Vernetzte Unternehmen und ihre Cyberrisiken

QBE

Überblick

Menschen und Organisationen auf der ganzen Welt verlassen sich zunehmend auf digitale Technologien. Computer und AI-Tools (Artificial Intelligence) ermöglichen und automatisieren sowohl einfache als auch komplexe Geschäftsabläufe, indem intelligente Geräte Industrieanlagen, Fahrzeuge und andere Geräte mit dem Internet verbinden.

Die globalen Technologiemärkte werden in den kommenden fünf Jahren exponentiell wachsen. Der Markt für AI-as-a-Service (AIaaS) wird um das Neunfache von ca. 200 Mrd. USD auf 1,85 Trill. USD wachsen, der Markt für Software-as-a-Service (SaaS) um das Dreifache auf 850 Mrd. USD und der Markt für Infrastructure-as-a-Service (IaaS) um das Fünffache auf 532 Mrd. USD. Das Ausmaß verdeutlicht die Chancen, die sich durch die neuen digitalen Technologien eröffnen.

Allerdings haben Cyberkriminelle bereits sensible Daten gestohlen, um Unternehmen aller Größen und Branchen zu erpressen und zu betrügen. Gleichzeitig nutzen gefährliche Akteure die Technologie, um ihre Gegner zu destabilisieren und ihre ideologischen Narrative zu verbreiten.

Globale technologische Disruption

Der Massenausfall von Systemen am 19. Juli, auf denen Falcon Sensor von CrowdStrike lief, hat die wechselseitigen Abhängigkeiten und die Anfälligkeit globaler Technologiesysteme deutlich vor Augen geführt. Der Ausfall hat die Fortune-500-Unternehmen schätzungsweise 5,4 Mrd. USD an Schaden und 25 Mrd. USD an Aktienwert gekostet – Microsoft nicht mitgerechnet.

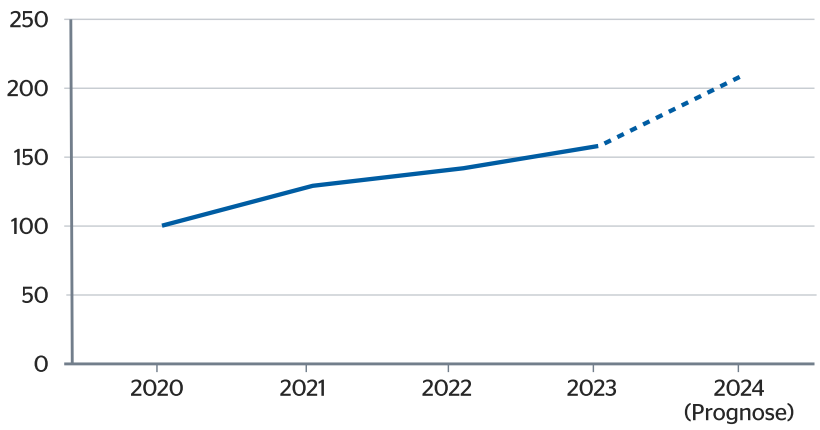
Das fehlerhafte Content-Update von CrowdStrike legte rund 8,5 Mio. Windows-Computer lahm, das sind weniger als 1 % aller Windows-Geräte. Verschiedene Branchen auf der ganzen Welt waren beeinträchtigt, am stärksten Luftfahrt, Transport und Gesundheitswesen. Cyberkriminelle nutzten die Gelegenheit und starteten Phishing-Kampagnen mit CrowdStrike-bezogenen Ködern, um Systeme zu kompromittieren, Daten zu stehlen und Opfer zu erpressen. Bei diesem CrowdStrike-Vorfall handelte es sich eher um einen Fehler als um eine absichtliche Störung – bei vielen Cybervorfällen handelt es sich jedoch um gezielte Angriffe.

Im Juni 2017 griff die Massen-Cyber-Attacke NotPetya ukrainische Organisationen an, was letztlich zur Infektion in ganz Europa, Nordamerika und im asiatisch-pazifischen Raum führte. Die NotPetya-Malware als Ransomware getarnt traf kritische Sektoren wie Transport, Logistik sowie Schifffahrt und verursachte einen geschätzten Schaden von rund 10 Mrd. USD. Obwohl weit weniger Geräte betroffen waren als beim CrowdStrike-Zwischenfall, führte dieser vorsätzliche Angriff zu einem höheren Maß an Störung.

Da die technologischen Interdependenzen zunehmen, erwarten wir mehr Cybervorfälle, die mit einem einzigen Angriff bei vielen Unternehmen Störungen verursachen. Daraus folgt, dass für Unternehmen die Wahrscheinlichkeit steigt, von einem Cyber-Vorfall betroffen zu sein. Böswillige Akteure können zudem bestimmte Unternehmen ins Visier nehmen, um größeren Schaden anzurichten, sei es, um Lösegeld zu erpressen oder geopolitische Rivalen zu destabilisieren.

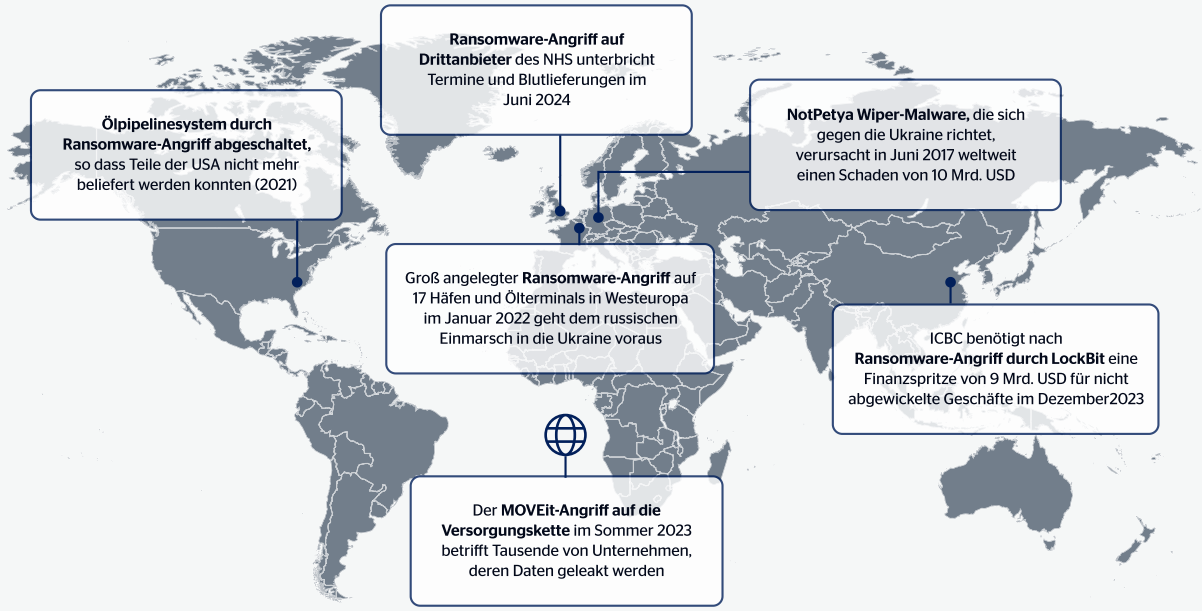
> Der CrowdStrike-Vorfall kostete den Fortune-500-Unternehmen geschätzt 5,4 Mrd. USD und 25 Mrd. USD im Aktienwert.

Anzahl der registrierten destruktiven und störenden Cyberangriffe seit 2020



Quelle: Control Risks

Bedeutende Cyberbedrohungen seit 2017



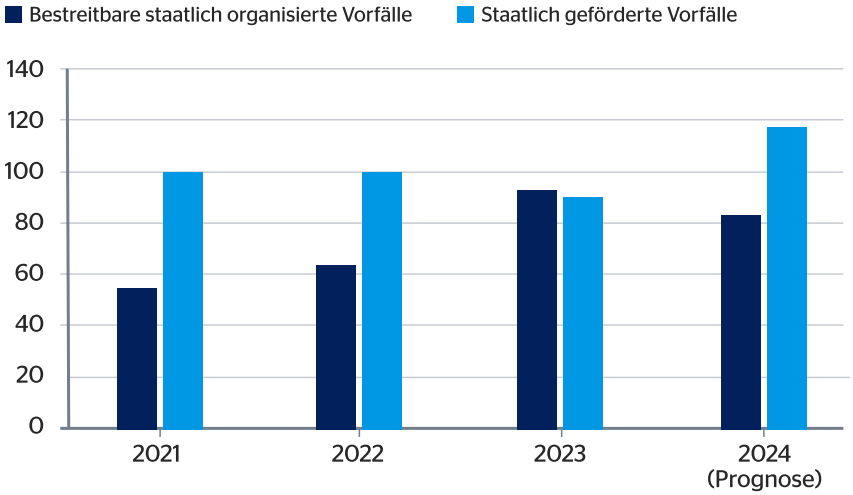
Unternehmen im Energiesektor sind attraktive Ziele für Spillover-Angriffe, die Finanzmärkte und Regierungen destabilisieren können.

Spillover-Angriffe

Der zunehmende geopolitische Wettbewerb führt dazu, dass die Welt immer multipolarer wird. Staatlich gesteuerte Cyber-Akteure versuchen verstärkt, kritische nationale Infrastrukturen (Critical National Infrastructure, CNI) zu sabotieren, zum Beispiel durch den Einsatz von Ransomware. Solche Angriffe können durch geopolitische Ereignisse wie die Konflikte zwischen Israel und der Hamas oder zwischen der Ukraine und Russland ausgelöst werden. Diese Angriffe manifestieren sich häufig als staatlich unterstützte Cyberkriminalität oder aktivistische Attacken auf strategische Sektoren außerhalb der Konfliktzonen. Unternehmen im Energiesektor sind besonderst attraktive Ziele für solche Spillover-Cyberangriffe, die potenziell die Finanzmärkte und Regierungen destabilisieren können.

Einige Staaten unterstützen Cyber-Aktivisten, die störende und zerstörerische Angriffe ausführen, um sich selbst vor Anschuldigungen oder diplomatischen Strafen zu schützen und ihre Glaubwürdigkeit zu wahren. CNI-Organisationen sind besonders anfällig für solche Spillover-Bedrohungen, da Angreifer glauben, sie stören zu können, ohne eine militärische Reaktion zu provozieren. Zudem breiten sich Spionageeinheiten aus, die sich als finanziell motivierte Ransomware-Gruppen tarnen, was die Bedrohung für sensibles geistiges Eigentum und Unternehmensdaten durch staatlich gesteuerte Aktuere weiter verstärkt.

Anzahl signifikanter nichtstaatlicher Stellvertreterangriffe und erfasster staatlich gelenkter Kampagnen seit 2021



Quelle: Control Risks

Von Russland gesteuerte Ransomware-Angriffe auf 17 europäische Erdölterminals vor dem Einmarsch in die Ukraine

Im Januar 2022 zielte eine Serie von Ransomware-Angriffen auf Hafenterminals in Belgien, Deutschland und den Niederlanden ab. Diese Angriffe, die vermutlich von russischen Akteuren ausgingen, legten IT-Systeme lahm und beeinträchtigten die Abfertigung von Ölprodukten in den Häfen erheblich. Die Angriffe fanden drei Wochen vor dem Einmarsch Russlands in die Ukraine statt und verdeutlichen, wie solche Spillover-Attacken auf sekundäre Sektoren und Regionen abzielen können.

> Im Jahr 2023 stieg die Zahl der Ransomware-Angriffe um 74 %.

Triebkräfte für die Zunahme von Cyberangriffen

Geopolitik

Spannungen zwischen den USA und China, wachsende Multipolarität und anhaltende Konflikte führen weltweit zu Störungen, die beabsichtigte und unbeabsichtigte Opfer treffen.

Ransomware

Cybercrime-Banden sind aktiver und gefährlicher als je zuvor, mit einem höheren Volumen an Angriffen, enormen Einnahmen und höheren Lösegeldforderungen.

Bedrohungen im Zusammenhang mit Drittanbietern

Infrastruktur-Anbieter, Software-Services, Daten-Hosts und Technologien sind die wichtigsten Cyber-Fronten und zunehmend die bevorzugten Ziele.

Technologie

KI-Fortschritte führen schnell zu neuen Risiken, während die zunehmende Konnektivität und Vernetzung die Angriffsfläche immer weiter vergrößert.

Control Risks

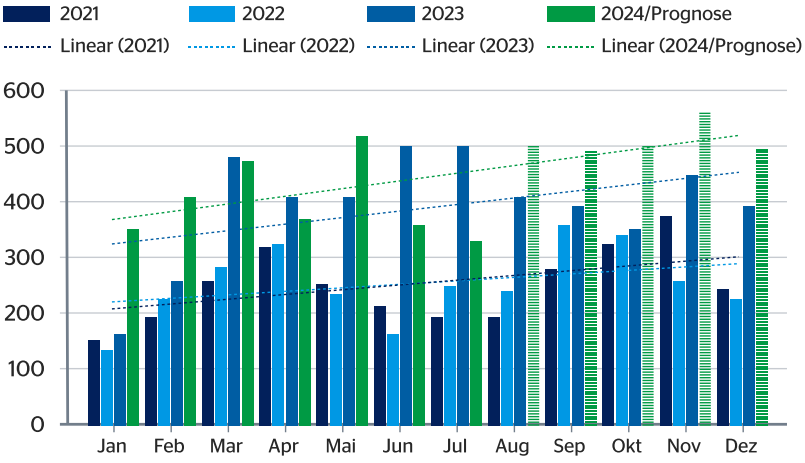
Ransomware

Steigende Einnahmen bei zunehmender Anzahl von Angriffen

Im Jahr 2023 stieg die Zahl der Ransomware-Angriffe im Vergleich zu 2022 um 74 %, und die von den Opfern gezahlten Lösegelder überstiegen weltweit 1 Mrd. USD. Nach der Zerschlagung der Hive-Gruppe durch Strafverfolgungsbehörden im Jahr 2022 zerfiel das kriminelle Ökosystem, wodurch Ransomware-Code öffentlich zugänglich wurde. Dies ermöglichte es weniger erfahrenen Gruppen eigene Angriffe durchzuführen.

Dieses Wiederaufleben der Ransomware setzte sich 2024 fort, wobei die Zahl der öffentlich bekannten Opfer die höchsten monatlichen Werte der letzten drei Jahre erreichte *(*Anmerkung: Die Grafik unten schließt MOVEit ein, einen Vorfall aus dem Jahr 2023 mit einer hohen Zahl von Opfern. Real betrachtet sind die Zahlen für 2024 deutlich höher als 2023, wenn man den MOVEit-Vorfall als Anomalie außer Acht lässt).*

Anzahl der Ransomware-Opfer, die auf Datenleckseiten genannt wurden



Quelle: Control Risks

Anzahl der von Ransomware- und Datenleck-Erpressergruppen öffentlich benannten Opfer

2021	2022	2023	2024 (Prognose)	2025 (Prognose)
2.964	2.981	4.698	4.800	5.200

Quelle: Control Risks

Sektoranalyse

Im Jahr 2023 richteten sich Ransomware-Angriffe hauptsächlich gegen die Sektoren Produktion, Gesundheitswesen, IT, Bildung und Regierung. Da die Widerstandsfähigkeit von Branche zu Branche variiert, nehmen Angreifer zunehmend alle Branchen ins Visier. Sie konzentrieren sich jedoch besonders auf die Fertigungsindustrie und das Gesundheitswesen, da Störungen in diesen Bereichen schwerwiegende Auswirkungen haben können.

> Die Ransomware-Angriffe auf Gesundheits-organisationen stiegen von 214 im Jahr 2022 auf 389 im Jahr 2023, ein Plus von 81,7%.

Ransomware stellt eine erhebliche Bedrohung für Fertigungs- und Produktions-unternehmen dar. Im Jahr 2023 meldeten 65 % der Unternehmen in diesem Sektor einen Ransomware-Angriff, wobei durchschnittlich 2,4 Mio. USD Lösegeld gezahlt wurden. Von den betroffenen Unternehmen zahlten 62 % das Lösegeld, um gestohlene Daten zurückzuerhalten.

Zur Berechnung der durchschnittlichen Lösegeldforderung fehlen ausreichende Informationen, da diese stark je nach Region, Sektor und Unternehmen variieren können. Es ist jedoch sehr wahrscheinlich, dass große Unternehmen, die besonders anfällig für Betriebsunterbrechungen sind, mit Lösegeldforderungen in Höhe von mehreren zehn Millionen USD konfrontiert werden, während kleinere Unternehmen Forderungen im Bereich von Hunderttausenden erwarten müssen. Organisationen, die den höchsten Lösegeldforderungen ausgesetzt sind, befinden sich wahrscheinlich in den Bereichen Gesundheit, Regierung, IT und Kommunikation sowie in der verarbeitenden Industrie.

Organisationen im Gesundheitswesen sind besonders attraktive Ziele für Cyberangriffe, da sie umfangreiche Mengen an personenbezogenen Daten (Personally Identifiable Information, PII) und geschützten Gesundheitsinformationen (Protected Health Information, PHI) besitzen und für die die Verfügbarkeit ihrer Systeme von entscheidender Bedeutung ist. Ein weiterer Grund für diese Angriffe ist die Annahme, dass die Cybersicherheit im Gesundheitswesen im Vergleich zu anderen Sektoren weniger ausgereift ist. Die Zahl der Gesundheitsorganisationen, die von Ransomware-Angriffen betroffen waren, stieg von 214 im Jahr 2022 auf 389 im Jahr 2023, was einem Anstieg von 81,7 % entspricht.

Big Game Hunting

Ransomware-Gruppen wenden zunehmend die Taktik des sogenannten „Big Game Hunting" an, also der 'Großwildjagd', indem sie umsatzstarke und bekannte Unternehmen als Ziele für ihre Erpressungsangriffe auswählen. Big Game Hunting ermöglicht es Ransomware-Gruppen, die durchschnittlichen Lösegeldzahlungen zu erhöhen, indem sie höhere Anfangsforderungen stellen, die sich kleine und mittlere Unternehmen nicht leisten können. Zudem nutzen sie die potenziellen Betriebsstörungen bei einer großen Anzahl von Klienten und/oder Kunden der Opfer aus.

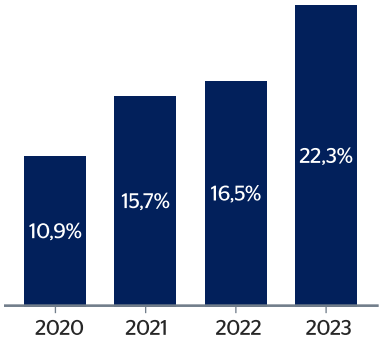
In den letzten Jahren erzielten Strafverfolgungsbehörden bedeutende Erfolge bei der Zerschlagung von Ransomware-Gruppen, wie die vollständige Zerschlagung der Ransomware Hive und die teilweise Zerschlagung leistungsstarker Gruppen wie LockBit und BlackCat. Daher haben Ransomware-Gruppen versucht, ihre Lösegeldforderungen durch Big Game Hunting zu maximieren, bevor die Strafverfolgungsbehörden sie einholen und ihre Vermögenswerte und Infrastruktur beschlagnahmen. Im Jahr 2023 stieg die durchschnittliche Lösegeldzahlung auf 2 Mio. USD, während sie im Vorjahr bei 400.000 USD lag. Diese Erhöhung ist vor allem auf Big Game Hunting zurückzuführen, bei dem einige Angreifer mehr als 50 Millionen USD gefordert haben. Trotz dieser hohen Forderungen bleibt die durchschnittliche Lösegeldforderung stabil bei etwa 300.000 USD.

Bedrohungsakteure gehen davon aus, dass große Organisationen eher bereit sind, Lösegeld zu zahlen. Im Durchschnitt leisten 61 % der Unternehmen mit einem Jahresumsatz von 5 Mrd. USD nach einem Angriff Lösegeldzahlung, verglichen mit nur 25 % der Unternehmen mit einem Jahresumsatz von weniger als 10 Mio. USD. Einige umsatzstarke Unternehmen betrachten Betriebsunterbrechungen als kostspieliger als die Zahlung des geforderten Lösegelds.

LockBit-Angriff auf ICBC verdeutlicht opportunistische Ransomware-Bedrohung für den Finanzsektor

Im November 2023 griff die Ransomware-Gruppe LockBit den in den USA ansässigen Finanzdienstleistungszweig der Industrial and Commercial Bank of China (ICBC) an und störte den Handel mit US-Treasuries. Dies führte zur erzwungenen Umleitung von Finanztransaktionen und hinderte die ICBC Financial Services daran, Treasury-Geschäfte für andere Marktteilnehmer abzuwickeln, was dazu führte, dass die ICBC ihrer US-Einheit 9 Mrd. USD zuführen musste. Die Angreifer drangen wahrscheinlich über eine ungepatchte Citrix NetScaler-Box in das Netzwerk der ICBC ein und konnten so die Authentifizierungsmaßnahmen umgehen.

Anteil der globalen Cyber-Vorfälle, die IT-Drittanbieter betreffen (2020-23)



Quelle: Control Risks

Gefährdung von Lieferketten

Vorfälle bei Drittparteien

Mindestens 22 % aller Cyber-Sicherheitsverletzungen im Jahr 2023 waren wahrscheinlich auf Vorfälle bei Drittparteien zurückzuführen. Um das Risiko solcher Vorfälle effektiv zu minimieren, müssen Unternehmen intern bewährte Praktiken anwenden, um ihre Widerstandsfähigkeit gegenüber Angriffen, die durch externe Vorfälle verursacht werden, zu stärken. Gleichzeitig sollten sie die Risikolage, Strategien zur Risikominderung und die Versicherungsbedingungen ihrer externen IT-Anbieter sorgfältig prüfen.

Sektoren

IT-Anbieter, wie Software-as-a-Service-Organisationen (SaaS), sind für Cyberkriminelle und staatlich gesteuerte Bedrohungsakteure ein Hauptziel. Im Jahr 2023 wurden 75 % der Vorfälle im Zusammenhang mit Drittanbietern durch Angriffe auf Service- und Softwareanbieter verursacht.

Anteil der gemeldeten Sicherheitsverletzungen bei Dritten im Jahr 2023, nach Sektor

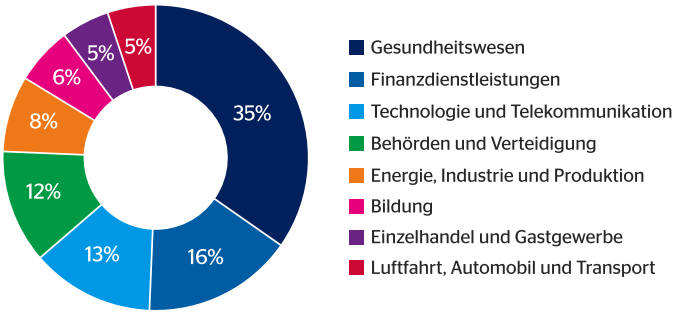


Diagram: Control Risks • Quelle: Security Scorecard

Über 75 % der Vorfälle mit Drittanbietern in 2023 sind auf drei Lieferketten-Schwachstellen zurückzuführen.

Zero-Day-Angriffe können für Ransomware-Gruppen die größte Wirkung haben

Ransomware-Gruppen betrachten IT-Lieferketten als attraktive Ziele, da sie die Möglichkeit bieten, mit einem einzigen Angriff zahlreiche Organisationen in verschiedenen Sektoren zu treffen. Solche Organisationen haben hohe Anforderungen an die Betriebszeit, was bei Lösegeldverhandlungen ausgenutzt werden kann. Im Jahr 2023 wurden 64 % der Sicherheitsverletzungen im Zusammenhang mit Drittparteien der Ransomware-Gruppe Clop in Verbindung gebracht, die einen Zero-Day-Bug (eine unbekannte und ungepatchte Sicherheitslücke in einem System oder Gerät) ausnutzte. 61 % dieser Sicherheitsverletzungen wurden auf die MOVEit-Schwachstelle zurückgeführt, was die direkten Auswirkungen von Risiken bei Drittanbietern auf Kunden in der Lieferkette verdeutlicht. Die nachstehende Grafik zeigt, dass über 75 % der Zwischenfälle im Zusammenhang mit Drittanbietern im Jahr 2023 auf nur drei Schwachstellen in der Lieferkette zurückzuführen sind.

Anteil der Vorfälle bei Dritten im Jahr 2023, nach Schwachstellen

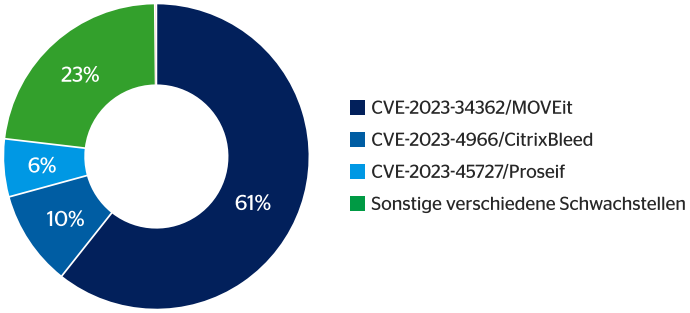
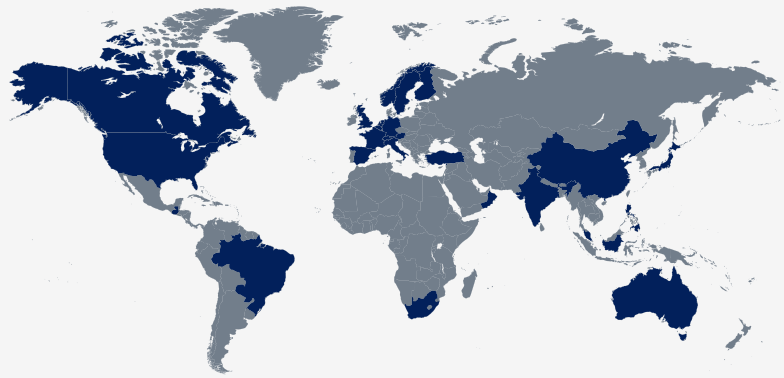


Diagram: Control Risks • Quelle: Security Scorecard

Die MOVEit-Kampagne zeigt, dass Angriffe auf Daten von IT-Anbietern weitreichende Auswirkungen haben können

Im Mai 2023 nutzte die Cyberkriminellen-Gruppe Clop eine Zero-Day-Schwachstelle im Datenübertragungsdienst MOVEit aus und stahl Daten von Unternehmen, die sich der Sicherheitslücke nicht bewusst waren. Diese Welle von Datendiebstählen und Erpressungen betraf mindestens 2.180 Organisationen. Clop hat vermutlich über 100 Millionen USD an Lösegeldzahlungen erhalten.

Geografische Verteilung der MOVEit-Opfer



Technologie

Cloud-Bedrohungen

Seit der Einführung von Cloud-Diensten in Unternehmen haben Bedrohungsakteure Tools und Taktiken entwickelt, die ihnen einen leichteren und längeren Zugang zu Cloud-basierten Anwendungen ermöglichen, um infizierte Netzwerke zu erkunden und weitere Schwachstellen zu identifizieren. Die Navigation durch Cloud-basierte Setups erlaubt es ihnen zudem, typische Erkennungsprotokolle wie die erweiterte IP-Analyse zu umgehen. Staatlich gesteuerte Akteure und raffinierte Cyberkriminelle nutzen ebenfalls die Cloud und exfiltrieren Daten in ihre eigenen Cloud-Speicher.

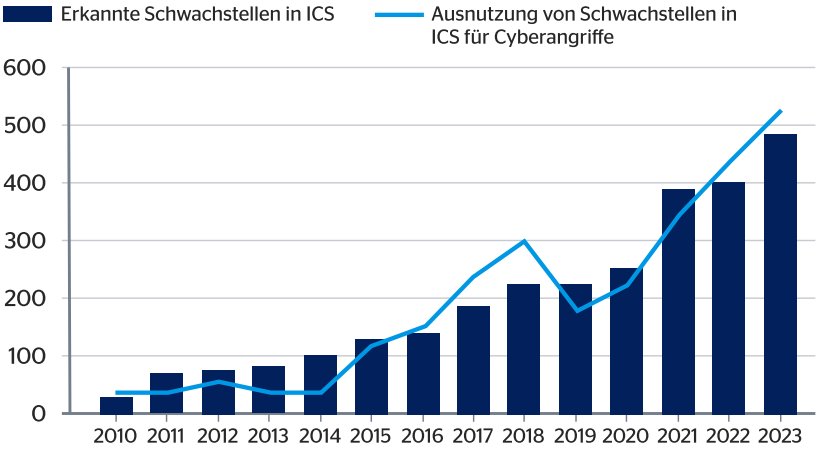
Nutzung von Betriebstechnologie und IoT

Ransomware-Angriffe auf Unternehmen im Industriesektor nahmen 2023 im Vergleich zu 2022 um 50 % zu. Erfolgreiche Angriffe, die die Betriebstechnologie (Operational Technology, OT) – also die Soft- und Hardware zur Überwachung und Steuerung von Industrieanlagen – stören, ermöglichen es Cyberkriminellen, Lösegeldzahlungen zu erpressen, da Betriebsunterbrechungen finanziell schwerwiegender sind als das geforderte Lösegeld. OT-Störungen können auch strategische Ziele staatlich gelenkter Akteure unterstützen. Die Unterbrechung von Produktionsprozessen kann sowohl lukrativ als auch strategisch wertvoll sein.

Maschinenbau, Fertigungs- und Versorgungsunternehmen sind attraktive Ziele für Angriffe auf OT-Umgebungen. Bedrohungsakteure mit unterschiedlichen Fähigkeiten zielen zunehmend auf OT ab, die über das Internet zugängliche Steuerungen oder Geräte verwendet. Die starke Zunahme von Internet-of-Things-Geräten (IoT) – Hardware, die drahtlos mit Netzwerken verbunden ist – hat diese OT-Bedrohungen wahrscheinlich noch verschärft, insbesondere in den Bereichen Fertigung und Energieversorgung. Eine effektive Netzwerksegmentierung sowie die Begrenzung oder vollständige Entfernung von Ports, die dem Internet ausgesetzt sind, können das Risiko von Störangriffen auf OT erheblich verringern.

> Ransomware-Angriffe auf Industrieunternehmen stiegen 2023 um 50 % gegenüber 2022.

Anzahl der Schwachstellen in ICS (Industrielle Steuerungs- und Automatisierungssysteme) im Vergleich zu Vorfällen, die ICS-Schwachstellen ausnutzen, 2010-2023



Quelle: Control Risks

Organisationen werden zunehmend generative KI und Automatisierung zur Erkennung von Cyberangriffen einsetzen.

Aktivisten nehmen Betriebstechnik ins Visier und unterbrechen die Wasserversorgung

Im Dezember 2023 griff die mit dem Iran verbundene Aktivistengruppe Cyber Av3ngers ein privates Wasserversorgungssystem in Erris, Irland, an. Die Angriffe erfolgten über speicherprogrammierbare Steuerungen (SPS) des israelischen Unternehmens Unitronics und führten zu einem zweitägigen Ausfall der Wasserversorgung für die Anwohner. Cyber Av3ngers erklärte, dass die Angriffe auf SPSen ein Teil ihrer Kampagne gegen israelische Produkte und Organisationen im Kontext des Konflikts zwischen Israel und der Hamas seien.

KI

Derzeit entwickelt sich die KI von rein vorprogrammierten Tools für spezifische Aufgaben, die menschliche Eingaben erfordern, hin zu einer KI mit begrenztem Speicher oder einer sogenannten engen KI, die Massendaten nutzen kann, um Entscheidungen zu treffen. Generative Open-Source-KI-Tools können beispielsweise Code für Malware schreiben oder viele der traditionellen Taktiken verbessern, die von staatlich gesteuerten Bedrohungsakteuren und Cyberkriminellen eingesetzt werden, wie Spear-Phishing und Malware-Angriffe.

Mit der zunehmenden Verfügbarkeit von KI und der Verbreitung großer Sprachmodelle (Large Language Models, LLMs) werden auch weniger erfahrene Bedrohungsakteure, wie Cyberkriminelle und Cyberaktivisten, in der Lage sein, schneller umfangreichere Angriffe durchzuführen. Diese gesteigerten Fähigkeiten in Bezug auf Umfang und Geschwindigkeit wird die Cyber-Bedrohungslandschaft erheblich beeinflussen.

Kriminelle nutzen zunehmend generative KI-Tools, um täuschend echte Fälschungen von vertrauenswürdigen Mitarbeitern und Führungskräften zu erstellen. Diese Deepfakes werden eingesetzt, um Unternehmen aller Größen zu betrügen. Ein bemerkenswerter Fall ereignete sich Anfang des Jahres, als ein international tätiges Unternehmen durch einen Deepfake-Angriff 20 Millionen USD verlor. Obwohl solche Methoden seit 2019 bekannt sind, steigt ihre Häufigkeit und Erfolgsquote erheblich an; mit der fortschreitenden Verbesserung der Technologie wird immer weniger Fachwissen benötigt, um solche Angriffe durchzuführen.

Gleichzeitig spielt KI eine wichtige Rolle bei der Erkennung von bösartigem Verhalten in Unternehmensnetzwerken. Wir erwarten, dass sie die Cybersicherheitsfähigkeiten insgesamt weiter verbessert, indem sie die Effizienz von Sicherheits- und Verteidigungsmaßnahmen steigert. Organisationen werden vermehrt generative KI- und Automatisierungstechniken nutzen, um Cyberangriffe in einer innovativen, dynamischen und sich ständig wandelnden Bedrohungslandschaft zu identifizieren.

Diversifizierung von Technologien

Die Cloud und neue Technologien haben Unternehmen kostengünstige Infrastrukturlösungen ermöglicht. Allerdings hat die zunehmende Verbreitung von Infrastructure-as-a-Service und AI-as-a-Service die Angriffsfläche für Bedrohungsakteure erweitert und bietet ihnen mehr Möglichkeiten, bei einem einzigen Angriff mehrere Opfer zu infizieren.

Die zunehmende Verbreitung von IoT-Geräten hat dazu geführt, dass Cyberangriffe immer häufiger wichtige öffentliche Dienste wie zum Beispiel die Wasserversorgung beeinträchtigen. Fortschritte in der generativen KI ermöglichen es Cyberkriminellen, täuschend echte Deepfakes von Führungskräften zu erstellen, um Social Engineering-Angriffe zu erleichtern. Staatlich gesteuerte Bedrohungsakteure und Cyber-Aktivisten nutzen kriminelle Lösungen, um Wahlen zu beeinflussen oder Kampagnen zu unterstützen. Immer mehr Bedrohungsakteure entwickeln ihre eigenen Tools und setzen KI ein, um die Angriffsvorbereitung zu automatisieren und Malware zu verbreiten. Die Einführung neuer Technologien, die je nach Branche und Region unterschiedlich schnell und umfassend erfolgt, vergrößert die Angriffsfläche. Gleichzeitig bemühen sich Unternehmen, ihre Reaktionsfähigkeit aufrechtzuerhalten.

Fazit

Gegenseitige technologische Abhängigkeiten, die durch fortschreitende Vernetzungen, KI und neue Technologien entstehen, bieten Cyber-Akteuren zahlreiche Möglichkeiten, Unternehmen anzugreifen. Instabile globale Konflikte, geopolitische Verschiebungen und eine florierende Cyberkriminalität werden voraussichtlich die Risiken für Unternehmen erhöhen, die neue Technologien in ihre Arbeitsabläufe integrieren.

Die Verflechtungen zwischen verschiedenen Branchen und Unternehmen werden solche Risiken unvermeidlich machen, da Bedrohungsakteure zunehmend ausgefeilte Malware entwickeln, um OT-Umgebungen oder Drittanbieter von Diensten und Software zu schädigen. Gleichzeitig werden sich KI und andere Technologien weiterentwickeln und dazu beitragen, eine Reihe von Bedrohungen zu verringern, die darauf abzielen, technologische Abhängigkeiten auszunutzen.

Eine zukunftssichere Strategie für die digitale Transformation kann der Schlüssel zum Erfolg sein. Strategien zur Risikominderung müssen die zunehmende Wahrscheinlichkeit von Cybervorfällen berücksichtigen und proaktiv auf Widerstandsfähigkeit abzielen. Gleichzeitig sollten Reaktionsprotokolle implementiert werden, um schnell und effektiv auf Cyberangriffe reagieren zu können.

Anhang – Referenzen

„Global ransomware threat expected to rise with AI, NCSC warns", ncsc.gov.uk
„2023 Ransomware Attack Report", blackfog.com
„Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline", chanalysis.comv
„#StopRansomware: CLOP Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability", cisa.gov
„Two-day water outage in remote Irish region caused by pro-Iran hackers", therecord.media
„NCC Group Releases Annual Cyber Threat Monitor Report 2023", nccgroup.com
„Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double", dni.gov
„The State of Ransomware 2024", sophos.com
„The State of Ransomware in Manufacturing and Production 2024", sophos.com
„Helping our customers through the CrowdStrike outage", blog.microsoft.com
„Dragos 2023 OT Cybersecurity Year in Review", dragos.com
„Global Third-Party Cybersecurity Breach Report", securityscorecard.com

Am 9. Oktober 2024 wurde eine Korrektur veröffentlicht, um einen Fehler in der sektoralen Analyse auf Seite 7 zu beheben. Im Jahr 2023 waren weltweit insgesamt 389 Gesundheitsorganisationen von Ransomware-Angriffen betroffen (Control Risks, 2024).

QBE Cyber-Versicherung

Das Cyber-Produkt von QBE bietet Schutz bei vielfältigen Risiken, die mit digitaler Technologie einhergehen, und leistet im Falle eines Cyber-Angriffs entscheidende Unterstützung. Das Angebot umfasst QCyberProtect eine neue globale Cyber-Versicherungspolice, die mit einer weltweit einheitlichen Deckung vor Schäden durch aktuelle und aufkommende Cyber-Risiken schützt. Diese umfasst unter anderem die Netzwerksicherheit, Datenschutzverfahren, Betriebsunterbrechungen sowie Folgeschäden durch Reputationsverlust.

Maßgeschneiderter Schutz und individueller Service

Um einen umfassenden Schutz zu gewährleisten, arbeiten die Versicherungsexperten von QBE eng mit den Kunden zusammen, um maßgeschneiderte Versicherungslösungen zu entwickeln, die genau auf deren spezifische Bedürfnisse abgestimmt sind. Wir nehmen uns die Zeit, Ihr Unternehmen genau zu verstehen, um Ihnen einen individuellen Versicherungsschutz zu bieten, der Sie bei aktuellen und aufkommenden Cyberrisiken schützt.

Wir unterstützen Sie beim Risikomanagement

Wir sichern nicht nur Ihre Risiken ab, sondern helfen Ihnen dabei, diese zu kontrollieren und zu minimieren. Dazu bieten wir Ihnen Tools zur Unterstützung des Risikomanagements an, darunter:

- QBE QCyberPrepare– ein Online-Sicherheitsraum, der Kunden hilft, sich auf einen Cybervorfall vorzubereiten.
- Zugang zum QBE Cyber Risk Management Portal, das umfangreiche Informationen über Cyber-Risiken bereitstellt und zeigt, wie man sich davor schützen kann.
- Zugang zu QBE-Tools und -Dienstleistungen sowie Vergünstigungen für eine Reihe von Dienstleistungen im Bereich Cyber Risk Management Services von unseren vertrauenswürdigen Partnern.

Unterstützung in der Krise

QBE arbeitet mit einem Dienstleitungsnetzwerk zusammen, das Sie im Falle eines Cyber-Angriffs zu jeder Zeit tatkräftig unterstützt. Experten unter anderem aus den Bereichen Forensik, Recht und PR arbeiten gemeinsam mit Ihnen an der Problemlösung. Diese helfen Ihnen bei der schnellen und effektiven Wiederherstellung der digitalen Systeme, bei der Erfüllung rechtlicher Anforderungen sowie bei der Vermeidung von Imageschäden.

Weitere Informationen finden Sie unter Cyber Versicherungen - QBE Deutschland

Dieser Bericht
wurde von
Control Risks
für QBE erstellt.

QBE European Operations

QBE Europe SA/NV
Breite Straße 31
40213 Düsseldorf, Deutschland
+49 (0) 211 99419 0
QBE.de

641209/2405