eraneos

E-Paper

Cybervorfälle weltweit als Top-Risiko eingestuft

Zusammenfassung verschiedener Marktumfragen zum Thema Cyber Security

Adrian Marti
Partner, Cyber Security

Inhalt

Cybervorfälle weltweit als Top-Risiko eingestuft

Die letzten 18 Monaten waren geprägt von einem massiven Digitalisierungsschub, der mit einem Anstieg der Cyberbedrohungen einherging, dem die Gesellschaft je länger je weniger gewachsen ist. Niedrigere Einstiegshürden für Cyberbedrohungen, aggressivere Angriffsmethoden, ein 435 % Anstieg von Ransomware im Jahr 2020, weltweit rund 3 Millionen fehlende Cybersecurity-Experten und lückenhafte Governance-Mechanismen verschärfen das Risiko zusätzlich. Wenn wir nicht handeln und das digitale Vertrauen durch gezielte und anhaltende vertrauensbildende Initiativen verbessern, wird die digitale Welt weiter in Richtung Fragmentierung abdriften. Diese digitale Fragmentierung beeinträchtigt nicht nur die globale Wirtschaft. Sie bedroht auch die langfristigen Wachstumssausichten und Innovationsstrategien von Unternehmen und könnte dazu führen, dass die Chancen einer der dynamischsten Epochen des menschlichen Fortschritts ungenutzt verstreichen.

Sowohl Regierungen und Unternehmen wie auch die Gesellschaft verlassen sich in jeder Situation zunehmend auf Technologie – von öffentlichen Diensten über Geschäftsprozesse bis hin zum täglichen Lebensmitteleinkauf. In Zukunft wird die Vernetzung und Konvergenz dieser digitalen Werkzeuge weiter zunehmen. Entsprechend müssen sich die Nutzer mit den Sicherheitslücken auseinandersetzen, die sich aus der zunehmenden Abhängigkeit von und der wachsenden Fragmentierung dieser komplexen Technologien ergeben. Denn aktuell werden 95 % der Cybersicherheitsprobleme auf menschliches Versagen zurückgeführt. Zudem müssen fehlende Standards und lückenhafte Durchsetzungsmechanismen in den verschiedenen Rechtsordnungen gezielt abgebaut werden, damit die Bemühungen zur wirkungsvollen Kontrolle der Cyberkriminalität flächendeckend greifen.

Steigende digitale Abhängigkeit führt zu einer massiven Erhöhung der Cyberbedrohungen

Mit der fortschreitenden Migration der Gesellschaft in die digitale Welt steigt die Bedrohung durch Cyberkriminalität immer schneller und kostet Unternehmen regelmässig Dutzende oder sogar Hunderte von Millionen Dollar. Selbst bei ausgefeilten und umfassenden Schutzmassnahmen vor digitalen Bedrohungen werden die Betriebskosten für alle Beteiligten erheblich steigen. Dies könnte eine besondere Herausforderung für KMU darstellen, die möglicherweise 4 % oder mehr ihres Betriebsbudgets für Sicherheit ausgeben müssen, während grössere Organisationen hierzu rund 1 bis 2 % aufwenden. Die Teilnehmenden an der Global-Risk-Perception-Umfrage 2022 des Weltwirtschaftsforums gaben an, dass sie sich langfristig Sorgen über diese Entwicklungen machen, wobei „ungünstige technologische Fortschritte" als Top-10-Risiko über einen Zeitraum von 5 bis 10 Jahren genannt wurden.

Angriffe auf grosse und strategische Systeme werden gravierende physische Folgen für die gesamte Gesellschaft haben. Zugleich werden immaterielle Risiken, wie Desinformation, Betrug und mangelnde digitale Sicherheit, das Vertrauen der Öffentlichkeit in digitale Systeme beeinträchtigen.

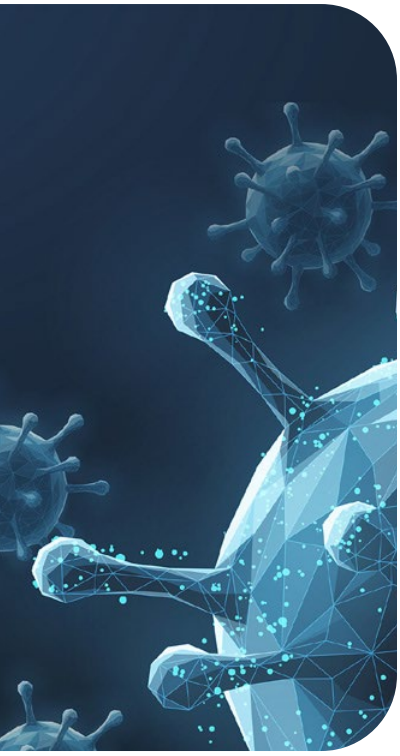
Die zunehmenden Cyberbedrohungen werden auch die länderübergreifende Zusammenarbeit erschweren, wenn die Regierungen weiterhin unilaterale Wege zur Risikokontrolle beschreiten. Und: da die Angriffe immer weitreichender ausfallen, werden sich bestehende Spannungen zwischen Regierungen, die von Cyberkriminalität betroffen sind, und Regierungen, die sich an deren Begehung mitschuldig gemacht haben, weiter verschärfen.

Auch für Unternehmen wird die Absicherung gegen Cyberrisiken immer schwieriger. Kommt es zu einem Angriff, werden viele Unternehmen gezwungen sein, immer höhere Lösegelder zu zahlen. Andernfalls müssen sie mit Imageschäden, finanziellen Einbussen sowie gegebenenfalls sogar mit rechtlichen und regulatorischen Konsequenzen rechnen. Zudem riskieren Unternehmen, die keine strenge Corporate Governance im Bereich der Cybersicherheit vorweisen können, einen Reputationsverlust bei ESG1-orientierten Investoren.

Hinzu kommt, dass Unternehmen heute in einer Welt agieren, in der absichtliche oder versehentliche Insider-Bedrohungen 43 % aller Sicherheitsverletzungen ausmachen. Einige Unternehmen reagieren mit einer stärkeren Segmentierung digitaler Systeme, um solche Risiken besser zu berücksichtigen. Ander halten wichtige Daten unter Verschluss. Dies könnte sich jedoch negativ auf die Effizienz der Mitarbeitenden auswirken, da der Zugriff auf Daten und Informationen dadurch weniger nahtlos erfolgten kann.
Akuter Handlungsbedarf besteht im Hinblick auf neue gesetzliche Regelungen auch beim Datenschutz. Datenschutz-Compliance ist heute ein Muss für jedes Unternehmen, um die Gefahr von Datenschutzverletzungen wirkungsvoll einzudämmen. Dies könnte u. a. bedeuten, dass die Datenverarbeitung in Länder verlagert werden muss, die einen besseren Kundenschutz in Bezug auf Datenschutzfragen anbieten.

Vor diesem Hintergrund ist es wenig erstaunlich, dass ein „Versagen der Cybersicherheit" für die Teilnehmenden der Global Risk Perception Studie 2022 des Weltwirtschaftsforums (WEF) weltweit zu den Top-10 Risiken gehört. Darüber hinaus haben 85 % der Cybersecurity Leadership Community des WEF betont, dass Ransomware zu einer gefährlich wachsenden Bedrohung wird und ein grosses Problem für die öffentliche Sicherheit darstellt.

Noch klarer fielen die Resultate der globalen CEO-Umfrage 2022 von PwC aus, an der 4´446 CEOs aus 89 Ländern teilgenommen haben: 100 % der Befragten gaben an, dass Cyberrisiken für sie an der Spitze des diesjährigen Bedrohungsbarometers stehen.



COVID-19 als Haupttreiber der steigenden Cyber-Bedrohungen

Begründet liegt dieser weltweite Aufstieg zum Top-Risiko in der Corona-Pandemie, die Unternehmen gezwungen hat, ihre Digitalisierung massiv zu beschleunigen, um virtuelle Arbeit zu unterstützen. Das Home-Office wurde zur „neuen Normalität". Damit einhergehend ist nicht nur die Zahl der Heimarbeitsplätze, sondern auch die Nutzung von virtuellen Kommunikations- und Kollaborations-Tools geradezu explodiert. Laut Gartner gehen drei Viertel der Unternehmen davon aus, dass zumindest ein Teil der Arbeit auch nach der Pandemie „remote" erfolgen wird.

Die Pandemie hat aber nicht nur die Digitalisierung in den Unternehmen dynamisch vorangetrieben. Auch die Akteure der Cyberkriminalität haben sich rasant weiter professionalisiert und ihre Methoden perfektioniert. Dadurch ist die Zahl der Bedrohungen um das 1000-fache angestiegen. Sowohl Konzerne als auch KMU sehen sich immer häufiger mit existenzbedrohenden Angriffen aus dem Cyberspace konfrontiert. Sicherheitsexperten gehen davon aus, dass vor allem der Grad der Raffinesse und das Ausmass der Cyberangriffe 2022 weiter zunehmen und rekordverdächtige finanzielle Verluste verursachen werden.

Verbreitete Herausforderungen und Hürden bei der Gewährleistung der Cybersicherheit

Obwohl sich in den letzten zwei Jahren ein besseres Verständnis für Cyberangriffe und ihre Folgen entwickelt hat, herrscht bei den meisten Befragten der globalen CEO-Umfrage 2022 von PwC eine gewisse Ratlosigkeit, wie dieser Gefahr zu begegnen ist und welche Investitionen am schnellsten und effektivsten greifen. Hundertprozentigen Schutz gibt es nicht. Wichtig ist jedoch, eine ausreichende Resilienz gegen Cyberattacken aufzubauen. Entsprechend muss der lückenlose Umgang mit entsprechenden Vorfällen präventiv geplant, umgesetzt und geprobt werden. Hierzu müssen nicht nur die Sicherheitsbedürfnisse in den Unternehmen angepasst, sondern auch die erforderlichen technischen und personellen Ressourcen bereitgestellt werden. Dies setzt jedoch voraus, dass die CEOs das Thema nicht nur als Besorgnis Nummer eins werten, sondern auch gezielt agieren.

Weltweit fehlen mehr als 3 Millionen Fachkräfte, die eine Führungsrolle im Cyberbereich übernehmen, Systeme testen und sichern sowie Menschen in digitaler Hygiene schulen können.

Zeitmangel und Ressourcenprobleme erschweren die Cyber Security

Wie der WEF Global Risk Report 2022 klar aufzeigt, ist der weltweite Mangel an qualifizierten IT- und Cybersicherheitsexpert* innen gravierend. Es fehlen mehr als 3 Millionen Fachkräfte, die eine Führungsrolle im Cyberbereich übernehmen, Systeme testen und sichern sowien Menschen in digitaler Hygiene schulen können. Dies hat Konsequenzen: Ein Tool zu kaufen ist relativ einfach. Es richtig zu nutzen, allerdings weniger. Hierzu braucht es Ressourcen, Zeit und letztlich auch Budget.

Sicherheitsfachleute sind zudem mit der ständig wachsenden Belastung konfrontiert, die mit der Gewährleistung der Security Operations verbunden ist. Die meisten Experten sind sich einig, dass es zu lange dauert und zu teuer ist, Sicherheitsvorfälle zu erkennen und darauf zu reagieren. Denn oftmals verbringen Sicherheitsteams zu viel Zeit mit der Untersuchung von Warnmeldungen und der Bewältigung von Notfällen, wohingegen die Zeit für Strategie und Prozessverbesserung fehlt.

Zu den weiteren Herausforderungen und Hemmfaktoren bei der Umsetzung und Einhaltung von ICT-Sicherheitskonzepten zählen gemäss einer aktuellen Studie von MSM Research die vielfach geringe Priorität seitens des Business, fehlende organisatorische Prozesse, Richtlinien, Kontrollmechanismen und Budgets sowie ein unzureichendes Awareness-Training der Mitarbeitenden.

Cyberbedrohungen, mit denen sich Unternehmen auseinandersetzen müssen

435 % Anstieg von Ransomware im Jahr 2020

85 % der Cybersecurity Leadership Community des Weltwirtschaftsforums betont, dass Ransomware bedrohliche Ausmasse annimmt und damit ein grosses Problem für die öffentliche Sicherheit darstellt.

Ransomware-Angriffe nehmen nicht nur exponentiell zu, sie werden auch immer aggressiver. Allein in der Schweiz wurden 2020 insgesamt 20 ´544 Fälle gemeldet, davon 16 ´395 als Cyberbetrug. Die durchschnittliche Schadenssumme betrug rund 6 Mio. CHF – steigt weiterhin rasant an. In Fällen der kompletten Verschlüsselung von IT-Infrastrukturen liegt der Durchschnitt bereits über 100 Mio. CHF. Neben der Schadenssumme nimmt auch die Angriffsfrequenz laufend zu: Durchschnittlich alle 11 Sekunden wird ein Schweizer Unternehmen mit dem Ziel eines Erpressungsversuchs (Ransomware) angegriffen, wobei Firmen jeder Art und Grösse im Fokus stehen. Gefährdet sind insbesondere Unternehmen, die sich nicht im Visier von Cyberkriminellen sehen und entsprechend unvorbereitet sind.

Da es aktuell keine Verpflichtung (Ausnahmen: Finanzwelt und medizinischer Bereich) zur Meldung von Cyberattacken gibt, liegen die effektive Zahl der Angriffe und der daraus entstandene Schaden mit Sicherheit noch um ein Vielfaches höher. Mit konsequenteren Meldungen liesse sich diese Dunkelziffer reduzieren und die Opfer könnten voneinander lernen. Zudem könnten diese Informationen gezielt für die Bekämpfung, Vorbereitung und Strafverfolgung genutzt werden.

Cybercrime as a Service

Neben Angriffen mithilfe von Schadsoftware wird auch deren Vermarktung immer professioneller. Cyberkriminelle haben damit ein lukratives Geschäftsmodell geschaffen, und es zeichnet sich klar ab, dass dieser Markt 2022 deutlich weiterwachsen wird. Die häufigsten Einfallstore sind gestohlene Anmeldedaten, die Ausnutzung bekannter Sicherheitslücken und Phishing. Regelmässige Awareness-Trainings für die Mitarbeitenden sind hier von zentraler Bedeutung. Denn Untersuchungen haben gezeigt, dass risikobewusste Mitarbeitende mit achtmal geringerer Wahrscheinlichkeit zu Opfern werden.

Cybersicherheitsrisiken bei der Remote-Arbeit

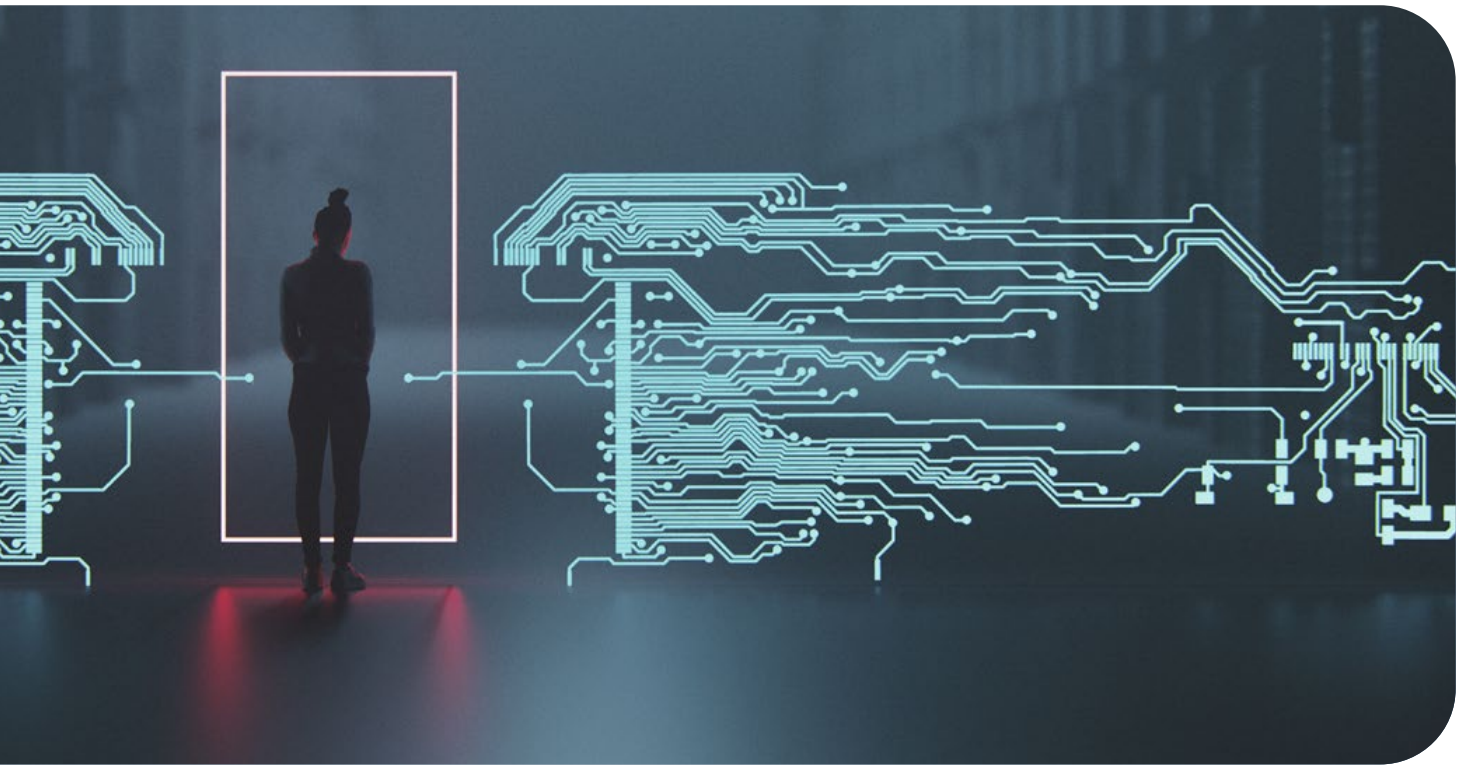
Die Arbeit von zu Hause aus birgt neue Cyberrisiken und erfordert einen starken Fokus auf die Sicherheitsherausforderungen verteilter Arbeitskräfte. Homeoffices sind oft weniger geschützt als die Arbeitsplätze in Unternehmen, was dazu führt, dass Cyberkriminelle ihre Taktiken anpassen, um daraus Nutzen zu ziehen. Viele Mitarbeitende verwenden ihre persönlichen Geräte für die Zwei-Faktor-Authentifizierung und verfügen möglicherweise über mobile Versionen von Instant-Messaging-Clients wie Microsoft Teams und Zoom. Diese verschwimmenden Grenzen zwischen Privat- und Berufsleben erhöhen das Risiko, dass sensible Informationen in die falschen Hände geraten.

Der Trend zur Remote-Arbeit beschleunigt auch das Wachstum des Mobilfunks. Infolgedessen nehmen die mobilen Bedrohungen zu und entwickeln sich weiter.

Sie reichen von Spyware, die darauf ausgelegt ist, verschlüsselte Messaging-Anwendungen auszuspionieren, über Kriminelle, die kritische Sicherheitslücken in Android-Geräten ausnutzen, bis hin zu mobiler Malware, deren Anwendungsszenarien von DDoS-Angriffen (Distributed Denial of Service) über SMS-Spam bis hin zu Datendiebstahl reichen.

Social Engineering – der Mensch als Schwachstelle

Beim Social Engineering nutzt der Täter den „Faktor Mensch" als vermeintlich schwächstes Glied der Sicherheitskette aus, um seine kriminelle Absicht zu verwirklichen. Neben gezielten Angriffstaktiken wie Spear-Phish-ing kommen zunehmend auch neue Technologien wie Deepfakes zum Einsatz. Deepfakes wirken sehr überzeugend und werden von Cyberkriminellen verwendet, um die Zielpersonen dazu zu bringen, persönliche Daten, Kontodaten oder Geld zu übermitteln. Für Organisationen werden in Zukunft besonders Voice-Phishing-Angriffe, bei denen ein Bot eine bekannte Stimme imitiert, eine grosse Gefahr darstellen. Darüber hinaus werden Audio-Deepfakes auch genutzt, um eine darauffolgende Phishing-Mail vorab zu legitimieren. Mit der zunehmenden Nutzung von AI Technologien in der Cyberkriminalität werden solche Angriffe immer raffinierter.



Vielfach haben es Angreifer auch auf Personen abgesehen, die sich von zu Hause aus in das Netzwerk ihres Arbeitgebers einwählen. Neben den traditionellen Phishing-Angriffen auf Mitarbeitende sind zudem vermehrt Whaling-Angriffe auf Führungskräfte zu beobachten.
Messaging-Phishing gewinnt dank der Beliebtheit von Whats-App, Slack, Skype, Signal, WeChat, etc. ebenfalls an Bedeutung. Angreifer nutzen diese Plattformen, um Benutzer dazu zu verleiten, Malware auf ihr Smartphone herunterzuladen.

Sicherheitsherausforderungen durch Cloud-Strategien und moderne Technologien

Zunehmende Komplexität und fehlendes Personal mit guter Ausbildung in Kombination mit rasanter technologischer Entwicklung treiben hybride und Multi-Cloud-Strategien und die Ausbreitung von modernen Techologien (Internet of Things (IoT), 5G, Blockchain, Edge Computing, Künstliche Intelligenz, Machine Learning) voran und bieten sich Akteuren mit böswilligen Absichten wachsende Angriffsflächen. Denn diese Technologien bieten zwar enormes Nutzungspotenzial, setzen die Anwender aber gleichzeitig erhöhten und schädlicheren Formen von digitalen und Cyber-Risiken aus.

95 % der Cybersicherheitsprobleme werden auf menschliches Versagen zurückgeführt.

Bei **Angriffen über die Cloud** loggen sich Angreifer heutzutage einfach ein, da für nahezu alle Attacken auf die Cloud gestohlene privilegierte Anmeldedaten genutzt werden. Auch Fehlkonfigurationen und unzureichende Cloud-Migrationsstrategien sind wesentliche Ursachen für Datenschutzverletzungen und unbefugten Zugriff, unsichere Schnittstellen und Account-Hijacking. Die durchschnittlichen Kosten einer Datenschutzverletzung belaufen sich auf 3,86 Millionen US-Dollar.

Zu den weiteren Sicherheitsrisiken beim Cloud-Computing gehören Sicherheitslücken bei der Datenübertragung, die Sicherstellung der Einhaltung gesetzlicher Vorschriften in verschiedenen Rechtsordnungen, die Überwachung der vielen potenziellen Einstiegspunkte für Angreifer sowie Insider-Bedrohungen durch schwache Passwörter, ungesicherte Netzwerke und den Missbrauch von persönlichen Geräten. Entsprechend sollte das Sicherheits-Portfolio von Unternehmen eine zentrale Privileged Access Management (PAM) Lösung enthalten, die in der Cloud für die Cloud entwickelt wurde. Dieser Ansatz minimiert die Angriffsfläche und kontrolliert den privilegierten Zugriff auf hybride und Multi-Cloud- Umgebungen.

Cloud-basierte Unternehmen mit Remote-Mitarbeitenden sind mit besonderen Herausforderungen in der Cybersicherheit konfrontiert. Sie müssen transparent darlegen, wie sie gesetzlich geschützte Daten sammeln, schützen und handhaben – und wie sie diese vor unbefugtem Zugriffen schützen.

Auch die **Verwaltung von Maschinenidentitäten** gewinnt an Bedeutung. Moderne Anwendungen bestehen heutzutage aus einer Vielzahl von Diensten, die über APIs verbunden sind. Jeder dieser Dienste muss authentifiziert und überwacht werden, da Angreifer den API-Zugriff von Lieferanten auf

wichtige Daten zu ihrem Vorteil nutzen können. Mit einer unternehmensweiten Strategie zur Verwaltung von Maschinenidentitäten, Zertifikaten und Geschäftsgeheimnissen können Unternehmen ihre digitale Transformation besser absichern.

Von wachsender Bedeutung ist die **IoT-Sicherheit**. Die Zahl der vernetzten Geräte wird Prognosen zufolge 2022 rund 18 Milliarden erreichen. Dies führt unter anderem dazu, dass die Zahl der potenziellen Zugangspunkte zu digitalen Systemen massiv steigt. Für Hacker stellen sowohl die 5G-Netze als auch die mobilen Geräte, welche diese Netze nutzen, lohnende Ziele dar. Durch **Angriffe auf 5G-Netze** können Cyberkriminelle kritische staatliche Infrastrukturen destabilisieren und mit Angriffen auf mobile Geräte können sie sich Zugang zu Unternehmensnetzen verschaffen. Entsprechend könnten sich die Sicherheitsprobleme im Zusammenhang mit dem IoT als weitaus gravierender erweisen, als bisher angenommen, zumal die potenziellen Angriffsziele nahezu jedes Gerät umfassen, das mit dem Internet verbunden ist. Zudem haben die meisten IoT-Geräte im Vergleich zu Laptops und Smartphones weniger Verarbeitungs- und Speicherkapazitäten. Dies kann den Einsatz von Sicherheits-Tools wie Firewalls, Antivirenprogramme und andere Sicherheitsanwendungen erschweren.

Besorgniserregend ist ferner, dass **Quantencomputer** durch ihre Architektur in der Lage sind, gängige Verschlüsselungsalgorithmen zu knacken. Dies stellt aufgrund der Sensibilität und Kritikalität der durch diese Schlüssel geschützten finanziellen, persönlichen und anderen Daten ein erhebliches Sicherheitsrisiko dar. Da der Betrieb solcher Geräte heute aber noch sehr aufwändig ist, sind sie noch nicht weit verbreitet.

Nicht zuletzt werden mit der Entwicklung des **Metaverse** immer mehr Einfallstore für Malware und Datenverletzungen verfügbar sein. Angesichts der Zunahme des digitalen Handels im Metaverse – Schätzungen gehen von einem Wert von über 800 Milliarden US-Dollar bis 2024 aus – werden Angriffe dieser Art in Zukunft immer häufiger und aggressiver.

Die SaaS-Explosion und ihre Auswirkungen

Da Software as a Service in der Regel nicht nur sehr kosteneffizient und superschnell einsatzbereit ist, sondern auch fast unmittelbare Produktivität bei sehr geringen Wartungskosten liefert, führen Unternehmen Hunderte von SaaS-Tools ein. Viele dieser Tools sind der IT-Abteilung möglicherweise nicht bekannt und könnten unbekannte Sicherheitsprobleme und Herausforderungen mit sich bringen. Laut Blissfully gibt es bereits in Unternehmen mit bis zu 100 Mitarbeitenden durchschnittlich 100 SaaS-Apps. Bei Unternehmen mit mehr als 1 ‘000 Mitarbeitenden sind es sogar satte 288 Apps. Ungeschützte Daten, riskante Verknüpfungen und Fehlkonfigurationen gehören zu den typischen Security-Risiken bei der SaaS-Nutzung, um die sich IT-Teams kümmern müssen.

Schwachstellen durch veraltete Systeme und Schatten-IT

Ein beachtliches Risiko stellt der Betrieb von veralteten Systeme und Technologien dar, da diese oft zahlreiche Sicherheitslücken aufweisen, die von den Angreifern ausgenutzt werden. Nicht zu unterschätzen ist zudem die Schatten-IT. Dazu gehören alle Geräte, von denen die IT-Abteilung nicht einmal weiss, dass sie existieren.

Zu viele Sicherheits-Tools im Einsatz

Eine IBM-Studie aus dem Jahr 2020, bei der 3 ´439 IT- und Sicherheitsexperten in 11 Ländern befragt wurden, ergab, dass Unternehmen im Durchschnitt 45 Sicherheitslösungen und -technologien für ihre Netzwerke kaufen und installieren. Wenn Dutzende verschiedener Cyber-Security-Tools im Einsatz sind, ist es jedoch fast unmöglich zu erkennen, was abgedeckt wird und wo es Sicherheitslücken geben könnte. Zu viele Tools reduzieren somit die Sicherheit.

Laut Gartner treten 90 % der Sicherheitsverletzungen auf, weil Angreifer Software ausnutzen, die IT-Mitarbeitende entweder falsch konfiguriert oder nicht gepatcht haben. Da mehr Tools die Komplexität massiv erhöhen, sind Unternehmen mit über 50 Tools gemäss IBM um 8 % schlechter fähig, einen Cyberangriff zu erkennen, und um 7 % schlechter in der Lage, auf einen Angriff zu reagieren.

Relevante Trends und Technologien zur Erhöhung der Cyber-sicherheit

Gut geschulte Mitarbeitende sind der Schlüssel zur Cybersicherheit

Cyberkriminelle professionalisieren sich und bauen ihr Tätigkeitsfeld aus – in demselben Masse müssen auch Unternehmen und öffentliche Verwaltungen ihre IT- und Informationssicherheit ausbauen, um sich zu schützen. Die Attacken in 2021 haben klar gezeigt, wie wichtig es ist, Cybersicherheit als Teil der Unternehmenskultur zu etablieren, da der Faktor Mensch und sein Sicherheitsverhalten die Umsetzung von Sicherheitsvorgaben stark beeinflussen kann.

Eine möglichst flächendeckende Sicherheit sollte deshalb nicht nur die Sicht nach aussen und Massnahmen aufgrund aktueller Bedrohungslagen und Risiken, sondern erfordert auch Vorkehrungen auf Basis einer kritischen Sicht auf die Organisation und deren Mitarbeitende. Von zentraler Bedeutung sind Schulungs- und Trainingseinheiten im Bereich der Anwenderrichtlinien der IT-Sicherheit, der sichere Umgang mit Passwörtern und der ICT-Infrastruktur sowie klare Sicherheitsregeln für die Nutzung, Bearbeitung, Speicherung und den Transfer von Daten.

Einsatz von Zero-Trust Technologien

In der digitalen Wirtschaft muss neben Identitäten und Zugriffen verstärkt auch die Sicherheit der Daten in den Fokus der Überwachung gerückt werden. Daher werden 2022 immer mehr Unternehmen auf Zero-Trust-Technologien wie Content Disarm and Reconstruction (CDR) setzen. CDR, auch bekannt als Threat Extraction, schützt proaktiv vor bekannten und unbekannten Bedrohungen, die in Dokumenten enthalten sind, indem es aktive Inhalte entfernt und eine bereinigte Datei erstellt.

Im Kontext von Identitäten und Zugriffen stellt Zero Trust sicher, dass jedes Gerät und jeder Benutzer, der eine Verbindung mit Unternehmensanwendungen und -systemen herstellen will, überprüft wird. Dabei beschränkt sich Zero Trust nicht auf das Scannen am Eingang, sondern gewährleistet vielmehr, dass Geräte und Benutzer kontinuierlich auf verdächtige Aktivitäten und Verhaltensweisen überprüft werden.

KI-basierte Cybersicherheit

Die enorme Anzahl von Cybersicherheitsbedrohungen ist für Menschen allein nicht mehr zu bewältigen. Daher setzen Unternehmen zunehmend auf KI und maschinelles Lernen, um automatisierte Sicherheitssysteme, natürliche Sprachverarbeitung, Gesichtserkennung und automatische Bedrohungserkennung zu entwickeln. Mit KI lassen sich riesige Mengen von Risikodaten viel schneller analysieren. Dies ist sowohl für grosse Unternehmen mit entsprechenden Datenvolumen ein Vorteil als auch für KMU, deren Sicherheitsteams oftmals nicht über ausreichende Ressourcen verfügen.

Die Unternehmen müssen sich jedoch darüber im Klaren sein, dass im Gegenzug auch Cyberkriminelle diese Technologie nutzen, um ihre Angriffe zu automatisieren und weiter zu perfektionieren. Die meisten Unternehmen, die KI einsetzen, sind sich der Sicherheitsrisiken, die damit verbunden sind, noch nicht ausreichend bewusst. 2022 könnte es zu einer explosionsartigen Zunahme an Fällen kommen, bei denen gerade Künstliche Intelligenz als Einfallstor für Hacker fungiert. Aus diesem Grund müssen Unternehmen bei der Implementierung von KI ein grösseres Sicherheitsbewusstsein entwickeln.

Cybersecurity Mesh

Das Konzept des Cybersecurity Mesh ist ein moderner Ansatz für die Sicherheitsarchitektur, der es dezentral organisierten Unternehmen ermöglicht, Sicherheit dort einzusetzen und zu erweitern, wo sie am dringendsten benötigt wird, um mehr Skalierbarkeit und Flexibilität sowie eine zuverlässige Kontrolle der Cybersecurity zu ermöglichen.

Managed Detection and Response

Sicherheits- und Risikomanagementverantwortliche sind sich zunehmend bewusst, dass eine Verkürzung der Zeit bis zur Erkennung einer Bedrohung bedeutungslos ist, wenn die Zeit bis zur Reaktion auf die Bedrohung und die Ausfallzeit bis zur Wiederherstellung der Daten und Systeme nicht auch entsprechend verkürzt werden. MDR-Dienste füllen diese Lücke und setzen sich dementsprechend immer mehr durch.

MDR-Dienste helfen Unternehmen, interne Hindernisse, wie beispielsweise die hohen Kosten für moderne Sicherheitstechnologien und das Security Operations Management, zu überwinden, indem sie Bedrohungen rund um die Uhr überwachen und identifizieren sowie im Ernstfall unmittelbar reagieren. Hierzu stellen sie den Kunden die Mitarbeitenden, das Fachwissen, die Prozesse und die Technologien eines Security Operation Centers (SOC) zur Verfügung. MDR-Services unterscheiden sich von herkömmlichen remote bereitgestellten SOC-Services, da sie für den Kunden auch Massnahmen zur Abwehr von Bedrohungen einleiten und somit wie eine Erweiterung des Sicherheitsteams des Kunden agieren.

Gartner geht davon aus, dass bis 2025 die Hälfte der Unternehmen MDR-Dienste nutzen werden und schätzt, dass der MDR-Markt bis zu diesem Zeitpunkt einen Umsatz von 2,15 Milliarden US-Dollar erreichen wird, gegenüber 1,03 Milliarden US-Dollar im Jahr 2021. Bereits im vergangenen Jahr gab es laut Gartner einen Zuwachs von 35 Prozent bei den Anfragen von Endanwendern zu diesem Thema.

Wichtig für eine erfolgreiche Zusammenarbeit mit MDR-Anbietern sind klar definierte Ergebnisse und Ziele, die sich auf bestimmte Anwendungsfälle beziehen, sowie eine solide Vorstellung davon, wie der zukünftige stabile Zustand aussehen soll. Der Bezug von MDR-Diensten ist jedoch kein Ersatz für die Bereitstellung der Grundlagen für die Reaktion auf Vorfälle.

Breach and Attack Simulation

Bereits 2017 wurde Breach and Attack Simulation (BAS) von Gartner als neue Kategorie in den „Hype Cycle for Threat-Facing Technologies" aufgenommen. Auch die Expert:innen des Eraneos Cyber Security Teams setzen sich mit diesem Thema intensiv auseinander. Die Technologie hat das Potenzial, innerhalb der nächsten 10 Jahre zum Mainstream zu werden. BAS ermöglicht eine kontinuierliche Prüfung und Validierung von Sicherheitskontrollen und testet die Resilienz des Unternehmens gegenüber externen Bedrohungen. Damit liefern BAS-Lösungen Unternehmen eine Antwort auf die Frage „Funktionieren unsere Cyber-Sicherheitsmassnahmen wirklich?"

Datenverarbeitungstechniken zur Verbesserung der Privatsphäre

Technologien, die Daten während ihrer Nutzung schützen, erschliessen die sichere Datenverarbeitung, gemeinsame Nutzung, gesicherte Übermittlung und Analyse selbst in nicht vertrauenswürdigen Umgebungen. Entsprechende Technologien entwickeln sich zurzeit rasch von der akademischen Forschung zu realen Projekten, die dank neuer Formen der Datenverarbeitung und einem Datenaustausch mit geringerem Risiko von Datenschutzverletzungen echten Mehrwert bieten.

Optimierte Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung (MFA) gilt als Goldstandard. Böswillige Akteure finden jedoch immer neue Wege, diese zu umgehen – insbesondere die Authentifizierung per SMS oder Telefonanruf. SMS bieten zwar eine gewisse Sicherheit, aber die gesendeten Nachrichten sind nicht verschlüsselt. Dies ermöglicht automatisierte „Man-in-the-Middle-Angriffe" auf Passcodes und gefährdet insbesondere Aktivitäten wie das Online-Banking. Entsprechend setzen sowohl Banken wie auch andere Organisationen zunehmend auf anwendungsbasierte MFA-Lösungen wie Google Authenticator, Authy.

Mobile Cybersicherheit

Mobile Cybersicherheit ist ein umfassendes Thema, das auch Elemente wie Back-End-/Cloud-Sicherheit, Netzwerk- und IoT-Sicherheit umfasst. Es gibt keine Gesamtlösungen zum Schutz von Anwendungen in unsicheren Umgebungen – vielmehr geht es darum, zusätzliche Sicherheitsebenen einzubauen, um das Sicherheitsniveau zu erhöhen. Viele Sicherheitsspezialisten kombinieren mobile Sicherheitssoftware hierzu mit hardwarebasierten Sicherheitslösungen, um die Speicherung sensibler Daten zu verstärken.

Konsolidierung der Anwendungslandschaft

Viele Sicherheitsverantwortliche haben zu viele Sicherheits-Tools im Einsatz. Dies führt zu komplexen Sicherheitsabläufen und einem erhöhten Personalbedarf im Sicherheitsbereich. Die meisten Unternehmen sehen in der Konsolidierung von Anbietern einen Weg zu effizienterer Sicherheit. 80 % der Unternehmen verfolgen bereits eine entsprechende Strategie oder sind daran interessiert. Die grossen Sicherheitsanbieter reagieren darauf mit besser integrierten Produkten.

Einheitliche Sicherheitsstandards für die gesamte Lieferkette

Die Digitalisierung von Lieferketten schafft neue Schwachstellen, die von Cyberkriminellen auch in Zukunft gezielt ausgenutzt werden, um aus diesem komplexen Teil der Weltwirtschaft Kapital zu schlagen.

Moderne Lieferketten sind längst komplizierte, miteinander verflochtene Partnernetzwerke. Und wenn ein Partner kompromittiert wird, hat dies Auswirkungen auf alle Partner in der Lieferkette. Die Auswirkungen eines Angriffs auf einen First-Tier-Lieferanten können dabei genauso verheerend sein, wie ein Angriff auf die eigenen Systeme: Ganze Produktionslinien können ausfallen, was erhebliche Kosten verursacht, sich negativ auf den Umsatz auswirkt und den Ruf des Unternehmens schädigt.

Vergangene Vorfälle zeigen, dass besonders die Lieferkette in der Software-Entwicklung noch mehr Awareness für Cyberbedrohungen benötigt. Zudem muss es gemeinsame Standards für sichere Software geben, wie sie beispielsweise von der Charter of Trust, einer globalen Cybersicherheitsallianz, gefordert werden. Hersteller sollten ihre Partner und Zulieferer bezüglich der Einhaltung neuer Vorschriften unterstützen, um sie zu motivieren.

Cyber-affine Verwaltungsräte

Angesichts der zunehmenden Sicherheitsverletzungen und Unterbrechungen des Geschäftsbetriebs durch Ransomware schenken die Verwaltungsräte der Cybersicherheit mehr Aufmerksamkeit. Sie bilden immer häufiger Ausschüsse, die sich mit Fragen der Cybersicherheit befassen und häufig von einem Vorstandsmitglied mit entsprechender Expertise oder einem externen Berater geleitet werden. Dies bedeutet, dass CISOs mit einer verstärkten Kontrolle und höheren Erwartungen rechnen müssen, aber auch mehr Unterstützung und Ressourcen erwarten dürfen.

Datenschutz wird zum „Pflichtfach"

Zahlreiche aufsehenerregende Cyberangriffe haben Millionen von Datensätzen mit personenbezogenen Daten offengelegt. Unternehmen, die sich nicht an die Vorschriften und die Erwartungen der Verbraucher halten, riskieren Geldstrafen, schlechte Publicity und Vertrauensverlust. Infolgedessen fokussieren Unternehmen verstärkt auf die Einstellung von Datenschutzbeauftragten, rollenbasierte Zugangskontrolle, mehrstufige Authentifizierungen, verschlüsselte Datenübertragungen, Netzwerksegmentierungen im Ruhemodus sowie Assessments durch externe Berater*innen.

Die Trendlinien für den Datenschutz, die sich im Jahr 2021 herausgebildet haben, werden sich beschleunigen und neue Risiken und Komplexität für Unternehmen mit sich bringen, da weitere nationale Gesetze verabschiedet werden. Damit gehört der Aufstieg des Datenschutzes zu einer eigenständigen Disziplin 2022 zu einem der wichtigsten Trends im Bereich der Datensicherheit.

Sicherheits-Prioritäten im Schweizer KMU-Umfeld

(Quelle: Multi-Client Studie 2021 von MSM Research)

Sicherheitsprioritäten bis 2024

Mit Blick auf die kommenden 24 Monate wollen die Unternehmen mit höchster Priorität folgende ICT-Sicherheitshemen angehen: Mitarbeitersensibilisierung (Awareness-Training), Sicherheit der Endgeräte (Antivirus, Patch- & Update Management, etc.), Netzwerksicherheit sowie die Überprüfung der ICT auf Schwachstellen (Security Assessments). Als weitere zentrale Themen wurde die Entwicklung und Implementierung eines ICT-Sicherheitskonzepts, die Datensicherheit und die Business Continuity genannt.

Den steigenden Anforderungen an die ICT-Sicherheit wollen 43% mit einem hybriden Modell (interne Sicherstellung mit Unterstützung eines externen Providers) begegnen. 34% wollen diese auch in Zukunft schwerpunktmässig mit eigenem Personal gewährleisten und 23% haben diesbezüglich noch kein klares Konzept.

Im Falle der Zusammenarbeit mit einem externen Security-Dienstleister ist es für 54% der Unternehmen wichtig, dass sie alle für sie relevanten Security Leistungen aus einer Hand beziehen können. 29% wünschen sich sogar einen Anbieter, der auch alle weiteren ICT-Belange mit seinem Portfolio abdecken kann.

Prioritäten auf der Projektebene

Bei den IT-Projekten hat mit 65% ganz klar die Gewährleistung der ICT-Sicherheit oberste Priorität, gefolgt von Infrastrukturthemen und der Business Continuity, während bei den Fachabteilungen Projekte für einen verbesserten Datenschutz (45%) sowie die sichere Abwicklung von digitalen Geschäftsprozessen im Vordergrund stehen.

Technische Massnahmen

Zu den wichtigsten technischen Massnahmen, um Risiken zu minimieren, zählen bei den befragten Unternehmen die laufende Aktualisierung von Betriebssystemen und Anwendungen sowie entsprechender Antivirus-Programme auf allen Endgeräten. Zusätzlich gaben die Befragten an, dass allen Mitarbeitenden persönliche Logins für alle Systeme (z. B. ERP, Unternehmenssoftware, Webanwendungen) zugeteilt werden.

Mitarbeiterorientierte Massnahmen

Eine möglichst flächendeckende Sicherheit beinhaltet aber nicht nur die Sicht nach aussen und Massnahmen aufgrund aktueller Bedrohungslagen und Risiken, sondern erfordert auch Vorkehrungen auf Basis einer kritischen Sicht auf die Organisation und deren Mitarbeitende.

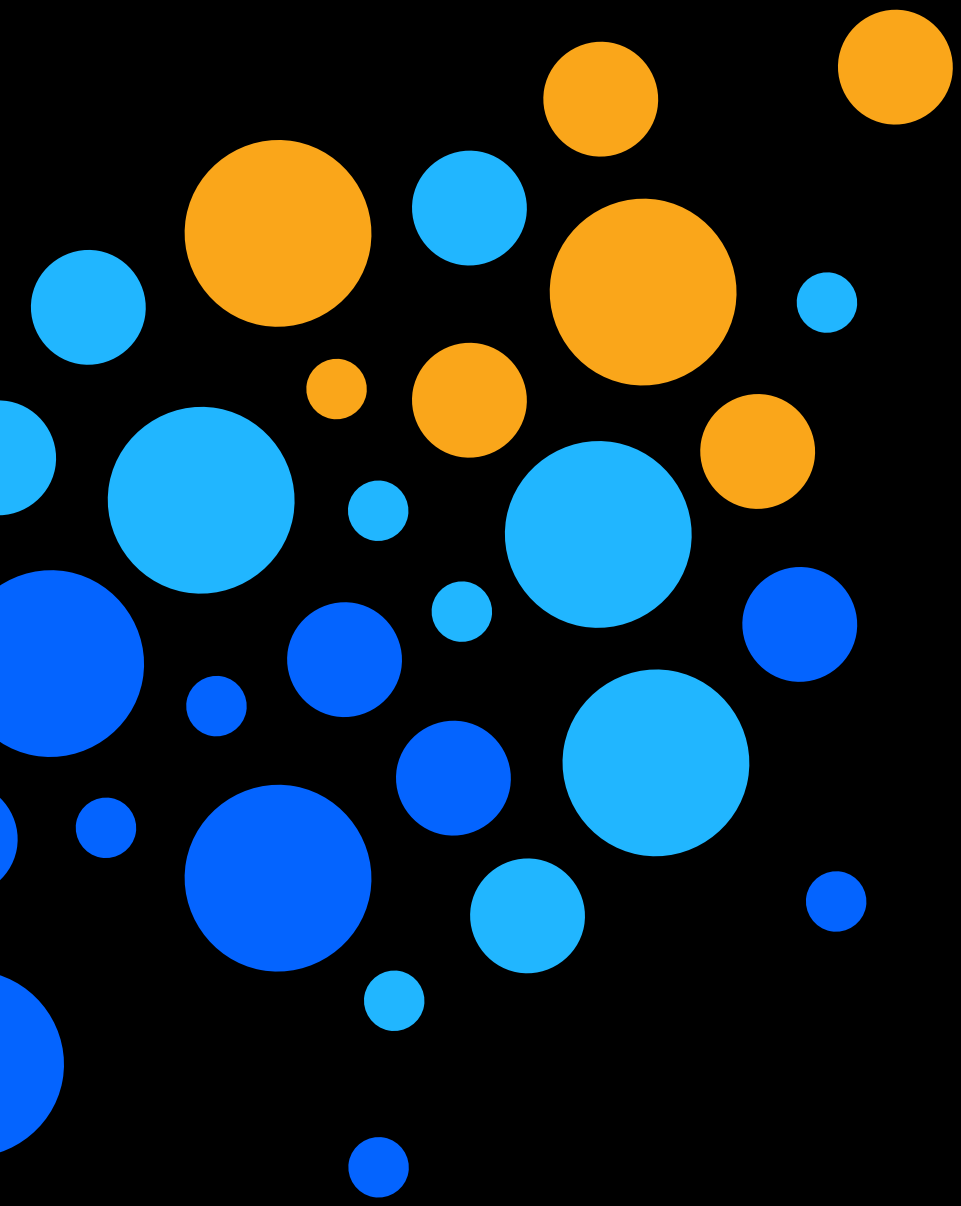
Von zentraler Bedeutung für die befragten Unternehmen sind insbesondere Awareness-Trainings und Schulungen im Bereich der Anwenderrichtlinien der IT-Sicherheit, der sichere Umgang mit Passwörtern und der ICT-Infrastruktur sowie klare Sicherheitsregeln für die Nutzung, Bearbeitung, Speicherung und den Transfer von Daten. Entsprechende Schulungen werden sporadisch oder auch nur einmalig durchgeführt. Dabei führen die Unternehmen ihre Schulungen zu gleichen Teilen intern und mit einem extern beauftragten Trainer durch. Externe Kurse sind weniger gefragt.

Globale Harmonisierung: Gemeinsam für mehr Cybersicherheit

Durch die rasch fortschreitende Abhängigkeit von digitalen Technologien und der Entwicklung des Internet 3.0, werden die Bemühungen um die Festlegung von Verhaltensregeln für alle Beteiligten im Cyberspace immer intensiver. **Internationale Multi-Stakeholder-Dialoge** können dazu beitragen, die Verbindungen zwischen den Akteuren zu stärken, die im Bereich der digitalen Sicherheit tätig sind, und die Zusammenarbeit zwischen Organisationen könnte **Best Practices** erschliessen, die branchen- und wirtschaftsübergreifend repliziert werden können.

Standards sind das Rückgrat einer wirkungsvollen Cybersicherheit

Dieses Motto muss international gelebt werden und erfordert eine grenzüberschreitende Zusammenarbeit. Der Gesetzgeber und die Wirtschaft müssen reagieren. Im Rahmen von **Public-Private-Partnerships** muss gemeinsam an harmonisierten Mindestanforderungen gearbeitet werden, die über Branchen und Technologien hinweg dafür sorgen, dass digitale Produkte und Services „ab Werk" cybersicher sind. Denn nur durch einheitliche und allgemeingültige Standards für Cybersicherheit wird es möglich sein, das Sicherheitsniveau nachhaltig zu stärken.



eraneos

Experienced in a wide range of industries

Eraneos Group ist eine internationale Management- & Technologieberatungsgruppe, die Dienstleistungen von Strategie bis Implementierung anbietet. Sie ist aus dem 2021 angekündigten Zusammenschluss von Ginkgo Management Consulting, Quint Group und AWK Group hervorgegangen. Die Gruppe betreut Kun-den auf drei Kontinenten, wo rund 1.000 engagierte und hochqualifizierte Fachleute gemeinsam daran ar-beiten, das volle Potenzial der Digitalisierung auszuschöpfen. Die Dienstleistungen reichen von der Entwick-lung digitaler Geschäftsmodelle und Datenanalysen bis hin zu Cybersicherheit, von Sourcing und IT-Beratung zum Management komplexer Transformationsprojekte. Eraneos Group hat Niederlassungen in der Schweiz, Deutschland, Luxemburg, Spanien, den Niederlanden, China, Singapur und den USA. 2021 er-zielte die Gruppe einen Umsatz von fast 200 Millionen Euro.

Contact us >

Our offices >

Visit our website >