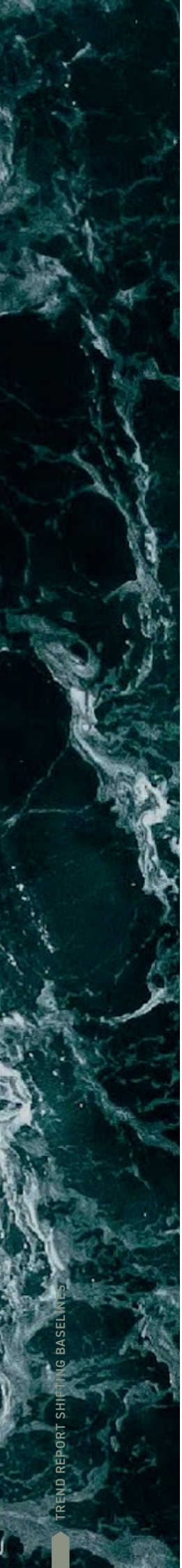
SHIFTING BASELINES

IT-Sicherheit aus der CFO- und CEO-Perspektive

GREEN FIELD

TRENDREPORT



Agenda

Vorwort

Sehr geehrte Leser, liebe Digital Leader,

nicht nur die Covid-Pandemie, gestörte Lieferketten und geopolitische Verwerfungen gefährden den Fortbestand und den profitablen Geschäftsbetrieb vieler Unternehmen in Europa. Auch die Angriffe auf die IT-Systeme von Unternehmen stellen mittlerweile eine existenzielle Bedrohung für die betroffenen Unternehmen dar.

Durch die Digitalisierung der Prozesse und Geschäftsmodelle sowie die Flexibilisierung der Arbeitswelt durch die massenhafte Verbreitung von Homeoffice sind die Unternehmen ihren Angreifern viel stärker exponiert als noch vor der Pandemie. Der Zugriff auf Unternehmensdaten erfolgt millionenfach über mobile Endgeräte und hunderte von Cloud-Diensten – und nicht mehr innerhalb der relativ sicheren Grenzen des eigenen Firmennetzwerks.

Gleichzeitig professionalisiert sich die Cybercrime-Branche in atemberaubendem Tempo. Besonders deutlich ist dies an der Zunahme sogenannter Ransomware-Attacken abzulesen, bei der Unternehmensdaten oder ganze Systeme verschlüsselt und nur gegen Lösegeld wieder freigegeben werden.

In der digitalen Welt wird IT-Sicherheit immer mehr zum Kosten- und Risikofaktor. Und somit Thema auch für CIOs. Wie Finanz- und Risikoverantwortliche mit den neuen Herausforderungen umgehen können und was sie tun können, um in ihrem Unternehmen die „Cyber Resilience" nachhaltig zu erhöhen, möchten wir Ihnen im folgenden Trend Report näherbringen.

Wir wünschen Ihnen viel Spaß beim Lesen!

Christian Grusemann
Business Manager Security
Bechtle AG

Dr. Carlo Velten
Principal Analyst
Atlantic Ventures GmbH

Von der Cyber Security zur Cyber Resilience

Shifting Baselines

Mit dem Begriff der „Shifting Baselines" beschreibt der Meeresbiologe Daniel Pauly das Phänomen der kollektiven Wahrnehmungsverschiebung. Er zeigt in seiner Forschung, wie sich die Referenzpunkte zur Bewertung dessen, was „normal" ist, innerhalb bestimmter Zeiträume verschieben können. Und wie sich eine „neue Normalität" konstituiert. Das Konzept lässt sich gut auf die schnelllebige und disruptive Welt der Digitalisierung anwenden. Und auch in Bezug auf die Entwicklung der Cybersecurity und Cyberkriminalität können wir enorme Verschiebungen und ein „New Normal" konstatieren.

Cybercrime – na und!

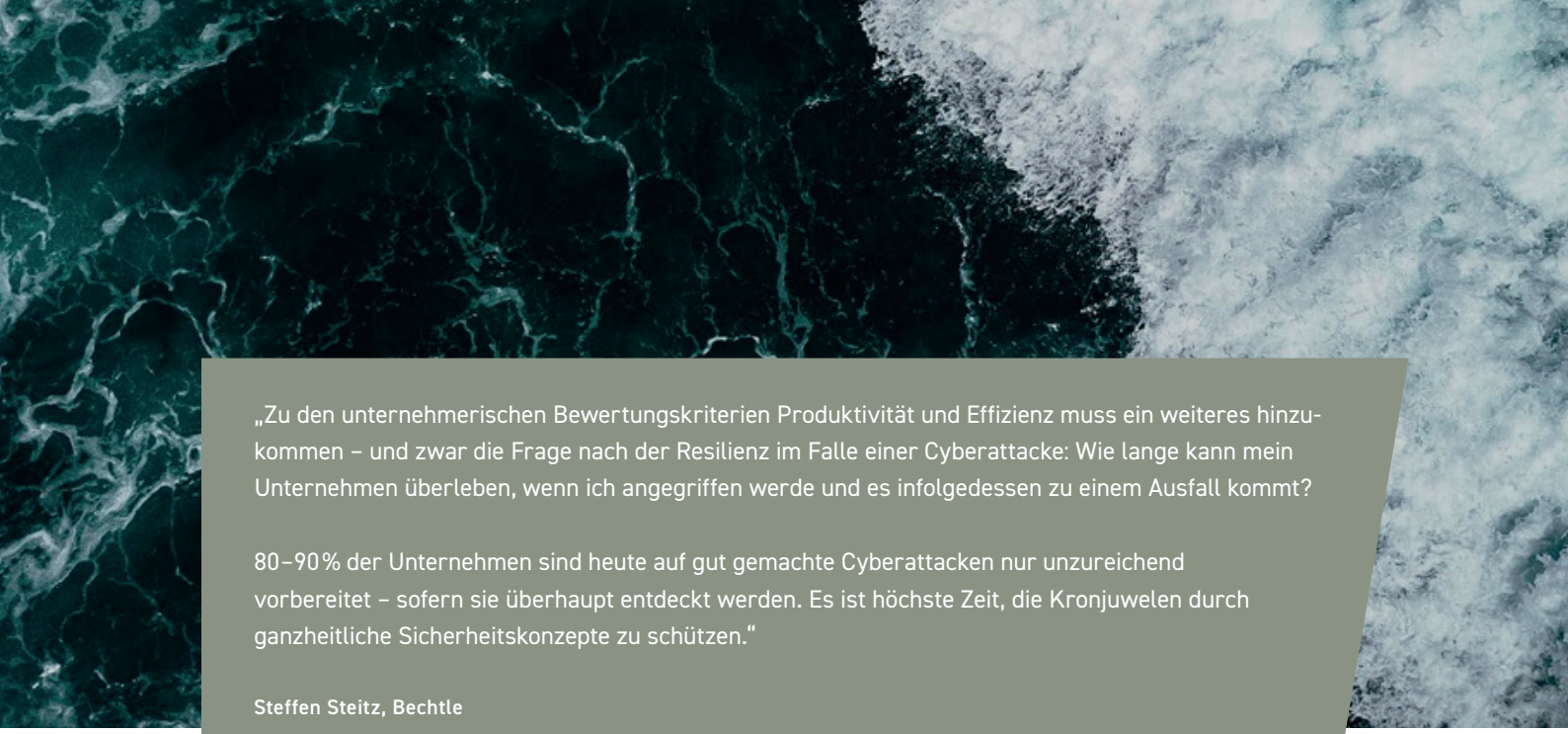
Durch die mediale Präsenz des Themas ist ein gefährlicher Gewöhnungseffekt eingetreten. Selbst viele Executives können nur noch müde lächeln, wenn das Bundeskriminalamt (BKA) in seinem aktuellen Lagebericht zur Cyberkriminalität von rund 146.000 erfassten Cyberstraftaten im vergangenen Jahr berichtet oder der IT-Branchenverband Bitkom von rund 203 Milliarden Euro Schaden in der deutschen Wirtschaft durch Cyberkriminalität im Jahr 2021 ausgeht. Auch bei konkreten Cyberattacken auf renommierte Top-Unternehmen in Deutschland erhebt sich unter den DAX-Vorständen kein kollektiver Protest und entsteht wenig gemeinsames Handeln. Das ist gefährlich, denn in Zeiten digitaler Vernetzung und digitaler Ökosysteme, die Unternehmen auf Basis von Daten und Software-Schnittstellen (APIs) miteinander verbinden, können Cyberattacken sich schnell auf ganze Lieferketten ausbreiten. Zudem kann der temporäre Ausfall eines Unternehmens zu schweren Problemen entlang der gesamten Lieferkette führen. Auch schwächt der immense Schaden durch Cyberkriminalität die gesamte Volkswirtschaft.

Not if but when

Leider signalisiert die Datenlage, dass CIOs sich mit der Tatsache anfreunden müssen, früher oder später nicht nur Ziel, sondern auch Opfer einer Cyberattacke zu werden. Die stetig wachsende Angriffsfläche durch mobiles Arbeiten, Cloud, digitale Produkte und IoT-Vernetzung sowie die verbesserten Angriffsmethoden und Skalenvorteile auf Seiten der Cyberkriminellen lassen keine andere Schlussfolgerung zu. Diese neue Einsicht muss unweigerlich zu einer Anpassung der Strategien und Investitionen im Bereich Cybersecurity führen.

Von der Ransomware zum Out-of-Business

Neben klassischem Datendiebstahl („Data Leaks") und DDos-Attacken haben sich in den letzten Jahren sogenannte Ransomware-Attacken einen Platz unter der gefährlichsten Angriffsvarianten erobert. Hier bedienen sich die kommerziell ausgerichteten Cyberkriminellen sogenannter Verschlüsselungs-Trojaner, die in der Lage sind, Daten, Applikationen und komplette Systeme asymmetrisch zu verschlüsseln. Die betroffenen Unternehmen sind meist handlungsunfähig und kommen nur gegen Zahlung bestimmter Lösegeld-Summen „wieder frei" bzw. zurück ins Geschäft. Selbst wenn Unternehmen über nicht komprimierte Backups ihrer Systeme verfügen, dauert deren komplette Wiederherstellung meist Tage, manchmal sogar Wochen. Nicht auszudenken, was passieren würde, wenn Ransomware-Attacken nicht durch monetär motivierte Täter erfolgen, sondern von politischen Aktivisten oder cybermilitärischen Gruppierungen durchgeführt würden, mit dem Ziel, Unternehmen komplett lahm zu legen. Zumindest erscheint dies denkbar und IT-Leiter und Geschäftsführer bzw. Vorstände sollten sich diesem Risiko zukünftig bewusst sein – und es in die eigenen Risikomodelle und Cyberresilienz-Strategien integrieren.



„Zu den unternehmerischen Bewertungskriterien Produktivität und Effizienz muss ein weiteres hinzukommen – und zwar die Frage nach der Resilienz im Falle einer Cyberattacke: Wie lange kann mein Unternehmen überleben, wenn ich angegriffen werde und es infolgedessen zu einem Ausfall kommt?

80–90 % der Unternehmen sind heute auf gut gemachte Cyberattacken nur unzureichend vorbereitet – sofern sie überhaupt entdeckt werden. Es ist höchste Zeit, die Kronjuwelen durch ganzheitliche Sicherheitskonzepte zu schützen."

Steffen Steitz, Bechtle

Security is Money

Mit steigender Anzahl der Cyberattacken, Meldepflichten gegenüber Behörden und Versicherungen sowie der Sammlung von Security Logs auf Seiten der Cloud- und Security Provider hat sich die Datenlage deutlich verbessert. Und dies nicht nur aus technischer Perspektive. Mittlerweile liegen belastbare Daten für die Kosten von Datenlecks und Cyberangriffen vor, die durch eine Vielzahl an empirischen Erhebungen untermauert werden. Nach einer Studie von IBM und dem Ponemon Institute verursachen beispielsweise Ransomware-Attacken bei großen Unternehmen durchschnittliche Kosten von 4,5 Millionen USD. So belaufen sich die Kosten für IT-Security nicht mehr nur auf den Kauf von entsprechender Security-Software, -Dienstleistungen und -Services sowie die Personalkosten für teure Experten. Die „echten" Kosten für IT-Sicherheit beinhalten mittlerweile auch Lösegeld, Kosten für die Aufarbeitung und Dokumentation der Schäden für Versicherer sowie für die Wiederherstellung der Geschäftstätigkeit nach einem Hack. Dies betrifft einfache Aufgaben, wie das Einspielen von Backups in die IT-Systeme, bis hin zum Wiederanfahren einer komplexen Fertigungsstraße nach einem Produktionsausfall. CFOs und Risk Manager sollten sich dieser Dimensionen bewusst sein und diese in ihren Budgetplanungen, Rückstellungen und Versicherungsprämien mit einkalkulieren.

Digitale Resilienz als neues Zielbild

Die Schwerpunkte bei der Arbeit an Cybersecurity-Strategien müssen sich grundlegend verändern, von der reinen Prävention und Abwehr von Angriffen hin zu Methoden der digitalen Resilienz, um im Fall eines Angriffs schnell wieder auf die Beine zu kommen. Im Zeitalter von Cloud und künstlicher Intelligenz sind hier neue und adaptive Business Continuity- und Incident Response-Strategien gefordert. Wichtig ist hier vor allem, dass Cyber Resilience gelebt und immer wieder trainiert und nicht nur in Handbüchern für die Compliance dokumentiert wird – und in der Schublade verstaubt.

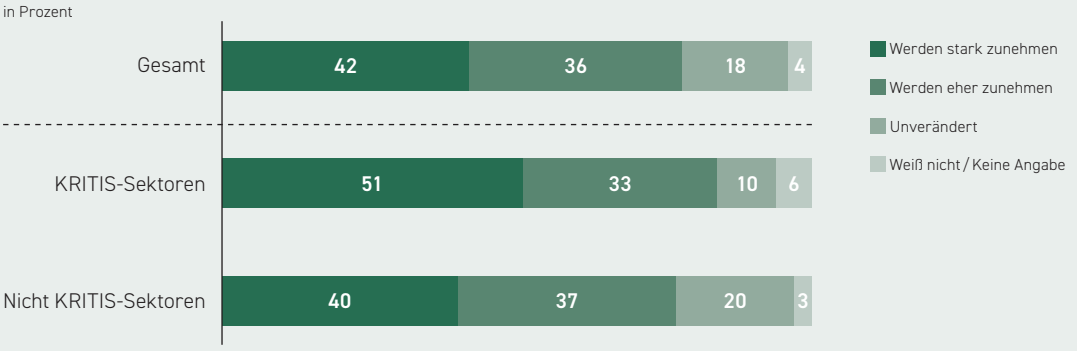
Die Top-Trends digitaler Bedrohungsmuster

Warum die digitale Welt immer gefährlicher wird

Um zu verstehen, warum sich die Angriffsfläche mit jedem Jahr vergrößert und auch die Wahrscheinlichkeit für erfolgreiche Angriffe steigt, müssen wir uns folgende Entwicklungen auf Seiten der Unternehmen und auf Seiten der organisierten Cyberkriminalität vor Augen halten.

Wirtschaft rechnet mit verstärkten Cyberangriffen

Wie wird sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den nächsten 12 Monaten im Vergleich zu den letzten 12 Monaten voraussichtlich entwickeln?



Basis: Alle befragten Unternehmen (n=1.066) | Quelle: Bitkom Research 2022

https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

Trends und Treiber für die Angriffsfläche und das Risiko auf Seiten der Unternehmen:

Kundendaten und digitale Geschäftsmodelle

Mit der zunehmenden Digitalisierung von Geschäftsmodellen und Kundenbeziehungen erfolgt ein Großteil der Kommunikation und Leistungserbringung mittlerweile virtuell. Das Vertrauen der Kunden in eine korrekte Abwicklung von Transaktionen (eCommerce), sichere Aufbewahrung (Datensicherheit) und rechtskonforme Nutzung (Datenschutz) der bereitgestellten Daten muss jederzeit gewährleistet sein. Sonst drohen neben Imageschäden auch direkte Umsatzeinbußen infolge der Abwanderung von Kunden. Dies gilt insbesondere in B2B-Geschäftsbeziehungen.

IIoT

Mit der Vernetzung, Wartung und (teil-)autonomen Steuerung von Maschinen, kompletten Produktionsanlagen und Warenlagern sind in den letzten Jahren erstmalig Kernprozesse nicht nur Teil der digitalen Infrastruktur geworden, sondern über den Einsatz internetbasierter Protokolle, Standards und Topologien auch erstmals potenziell exponiert für externe Angriffe oder Manipulation („Vernetzungsgrad und Verletzungsgrad").

Die Top-Trends digitaler Bedrohungsmuster

Covid und Homeoffice

Die breite Umstellung auf Arbeit im Homeoffice im Zuge der Corona-Krise hat in einigen Branchen und Unternehmen, welche darauf nicht vorbereitet waren, zu einer signifikanten Ausweitung der Angriffsfläche für Hacker und Ransomware geführt. Ungeschulte Mitarbeiter und unzureichend abgesicherte Endgeräte und Verbindungen schaffen potenziell Einfallstore in die ansonsten gut abgesicherte Unternehmens-IT.

Intellectual Property

Im Land der „Hidden Champions" werden laut Eurostat rund 100 Mrd. Euro für Forschung und Entwicklung ausgegeben. Vieles mündet in Patenten, Produktkonzepten und Forschungsergebnissen und liegt, hoffentlich verschlüsselt, in den digitalen Safes der Unternehmen und Forschungseinrichtungen. Sind Netzwerke, Speicher und Verschlüsselung auf keinem aktuellen Stand, wird aus Intellectual Property und Unternehmensgeheimnissen schnell ein global handelbares Gut.

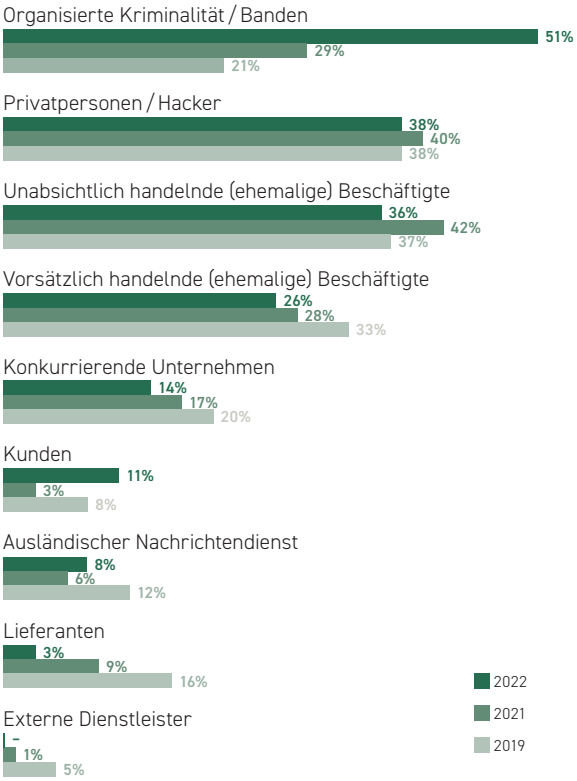
Digitale Zahlungsabwicklung und Währungen

Infolge von eCommerce und Online Procurement steigt in fast allen Branchen und Unternehmen der Anteil digitaler Zahlungsabwicklungen und somit auch das Risiko für Betrug und Diebstahl – auch wenn die etablierten Payment Provider bislang relativ erfolgreich Fraud Detection betreiben. Mit dem Aufkommen neuer digitaler Währungen à la Bitcoin, Ether und Co. und deren Akzeptanz für Transaktionen oder Unternehmensprozesse, potenziert sich das Risiko und erfordert in den dezentralen, Blockchain-basierten Netzwerken auch vollkommen neue Analyse- und Absicherungsstrategien.

KI-gesteuerte Prozesse

Nicht zuletzt die sukzessive Übertragung von betrieblicher und persönlicher Verantwortung an Algorithmen und smarte Maschinen (vom Fertigungsroboter über den Call-Center-Bot bis zur autonomen Steuerung von Labor- und Medizintechnik) erweitert sich das Risikospektrum enorm. Werden diese extern manipuliert oder mit falschen Daten gefüttert, können die Ergebnisse teuer bis verheerend sein. Hinzu kommt, dass sich die Nachvollziehbarkeit von Ergebnissen bei autonomen, selbstlernenden Systemen nur schwer gewährleisten lässt, was die Identifikation von Fehlern, Ursachen und auch Verursachern deutlich erschwert.

Attacken auf die Wirtschaft werden professioneller
Von welchem Täterkreis gingen Handlungen in den letzten 12 Monaten aus?



Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022:n=899; 2021: n=935; 2019: n=801) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

Die Top-Trends digitaler Bedrohungsmuster

Trends und Treiber auf Seiten der Cyberkriminellen und Angreifer:

Ransomware-as-a-Service

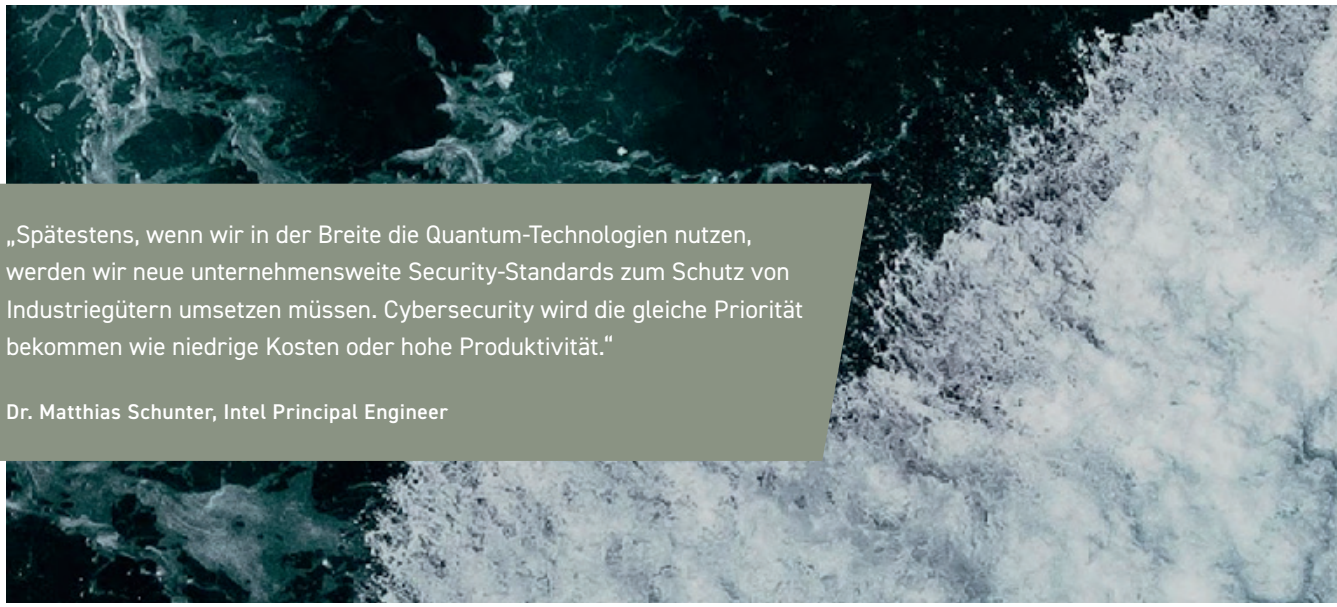
In der Branche der organisierten Cyberkriminalität nimmt der Level an Arbeitsteilung und Automatisierung immer weiter zu. Neben Bot-Netzwerken zur Ausführung von DDoS-Attacken, Marktplätzen für Verschlüsselungstools und Schadsoftware existieren mittlerweile auch komplette Cloud-Plattformen, die sich zur Ausführung von elaborierten Ransomware-Kampagnen mieten lassen („Ransomware-as-a-Service"). Hinzu kommt die Möglichkeit, via Kryptowährungen Lösegeld-Transfers weltweit durchzuführen oder kriminelle Leistungen, Passwörter und Hacker-Tools einzukaufen. Und dies bei geringen Transaktionsgebühren und nahezu ohne das Risiko zurückverfolgt werden zu können.

Hacker AI

Die Innovationen im Bereich der künstlichen Intelligenz wissen auch Cyberkriminelle für sich zu nutzen. Die Möglichkeit, betrügerische Anrufe per Sprachassistent gleichzeitig und millionenfach bei illegal gekauften Telefonnummern durchzuführen, macht die Möglichkeit zur Skalierung der kriminellen Geschäftsmodelle klar. Selbst Video-Calls lassen sich mittlerweile „faken", da Sprache und Bewegtbild sich kopieren und zweckentfremden lassen („Deep Fakes"). Hinzu kommt die Möglichkeit zur Entwicklung einer neuen Generation selbstlernender Schadsoftware und Verschlüsselungstrojanern, welche die IT-Sicherheitsindustrie vor neue Herausforderungen stellt.

Infrastruktur-Sabotage

Seit dem Beginn der militärischen Auseinandersetzungen in der Ukraine-Krise und der Sabotage an der Nordstream-Gas-Pipeline in der Nordsee, sind großangelegte Sabotage-Akte und die Zerstörung von kritischer digitaler Infrastruktur in Europa nicht mehr undenkbar und ein „schwarzer Schwan", sondern müssen als neue Risiken in die Business Continuity-Strategien der Unternehmen und Risikomodelle der Versicherungen integriert werden.



„Spätestens, wenn wir in der Breite die Quantum-Technologien nutzen, werden wir neue unternehmensweite Security-Standards zum Schutz von Industriegütern umsetzen müssen. Cybersecurity wird die gleiche Priorität bekommen wie niedrige Kosten oder hohe Produktivität."

Dr. Matthias Schunter, Intel Principal Engineer

Die Top-Trends digitaler Bedrohungsmuster

Cybercrime als Finanz- und Bilanzrisiko
Die oben skizzierten Entwicklungen und Trends führen zu einer strategischen Veränderung der digitalen Bedrohungslage in den Unternehmen. Und zwar in einer qualitativen und quantitativen Dimension. Denn es nehmen die Anzahl und die Kritikalität der Cyberangriffe und -Vorfälle von Jahr zu Jahr zu. Das gilt längst nicht mehr nur für die besonders bekannten DAX-Unternehmen, sondern zunehmend auch für Unternehmen im Mittelstand. Auch sie bieten für Hacker und die organisierte Kriminalität eine zunehmend attraktive Zielgruppe.

In der Folge müssen nicht nur mehr Ressourcen in die IT-Forensik und -Problembehebung fließen, sondern auch die direkten und indirekten Schäden aufgrund von Cyberattacken werden immer umfangreicher.

In einer Welt der digitalen Geschäftsmodelle und Geschäftsprozesse müssen sich Unternehmenslenker und gerade CFOs auf folgende Risiken und Szenarien einstellen:

Umsatzausfälle
Sind Onlineshops aufgrund von DDoS-Attacken nicht erreichbar oder digitale Services durch Ransomware-Attacke lahmgelegt, verlieren Unternehmen ab der ersten Minute Umsätze und gegebenenfalls auch die Kundenbeziehung. Gleiches gilt für online-basierte Buchungs- und Reservierungssysteme und deren Nutzung über Portale und Apps. Auch der B2B-Geschäftsverkehr kann beeinträchtigt werden, wenn digitale Plattformen und APIs für Partnerunternehmen nicht mehr erreichbar sind. Durch die Transformation in Richtung miet- und servicebasierter Geschäftsmodelle („Subscription Economy") trifft dies zukünftig immer mehr Unternehmen in signifikanter Form.

Produktionsausfälle und Betriebsunterbrechungen
Durch elaborierte Ransomware gelangt in fast allen Unternehmen immer wieder Schadsoftware in die IT-Netzwerke. Je nach Art der Schadsoftware und den Verbreitungsmöglichkeiten innerhalb der Netzwerkarchitektur, richten diese mehr oder weniger Schaden an. Mit der Verschlüsselung produktionsrelevanter Systeme und Applikationen sollten Unternehmenslenker zukünftig kalkulieren und dies in ihren Risikoszenarien berücksichtigen. Der Aufbau redundanter Architekturen und der Entwicklung von entsprechenden Business Continuity- und Back Up-Konzepten kommt zukünftig ein hohes Gewicht zu. Vor allem müssen diese in der Praxis immer wieder unter Live-Bedingungen „trainiert" werden und dürfen nicht nur als Anweisung „auf dem Papier" stehen.

Produktivitätseinbußen
Auch wenn im Falle von Ransomware-Attacken keine produktionsrelevanten Systeme betroffen sind, kann der Ausfall von z.B. eMail-, Collaborations- oder Business-Applikationen zu massiven Produktivitätseinbußen führen und die Geschäftsprozesse signifikant stören.

Imageschäden
Mögliche Reputationsschäden lassen sich meist nur schwer beziffern, wirken aber nachhaltig und oft schwer. Hier gilt es vor allem die Kommunikation gegenüber Kunden und Partnern auf einen solchen Fall vorbereitet und durchgespielt zu haben.

Die Top-Trends digitaler Bedrohungsmuster

Folgeschäden

Das „Aufräumen" und Wiederherstellen von Systemen und Daten nach einem Hack oder Leak verursacht hohe Kosten, die bei internationalen Unternehmen in Millionenhöhe liegen. Hinzu kommen die internen sowie externen Kosten für die Aufarbeitung und Dokumentation von Cybervorfällen für Versicherungen und Behörden.

Versicherungsprämien

Analog zur Bedrohungslage entwickelt sich auch der Markt für Cybersecurity-Versicherungen sehr dynamisch. So geht Mordor Intelligence[1] von einem weltweiten Marktvolumen von rund 9,3 Mrd. USD im Jahr 2021, das sich auf rund 28,2 Mrd. USD im Jahr 2027 mehr als verdreifachen soll, was einerseits an der Anzahl neuer Abschlüsse sowie andererseits an den stark steigenden Prämien liegt. Diese sollten CFOs antizipieren und entsprechend budgetieren sowie gemeinsam mit dem CIO Strategien entwickeln, um ein möglichst gutes Risiko-Scoring zu erhalten. So werden Prämien für Cyberversicherungen von Großunternehmen zukünftig stark dynamisch sein und sich an der Risikomodellierung, Datentransparenz (z.B. Security Logs, System- und Security-Architektur), wiederkehrenden Audits sowie gegebenenfalls auch der Möglichkeit zum Live-Zugriff auf das SOC durch Spezialisten der Versicherungen orientieren.

[1] https://www.mordorintelligence.com/de/industry-reports/cyber-security-insurance-market

Der Weg zur digitalen Resilienz

Um das eigene Unternehmen resilient gegenüber den vielfältigen und heimtückischen Cybergefahren zu machen, muss das gesamte Führungsteam eingebunden sein – und gemeinsam die Verantwortung tragen. Ein paar Euro mehr Security-Budget bereitzustellen und die Verantwortung komplett dem CIO oder CISO zu überlassen, wird in den kommenden Jahren nicht funktionieren – und ist sicherlich ein Konzept von gestern.

Viel eher gilt es, mit fortschreitender Digitalisierung der Geschäftsprozesse, die jeweiligen Business-Entscheider zu sensibilisieren und mit in die Entwicklung einer gesamtheitlichen Sicherheitsarchitektur für das Unternehmen einzubinden. Da ein Großteil der erfolgreichen Cyberattacken auf menschliches (Fehl-)Verhalten zurückzuführen ist, zeigt sich, wie wichtig die Sensibilisierung und Schulung der Mitarbeiter und die Vorbildfunktion der Führungskräfte ist.

Mit folgenden Schritten können Unternehmen den Weg zu mehr digitaler Resilienz und IT-Sicherheit beginnen:

Security Back to the Business
Die Verantwortung für die Sicherheit und Integrität klar definierter Geschäftsprozesse und Systeme sollte beim jeweiligen Business Owner liegen. Diese sollten in Kooperation mit dem CIO oder CISO ein jährliches Review zur Sicherheitslage in ihrem Geschäftsbereich durchführen. Auf diese Weise werden Schwachstellen sichtbar, Risikobewusstsein und Verantwortung sukzessive entwickelt und Handlungsszenarien für den Ernstfall mit allen Stakeholdern entworfen und durchgespielt.

Risk Management und Simulation
Unternehmen sollten sich über ihre individuellen Risiko- und Schadensszenarien genau im Klaren sein. Die Simulation von Produktionsausfällen oder unterbrochenen Prozessen kann helfen, Schäden und Risiken ex ante zu kalkulieren sowie Verhaltensmaßnahmen vorab zu evaluieren.

Security Operations Center (SOC)
Der Aufbau und Betrieb eines zentralen Security Operations Center ist ein weiterer Baustein auf dem Weg zu einem digital resilienten Unternehmen. In diesem werden alle sicherheitsrelevanten Funktionen und Prozesse zusammengefasst, integriert sowie ein proaktives 24/7 Monitoring aller kritischen Systeme und Infrastrukturen aufgesetzt. Zu den weiteren Funktionen eines SOCs zählen Security Alerting, Assessment, Reporting sowie die Umsetzung von Abwehrmaßnahmen im akuten Krisenfall.

Security Expertise und Investment
Der Auf- und Ausbau von entsprechender Expertise zählt zu den wichtigsten und schwierigsten Aufgaben, da IT Security-Spezialisten am Markt nur schwer verfügbar sind. Dies gilt gerade in den Feldern Cloud Security, IoT- und Netzwerk Security sowie in der IT-Forensik. Zudem sollten die Unternehmen ihre Ausgaben der Gefahrenlage anpassen und die Investitionen in IT-Security ausbauen.

Security Experience und Culture
Zum Aufbau einer unternehmensweiten Sicherheitskultur braucht es Maßnahmen auf allen Ebenen. So gilt es – analog zum politischen Bereich – ein „Morning Briefing" für die Top-Entscheider zu installieren, welches die Gefahrenlage und Incidents auch für das Top-Management aufbereitet und diesen die Relevanz des Themas nachhaltig vor Augen führt. Die Einführung entsprechender Sicherheitsprozesse, wie z.B. der 2-Faktor Authentifizierung, muss für alle Mitarbeiter zu einer verbindlichen Routine werden – analog zum Zähneputzen. Die IT-Abteilung kann dafür sorgen, dass diese Routinen den Arbeitsablauf nicht stören, sondern nutzerfreundlich z.B. über eine Gesichtserkennung integrieren lassen.

Autoren

Christian Grusemann ist als Business Manager Security seit fünf Jahren bei der Bechtle AG verantwortlich für die Security-Strategie des Unternehmens. Zuvor hatte er verschiedene Führungspositionen in der IT-Industrie inne. So verantwortete er bei NTT u. a. Themen wie Managed Services und war rund 13 Jahre bei Computacenter tätig, zuletzt als Business Unit Director Security.

christian.grusemann@bechtle.com
www.bechtle.com

Christian Grusemann
Business Manager Security
Bechtle AG

Dr. Carlo Velten
Principal Analyst
Atlantic Ventures GmbH

Dr. Carlo Velten ist Gründer und Principal Analyst beim unabhängigen Technologie Research und Beratungsunternehmen Atlantic Ventures. Seit über 20 Jahren berät Carlo Velten als erfahrener Technologie Analyst namhafte Unternehmen bei der Ausgestaltung Ihrer IT-, Digital- und Innovationsstrategien. In den Technologiefeldern Cloud Computing und AI zählt er zu den führenden Experten im deutschsprachigen Raum. Als Serial Entrepreneur, Investor und leidenschaftlicher Surfer verfügt Carlo Velten über das richtige Gespür für die nächsten „Technology Waves". Bei Atlantic Ventures unterstützt er Kunden bei der Ausarbeitung ihrer Wachstums- und Investmentstrategien in den neuen digitalen Märkten.

carlo.velten@atlantic-ventures.com
www.atlantic-ventures.com

Über Bechtle Greenfield

Bechtle Greenfield ist das innovative Format für IT-Führungskräfte, -Entscheider und technisch affine Unternehmenslenker. Bechtle Greenfield schafft Platz für neues Denken und kollaboratives, fokussiertes Arbeiten an Lösungen. Basierend auf den Erfahrungen aus über 70.000 Firmen-Kunden-Beziehungen und mehr als 200 führenden Partnerschaften mit führenden Technologieanbietern beschäftigt sich Bechtle Greenfield mit der Integration innovativer Technologien, der Transformation klassischer Geschäftsmodelle in digitale Ökonomien und der Umsetzungskompetenz der IT-Lenker der deutschen Wirtschaft.

GREEN FIELD

Dabei sein, wenn Neues entsteht. Von Anfang an.

Werden Sie Teil der exklusiven Executive Community auf **LinkedIn** und besuchen Sie uns auf unserer Webseite:
bechtle.com/aktion/greenfield

Powered by intel

Bechtle Greenfield
Bechtle Systemhaus Holding AG
Bechtle Platz 1 · DE-74172 Neckarsulm
greenfield@bechtle.com

Ihr starker IT-Partner.
Heute und morgen.

BECHTLE