QBE
At the heart of it



Wolken mit Gewitterpotenzial:

Cloud, KI & die Prognose digitaler Störungen im Zeitalter der Cyberkriminalität



Drei zentrale Erkenntnisse:

1. Wie Cloud- und KI-Einsatz die Effizienz steigern können – und zugleich das Risiko einer größeren Angriffsfläche für Unternehmen erhöhen.

2. Wie sich Bedrohungsakteure weiterentwickeln und neue Tools mit alten Taktiken kombinieren, um Unternehmen anzugreifen und zu stören.

3. Wie Unternehmen Risikomanagement in ihre Technologien integrieren können, sodass Resilienz von Beginn an Teil der Planung ist – und nicht erst im Nachhinein ergänzt werden muss.

Die Umstellung auf öffentliche, private und hybride Cloud-Plattformen eröffnet neue Effizienzpotenziale, treibt die Automatisierung voran und unterstützt die Einführung künstlicher Intelligenz (KI)

All diese Fortschritte schaffen Wettbewerbsvorteile, bringen aber zugleich eine Bedrohungslage mit sich, die sich noch schneller verändert. Da Unternehmen immer mehr auf Cloud-Dienste setzen, versuchen Angreifer, Schwachstellen wie unzureichende Identitätskontrollen, Fehlkonfigurationen und ungesicherte Daten zum eigenen Vorteil auszunutzen.

Generative künstliche Intelligenz (GenAI) verstärkt insofern Risiken, als sie Angreifern ein schnelleres und präziseres Vorgehen ermöglicht und gleichzeitig die technischen Hürden für Neulinge im Bereich Cyberkriminalität senkt. Wird GenAI eingesetzt, um Sicherheitssysteme auszuhebeln, führt das für Unternehmen zu Betriebsstörungen mit negativen finanziellen Folgen, Schäden für das Image sowie potenziellen Konsequenzen für die Regulierung. Die Gefahren, die von dem Einsatz von GenAI ausgehen, reichen von Deepfake±-Betrug über Identitätsdiebstahl bis hin zu automatisierten Phishing†-Angriffen. Kein Wunder, dass Ransomware-Delikte zunehmen: IT-ISAC verzeichnete im ersten Quartal 2025 1.537 solcher Angriffe, nach 572 im ersten Quartal 2024. Die dadurch verursachten Störungen stellen heute ein grundlegendes Risiko für alle Unternehmen dar, die von externen Partnern wie Cloud-Anbietern abhängig sind.



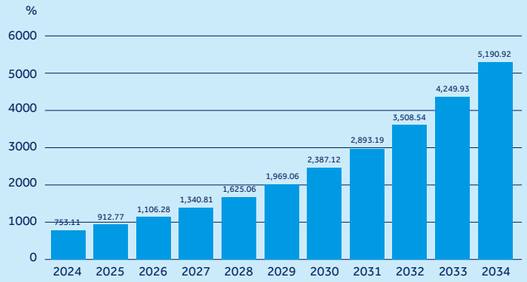
Glossar

± **Deepfake:** Eine KI-basierte Technologie, mit der künstliche, aber überzeugend echt erscheinende Video- oder Audioinhalte erzeugt werden.

† **Phishing:** Der Versuch, private und vertrauliche Informationen von Internetnutzern zu erhalten, zum Beispiel Benutzernamen, Passwörter und Kreditkartendaten. Cyberkriminelle versenden in der Regel E-Mails oder kontaktieren ihre Opfer über Instant Messaging, wobei sie sich als rechtmäßige oder offizielle Korrespondenzpartner ausgeben. Diese Phishing-E-Mails oder Nachrichten enthalten oft Links, die mit Malware infiziert sind.

Gefragt ist daher ein proaktiver Ansatz mit besonderem Fokus auf Resilienz. Es ist für Unternehmen unerlässlich, ein solides Risikomanagement in ihre Technologiesysteme zu integrieren, Schwachstellen bei externen Partnern zu antizipieren und Kontinuitätsplanung in ihre Betriebsabläufe einzubauen.

Grafik 1: Prognostizierter Wert des globalen Cloud-Computing-Marktes pro Jahr (in Milliarden US-Dollar)



Quelle: ControlRisks/Precedence Research[1]

Das Ausmaß der Cloud-Nutzung zeigt, wie dringend es geboten ist, die Risiken zu mindern. Der weltweite Markt wird voraussichtlich bis 2034 ein Volumen von über 5 Billionen US-Dollar erreichen, ausgehend von 912 Milliarden US-Dollar im Jahr 2025.[2] Da immer mehr Unternehmen ihre Infrastruktur und Daten auf Cloud-Server übertragen, werden diese zu bedeutenden Angriffszielen. Die Zahl der Cloud-Warnmeldungen mit hohem Risikopotenzial stieg 2024 um 235 % gegenüber dem Vorjahr,[3] was sowohl die verstärkte Cloud-Nutzung als auch die zunehmenden Fähigkeiten der Angreifer widerspiegelt.

Die meisten über die Cloud organisierten Angriffe sind Betrugsfälle per E-Mail (BEC).[4] Dabei nutzen Kriminelle Plattformen wie Microsoft 365, um mithilfe von BEC-Phishing-Kampagnen auf Konten zuzugreifen oder Anmeldedaten zu sammeln – und zwar über eine vertrauenswürdige Cloud-Plattform anstatt über Typosquatting‡-Domains oder E-Mail-Spoofing**. Auf diese Weise lassen sich Angriffe durchführen, ohne dass die üblichen Sicherheitsvorkehrungen ausgelöst werden.[5] Auch staatlich gelenkte Angreifer und professionell organisierte Cyberkriminelle bevorzugen Attacken auf digitale Infrastrukturen, die über die Cloud laufen.

1 precedenceresearch.com/cloud-computing-market
2 precedenceresearch.com/cloud-computing-market
3 unit42.paloaltonetworks.com/2025-cloud-security-alert-trends
4 ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index
5 guardz.com/blog/sophisticated-phishing-campaign-exploiting-microsoft-365-infrastructure

Glossar

‡ **Typosquatting:** Dabei werden häufig falsch geschriebene Versionen rechtmäßiger Domainnamen registriert, um über Links in Phishing-E-Mails oder Drive-by-Downloads Malware zu verbreiten. Beispielsweise könnte eine Variante der rechtmäßigen Domain example.com arglistig als exxample.com registriert werden.

** **E-Mail-Spoofing:** Eine Taktik, bei der ein Angreifer die Absenderadresse einer E-Mail fälscht, um die wahre Herkunft zu verschleiern, sodass der Eindruck entsteht, als stamme die E-Mail von einer vertrauenswürdigen

Doppelte Gefahr: Ransomware und Phishing

Fast die Hälfte der auf Cloud-Servern gespeicherten Unternehmensdaten gilt als vertraulich[6] und ist daher für Ransomware-Akteure attraktiv. Neue Ransomware-Varianten sind darauf ausgelegt, cloudbasierte Collaboration-Tools zu scannen und anzugreifen. Die Angreifer sind immer öfter in der Lage, sich zwischen lokalen und Cloud-Systemen zu bewegen und dabei Daten zu verschlüsseln oder zu exfiltrieren.[7]

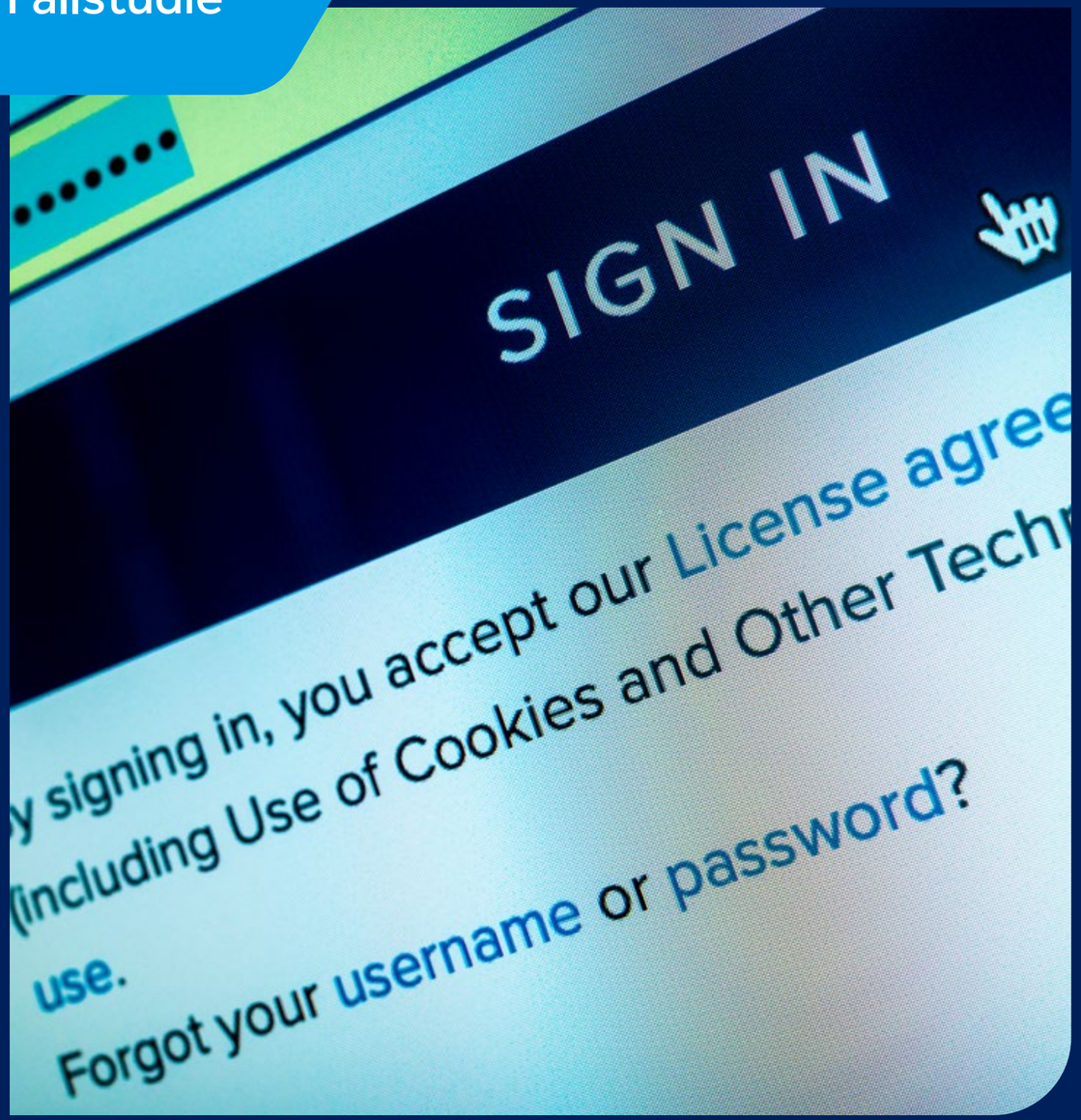
Phishing bleibt das häufigste Einfallstor für Cloud-bezogene Vorfälle: 2023 und 2024 ließ sich ein Drittel aller Angriffe darauf zurückführen.[8] Oft nutzen Angreifer Phishing-Taktiken, um durch adversary-in-the-middle (AitM)‡ attacks Anmeldedaten zu stehlen. Auch gab es Täter, die erfolgreich Schwachstellen in Cloud-Anwendungen ausgenutzt, gestohlene rechtmäßige Anmeldedaten verwendet und sich Zugang zu privilegierten Nutzern oder Servicekonten verschafft haben.

6 cpl.thalesgroup.com/resources/webinars?commid=615147&bt_tok=%7b%7bRecipient.ID%7d%7d
7 microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments
8 ibm.com/new/announcements/x-force-cloud-threat-landscape

Glossar

‡ **Adversary-in-the-Middle-Angriff (AITM):** Bei dieser auch als Man-in-the-Middle-Angriff (MITM) bekannten Variante schaltet sich der Angreifer in einen Dialog zwischen dem Nutzer (Opfer) und dem System ein. In dieser Zwischenstellung ist der Angreifer in der Lage, Daten abzufangen, zu senden und zu empfangen, die für einen Part des rechtmäßigen Dialogs bestimmt sind oder gar nicht erst übertragen werden sollten.

Fallstudie



Okta, 2023

Der Single-Sign-On-Anbieter (SSO) Okta wurde Ziel eines Angriffs, bei dem Unbekannte Anmeldedaten stahlen und sich Zugang zum Support-Case-Management-System verschafften. Durch den Diebstahl sensibler Informationen wie Cookies und Sitzungstoken waren die Angreifer in der Lage, sich als rechtmäßige Nutzer auszugeben.

Ein Kunde (1Password, ein Passwortmanager mit über 100.000 Geschäftskunden) entdeckte am 29. September verdächtige Aktivitäten auf seinem (für Mitarbeiter-Apps genutzten) Okta-Konto, woraufhin er die Nutzung sofort stoppte und Ermittlungen einleitete.[9] Okta wiederum informierte 1Password erst am 19. Oktober, also ganze 16 Tage später, über den Vorfall, obwohl ein anderer Cybersicherheitskunde (BeyondTrust) das Unternehmen bereits am 2. Oktober auf eine Unregelmäßigkeit hingewiesen hatte.[10]

Insgesamt waren 134 Geschäftskunden von Okta betroffen und der Marktwert des Unternehmens sank um 2 Milliarden US-Dollar.[11,12]

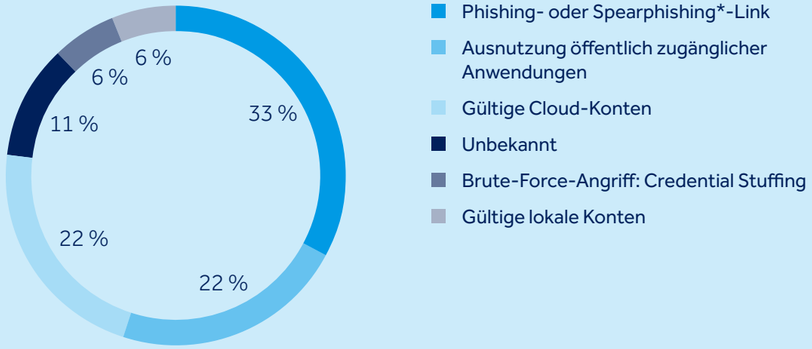
9 arstechnica.com/security/2023/10/1password-detects-suspicious-activity-in-its-internal-okta-account
10 portnox.com/blog/cyber-attacks/unpacking-the-okta-data-breach
11 nightfall.ai/blog/okta-data-breach-what-happened-impact-and-security-lessons-learned
12 cnbc.com/2023/10/23/okta-hack-wipes-out-more-than-2-billion-in-market-cap.html

Lieferketten und Abhängigkeiten von externen Partnern

Die zunehmende Konvergenz von Datenhosting und -management hat externe Dienstleister zu einem attraktiven Ziel für Cyberkriminelle gemacht. Es reicht bereits, einen einzigen Dienstleister erfolgreich anzugreifen, um gleich mehrere Unternehmen in Schwierigkeiten zu bringen – manchmal sogar hunderte auf einmal. Cloud- und Datenspeicher sind ein prädestiniertes Ziel für Angreifer aller Art, da Daten auf cyberkriminellen Marktplätzen immer höher gehandelt werden.

Bis 2025 wird das weltweit gespeicherte Datenvolumen voraussichtlich 200 Zettabyte (200 Billionen Gigabyte) erreichen, verteilt auf private und öffentliche IT-Infrastrukturen, Versorgungsinfrastrukturen, private und öffentliche Cloud-Rechenzentren, persönliche Geräte und Systeme des Internets der Dinge (IoT).[13] Die Hälfte dieser Daten wird in der Cloud gespeichert sein, nach 43 % im Jahr 2024[14], geschätzten 15 % im Jahr 2020[15] und lediglich 10 % im Jahr 2015.[16] Diese fortschreitende Konzentration wertvoller Daten macht Cloud-Anbieter und Speicherdienste für Angreifer attraktiv.

Grafik 2: Angriffe auf Cloud-Umgebungen nach ursprünglichem Einstiegsweg (2022-24)



Quelle: ControlRisks: IBM[17]

13 cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/
14 storagenewsletter.com/2023/01/25/43-of-data-to-be-stored-in-public-cloud-by-2024-on-average/
15 gartner.com/en/documents/3989101
16 statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/
17 ibm.com/new/announcements/x-force-cloud-threat-landscape

Glossar

* **Spearphishing:** Diese gezieltere Form des Phishing konzentriert sich auf bestimmte Personengruppen mit einem jeweils gemeinsamen Merkmal. So können die Personen beispielsweise in derselben Firma arbeiten, dieselbe Universität besuchen, dieselben Finanzdienstleistungen oder Institute nutzen oder auf denselben Websites bestellen.



MURKY PANDA, 2023 bis heute

MURKY PANDA ist ein bekannter, nationalstaatlich gelenkter Gefährder aus China. Es wurde beobachtet, wie die Gruppe Zero-Day-Schwachstellen bei Software-as-a-Service-Anbietern (SaaS) ausnutzte, um sich Zugang zu deren Netzwerk zu verschaffen. Die Gruppe ist in der Lage, Abwehrmaßnahmen zu umgehen und sich über längere Zeitspannen unentdeckt in Kundensystemen aufzuhalten. Der Vorteil ist, dass sie so ausreichend Zeit hat, auf private Daten zuzugreifen. MURKY PANDA hat unter anderem einen Microsoft-Cloud-Dienstleister durch den Missbrauch von Zugriffrechten für IT- und technisches Personal infiltriert.[18]

Die Gruppe stellt eine ernsthafte Bedrohung für Regierungs-, Technologie- und Dienstleistungsunternehmen in Nordamerika dar, insbesondere durch die Infiltrierung von Lieferanten mit Zugang zu sensiblen Informationen. Cloud-Umgebungen erweisen sich als extrem vulnerabel angesichts der avancierten Fähigkeiten und Kenntnisse von MURKY PANDA auf dem Gebiet der kundenspezifischen Anwendungslogik – Fähigkeiten, mit denen die Funktionalität von Anwendungen ausgenutzt wird, anstatt technische Schwachstellen zu missbrauchen.

18 crowdstrike.com/en-us/blog/murky-panda-trusted-relationship-threat-in-cloud

Nationalstaatliche Akteure

Staatlich gelenkte Gruppen nutzen zunehmend Schwachstellen in Cloud-Systemen aus

GenAI: Verteidigung oder Waffe?

GenAI verändert das durch Cyberkriminalität hervorgerufene Bedrohungsumfeld. Die Nutzung und die Verbreitungswege dieser Technologie werden in Nordamerika und Europa in den nächsten fünf Jahren mit Sicherheit rasant zunehmen, da GenAI-Tools für die meisten, wenn nicht sogar alle Branchen Produktivitätsvorteile bringen.

- ChatGPT hat 2025 755 Millionen und Microsoft Copilot 88 Millionen aktive Nutzer.[19]
- Die Zahl der ChatGPT-Nutzer stieg von Dezember 2024 bis Februar 2025 um 33 %.[20]
- 2025 haben 78 % der Unternehmen KI in mindestens einem Geschäftsbereich eingesetzt, nach 55 % im Jahr 2024.[21]
- Zwischen 20 % und 40 % der Mitarbeiter nutzen KI aktiv in ihrer Arbeit, besonders in der Programmierung.[22]

Allerdings hat sich auch der Missbrauch dieser Technologie für Betrug und Erpressung etabliert und zu einer weit verbreiteten Bedrohung entwickelt. Besonders alarmierend ist die Entwicklung von Deepfake-Betrug, bei dem Cyberkriminelle mithilfe synthetischer Stimmen, Videos und Bilder die Identität von Führungskräften, Vorstandsmitgliedern und Persönlichkeiten des öffentlichen Lebens imitieren.

Mit diesen Taktiken werden Mitarbeiter dazu verleitet, erhebliche Geldbeträge auf nicht autorisierte, von kriminellen Netzwerken kontrollierte Konten zu überweisen. 2024 gingen fast 10 % der erfolgreichen Cyberangriffe auf das Konto von Deepfakes, mit finanziellen Verlusten zwischen 250.000 US-Dollar und über 20 Millionen US-Dollar.[23]

19 firstpagesage.com/seo-blog/chatgpt-usage-statistics
20 demandsage.com/chatgpt-statistics
21 sqmagazine.co.uk/ai-tools-usage-statistics
22 sqmagazine.co.uk/ai-tools-usage-statistics
23 Control Risks

Fallstudie



Nicht näher benanntes Unternehmen aus Singapur, 2024

Ein Mitarbeiter eines multinationalen Unternehmens aus Singapur wurde von einem Betrüger getäuscht, der sich als CFO ausgab. Da er die Videokonferenz mit dem Täter für echt hielt, genehmigte er eine Überweisung in Höhe von fast 500.000 US-Dollar.[24] Obwohl das Geld von den Polizeibehörden in Singapur und Hongkong aufgespürt und sichergestellt werden konnte, entstanden sehr wahrscheinlich erhebliche Kosten für die Behebung und Aufarbeitung des Vorfalls.

24 channelnewsasia.com/singapore/deepfake-scam-impersonate-ceo-company-finance-director-5048706



Staatlich unterstützte Angreifer nutzen GenAI außerdem zum Schreiben von Schadprogrammen und verwenden Large Language Models (LLMs), um Erkundungen einzuholen und Malware-Operationen zu skalieren. Solche Akteure können auch LLMs ins Visier nehmen, die von Unternehmen für interne Zwecke eingesetzt werden, und auf diesem Wege Betriebsstörungen durch Ausfälle und Integritätsprobleme verursachen.

Cyberkriminelle Gruppen nutzen zunehmend GenAI- und Deepfake-Technologien, um weltweit finanziell motivierte Angriffe gegen diverse Branchen durchzuführen. GenAI ist in der Lage, effektive Phishing-Vorlagen zu erstellen oder in kurzer Zeit hochkomplexe Social-Engineering-Kampagnen auf den Weg zu bringen. Hat man es mit einer Tätergruppe mit eher begrenzten Fähigkeiten zu tun, wird die KI auch oft unterstützend für die Skriptentwicklung und die Malware-Codierung eingesetzt.[25] Unternehmen werden vermutlich in zunehmendem Maße mit Angriffen durch Gruppen konfrontiert sein, die zuvor als technisch zu inkompetent oder zu schlecht ausgestattet galten, um als Bedrohung ernst genommen zu werden.[26] Die Zahl der öffentlich bekannt gewordenen Fälle von Erpressung durch Ransomware stieg von Januar bis April 2025 um 54 % gegenüber dem Vorjahreszeitraum.[27]

25 hp.com/us-en/newsroom/press-releases/2024/ai-generate-malware.html
26 anthropic.com/news/detecting-countering-misuse-aug-2025
27 Control Risks

Fallstudie



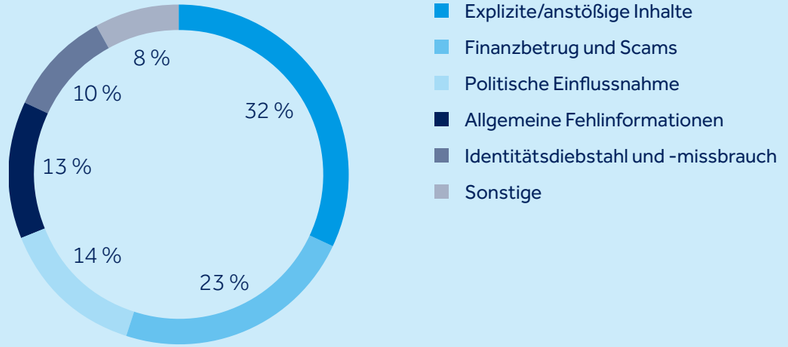
Amazon, 2025

Ein White-Hat-Hacker brachte neuralgische Punkte in der Q-Erweiterung von Amazon für Visual Studio Code zum Vorschein, indem er einen arglistigen Pull-Request einreichte. Obwohl er nur über ein nicht privilegiertes GitHub-Konto verfügte, wurden ihm versehentlich Administratorrechte zuteil. Dadurch war er in der Lage, den Assistant zu steuern, die Werkseinstellungen wiederherzustellen, lokale Dateisysteme zu löschen und Cloud-Ressourcen-Datenbanken zu entfernen. Der Angreifer, der seine Aktion als Demaskierung von Amazons „AI-Sicherheitstheater" bezeichnete, benötigte für sein erfolgreiches Vorgehen keine ausgeklügelte Malware – was die Schwachstellen in der Sicherheitsarchitektur und den Kontrollen externer Dienstleister umso deutlicher macht.[28] Zwar gingen bei dem Vorfall keine sensiblen Daten verloren, doch könnte dieser zu ähnlichen Angriffen auf die Sicherheit und die KI-gestützten Assistenzdienste von Amazon ermuntern.

28 404media.co/hacker-plants-computer-wiping-commands-in-amazons-ai-coding-agent



Grafik 3: Art der Deepfake-Angriffe, 1. Quartal 2025



Quelle: ControlRisks: Resemble AI[29]

Die Kosten eines Angriffs

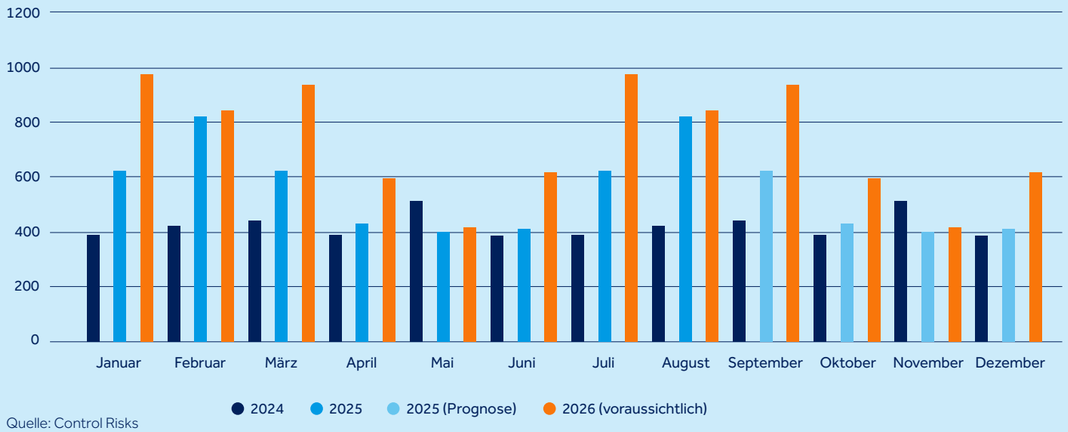
Erfolgreiche Ransomware-Angriffe können finanzielle Verluste, Imageschäden und sogar Rechtsstreitigkeiten nach sich ziehen – nicht nur für das angegriffene Unternehmen, sondern auch für externe Partner und deren Kunden. Die flächendeckende Nutzung von Cloud-Diensten und anderen neuen Technologien ging in den letzten Jahren mit einer stetigen Zunahme von Ransomware-Aktivitäten einher. Eine umfangreiche Angriffswelle, die im Mai 2025 unter der Regie der Cyberkriminellen-Gruppe Scattered Spider gegen britische Einzelhandels- und Finanzunternehmen gestartet wurde, macht dieses Muster deutlich. Die Gruppe nutzte modernste Social-Engineering- und Phishing-Techniken, um die Systeme der Unternehmen zu infiltrieren. Dabei imitierte sie vertrauenswürdige Plattformen und verleitete ihre Opfer mithilfe von Typosquatting-Domains von externen SaaS-Dienstleistern durch den Einsatz von Phishing-Kits dazu, Anmeldedaten und Sitzungsdaten preiszugeben.[30]

29 resemble.ai/wp-content/uploads/2025/04/ResembleAI-Q1-Deepfake-Threats.pdf
30 reliaquest.com/blog/scattered-spider-cyber-attacks-using-phishing-social-engineering-2025

Rund um den Globus haben Unternehmen heute mit erheblichen Störungen zu kämpfen, die durch Pannen bei externen Partnern entstehen. In den letzten zwei Jahren waren diverse Branchen von massiven Ausfällen und Cyberattacken betroffen. Besonders spektakulär war das fehlerhafte Update für den Falcon Sensor von CrowdStrike im Jahr 2024, von dem rund 8,5 Millionen Windows-Geräte betroffen waren. Obwohl es sich dabei effektiv um weniger als 1 % aller Windows-Rechner handelte, hatte der Ausfall globale Folgen, insbesondere für das Gesundheitswesen, die Luftfahrt und andere Transportbereiche.

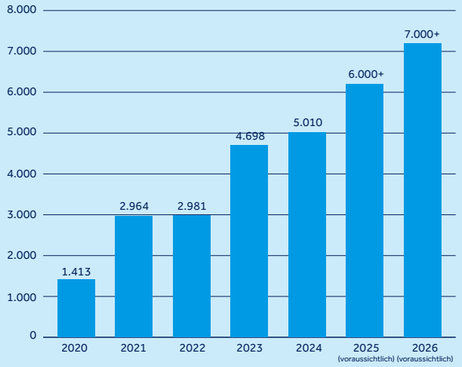
Die cyberkriminellen Akteure nutzten diese Situation schnell aus und starteten gezielte Phishing-Kampagnen. Dabei setzten sie auf CrowdStrike zugeschnittene Köder ein, um Systeme zu infiltrieren, Daten zu stehlen und Opfer zu erpressen. Obwohl es sich bei dem Vorfall nicht um einen geplanten Angriff handelte, verdeutlicht er die möglichen systemischen Auswirkungen solcher Pannen für Unternehmen, die in wichtigen Geschäftsprozessen auf SaaS angewiesen sind. Auch frühere Angriffe, wie die MOVEit-Massen-Sicherheitslücke und der NotPetya-Massen-Cyberangriff, verliefen ähnlich folgenschwer, mit erheblichen Konsequenzen für die Kunden weit über den ursprünglichen Angriffspunkt hinaus.

Grafik 4: Voraussichtliche monatliche Anzahl der Opfer von Ransomware, entsprechend den Angaben auf Datenleck-Websites



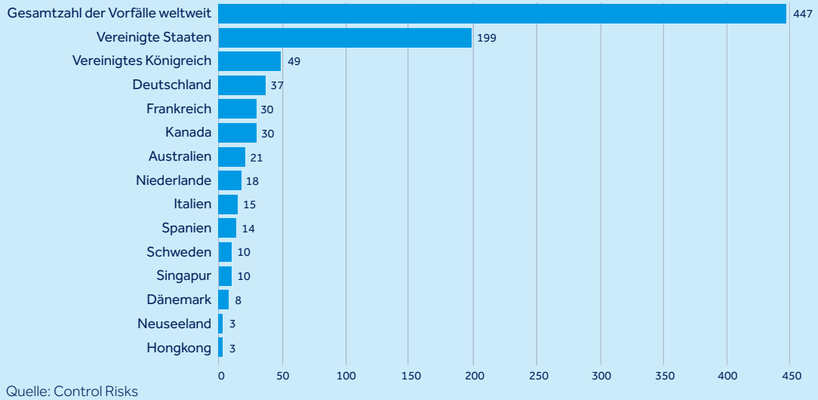
Quelle: Control Risks

Grafik 5: Gesamtzahl der auf Leak-Seiten angegebenen Ransomware-Opfer (weltweit)



Quelle: Control Risks

Grafik 6: Anzahl der gemeldeten schwerwiegenden Cybervorfälle nach Region (August 2023 bis August 2025)



Quelle: Control Risks

Fallstudie

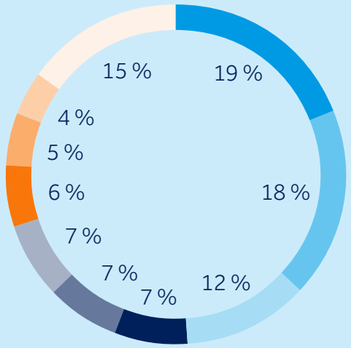


Rackspace, 2022

2022 störte eine Ransomware-Gruppe namens Play den E-Mail-Dienst „Hosted Exchange“ von Rackspace. Die Gruppe nutzte eine Zero-Day-Sicherheitslücke für eine Rechteausweitung in Microsoft Exchange. Mindestens 27 Hosted-Exchange-Kunden waren betroffen, nachdem sich die Angreifer mithilfe erbeuteter Anmeldedaten Zugang verschafft und den E-Mail-Zugang in den einzelnen Unternehmen blockiert hatten.[31] Die Folgen waren gravierend: So war Rackspace nicht nur gezwungen, seinen Hosted-Exchange-Dienst einzustellen, sondern musste sich auch diverser Kundenklagen erwehren. Insgesamt sollen Verluste in Höhe von rund 11 Millionen US-Dollar aufgelaufen sein.[32]

31 ir.rackspace.com/news-releases/news-release-details/update-recent-cybersecurity-incident
32 msspalert.com/news/rackspace-taking-losses-of-roughly-11-million-for-hosted-exchange-ransom-attack

Grafik 7: Cybervorfälle mit Auswirkungen auf wichtige Märkte, nach Sektoren (August 2023 bis August 2025)



- Regierung und Verwaltung
- IT und Telekommunikation
- Finanzen und Versicherungen
- Energie und Versorgungsunternehmen, einschließlich Öl und Gas
- Fertigung
- Pharmazeutika und Gesundheitswesen
- Logistik und Transport, einschließlich Seeverkehr
- Bildung und Ausbildung, einschließlich Denkfabriken
- Hotels und Unterhaltung
- Sonstige

Control Risks: Quelle

Weltweit sehen sich Unternehmen zunehmenden Risiken durch Betriebsausfälle, finanzielle Verluste und Imageschäden ausgesetzt, da kriminelle Täterkreise eine immer größere Angriffsfläche für sich nutzen können. Je mehr externe Dienste wie Cloud-Hosting, externe Software oder KI-Tools Einzug in das Tagesgeschäft halten, desto größer ist die Anzahl an Angriffspunkten für diese Täter.

Resilienz durch Planung

Sollte der Cloud-Einsatz und die Integration von KI weiter im erwarteten Tempo voranschreiten, werden sich möglichen Angreifern immer mehr Chancen und Angriffspunkte bieten. Die Unternehmen werden weiterhin anfällig für Attacken bleiben. Es bedarf daher einer belastbaren Strategie, um Cyberangriffe zu antizipieren und ihnen standzuhalten. Das gilt ganz besonders auch dann, wenn die Angriffe über externe Dienste und Cloud-Umgebungen, die mittlerweile wichtige Geschäftsprozesse unterstützen, geführt werden.

Um Resilienz aufzubauen, muss das Cyber-Risikomanagement von Anfang an in die Technologie-Lebenszyklen integriert werden. Dazu gehören die Implementierung strenger Identitäts- und Zugriffsmanagement-Protokolle (IAM), die Durchführung regelmäßiger Konfigurationsprüfungen sowie die Verschlüsselung sensibler Daten in allen Cloud-Umgebungen. Proaktive Maßnahmen wie kontinuierliche Überwachung, Aufklärung über mögliche Bedrohungen und Pläne zur richtigen Reaktion auf Vorfälle können dabei helfen, Gefahren zu erkennen und zu begrenzen, bevor sie eskalieren.

Darüber hinaus sollten Unternehmen die Sicherheitslage ihrer externen Partner bewerten und klare Protokolle für den Umgang mit Risiken innerhalb der Lieferkette festlegen. Durch die gemeinsame Umsetzung dieser Maßnahmen können Unternehmen ihre Betriebsabläufe besser schützen, die Kontinuität gewährleisten und trotz eines zunehmend volatilen Cyberumfelds Vertrauen schaffen.

Resilienz aufzubauen heißt, Cyber-Risikomanagement von Anfang an in Technologie-Lebenszyklen zu integrieren. Dazu gehören strengere Identitäts- und Zugriffsmanagement-Protokolle, regelmäßige Konfigurationsprüfungen sowie die Verschlüsselung sensibler Daten.



Fallstudie



Microsoft Azure, 2024

Im Juli 2024 führte ein Distributed-Denial-of-Service-Angriff (DDoS) zu einer Störung der Azure-Cloud-Plattform von Microsoft, sodass die Dienste bis zu acht Stunden lang nicht verfügbar waren. Verursacht wurde die Störung durch einen starken Nutzungsanstieg, der sich auf Azure Front Door und das Content Delivery Network auswirkte. Durch einen Fehler bei der Implementierung der Abwehrmaßnahmen wurde die Störung dann nicht behoben, sondern in ihren Auswirkungen weiter verstärkt.[33]

33 forbes.com/sites/kateoflahertyuk/2024/07/31/microsoft-confirms-new-outage-was-triggered-by-cyberattack

Schritte zum Aufbau von Cyber-Resilienz

Etablierte Organisationen können durch verschiedene Maßnahmen eine angemessene Cyber-Resilienz aufbauen:



Verstehen und Erfassen von Risikoprofilen, um kritische Vermögenswerte, Bedrohungen und Schwachstellen zu identifizieren und einen klaren Überblick über die Risiken des jeweiligen Unternehmens zu erhalten.



Definieren akzeptabler Unternehmensrisiken, damit die Entscheider im Unternehmen klare Grenzen für vertretbare Risiken und Gefährdungen festlegen können.



Priorisieren von Strategien zur Risikominderung, um Ressourcen dort einzusetzen, wo sie die größte Wirkung erzielen.



Vorbereiten von Worst-Case-Szenarien mit getesteten Notfallplänen und Wiederherstellungs-protokollen.



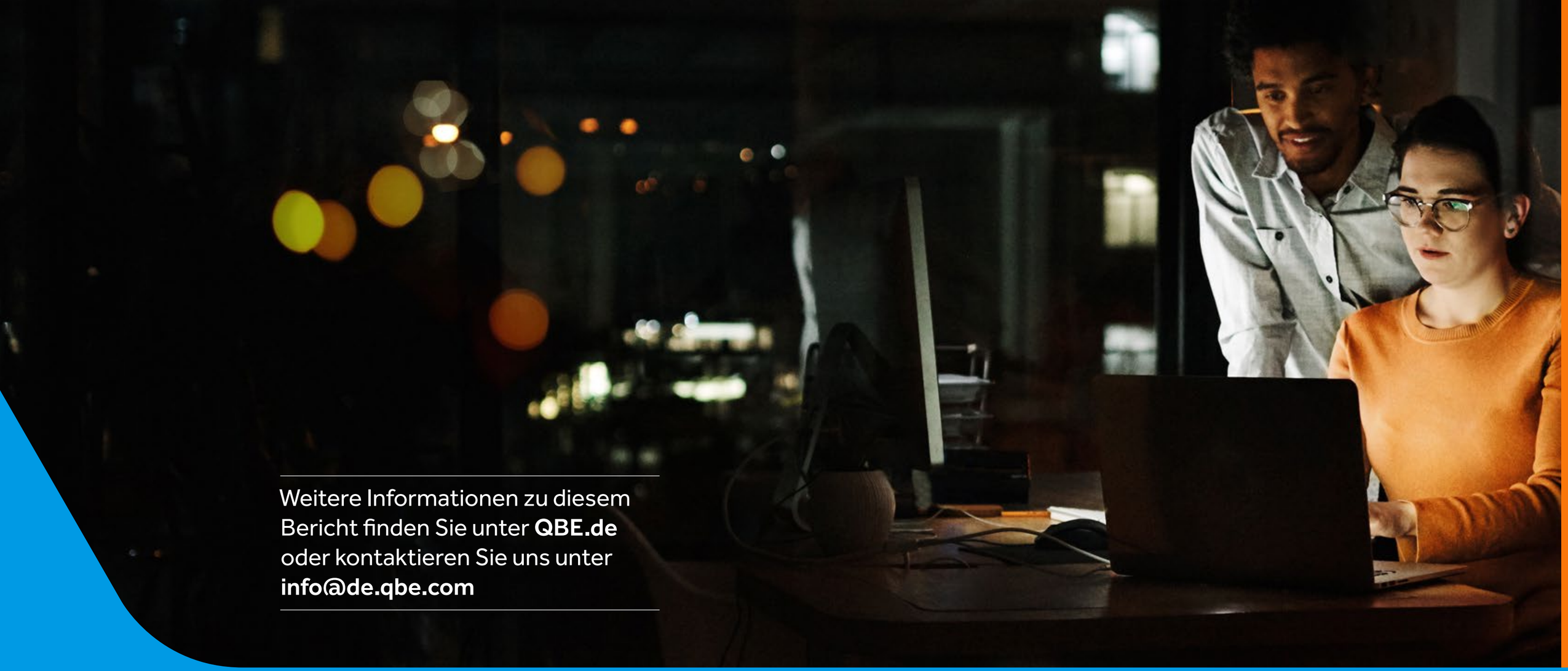
Prüfen der Krisenmanagement-fähigkeiten durch einen Stresstest hinsichtlich Entscheidungsfindung, Kommunikation und Krisenreaktion.



Einbeziehen der Unterstützung durch externe Partner in die Cybersicherheits-strategie, um die nötige Expertise zum Management von Restrisiken bereitzustellen.



Proaktives Beobachten von Trends und entsprechendes Anpassen der Cyberabwehr, um den aufkommenden Bedrohungen, neuen Technologien und wechselnden Geschäfts-anforderungen immer einen Schritt voraus zu sein.



Weitere Informationen zu diesem Bericht finden Sie unter **QBE.de** oder kontaktieren Sie uns unter **info@de.qbe.com**

QBE European Operations
QBE Europe SA/NV
Breite Straße 31
40213 Düsseldorf
Deutschland
+49 (0) 211 99419 0

QBE.de

Dieser Bericht wurde von QBE mit Control Risks erstellt.

QBE European Operations ist ein Handelsname der QBE UK Limited, QBE Underwriting Limited und QBE Europe SA / NV. QBE UK Limited und QBE Underwriting Limited sind beide von der Prudential Regulation Authority zugelassen und werden von der Financial Conduct Authority und der Prudential Regulation Authority reguliert. QBE Europe SA / NV, St.-Nr. BE 0690.537.456, RPM / RPR Brüssel, IBAN Nr. BE53949007944353 und SWIFT / BIC Nr. HSBCBEBB, ist von der belgischen Nationalbank unter der Lizenznummer 3093 zugelassen. 641209

QBE
At the heart of it

1023804/2510-DE