtig: Unternehmen stehen vor dem Ziel, ein hohes Maß an Sicherheit mit der Funktionalität und den Kostenanforderungen ihrer Prozesse in Einklang zu bringen. Wird die Nutzbarkeit vor die Sicherheit gestellt oder Risiken bewusst eingegangen, entstehen Schwachstellen, die Angreifer ausnutzen können.
Ein Vergleich mit der Automobilindustrie verdeutlicht diese Dynamik: So wie ein Auto bei unsachgemäßer Nutzung selbst durch die besten Schutzsysteme keine vollständige Sicherheit gewährleisten kann, sind auch IT-Systeme anfällig, wenn sie falsch eingesetzt werden oder das nötige Wissen zur sachgemäßen Nutzung fehlt. Der Faktor Mensch bleibt dabei das schwächste Glied in der Sicherheitskette. Fehlverhalten und mangelndes Bewusstsein können nicht vollständig durch Technik kompensiert werden.
Die steigende Geschwindigkeit der technologischen Weiterentwicklung erschwert es, dass Regulierungen mit den neuen Risiken Schritt halten. Cyberkriminalität entwickelt sich ebenso rasant weiter und verschmilzt zunehmend mit der realen Welt. Angreifer zielen selten direkt auf Technologien ab, sondern nutzen Schwachstellen in Prozessen aus. Daher ist eine ganzheitliche Perspektive erforderlich, die technische, organisatorische und menschliche Aspekte einbezieht.
Volkswagen hat 2024 eine strategische Neuausrichtung der Sicherheit vorgenommen, um IT-Sicherheitsansätze holistischer zu gestalten. Im engen Austausch mit der Polizei, dem BKA, dem BSI und der Allianz für Cybersicherheit wird daran gearbeitet, Prozesse und Sicherheitsmaßnahmen abzustimmen. Dabei verfolgt VW das Prinzip „Security with one voice“, um Angriffe gezielt und einheitlich zu adressieren.

Zukunftstechnologien wie Quantencomputing bieten große Chancen, aber auch neue Herausforderungen, die zusätzliche Sicherheitsmaßnahmen erfordern. Unternehmen müssen die damit verbundenen Kosten und Aufwände klar kommunizieren und das Thema stärker in die Gesellschaft tragen. Events wie die Handelsblatt-Messe spielen eine entscheidende Rolle, um den Dialog zwischen den Akteuren zu fördern.
Der Weg zur sicheren Zukunft erfordert gemeinsame Anstrengungen, bei denen Menschen und Organisationen zusammenarbeiten, anstatt in isolierten Silos zu agieren. Ziel ist es, präventive und reaktive Maßnahmen zu entwickeln, die Cyberkriminalität wirksam bekämpfen, ohne dabei die Menschen selbst zu überfordern. Denn in einer immer schnelleren digitalen Welt darf niemand zum „Crash-Test-Dummy" für Cybersicherheit werden.

Cybersicherheit: was wir von der Luftfahrt lernen können - Naby Diaw

Die Luftfahrtindustrie hat durch strikte Standards und klare Verfahren eine außergewöhnlich hohe Sicherheitsquote erreicht. Aus 14 tödlichen Unfällen pro eine Million Flüge in der Vergangenheit wurde durch kontinuierliche Optimierung eine Rate von nahezu 0,01 % erreicht. Dieser Fokus auf „Safety First" bietet wertvolle Lektionen für die Cybersecurity-Branche.
Ein zentrales Prinzip der Luftfahrt ist die Nutzung klar definierter Prozeduren wie Checklisten, die präzise und immer wieder durchlaufen werden. Ähnlich sollten Cybersecurity-Teams standardisierte Playbooks und Checklisten nutzen, um kritische Vorgänge systematisch abzuarbeiten und Fehler zu minimieren. Asset- und Changemanagement spielen eine entscheidende Rolle: Jede Änderung muss dokumentiert und doppelt überprüft werden, und Redundanzen sowie Backups sind unerlässlich, um den Betrieb auch im Krisenfall aufrechtzuerhalten.
Eine weitere wichtige Lehre ist das Konzept der „Minimum Requirement List". In der Luftfahrt werden minimale Komponenten definiert, die für den sicheren Betrieb erforderlich sind. Dieses Prinzip lässt sich auf IT-Systeme übertragen, indem ein Minimum Viable Set an Sicherheitsmaßnahmen festgelegt wird, das den Betrieb auch unter Druck gewährleistet.
Proaktives Risikomanagement ist ein weiteres Schlüsselelement. Methoden wie regelmäßige Schwachstellenscans, Bedrohungsjagd (Threat Hunting), Red-Teaming und Bug-Bounty-Programme erhöhen die Widerstandsfähigkeit von Systemen. Gleichzeitig ermöglicht Automatisierung, sich auf wesentliche Aufgaben zu konzentrieren und Alarmmüdigkeit zu vermeiden, ohne die menschliche Kontrollinstanz zu ersetzen.
Die Luftfahrt zeigt außerdem, wie wichtig ein krisenfestes Management ist. Piloten und Crew arbeiten in Krisensituationen nach klar strukturierten Prinzipien: zunächst Fakten erfassen, dann Optionen und Risiken bewerten, bevor Entscheidungen getroffen werden. Diese Methodik kann auch Cybersecurity-Teams helfen, strukturiert und fokussiert zu handeln. Offene Kommunikation, Training und eine „Just Culture", in der Fehler nicht bestraft, sondern als Lernchance betrachtet werden, fördern kontinuierliche Verbesserung.
Zusammengefasst kann die Cybersecurity-Branche von der Luftfahrt lernen, durch klare Standards, proaktives Risikomanagement, Defense-in-Depth-Strategien und gemeinschaftliche

Verantwortung ein ebenso hohes Sicherheitsniveau zu erreichen. Das Ziel ist es, Cybersecurity auf das Niveau der Luftfahrt zu heben – oder wie es treffend heißt: „Make Cyber Fly."

Der Tag an dem ich Staatsfeind Nr. 1 wurde – Red-Teaming eskaliert - Christoph Ritter

Red-Teaming und TIBER-Assessments sind essentielle Methoden, um Cybersecurity in Unternehmen und Finanzinstituten zu testen und zu stärken. Diese Verfahren simulieren reale Angriffe von Advanced Persistent Threat (APT)-Gruppen, um Schwachstellen in Sicherheitsstrukturen zu identifizieren. Der Prozess beginnt mit einer Thread Intelligence Phase, in der analysiert wird, welche Angreifergruppen auf das Unternehmen abzielen könnten und welche Taktiken sie nutzen.
Ein Ziel ist es, die Vorgehensweisen der APT-Gruppen möglichst realistisch nachzubilden. Dabei wird jedoch auf die Einhaltung rechtlicher Rahmenbedingungen geachtet, was die Arbeit des Red-Teams von echten Angreifern unterscheidet. Beispielsweise dürfen beim Phishing keine geschützten Logos oder geklonte Webseiten genutzt werden, die Urheberrechte verletzen. Stattdessen greift man auf Techniken wie die Verwendung von abgelaufenen Domains mit hoher Reputation zurück oder testet Malware in kontrollierten Sandbox-Umgebungen gegen die firmeneigenen Systeme.
Ein weiterer wichtiger Aspekt ist das Timing: Politische Ereignisse oder gesellschaftliche Lagen, die reale APT-Angriffe beeinflussen können, lassen sich im Testumfeld nur schwer simulieren. Hier zeigt sich, dass Red-Teaming und TIBER-Assessments immer nur einen Ausschnitt der möglichen Bedrohungen abbilden können.
In der zweiten Phase der Assessments wird das geplante Szenario umgesetzt. Dabei werden gezielt Mitarbeitende mit geringer Awareness durch Wellen von Phishing-Mails angesprochen, um Schwachstellen in den menschlichen Schutzmechanismen aufzudecken. Auch physische Assessments spielen eine wichtige Rolle, um Sicherheitslücken in der physischen Infrastruktur zu identifizieren.
Die Ergebnisse solcher Assessments sind nicht nur intern relevant, sondern auch von Interesse für Behörden und Medien, insbesondere wenn durchgeführte Tests öffentlich bekannt werden. Unternehmen tragen dabei die volle Verantwortung für die Einhaltung der Compliance, um Schäden oder Eskalationen zu vermeiden.
Fazit: Red-Teaming und TIBER-Assessments helfen, Sicherheitslücken realitätsnah zu identifizieren und Organisationen widerstandsfähiger zu machen. Sie erfordern jedoch ein hohes Maß an Professionalität, rechtliche Sensibilität und die enge Zusammenarbeit mit den zuständigen Behörden, um sowohl technische als auch menschliche Schwächen zu adressieren.

Next Generation Ransomware – Angriffe auf Behörden und Unternehmen und ihre Folgen - Volker Kozok

Ransomware und „Crime as a Service“ werden zunehmend professioneller, oft organisiert über das Onion-Netzwerk. HR-Abteilungen sind besonders gefährdet, da allgemeine Sicherheitsregeln wie „Keine unbekannten E-Mails öffnen“ hier schwer umsetzbar sind. Kriminelle nutzen gezielte Phishing-Mails mit Schadsoftware wie Emotet, um Netzwerke zu infiltrieren.
KI-unterstützte Ransomware verschärft die Bedrohung, indem sie gezieltere Angriffe ermöglicht. Alte Ransomware bleibt weiterhin effektiv, da grundlegende Sicherheitslücken, etwa veraltete Betriebssysteme, bestehen. Viele Gruppen reagieren flexibel auf Einschränkungen, etwa durch Umbenennungen oder neue Methoden.
Fazit: Praktikable Sicherheitsmaßnahmen, die sich in den Arbeitsalltag integrieren lassen, sowie technologische und rechtliche Anpassungen sind essenziell, um Resilienz gegen diese Bedrohungen aufzubauen.

Aus dem Waffenarsenal der NSA – Angriffe auf Smartphones - Sebastian Schreiber

Live-Demo: USB-basierte Angriffe, etwa über manipulierte Kabel mit integriertem Linux-System und eigenem Hotspot, zeigen, wie leicht Hardware zur Cyberbedrohung werden kann. Solche Angriffswerkzeuge, früher teuer und komplex, sind heute einfach selbst herzustellen. Betroffen sind nicht nur USB-Kabel, sondern auch Ladegeräte und Eingabegeräte wie Tastaturen.
Fazit: Unternehmen müssten auch physische IT-Infrastruktur wie Ladestationen und Zubehör schützen, um ungewollten Austausch und potenzielle Angriffe zu verhindern. Dies ist aber nahezu unmöglich.

Cybersecurity als entscheidender Treiber für Innovationen im Digitalen Zeitalter - Dr. Ralf Schneider

Innovation erfolgreich von der Idee in die Umsetzung zu bringen, ist eine zentrale Herausforderung für Unternehmen. Eine essenzielle Grundlage dafür ist Cyber Security.
Während Cyber Security nicht alles ist, gilt: Ohne sie ist alles nichts. Heutzutage erfordert jedes Geschäftsmodell eine Online-Präsenz, was Unternehmen zwangsläufig mit den Risiken des World Wide Web konfrontiert. Startups erleben dies hautnah, da neue Domains bereits am ersten Tag von bis zu 15.000 Angriffen betroffen sein können.
Cyber Security wird nicht nur als Schutzmaßnahme, sondern auch als Treiber für Innovationen gesehen. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) müssen innovative Unternehmen drei Schlüsselkompetenzen entwickeln:

1. Prävention: Sicherheitskonzepte wie "Security by Design" und die Fähigkeit, Sicherheits-Stacks schnell anzupassen.
2. Verteidigung: Der Wettbewerb mit Angreifern erfordert Geschwindigkeit und Agilität. Nach dem "Gesetz des Dschungels" gilt: Wer nicht schnell ist, braucht Glück. Eine

kollektive Verteidigung über Abteilungsgrenzen hinweg – von CEOs über Entwickler bis hin zu Einkäufer – ist entscheidend.

3. Reaktion und Wiederherstellung: Resilienz, also die Fähigkeit, auf Angriffe zu reagieren und Systeme wiederherzustellen, ist essenziell. Diese Resilienz ist eine wertvolle Fähigkeit, die auch in anderen IT-Bereichen Anwendung findet.

Cyber Security zeigt exemplarisch, dass Technik nur so stark ist wie die Menschen, die sie einsetzen. Mit dem Aufkommen von KI rückt der Mensch erneut ins Zentrum, indem Technologie ihn befähigt, schneller und effektiver zu reagieren. Zeit ist dabei der entscheidende Faktor.

Zusammengefasst ist Cyber Security nicht nur eine technische Herausforderung, sondern ein kollektives Thema, das alle Ebenen eines Unternehmens betrifft. Sie verbindet Prävention, Innovation und Zusammenarbeit und wird so zum Treiber für eine zukunftsfähige und widerstandsfähige Organisation.

Squaring the Circle – Logistics Cyber Resilience - Frank Fischer

Resilienz und proaktive Maßnahmen stehen im Zentrum der Diskussion über moderne Unternehmensführung und Cyber Security. Der Vergleich einer fallenden Vase verdeutlicht den Ansatz: Es ist besser, den Sturz zu verhindern, als die Scherben nachträglich zusammenzufügen. Resilienz bedeutet, auf alle Gefahrenlagen vorbereitet zu sein und dabei Mindestanforderungen wie regulatorische Standards einzuhalten.

Ein Unternehmen muss dynamisch und anpassungsfähig bleiben, da nicht jeder Prozess gleich wichtig ist und unerwartete Störungen immer auftreten können. Standards und Prozesse schaffen wichtige Grundlagen, sind jedoch kein Ersatz für eine resiliente Unternehmenskultur. Ein schnelles Umschalten in den Notfallmodus und die Überwindung des anfänglichen Schocks sind entscheidend. Hierfür braucht es regelmäßige Tests, wie etwa das Ausprobieren von Backups, um auf den Ernstfall vorbereitet zu sein.

Zeit ist ein Schlüsselfaktor. Schnelle Kommunikation, gegebenenfalls telefonisch, und eine hohe Visibilität der eingesetzten Systeme minimieren Verzögerungen. Regelmäßige Updates, etwa halbjährlich mit COO-Beteiligung, helfen, Best Practices und Prozesse aktuell zu halten. Die Einbindung von KI kann die Entscheidungsfindung und Kommunikation zusätzlich beschleunigen.

In einem komplexen Netzwerk (wie beispielsweise bei DHL) aus Kunden und Lieferanten können sekundäre Auswirkungen entstehen. Daher ist es wichtig, Redundanzen zu schaffen und Systeme auf ihre Zweckmäßigkeit („fit for purpose“) zu prüfen, statt auf eine universelle Lösung („one size fits all“) zu setzen.

Zusammengefasst erfordert Resilienz ein Zusammenspiel aus präventivem Handeln, Kultur, technologischer Unterstützung und einem ständigen Lernprozess. Proaktive Vorbereitung, regelmäßiges Testen und schnelle Reaktionen sichern die Handlungsfähigkeit auch in unerwarteten Situationen.

Aufbau von Cyberresilienz durch adäquates Risikomanagement - Prof.'in Dr. Gabi Dreo Rodosek

Die zunehmende Vernetzung aller Systeme und Prozesse stellt Unternehmen vor neue Herausforderungen in der Cyber Security. Angriffe sind unvermeidlich – die Frage ist nicht ob, sondern wann. Studien zeigen, dass 9 von 10 Unternehmen angegriffen werden. Resilienz wird damit zur obersten Priorität: Unternehmen müssen sicherstellen, dass sie auch während eines Angriffs weiterhin funktionsfähig bleiben.

Ein Umdenken ist erforderlich, weg von traditionellen Ansätzen wie einfachen Excel-basierten Risikoanalysen hin zu automatisierten, kontinuierlichen Plattformen, die Risiken umfassend bewerten und anpassen können. Diese Plattformen sollten nicht nur unternehmensintern arbeiten, sondern auch unternehmensübergreifende Netzwerke unterstützen. Redundanz und eine Diversifizierung der Daten sind zentrale Bausteine für zukunftsfähige Resilienz.

Künstliche Intelligenz ist bereits unverzichtbar für Cyber Security und wird in den kommenden Jahren an Bedeutung zunehmen. LLMs entwickeln sich wöchentlich weiter und eröffnen neue Möglichkeiten in der Automatisierung von Sicherheitsprozessen. Auch Quantum Computing wird bald Realität und bringt Herausforderungen wie „Store now, decrypt later" mit sich – ein Thema, das CISOs schon jetzt adressieren müssen.

Cyber Security ist kein Kostenfaktor und darf nicht allein als Aufgabe der IT-Abteilung gesehen werden. Sie erfordert ein starkes Ökosystem und bereichsübergreifende Zusammenarbeit. Gleichzeitig ist es wichtig, Erfolge in der Cyber Security sichtbar zu machen, etwa durch Risikominimierung. Die wachsende Bedeutung von Sicherheitsstrategien wird auch für IT-Fachkräfte zunehmend deutlich, da sie zu einem Kernbestandteil jedes erfolgreichen Unternehmens werden.

Zusammengefasst ist Cyber Security nicht nur eine technische Herausforderung, sondern eine kulturelle und strategische Aufgabe, die stark von Automatisierung, KI und resilienzorientierten Denkweisen geprägt ist.

Schlüsselkomponenten der Cyberresilienz: Welche Faktoren sind entscheidend? - Prof.'in Dr. Gabi Dreo Rodosek, Dr. Peter Dornheim, Frank Fischer

Die Diskussion konzentrierte sich auf kulturelle Unterschiede in Unternehmen und deren Einfluss auf Cybersecurity. Ein zentraler Aspekt war, wie Unternehmen ihre Anpassungsfähigkeit erhöhen können, um auf Disruptionen vorbereitet zu sein, anstatt nur auf althergebrachte Prozesse zu setzen. Dabei wurde betont, dass Begeisterung und Innovation in der Cybersecurity essenziell sind, insbesondere durch Ansätze wie Gamification oder „coole" Projekte, die die Mitarbeitenden motivieren.

Ein weiterer Schwerpunkt lag auf der Fehlerkultur. Innovation erfordert das Zulassen und Lernen aus Fehlern, anstatt diese zu sanktionieren. Dies ist wichtig, um eine Kultur zu fördern, die Cybersecurity nicht nur als Pflicht, sondern als lebendiges Element versteht. Der Umgang mit

Menschen und Kommunikation von Policies sind hierbei entscheidend. Es wurde diskutiert, wie eine Kulturänderung durch kontinuierliches Engagement und den Einsatz von „Nudges“ gefördert werden kann.
Die Rolle von Führungskräften und deren Einfluss auf Resilienz wurde ebenfalls angesprochen. Neben Zeit und Fehlertoleranz spielen Vorbereitung und regelmäßiges Testen eine zentrale Rolle. Die NIS2-Richtlinie und persönliche Haftung von Führungskräften unterstreichen die Bedeutung von Schulungen und Übungen. Auch wurde diskutiert, ob Regulierung selbst ein „Thread Actor“ sein könnte, der Unternehmen vor zusätzliche Herausforderungen stellt.
Der Einsatz von LLMs in der Compliance wurde kontrovers beleuchtet. Während sie als nützlich angesehen werden, sind Bedenken vorhanden, ob sie wirklich komplexe Themen wie Lieferkettenmanagement oder kulturellen Wandel sinnvoll unterstützen können. Der Vergleich zu Autos zeigt: Man muss nicht jedes Detail verstehen, um sie nutzen zu können. Abschließend wurde hervorgehoben, dass Resilienz unternehmensspezifisch ist und vom richtigen Umgang mit Risiken und Fehlern abhängt.

Etablierung einer Cybersecurity Kultur – Science meets Practice - Dr. Peter Dornheim

Cyber Security hat sich in vielen Unternehmen zu einem zentralen strategischen Thema entwickelt und rückt zunehmend in den Fokus des Top-Managements. Die Rolle des CISOs wird immer wichtiger, oft mit direktem Zugang zum Vorstand. Doch der Erfolg von Sicherheitsmaßnahmen hängt nicht nur von Technologie ab, sondern auch von einer gelebten Sicherheitskultur.
Die Etablierung einer nachhaltigen Sicherheitskultur ist eine kontinuierliche Aufgabe. Menschen ändern ihre Verhaltensweisen nur ungern, insbesondere nach längerer Zeit in der gleichen Rolle. Daher sind maßgeschneiderte, fachspezifische Cyber Security-Trainings von zentraler Bedeutung, um das Interesse zu wecken und die Relevanz aktueller Bedrohungen aufzuzeigen. Awareness-Maßnahmen müssen regelmäßig erneuert und an die aktuellen Herausforderungen angepasst werden. Führungskräfte spielen hierbei eine Schlüsselrolle: Ohne ihr Vorbildverhalten und Engagement wird das Thema im Unternehmen nicht gelebt.
Ein wesentlicher Aspekt für eine starke Sicherheitskultur ist Vertrauen – sowohl intern zwischen Mitarbeitenden und Führungskräften als auch extern mit anderen Unternehmen. Der offene Austausch über Schwachstellen, etwa durch Penetrationstests oder gemeinsame Projekte, kann die kollektive Resilienz stärken. Die Bereitschaft, Erkenntnisse und Best Practices unternehmensübergreifend zu teilen, ist essenziell, stößt jedoch häufig auf kulturelle und organisatorische Hürden.
Technologie kann die Sicherheitskultur unterstützen, etwa durch den Einsatz von KI für automatisierte Phishing-Erkennung oder andere präventive Maßnahmen. Dennoch bleibt der Mensch ein zentraler Faktor – die Kombination aus menschlichem Engagement und technologischer Unterstützung ist entscheidend.

Zusammengefasst zeigt die Diskussion, dass Cyber Security mehr als nur eine technische Herausforderung ist. Sie erfordert eine dauerhafte, ganzheitliche Integration in die Unternehmenskultur, unterstützt durch gezielte Schulungen, Vertrauensaufbau und die aktive Beteiligung des Top-Managements.

Cybersicherheit im Wandel: Mit Kundenfokus und Sicherheitskultur zum Wegbereiter der digitalen Transformation - Johannes Hackstette, Patrick Popa

Siemens Energy, als innovativer Treiber und strategischer Partner im Bereich Cyber Security, setzt auf eine ganzheitliche Sicherheitskultur, die weit über technologische Ansätze hinausgeht. Seit der Ausgliederung aus Siemens im Jahr 2020 verfolgt das Unternehmen einen klaren Fokus auf Risiko-Minimierung, profitables Wachstum und den Aufbau vertrauenswürdiger, nachhaltiger Netzwerke.

Cyber Security wird oft als komplex und abstrakt wahrgenommen, wodurch Mitarbeitende die Verantwortung häufig an andere delegieren. Viele Awareness-Kampagnen scheitern daran, dass sie lediglich Wissen vermitteln, ohne Motivation oder praktische Anwendungsmöglichkeiten zu fördern.
Das Unternehmen Siemens Energy verfolgt einen dreistufigen Ansatz:

1. Awareness: Wissen wird durch klare Kommunikation und Gamification aufgebaut. Storytelling und konkrete Beispiele helfen, abstrakte Themen greifbar zu machen.
2. Kultur: Motivation entsteht durch emotionale Ansprache und gezielte Kampagnen mit transparenten Zielen.
3. Training: Simulationen und beispielsweise kurze, zielgerichtete Videos schulen spezifisch jene Mitarbeitende, die noch wenig Berührungspunkte mit Cyber Security haben.

Siemens Energy arbeitet eng mit Startups und Marketing-Teams zusammen, um Best Practices zu entwickeln und Standards zu etablieren. Dies unterstreicht die Überzeugung, dass Cyber Security kein isoliertes Thema ist, sondern als strategischer Vorteil und Werttreiber für Unternehmen fungiert.
Cyber Security ist für Siemens Energy mehr als nur eine Schutzmaßnahme – sie wird als entscheidender Wettbewerbsvorteil und Innovationstreiber angesehen. Auch wenn Sicherheitsmaßnahmen mit Kosten verbunden sind, zahlen sie sich durch nachhaltiges Wachstum und stärkere Netzwerke aus.

Und was macht Ihr Baby Elefant? NIS2 im Deutschen Mittelstand - Max Gutberlet

Das Thema NIS2 ist zwar in Fachkreisen wie bei CISOs bekannt, hat aber in vielen Unternehmen – insbesondere im Mittelstand – noch nicht die nötige Aufmerksamkeit erhalten. Während die Anforderungen des neuen EU-Regelwerks einiges an Arbeit erfordern, betonten die Expert auf der Messe, dass kein Grund zur Panik besteht. Das Motto lautet: "Keine Panik mit NIS2!"

NIS2 bringt einen erhöhten Aufwand für Unternehmen mit sich, insbesondere in Bereichen wie Marken- und Reputationsschutz sowie der Sicherung der Lieferketten. Mittelständische Unternehmen sollten die folgenden Schritte angehen:

1. Betroffenheit feststellen: Dies sollte mit Unterstützung von Expert wie Rechtsanwält erfolgen.
2. Gap-Analyse: Identifizieren, welche Lücken es in der Organisation gibt, und darauf aufbauend einen Maßnahmenplan entwickeln.
3. Planung und Vorbereitung: Den zusätzlichen Aufwand einplanen, ohne überstürzt Tools zu kaufen, da die Anforderungen noch nicht in allen Ländern vollständig umgesetzt sind.

Während Deutschland noch mit der Umsetzung von NIS2 beschäftigt ist, hat Italien das Regelwerk in nur 12 Wochen verabschiedet, was Unternehmen dazu zwingt, sich länderspezifisch anzupassen. Besonders herausfordernd ist dies für international agierende Unternehmen, die je nach Standort unterschiedliche Compliance-Anforderungen erfüllen müssen.
Die ISO 27001 bleibt in Deutschland die Leitlinie für NIS2-Umsetzungen, allerdings weichen andere Länder, wie Italien, davon ab. Unternehmen sollten sich daher auf flexible und internationale Ansätze einstellen.
Die Implementierung von NIS2 erfordert erhebliche Budgets. Beispiele wie Rotkäppchen-Mumm, das 1,4 Millionen Euro investiert hat, zeigen, wie ressourcenintensiv die Anpassung sein kann – insbesondere für kleinere Unternehmen. In der aktuellen Wirtschaftslage könnte der zusätzliche Aufwand sogar die Resilienz gefährden.
Zusammengefasst bietet NIS2 Unternehmen zwar die Möglichkeit, Marken und Lieferketten besser zu schützen, doch die Umsetzung ist komplex und erfordert einen strukturierten, pragmatischen Ansatz.

KI-basierte Attacken – beyond the hype - Robert Wortmann

Die wachsende Rolle von Künstlicher Intelligenz zeigt sich zunehmend auch in Cyberangriffen, wobei sowohl die Bedrohungen als auch die Angriffsmethoden komplexer und gezielter werden. Hochriskante und ressourcenintensive Angriffe nehmen weltweit zu, während Ransomware-Akteure sich zunehmend auf zahlungsfähige Unternehmen konzentrieren. So wurde in diesem Jahr eine Rekordzahlung von 75 Millionen Euro dokumentiert.
KI wird immer stärker für Angriffe genutzt, oft durch lokale Modelle wie LLaMA, die beispielsweise zur gezielten Filterung und Exfiltration sensibler Daten verwendet werden. Gleichzeitig ermöglichen Technologien wie „Deepfakes as a Service“ kostengünstige, manipulative Angriffe – von gefälschten Produkten bis zu Spendenbetrügereien. Phishing-Attacken haben seit der Einführung von ChatGPT erheblich zugenommen, auch wenn die Qualität in nicht-englischen Sprachen oft immer noch nicht sehr gut ist.
KI wird weniger als revolutionäre Technologie, sondern vielmehr als Skalierungswerkzeug für Angriffe gesehen. Jailbreak-Ansätze für Sprachmodelle umgehen Sicherheitsregularien und können problemlos für die Erstellung von Phishing-E-Mails oder Betrugsmanipulationen genutzt

werden. Support-Scams, bei denen Angreifer vorgeben, Hilfe zu leisten, sind aktuell besonders stark im Kommen.
Die Kombination aus KI und Cyberangriffen verdeutlicht eine alarmierende Entwicklung: Während hochentwickelte Tools wie Deepfakes und KI-Modelle die Angriffslandschaft skalieren, konzentrieren sich Angreifer auf gezielte und lukrative Ziele. Unternehmen müssen ihre Sicherheitsstrategien entsprechend anpassen, um diesen zunehmend raffinierten Bedrohungen gewachsen zu sein.

Zuverlässige Wiederherstellung im Ernstfall: Datensicherung als Fundament der Cyberresilienz - Thomas Sandner

Während die IT-Sicherheitsbranche traditionell stark auf Prävention fokussiert, wird der Resilienz – der Fähigkeit, sich von Cyberangriffen schnell zu erholen – oft zu wenig Aufmerksamkeit geschenkt. Eine effektive Datenstrategie muss beides vereinen: präventive Maßnahmen und robuste Wiederherstellungsprozesse.
Cyberangriffe, die gezielt Backups ins Visier nehmen, sind keine Seltenheit – 93 % der Unternehmen berichten von solchen Vorfällen. Die durchschnittliche Downtime nach einem Angriff beträgt drei Wochen. Um dem entgegenzuwirken, braucht es unantastbare Backups (immutable), die nicht vom gleichen Server wie die Anwendungen verwaltet werden. On-Premises-Systeme bieten hier oft einen Vorteil. Zudem ist es essenziell, Backups regelmäßig auf ihre Funktionalität zu testen und potenzielle Schadsoftware zu identifizieren.
Die fünf Säulen der Datenstrategie:

1. Backup: Backups müssen sicher vor Ransomware und administrativen Eingriffen sein.
2. Data Recovery: Planung und Orchestrierung der Wiederherstellung sind entscheidend.
3. Data Portability: Daten müssen flexibel und unabhängig nutzbar bleiben.
4. Data Security: Schutzmaßnahmen müssen auch die Backup-Umgebungen umfassen.
5. Data Intelligence: Der Datenschatz aus Backups kann durch KI-gestützte Analysen in wertvolle Erkenntnisse umgewandelt werden.

Unternehmen sollten nicht nur Backups in ihre Prozesse integrieren, sondern auch Tools nutzen, die die Wiederherstellung orchestrieren und beschleunigen können. Dabei ist es wichtig, realistisch zu bleiben: Eine vollständig automatisierte Wiederherstellung ist aktuell kaum möglich, doch KI kann bei der Erkennung von Bedrohungen und bei der Integration von Backups in die Prozesse eine Schlüsselrolle spielen.
Die Zukunft der IT-Sicherheit liegt in einem ausgewogenen Ansatz aus Prävention und Resilienz. Immutable Backups, regelmäßige Tests und eine durchdachte Wiederherstellungsstrategie sind unverzichtbar, um die Ausfallzeiten zu minimieren und Cyberangriffe nachhaltig zu bewältigen.

The attacker's POV: How to build the right continuous threat exposure management (CTEM) program to reduce risk - Matt Baird

Traditionelle Penetrationstests bieten nur eine momentane Einschätzung der Sicherheit und sind zeitaufwändig sowie ineffizient. Viele Unternehmen fehlt ein ganzheitlicher Überblick über Bedrohungen, und Entscheidungen werden oft ohne genaue Kenntnis der Angreifer getroffen. Herausforderungen sind:

- Zeitintensive, manuelle Prozesse.
- Fehlendes Verständnis der Angreifer (79 %).
- Unklare Priorisierung relevanter Bedrohungen (84 % sorgen sich, wichtige Gefahren zu übersehen).

Lösungsansätze dafür könnten ein kontinuierliches Bedrohungsmanagement (Continuous Threat Exposure Management) sein, das Schwachstellen alle 2-3 Minuten scannt und relevante Risiken priorisiert. Moderne Profile analysieren branchenspezifische Risiken und Sichtbarkeit nach außen. CyberProof bietet eine solche Lösung.
Ein ganzheitlicher Ansatz mit kontinuierlichem Management verbessert die Reaktion auf Bedrohungen und schafft eine Grundlage für effektive Sicherheitsstrategien.

Bekämpfung digitaler Gewalt gegen Frauen: Eine datenschutzrechtliche Perspektive - Ines Duhanic

Digitale Gewalt hat sich zu einer ernsthaften gesellschaftlichen Herausforderung entwickelt, die auf Plattformen wie Messenger-Dienste, Dating-Apps oder soziale Medien zunehmend präsent ist. Im Gegensatz zu analoger Gewalt ist sie rund um die Uhr aktiv und oft vor einem Millionenpublikum sichtbar. Betroffene leiden häufig unter Scham, Wut und Isolation.
Dazu gehören bildbasierte Gewalt, Cybermobbing (z. B. über Airdrop), Demütigung durch Deepfakes, Doxxing, die Verbreitung von Fake News und antifeministische Inhalte sowie illegales Tracking über Technologien wie AirTags. Frauen sind von diesen Angriffen besonders häufig betroffen.
Zwar gibt es Gesetze gegen digitale Gewalt, wie das Strafgesetzbuch (StGB) oder die DSGVO, jedoch greifen diese oft nicht weit genug. Beispielsweise bleibt die Nachverfolgung von Tätern schwierig, was den Opferschutz beeinträchtigt.
Digitale Gewalt ist eine stetige Gefahr, die gezielte Maßnahmen und eine stärkere rechtliche Grundlage erfordert, um Betroffene besser zu schützen und Täter konsequent zu verfolgen.

Cybersicherheit und eine moderne, digitale Strafjustiz - Jana Ringwald

Der aktuelle Lagebericht des BSI hebt die wichtige Rolle von Justiz und Polizei bei der Bekämpfung von Cyberkriminalität hervor. Die Zusammenarbeit zeigt Wirkung, jedoch steht die digitale Transformation der Behörden weiterhin im Fokus, um den wachsenden Herausforderungen gerecht zu werden.
Cyberkriminalität ist zunehmend vernetzt und komplex. Moderne Tools wie „Stresser-Dienste“ ermöglichen technisch wenig versierten Personen, DDoS-Angriffe durchzuführen, was die Angriffsfrequenz massiv steigert. Ein großes Problem ist die dezentrale Bearbeitung, bei der

Informationen zwischen Polizeidienststellen oft nicht geteilt werden, was Effizienz und Effektivität einschränkt.
Schlüssel zur Bekämpfung von Cyberkriminalität:

1. Prävention: Die wichtigste Maßnahme, die jedoch über die Justiz hinausgeht.
2. Zentralisierung und Deconfliction: Ermittlungsergebnisse bündeln, um Doppelarbeit zu vermeiden.
3. Internationale Zusammenarbeit: Notwendig, da Täter global agieren.
4. Kooperation mit der Cyber-Sicherheitsindustrie: Expertenwissen einbeziehen.
5. Abbau von Vorbehalten bei Betroffenen: Vertrauen in die Justiz stärken.

Die Justiz muss digital denken und agieren, um Cyberkriminalität effektiv zu bekämpfen. Datenzentrierte Ansätze, internationale Kooperation und die Zentralisierung von Ermittlungen sind essenziell, um die digitale Kriminalitätslandschaft nachhaltig zu adressieren.

Cybercrime – „Operation Endgame“ als erfolgreiche Strategieumsetzung - Carsten Meywirth

Die größte Bedrohung für die deutsche Wirtschaft bleibt Ransomware, mit einem geschätzten Gesamtschaden von 267 Milliarden Euro im Jahr 2024. 65% der betroffenen Unternehmen fühlen sich existenziell bedroht. Die Professionalisierung der Angreifergruppen und die Kommerzialisierung ihrer Methoden machen Cyberkriminalität zu einer globalen Herausforderung.
Ransomware-Gruppen operieren wie Unternehmen mit klaren Strukturen: CEOs, CFOs, IT und Marketing. Dienstleistungen wie „Dropper-Dienste“ (Platzierung von Schadsoftware) und „Ransomware as a Service“ (Vermietung von Angriffstools) sind Teil eines breiten kriminellen Ökosystems, das sich zunehmend als Franchise-Modell organisiert. So maximieren die Gruppen ihre Reichweite und Profite, oft mit 20 % Umsatzbeteiligung für Suborganisationen. Nach einem Angriff – häufig gezielt am Wochenende – werden Daten verschlüsselt und zusätzlich geleakt, um den Druck auf Unternehmen zu erhöhen.
Die Polizei und Sicherheitsbehörden setzen auf drei Ansätze:

- Akteur-Ansatz: Identifikation und Verfolgung der Täter.
- Infrastruktur-Ansatz: Störung der kriminellen Infrastrukturen, etwa durch gezielte Takedowns.
- Finanz-Ansatz: Nachverfolgung und Beschlagnahmung von Zahlungsströmen.

Internationale Zusammenarbeit ist hierbei essenziell. Bereits erreichte Erfolge, wie die Zerschlagung von Netzwerken oder gezielte Leaks zur Schädigung der Reputation, zeigen die Wirksamkeit dieser Strategien.
Die Professionalisierung von Ransomware-Gruppen verlangt innovative und koordinierte Gegenmaßnahmen. Durch die Kombination von technologischen, operativen und finanziellen Ansätzen können Behörden den Tätern entgegenwirken und die Wirtschaft widerstandsfähiger machen.

Dialog zwischen Prävention & Organisation - Sabine Griebsch, Dirk Kunze

Die Bewältigung von Cyberangriffen erfordert eine klare Organisation und Vorbereitung. Oft erleben betroffene Unternehmen oder Behörden nach einem Angriff eine Phase des Chaos, geprägt von unklaren Zuständigkeiten und mangelnder Kommunikation. Dies führt nicht nur zu Verzögerungen in der Reaktion, sondern schwächt auch das Vertrauen der Öffentlichkeit in die Funktionsfähigkeit von Verwaltung und Unternehmen.

Die größten Herausforderungen sind:

- Kommunikation: Behörden und Unternehmen sind außerhalb der Betriebszeiten oft nicht erreichbar, was die Reaktionszeit auf Bedrohungen verlängert.
- Organisation: Fehlende Strukturen und unklare Zuständigkeiten behindern die initiale Gefahrenabwehr.
- Priorisierung: Es fehlt häufig ein Verständnis dafür, welche Prozesse innerhalb von 7 Tagen wiederhergestellt werden müssen und welche warten können.

Diskutierte Lösungsansätze sind dabei:

1. Üben und Lernen: Regelmäßige Notfallübungen und klare Krisenpläne verbessern die Resilienz und Reaktionsfähigkeit.
2. Vernetzung: Polizei und Sicherheitsbehörden nutzen Erkenntnisse aus Ransomware-Angriffen, um gezielte Warnungen und Handlungsempfehlungen zu geben.
3. Erreichbarkeit: Verbesserte Kommunikationsstrukturen und spezielle Meldestellen sind essenziell, um Angriffe schnell zu melden und Hilfe zu erhalten.
4. Zusammenarbeit: Die Polizei agiert zunehmend wie Incident-Response-Teams und unterstützt bei der Krisenbewältigung vor Ort, statt Systeme einfach zu beschlagnahmen.

Cyberabwehr ist keine reine IT-Aufgabe. Sie erfordert Zusammenarbeit, klare Zuständigkeiten und regelmäßiges Üben. Behörden und Unternehmen müssen ihre Kommunikations- und Krisenmanagementstrukturen stärken, um Angriffe schneller und effektiver abzuwehren.