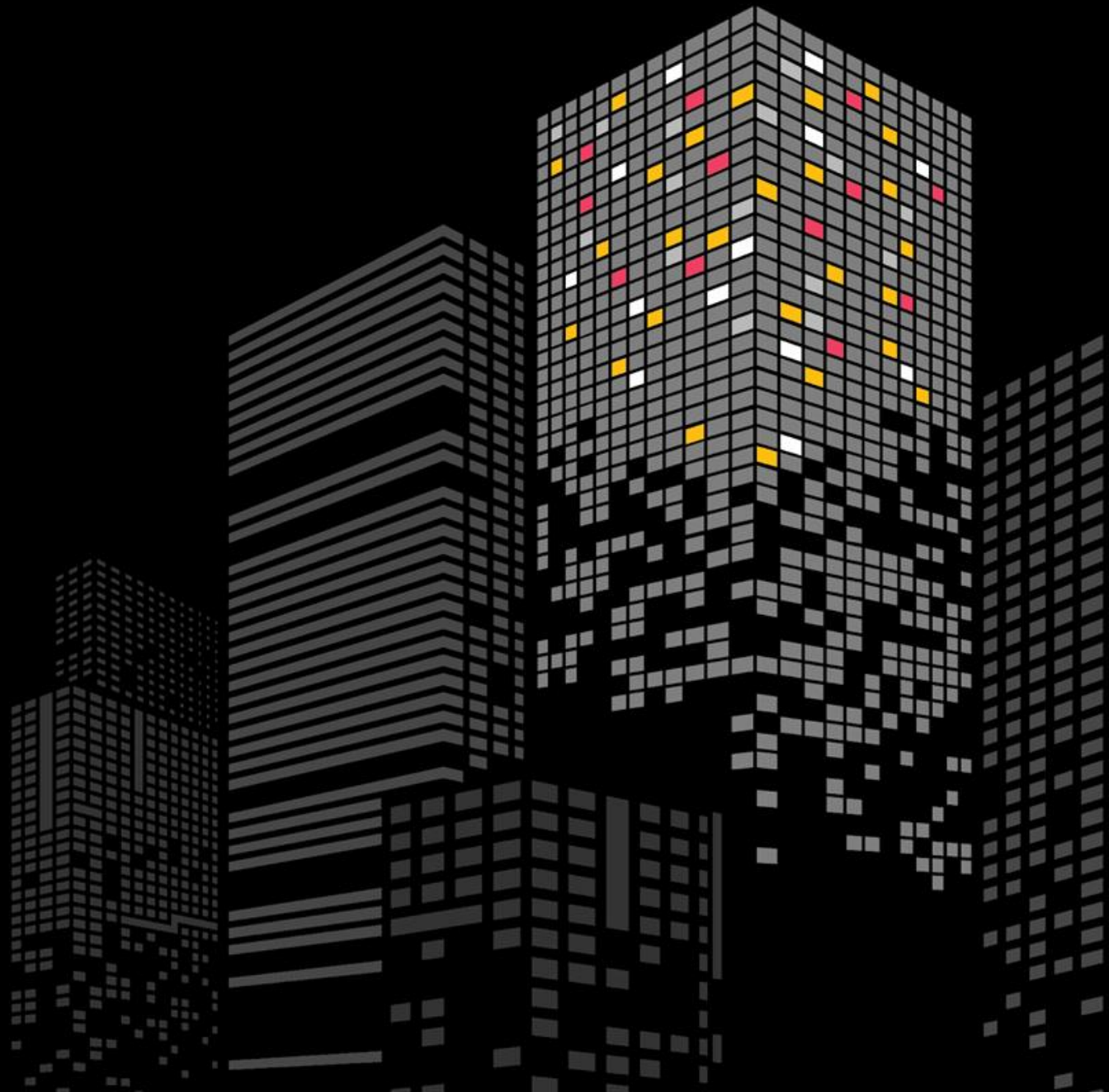
Global Digital Trust Insights 2023

Die Schweizer Ergebnisse einer weltweiten PwC-Befragung zum Thema Cybersicherheit



Agenda

Kühne neue Welt

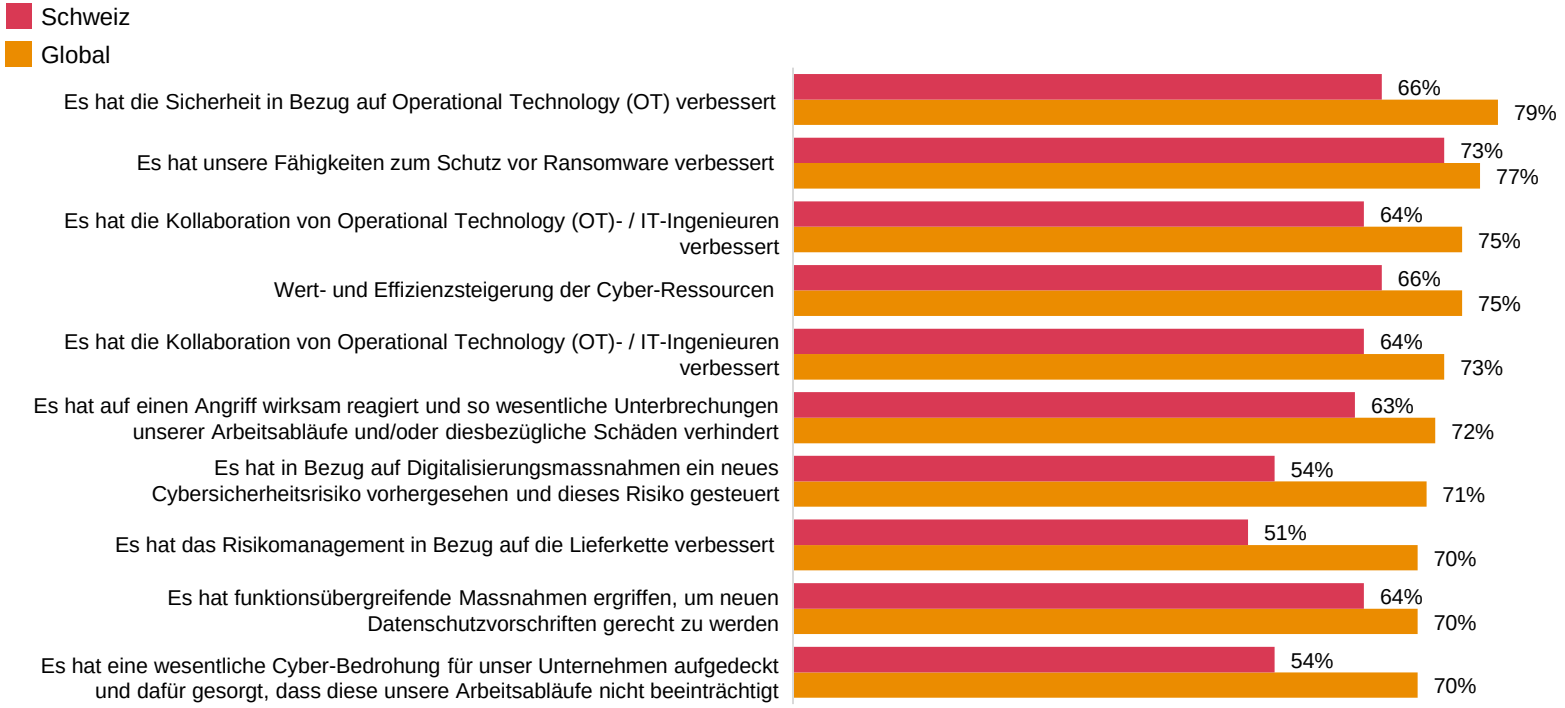
Mehr als 70% der Befragten haben im vergangenen Jahr Verbesserungen bei der Cybersicherheit festgestellt – zurückzuführen auf Investitionen und verstärkter Zusammenarbeit auf Führungsebene.

Führungskräfte stellen Verbesserungen der Cybersicherheit an verschiedenen Fronten fest

70%

der 3’522 befragten Unternehmens-, Sicherheits- und IT-Führungskräften haben im vergangenen Jahr Verbesserungen bei der Cybersicherheit in ihren Unternehmen festgestellt, **26%** gaben Verbesserungen in allen 10 Kategorien an

Führungskräfte stellen Verbesserungen der Cybersicherheit an verschiedenen Fronten fest
%-Anteil der Befragten, die davon berichten, dass ihr Cybersicherheitsteam in den letzten 12 Monaten folgende Tätigkeiten ausgeführt hat



Frage: Bitte geben Sie an, ob das Cybersicherheitsteam Ihres Unternehmens in den letzten zwölf Monaten folgende Tätigkeiten ausgeführt hat.
Grundlage: 3’522 Antworten | 70 Antworten aus der Schweiz

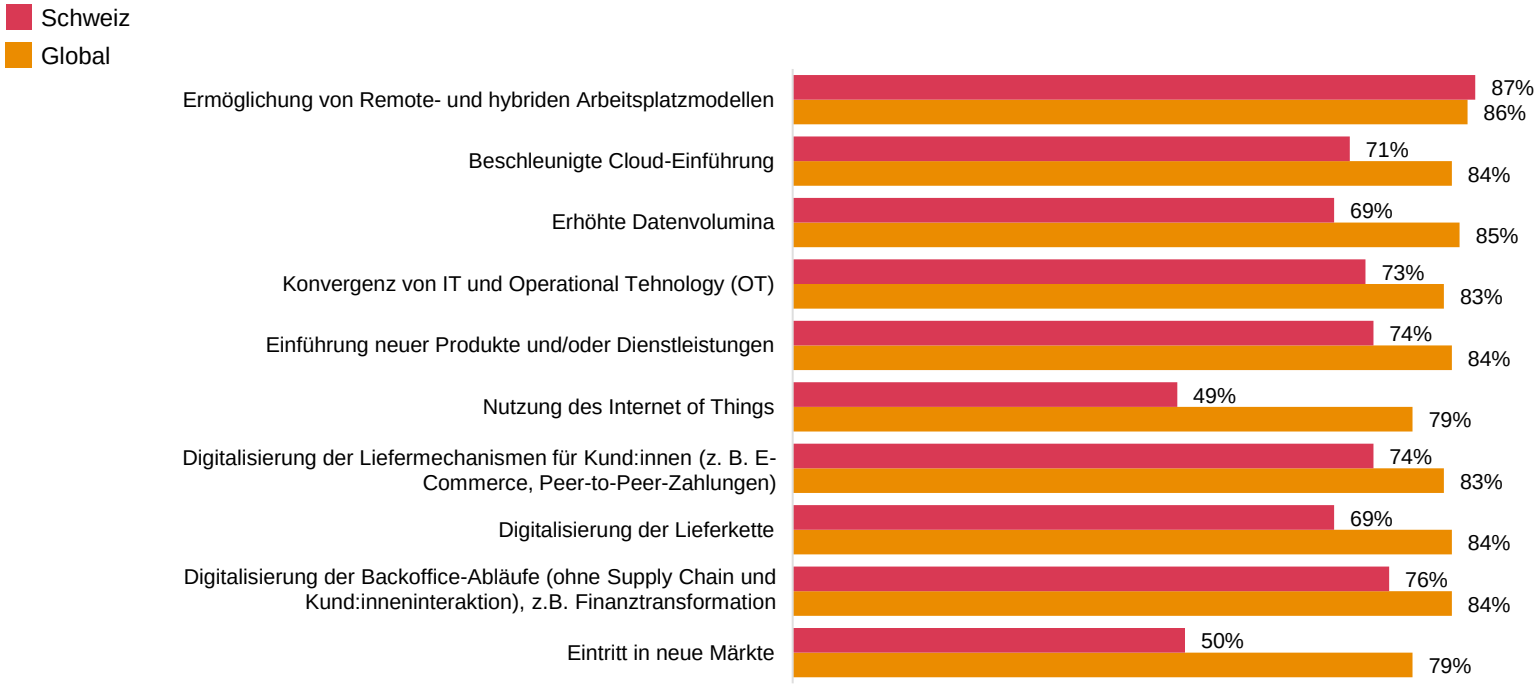
Weniger als 40% geben an, neu aufkommende Cyberrisiken vollständig reduziert zu haben

40% der Unternehmen aus der Technologie-, Kommunikations- und Medienbranche haben die Risiken in Bezug zu einer beschleunigten Cloud-Einführung vollständig reduziert

Grosse Unternehmen (Umsatz höher als 1 Mia. US-Dollar) geben signifikant häufiger an, alle aufgeführten Risiken vollständig reduziert zu haben

Nordamerikanische Unternehmen berichten signifikant häufiger von einer vollständigen Risikominderung im Vergleich zu den befragten west- und osteuropäischen Unternehmen

Weniger als 40% geben an, neu aufkommende Cyberrisiken vollständig reduziert zu haben
%-Anteil der Befragten, die angeben, dass sie die folgenden Risiken vollständig oder mässig reduziert haben



Frage: Auf einer Skala von 1 bis 10, in welchem Umfang konnte Ihr Unternehmen die Cyberrisiken in Verbindung mit folgenden Aspekten in den letzten zwölf Monaten reduzieren?
Grundlage: 3’522 Antworten | 70 Antworten aus der Schweiz
Befragte, die eine vollständige oder mässige Reduktion angaben.

Ausblick: Bedrohungslage 2023

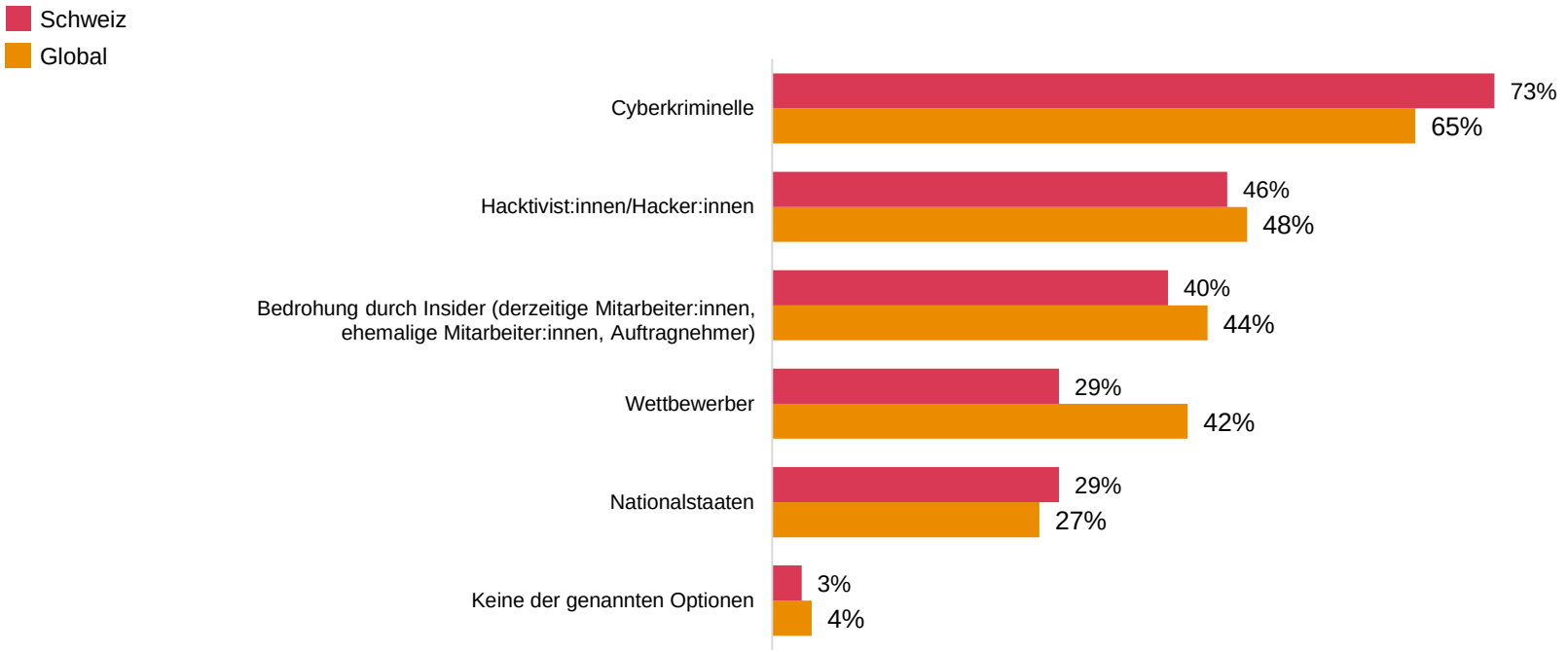
Es gibt noch viel zu tun – in einem aktuell schwierigen wirtschaftlichen und geschäftlichen Umfeld

Bedrohungsakteure, die Unternehmen im Jahr 2023 im Vergleich zu 2022 erheblich beeinflussen

65%

der Studienteilnehmer erachten Cyberkriminelle für 2023 als die grösste Gefahr für ihr Unternehmen

Unternehmen fürchten sich vor mehr Bedrohungen und Vorfällen im Jahr 2023
%-Anteil der Befragten, die angeben, dass die folgenden Akteure ihr Unternehmen 2023 im Vergleich zu 2022 negativ beeinflussen werden

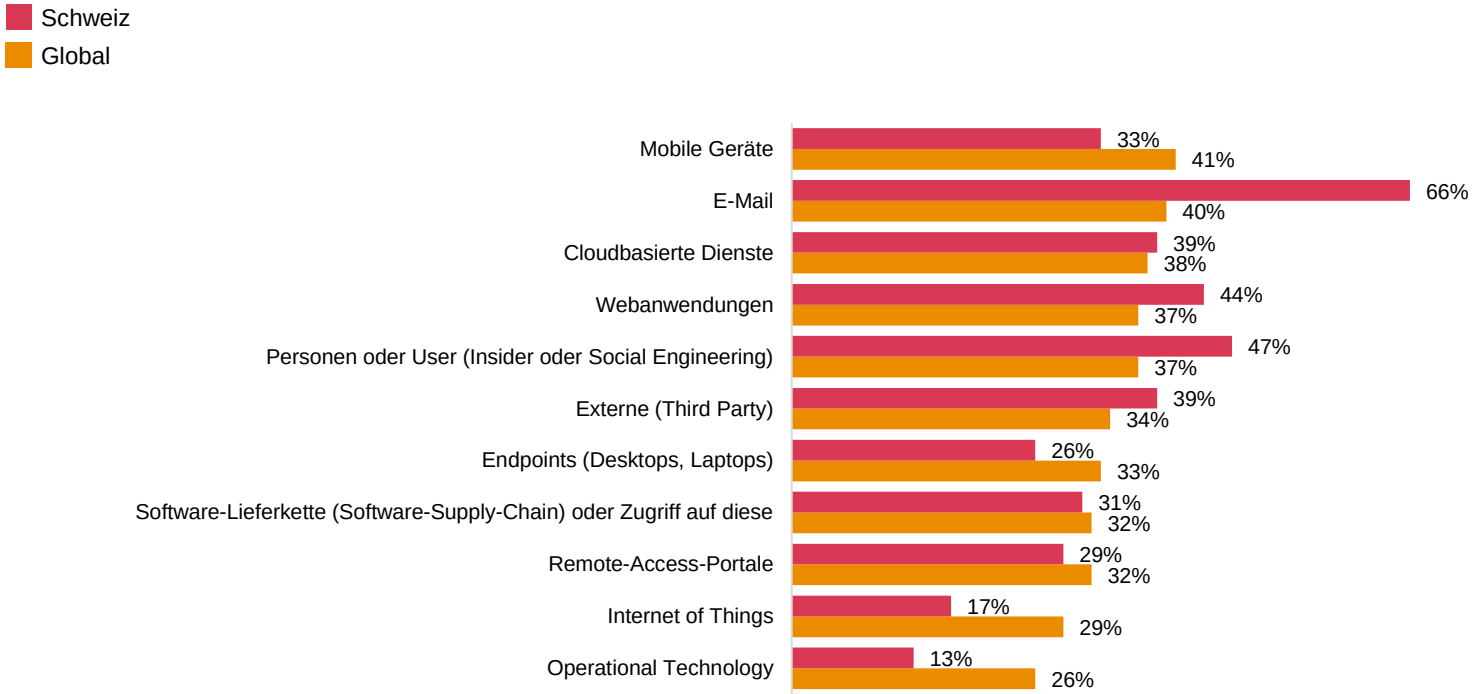


Frage: Von welchen dieser Akteure gehen Sie davon aus, dass diese Ihr Unternehmen 2023 im Vergleich zu 2022 negativ beeinflussen werden?
Grundlage: 3’522 Antworten | 70 Antworten aus der Schweiz

Einfallstore, die sich Angreifende zunutze machen

Grössere Unternehmen schätzen die Gefahr für Angriffe über die Software-Lieferkette (35%), cloudbasierte Dienste (43%) und Operational Technology (29%) als signifikant höher ein

Angriffsvektoren
%-Anteil der Befragten, die angeben, dass von den folgenden Schwachstellen im Jahr 2023 eine höhere Gefahr für Ihr Unternehmen ausgeht als 2022



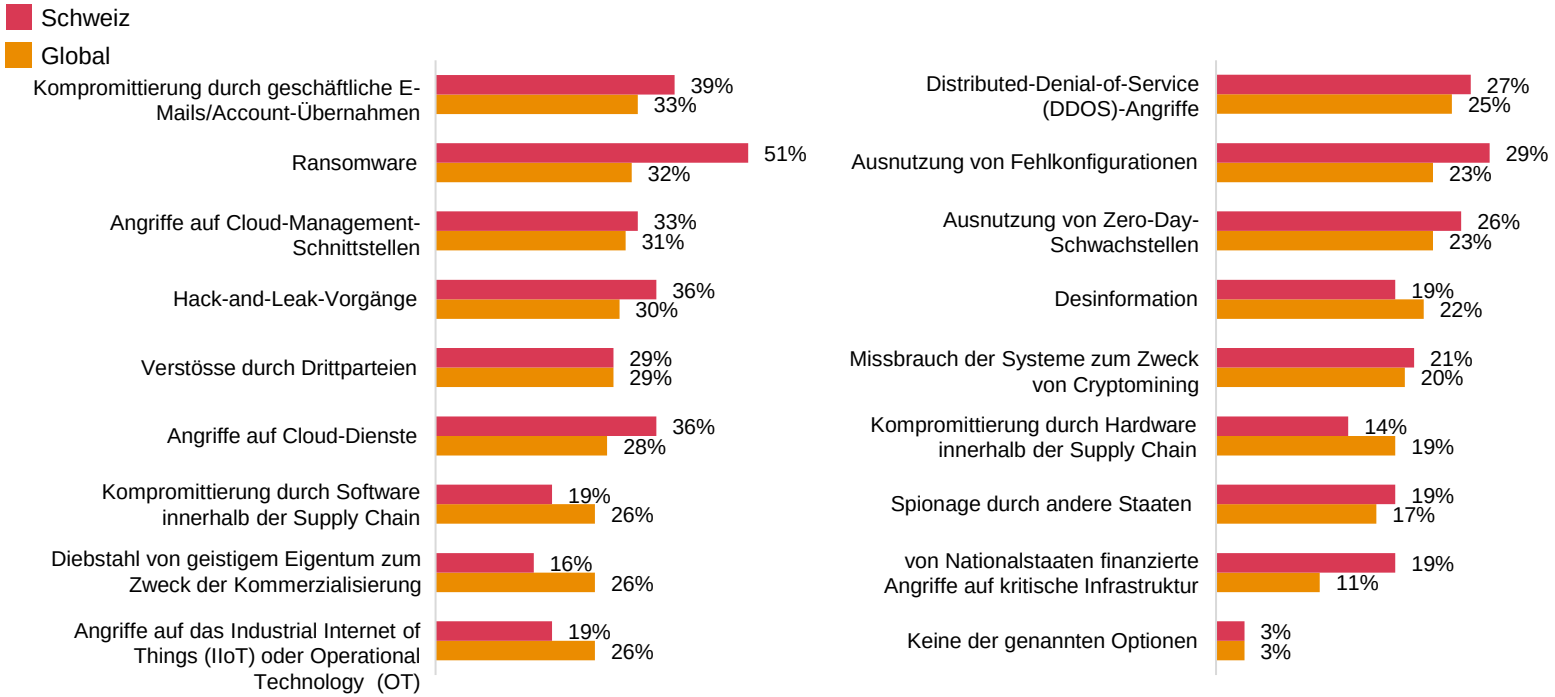
Frage: Über welchen Zugang erhalten Angreifer Zugriff auf Ihre Systeme? Wählen Sie diejenigen Schwachstellen aus, von denen aus Ihrer Sicht im Jahr 2023 eine höhere Gefahr für Ihr Unternehmen ausgeht als im 2022.
Grundlage: 3’522 Antworten | 70 Antworten aus der Schweiz

Signifikante (weitere) Zunahme an Cybervorfällen im Jahr 2023 wird erwartet

CISOs / CIOs / IT-Führungskräfte haben signifikant häufiger die folgenden Angriffsformen erwähnt:

- Ransomware (45%)
- Angriffe auf Cloud-Dienste (36%)
- Ausnutzung von Zero-Day-Schwachstellen (31%)
- Ausnutzung von Fehlkonfigurationen (31%)
- Verstösse durch Drittparteien («Third party breach») (42%)

Cybervorfälle
%-Anteil der Befragten, die angeben, dass die folgenden Angriffsszenarien im Jahr 2023 zunehmen werden



Frage: Bei welchen der folgenden Angriffe auf Ihr Unternehmen gehen Sie davon aus, dass diese 2023 im Vergleich zu 2022 wesentlich zunehmen werden?
Grundlage: 3'522 Antworten | 70 Antworten aus der Schweiz

Berichterstattung und Offenlegung

Offenlegung kommt allen zugute, und Unternehmen können aus den Angriffen auf andere Organisationen lernen. Vier Fünftel der Unternehmen weltweit sind der Meinung, dass eine obligatorische Offenlegung von Cybervorfällen in vergleichbaren und einheitlichen Formaten notwendig ist, um das Vertrauen der Stakeholder zu gewinnen.

Eine gute Berichterstattung und Transparenz sind der Schlüssel zu einem sicheren Unternehmen

Eine gute Berichterstattung und Transparenz sind der Schlüssel zu einer erfolgreichen Zusammenarbeit, die für die Cybersicherheit entscheidend ist. Die CEO- und Verwaltungsratsposition nehmen bei der Einführung und Verbesserung von Sicherheitsprogrammen eine zentrale Rolle ein.

Priorität unterschiedlicher Stakeholder-Gruppen in Unternehmen bei Cybersicherheitsfragen
(Ranked index)

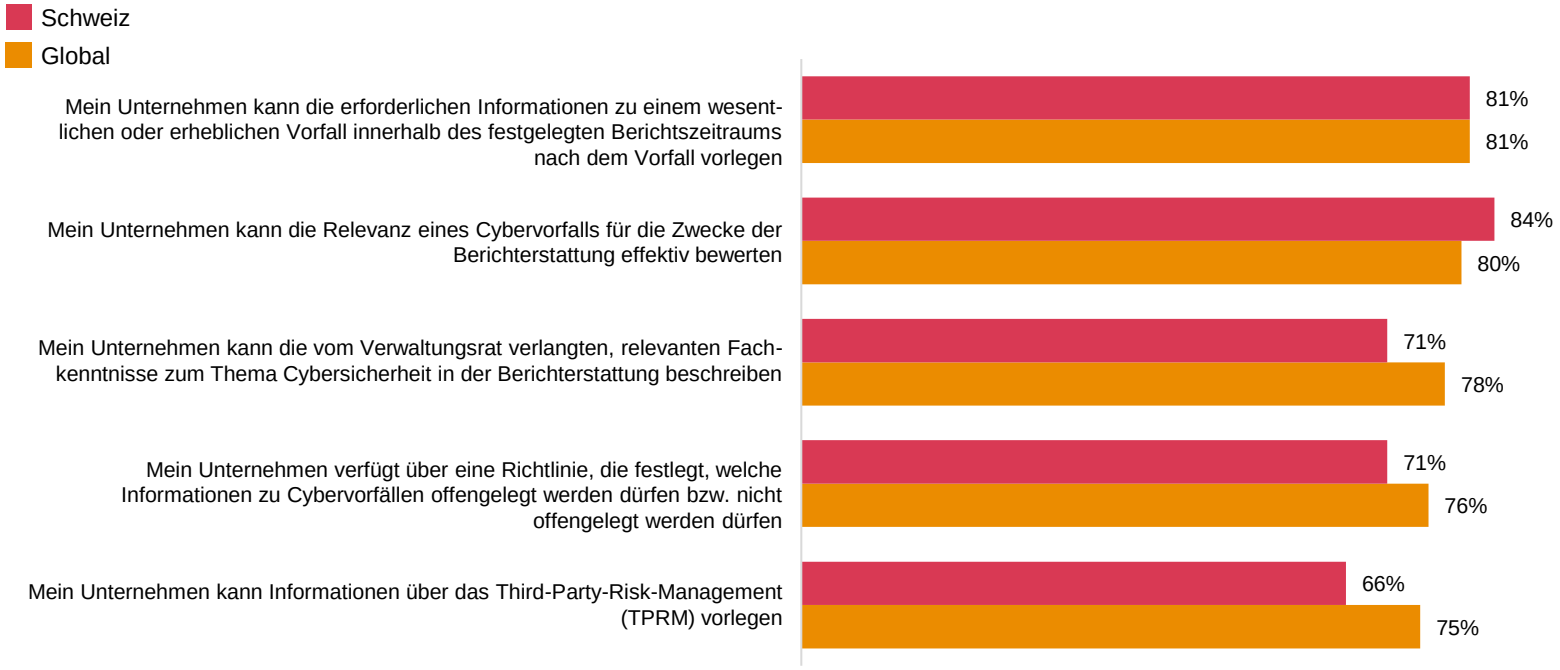
Frage: Mit Blick auf die Berichterstattung an die folgenden Stakeholder stufen Sie bitte jeden Stakeholder nach der Priorität für Ihr Unternehmen in den kommenden zwölf Monaten ein.
Grundlage: 3'522 Antworten | 70 Antworten aus der Schweiz

Weniger als 50% sind der Meinung, dass sie Cyber-Strategien und -Vorfälle effektiv nach aussen kommunizieren können

Weniger als 10% sind bzgl. allen fünf Aussagen zuversichtlich.

Unternehmen, die eine Zunahme an Cybervorfällen beobachten, stimmen den Aussagen signifikant häufiger völlig oder eher zu.

Fähigkeit der Unternehmen, Cyber-Strategien und -Vorfälle nach aussen hin offenzulegen

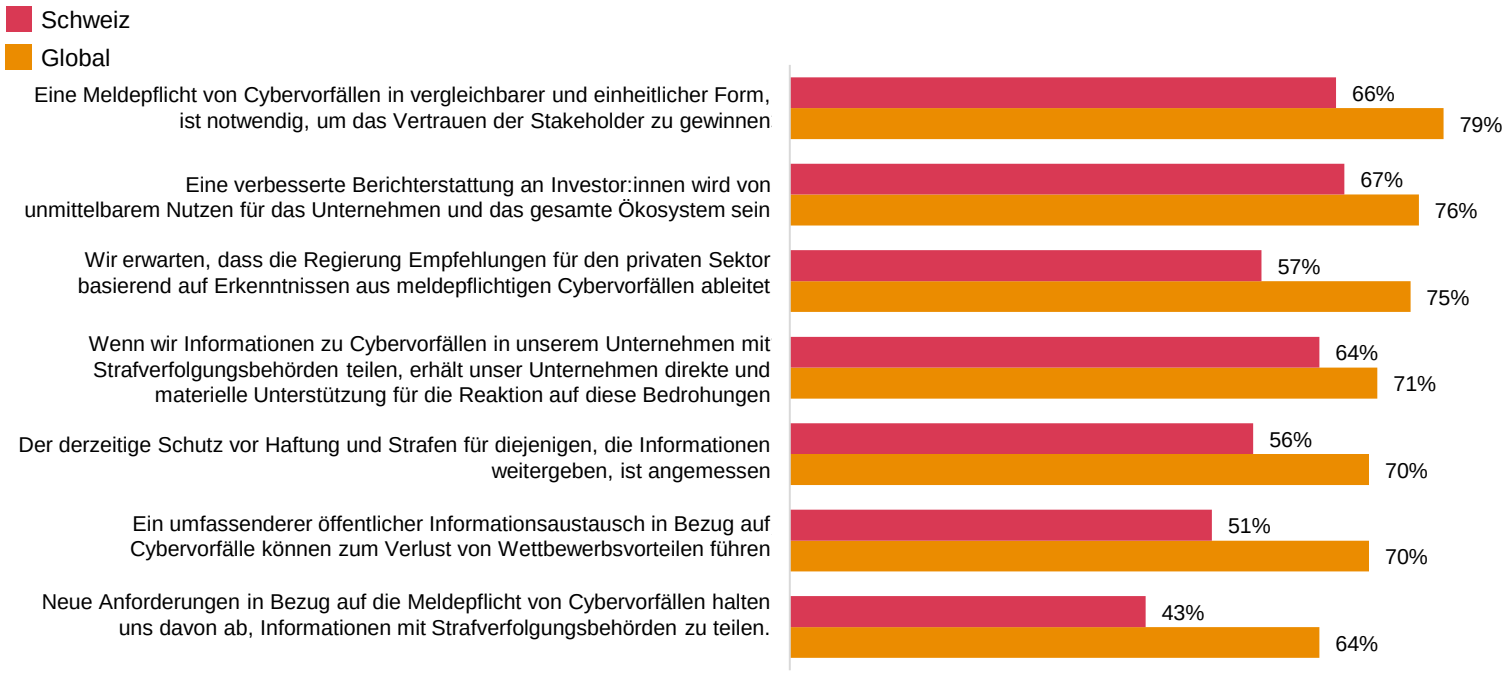


Frage: Bezugnehmend auf die Offenlegung von Cyber-Strategien oder -Vorfällen: Inwieweit stimmen Sie folgenden Aussagen zu bzw. nicht zu?
Grundlage: 3’522 Antworten | 70 Antworten aus der Schweiz
Befragte, die den Aussagen «völlig» oder «eher zustimmen»

Status quo – Offenlegungspraktiken von Cybervorfällen

Vier Fünftel der Unternehmen weltweit sind der Meinung, dass eine obligatorische Offenlegung von Cybervorfällen in vergleichbaren und einheitlichen Formaten notwendig ist, um das Vertrauen der Stakeholder zu gewinnen.

Offenlegungspraktiken von Cybervorfällen



Frage: Die folgenden Aussagen beziehen sich auf die Offenlegungspraktiken von Cybervorfällen: Inwieweit stimmen Sie folgenden Aussagen zur Position Ihres Unternehmens zu bzw. nicht zu?
Grundlage: 3’522 Antworten | 70 Antworten aus der Schweiz
Befragte, die den Aussagen «völlig» oder «eher zustimmen»

Cyber in der C-Suite

Das C-Suite-Playbook zur Cybersecurity und Privacy, gestützt durch die neuesten Ergebnissen unserer «Global Digital Trust Insights» zeigt, wie Führungskräfte zusammenarbeiten müssen, um eine cyberfähige Zukunft zu schaffen.

CISO

+

CEO

+

BOARD

Wo können Sie als CEO oder Verwaltungsratsmitglied am meisten für die Cybersicherheit tun?

51%

der CEOs und Verwaltungsräte fordern einen Plan für das Cyber-Risikomanagement bei grösseren geschäftlichen oder betrieblichen Veränderungen.

Die Digitalisierung macht Sicherheit zu einer Angelegenheit für alle, und dieser Kulturwandel beginnt beim CEO und Verwaltungsrat. Eine Steigerung der Resilienz trotz angespanntem Cyber-Arbeitsmarkt kann nur gelingen, wenn die oberste Führungsebene mit dem CISO als Team zusammenarbeitet.

Call to action:

- Sprechen Sie über Ihr Cyber-Engagement.
- Nutzen Sie Ihren Einfluss, um weitreichende Veränderungen anzuregen.
- Beseitigen Sie organisatorische Hindernisse, welche die die Koordination mit der C-Suite bisher erschwerten.

CISO

+

CIO/CTO

Ist Ihr Cloud-Sicherheitsplan so anpassungsfähig wie es Ihr Unternehmen in der Cloud ist?

19%

der CIOs, CISOs und CTOs sind sich sicher, dass ihr Unternehmen Massnahmen zum Schutz vor vier häufigen Ursachen für Cloud-Angriffen ergriffen hat.

CIOs und ihre DevOps-Teams geben oft das Tempo der Cloud-Einführung vor, aber Sie müssen enger mit Ihrem CISO und den Compliance-Teams zusammenarbeiten, um der C-Suite und dem Verwaltungsrat die Angst vor Cloud-basierten Cybervorfällen zu nehmen.

Fast **zwei Drittel** der Führungskräfte geben an, ihre Cloud-Risiken nicht vollständig reduziert zu haben.

Call to action:

- Zur Sicherung Ihrer Backend-, Frontend-, IoT- und OT-Technologien sollten Sie frühzeitig und immer mit dem CISO zusammenarbeiten.

CISO

+

CFO

Investieren wir genug, und in den richtigen Bereichen? Erzielen wir mit unseren Investitionen das richtige Mass an Risikominderung im Cyberspace?

39%

der CFOs sagen, dass mehr Cybertech-Lösungen zur Verbesserung der Cybersicherheit beitragen werden.

Viele CISOs und CFOs haben die Art und Weise geändert, wie sie in Cybersicherheit investieren. Sie fällen datenbasierte Finanzierungsentscheidungen unter Berücksichtigung der Geschäftsziele und der wichtigsten Risiken.

Wegen der zunehmenden Verbreitung von Technologielösungen müssen Sie gemeinsam mit dem CISO einen holistischen Plan ausarbeiten, um Ihr Unternehmen auf allen Ebenen zu schützen und gleichzeitig die gesamte Unternehmenssoftware zu vereinfachen.

Call to action:

- Bei der Modernisierung und Vereinfachung Ihrer IT sollten Sie sich fragen, wie Sie pro investiertem Franken die effektivste Reduktion Ihrer Cyberrisiken erzielen.

CISO

+

COO

Was können wir tun, um unsere Lieferkette und unsere Betriebsabläufe widerstandsfähiger und weniger anfällig für Cyberangriffe zu machen?

56%

der CROs und COOs sind äusserst oder sehr besorgt, ob ihr Unternehmen Angriffen auf die Lieferkette standhalten kann.

Die Lieferkette ist ein Kernpunkt für Cyber- und andere Bedrohungen, Wettbewerbsdruck, makroökonomische Herausforderungen und ESG-Anliegen. Starten Sie Ihre Sicherheitsinitiativen, indem Sie Ihre Mitarbeitenden schulen, in Technologie investieren und die Drittparteirisiken besser abdecken.

Die wachsende Anziehungskraft der «Operational Technology» (OT) auf Bedrohungsakteure bedeutet, dass Sie diese Technologie besonders gut gegen Angriffe schützen sollten.

Call to action:

- Planen Sie gemeinsam mit dem CISO und dem CIO, wie Sie Ihre OT- und Ihre IT-Systeme sichern können.

CISO

+

CRO

Wie wirkt sich das Cyber-Risikoprofil auf die Risikotoleranz unserer Organisation aus? Wie engagiert sind die Leitenden der einzelnen Geschäftsbereiche im Umgang mit Cyberrisiken?

46%

der CROs und COOs geben an, dass sie in ihrem ganzen Unternehmen Kontrollen haben, die schwerwiegende Cyberstörungen verhindern sollen.

CISOs und CROs arbeiten zusammen, um Cyberrisiken in das allgemeine Risikomanagement (ERM) des Unternehmens einzubeziehen. Aber es gibt immer noch Lücken.

Die fortschreitende Digitalisierung kann zu mehr Risiken führen, als Ihr Unternehmen verkraften kann. Um sich gegen immer raffiniertere Cyberangriffe zu wappnen, sollten Sie solide Pläne und Kontrollen für die betriebliche und technologische Widerstandsfähigkeit erstellen, testen und einführen.

Call to action:

- Überprüfen Sie Ihre Risikobereitschaft.
- Entwickeln Sie ein Resilienzprogramm, das die Kernkompetenzen Krisenmanagement, Betriebskontinuität, Wiederherstellung und Incident Response umfasst, sodass Sie unternehmensweit kohärent reagieren können.

CISO

+

CDO

Wie können wir Kundendaten sicher verwalten und nutzen?

31%

der CDOs, CPOs und CMOs haben eine sehr gute Beziehung zum CISO und berücksichtigen Datenschutz und Sicherheit im Marketing.

Datenverantwortliche (CDOs) müssen sich vielen Herausforderungen stellen, da Daten – im Guten wie im Schlechten – in den Mittelpunkt gerückt sind. Die **Hälfte** der Führungskräfte hat nicht genug Vertrauen in die Datenverwaltung und -sicherheit ihres Unternehmens, um datenbasierte Entscheidungen zu treffen.

Die gute Nachricht: CDOs erhalten immer mehr Verantwortung und Befugnisse für die Datensicherheit und den Datenschutz. Eine Partnerschaft mit Ihrem CISO kann Ihnen helfen, Daten und persönliche Informationen besser zu schützen.

Call to action:

- Arbeiten Sie mit Ihrem CISO zusammen, um die Erwartungen der verschiedenen Stakeholder zu erfüllen und alle wichtigen Aspekte der Datensicherheit und des Datenschutzes abzudecken, einschliesslich Governance, Datenzugang und Genauigkeit der Daten.

CISO

+

CHRO

Wie können wir schneller Cyberfachkräfte rekrutieren und unsere Talente an uns binden?

54%

der CISOs und CIOs sagen, Personalfluktuation sei ein Problem. Etwa **40%** beobachten die Situation genau; **15%** stellen fest, dass Fachkräftemangel den Fortschritt bei den Cyberzielen bremst.

CISOs und CHROs brechen mit alten Mustern und erweitern die Suchparameter für neue Talente über Zertifizierungen und technische Abschlüsse hinaus. Indem sie anerkennen, dass Eigenschaften wie Problemlösungsfähigkeit mindestens genauso wichtig sind, vergrössern sie den Pool ihrer Kandidatinnen und Kandidaten.

In der Zwischenzeit sollten Sie Ihre Mitarbeitenden schulen und «Managed Cyber Defence»-Services in Anspruch nehmen, um die Cybersicherheit Ihres Unternehmens zu gewährleisten.

Call to action:

- Stellen Sie sich die Frage, welche Fähigkeiten Sie in Ihrem Cyberprogramm brauchen, passen Sie Ihre Rekrutierungsmethoden entsprechend an und bieten Sie Ihren Cybertalenten Anreize und Entwicklungsmöglichkeiten, die sie zum Bleiben motivieren.

Notwendigkeit der Kooperation auf C-Level-Ebene

Ein Cyberangriff mit katastrophalen Folgen (z.B. Ransomware, Angriffe von Nationalstaaten auf kritische Infrastruktur) ist das wichtigste Szenario in organisatorischen Resilienzplänen im Jahr 2023. Eine solche Attacke würde die Kooperation sicherlich hart auf die Probe stellen.

38% rechnen im Jahr 2023 mit schwereren Angriffen über cloudbasierte Dienste

Der Vorfall:

Angreifende nutzen eine Fehlkonfiguration in einer in der Cloud gehosteten App des Unternehmens aus und stehlen Nutzerdaten, um sie auf dem Schwarzmarkt zu verkaufen.

Folgen:

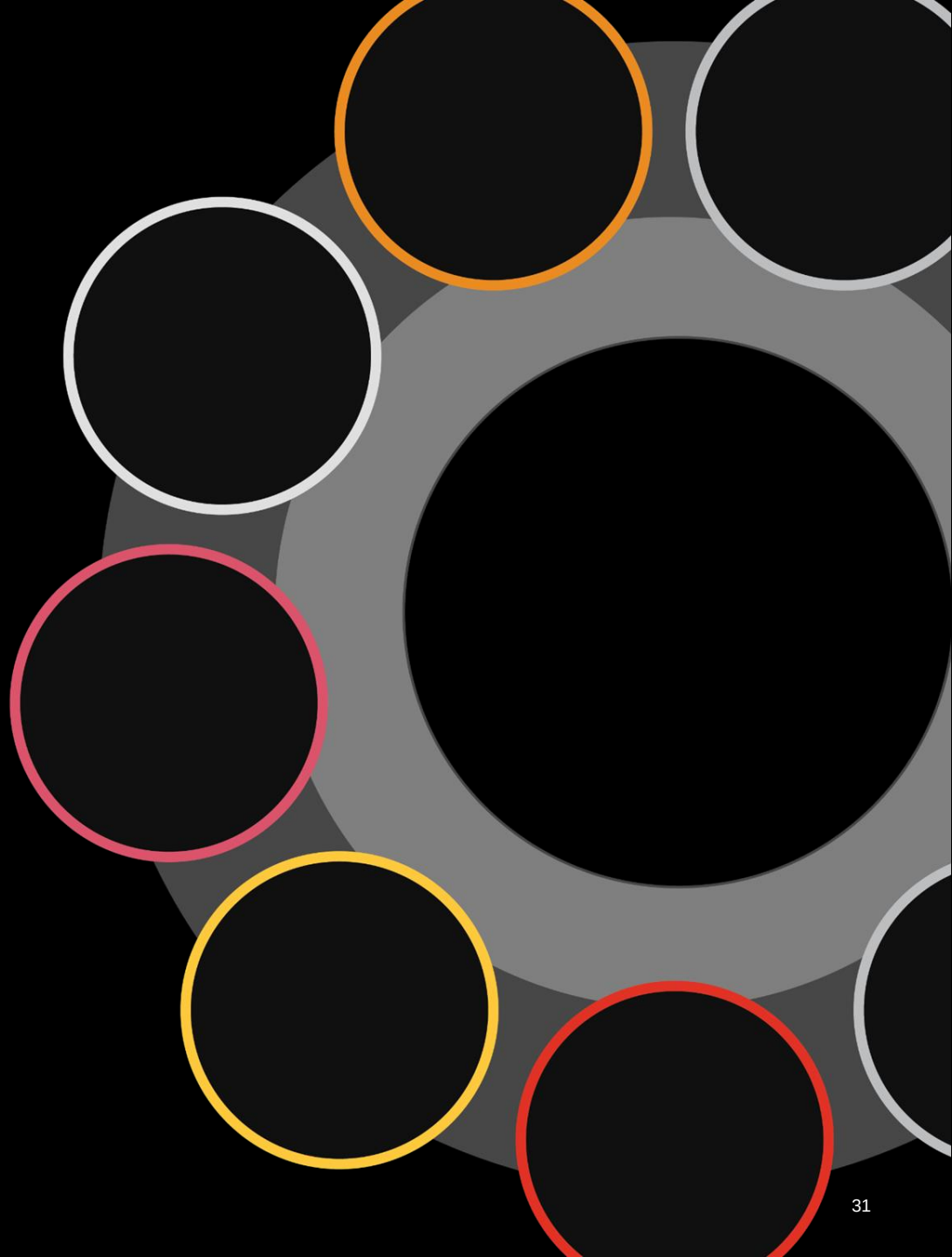
Ressourcen-intensiver und kostspieliger Benachrichtigungs-prozess der Dateneigentümer. Die Opfer könnten eine Sammelklage gegen Ihr Unternehmen einreichen. Der Ruf des Unternehmens leidet.

Was schief lief:

Programmierfehler, unzureichende Tests von Code Libraries, unzureichend verschlüsselte Daten.

Wie grösserer Schutz möglich wird

- **CIO:** Beharren Sie auf «Security-as-Code»-Methodologien bei der Anwendungsentwicklung und führen Sie gründliche Tests vor der Einführung durch. Beseitigen Sie Fehlkonfigurationen, die sowohl von Nutzer:innen als automatischem Deployment ausgehen können.
- **CISO:** Legen Sie Richtlinien und Verfahren fest, die die Anwendungssicherheit erhöhen, Vulnerability Tests und ein regelmässiges Patch Management beinhalten und setzen sie diese konsequent durch.
- **CTO:** Stellen Sie sicher, dass Sie von Cloud-Providern und Drittanbietern Dashboards und Tools zur Verfügung gestellt kriegen, mit denen sie Fehlkonfigurationen in deren Umgebungen leichter erkennen können.
- **CDO:** Stellen Sie sicher, dass Ihre Anwendungen die Datenschutzanforderungen erfüllen und dass Kundendaten partitioniert werden. Nutzen Sie Lösungen, die sicherstellen, dass Daten im Ruhezustand («Data at Rest»), bei der Übertragung («Data in Transit») und während der Nutzung verschlüsselt sind.



29% der grossen Unternehmen rechnen mit einem Anstieg an Angriffen auf OT-Netzwerke

Der Vorfall:

Endgeräte einer Fabrik werden über ein webbasiertes virtuelles Servernetzwerk angegriffen.

Folgen:

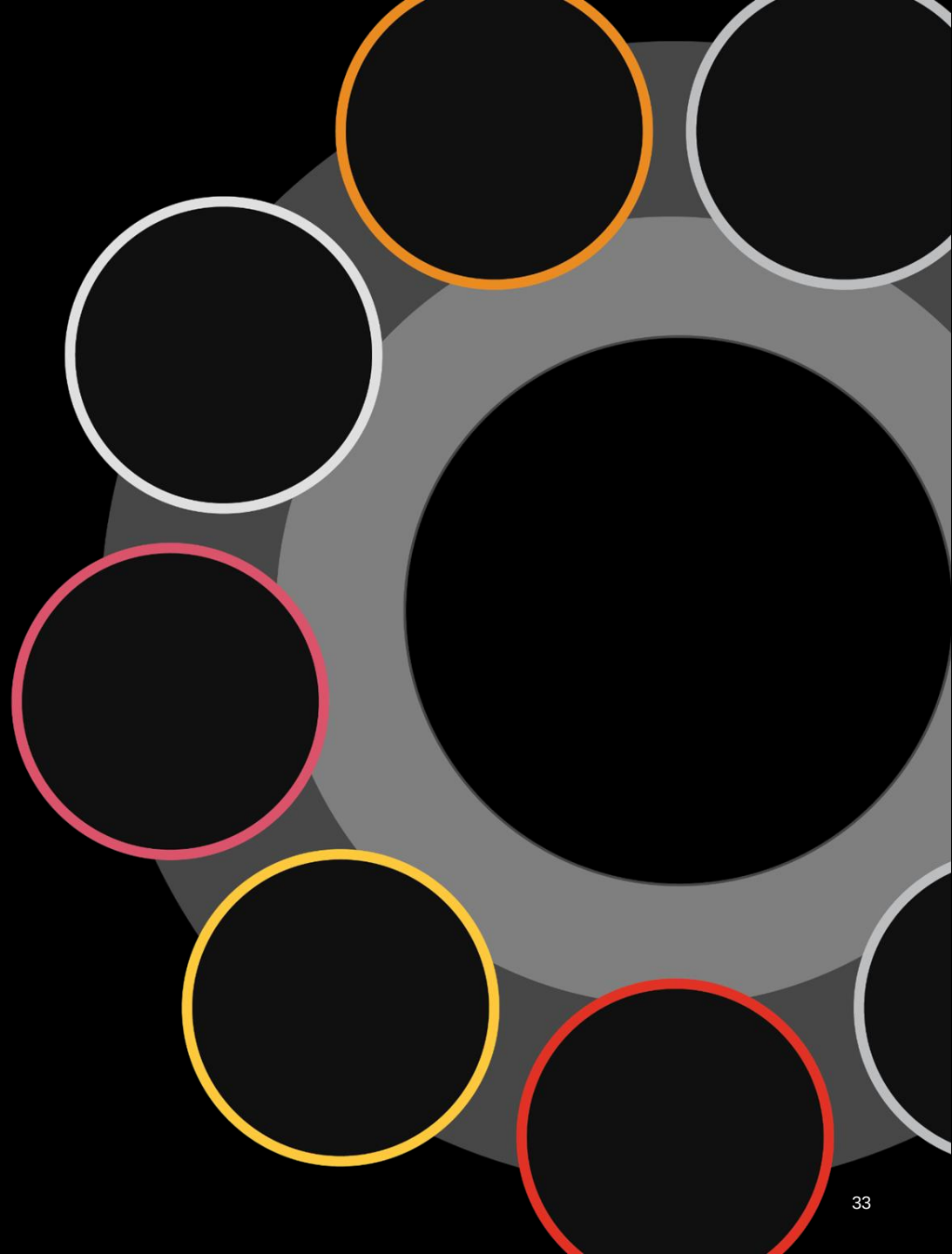
Die Produktion kommt zum Erliegen, da die Systeme heruntergefahren werden müssen, um eine weitere Ausbreitung zu verhindern; die Auswirkungen der Produktions-verzögerungen ziehen sich durch die gesamte Lieferkette.

Was schief lief:

Hacker:innen griffen auf ungeschützte Virtual Network Computing-Server zu, ohne sich authentifizieren zu müssen und konnten so in Systeme eindringen, die industrielle Fertigungsprozesse steuern.

Wie grösserer Schutz möglich wird

- **CIO:** Erfassen Sie zusammen mit dem CTO kritische Abhängigkeiten und Konvergenzen zwischen IT- und OT-Systemen.
- **CISO:** Verlangen Sie Zugriff via VNC oder über ein VPN. Schulen Sie IT- und OT-Mitarbeiter:innen und weiteres Sicherheitspersonal damit Indikatoren für eine mögliche Gefährdung frühzeitig erkannt werden.
- **CTO:** Erstellen Sie gemeinsam mit dem CISO und CIO einen Plan, um das Patch-Management und Monitoring von Endpoints zu verbessern.
- **CRO:** Bewerten Sie die VNC-Risiken. Entwickeln und üben Sie Incident Response-Pläne, die IT- und OT-Prozesse beinhalten.
- **COO:** Berücksichtigen Sie die Cybersicherheit im Beschaffungsprozess für industrielle Steuerungssysteme, bei der Auftragsvergabe an Cloud-Anbieter und bei der Festlegung von Servicevereinbarungen mit externen Dienstleistern.



45% der Sicherheits- und IT-Führungskräfte erwarten einen weiteren Anstieg von Ransomware-Angriffen

Der Vorfall:

Ein medizinischer Angestellter öffnet ein Dokument in einer Phishing-E-Mail und installiert dabei Malware.

Folgen:

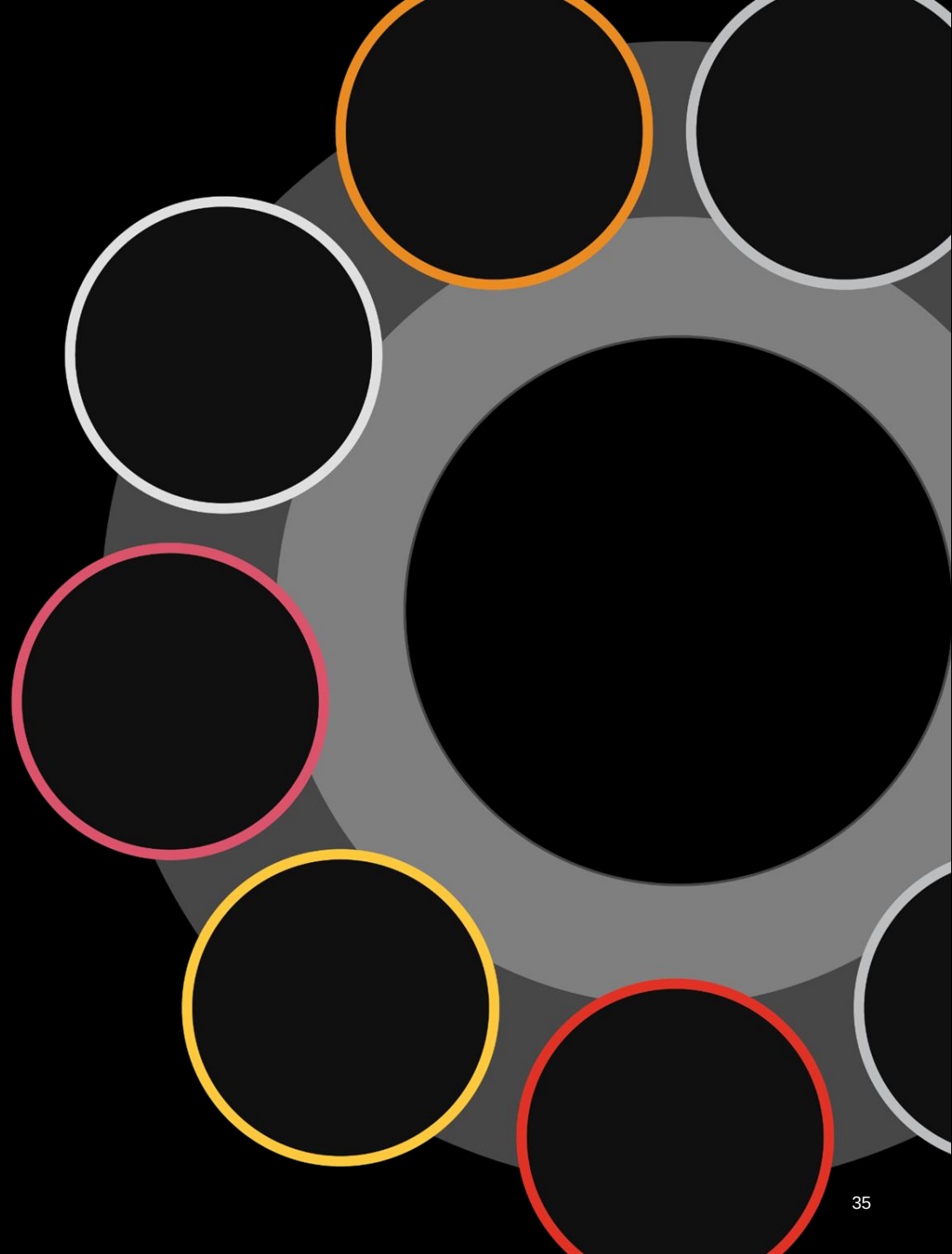
Massive Unterbrechungen und nahezu vollständige Abschaltung der Netzwerke.

Was schief lief:

Die Antivirus-Software war veraltet und hat die im Anhang eingebettete Malware nicht erkannt. Das Fehlen einer Multi-Faktor-Authentifizierung ermöglichte es den Angreifer:innen sich Zugang zum Unternehmensnetzwerk zu verschaffen, in dem sie acht Wochen lang unbemerkt blieben. Schliesslich kompromittierten sie ein Domain-Admin-Konto und verbreiteten weiter Malware, die einen Grossteil der zentralen IT-Infrastruktur lahmlegte und Backups kompromittierte.

Wie grösserer Schutz möglich wird

- **CEO:** Unterstützung von Schulungen zum Sicherheitsbewusstsein in der gesamten Organisation.
- **CIO:** Überprüfen Sie die Zusammenhänge zwischen IT-Systemen und dem Gesundheitsumfeld.
- **CTO:** Bewerten Sie die Anfälligkeit von medizinischen Geräten in einem Szenario.
- **COO:** Helfen Sie dem CIO und CISO bei der Bewertung der Auswirkungen auf die Patient:innensicherheit.
- **CISO:** Überbrücken Sie Sicherheitslücken zwischen der IT und dem Betrieb im Gesundheitswesen.
- **CDO:** Arbeiten Sie mit dem COO, CISO und CPO zusammen, um eine Bewertung des Schadens durch Diebstahl / Beschädigung von Kundendaten zu erstellen.
- **CRO:** Führen Sie Resilienztests mit Krisen- und BC/DR-Teams durch.
- **CFO:** Überprüfen Sie Ihre Ausgaben für die Cybersicherheit, einschliesslich einer Cyber-Versicherung, mit dem CISO und CIO unter Berücksichtigung der entdeckten Schwachstellen. Legen Sie Richtlinien zur Zahlung von Lösegeld fest.
- **Verwaltungsrat:** Fordern Sie Einblicke in die Übungen des Managements zur Vorbereitung auf einen Ransomware-Angriff. Legen Sie fest, wann der VR über einen Cybervorfall informiert werden soll.



Zur Studie

Die Global Digital Trust Insights 2023 sind eine Umfrage unter 3’522 Führungskräften aus den Bereichen Wirtschaft, Technologie und Sicherheit (CEOs, Unternehmensleiter, CFOs, CISOs, CIOs und C-Suite-Verantwortliche), die im Juli und August 2022 durchgeführt wurde. Weibliche Führungskräfte machen 31% der Stichprobe aus.

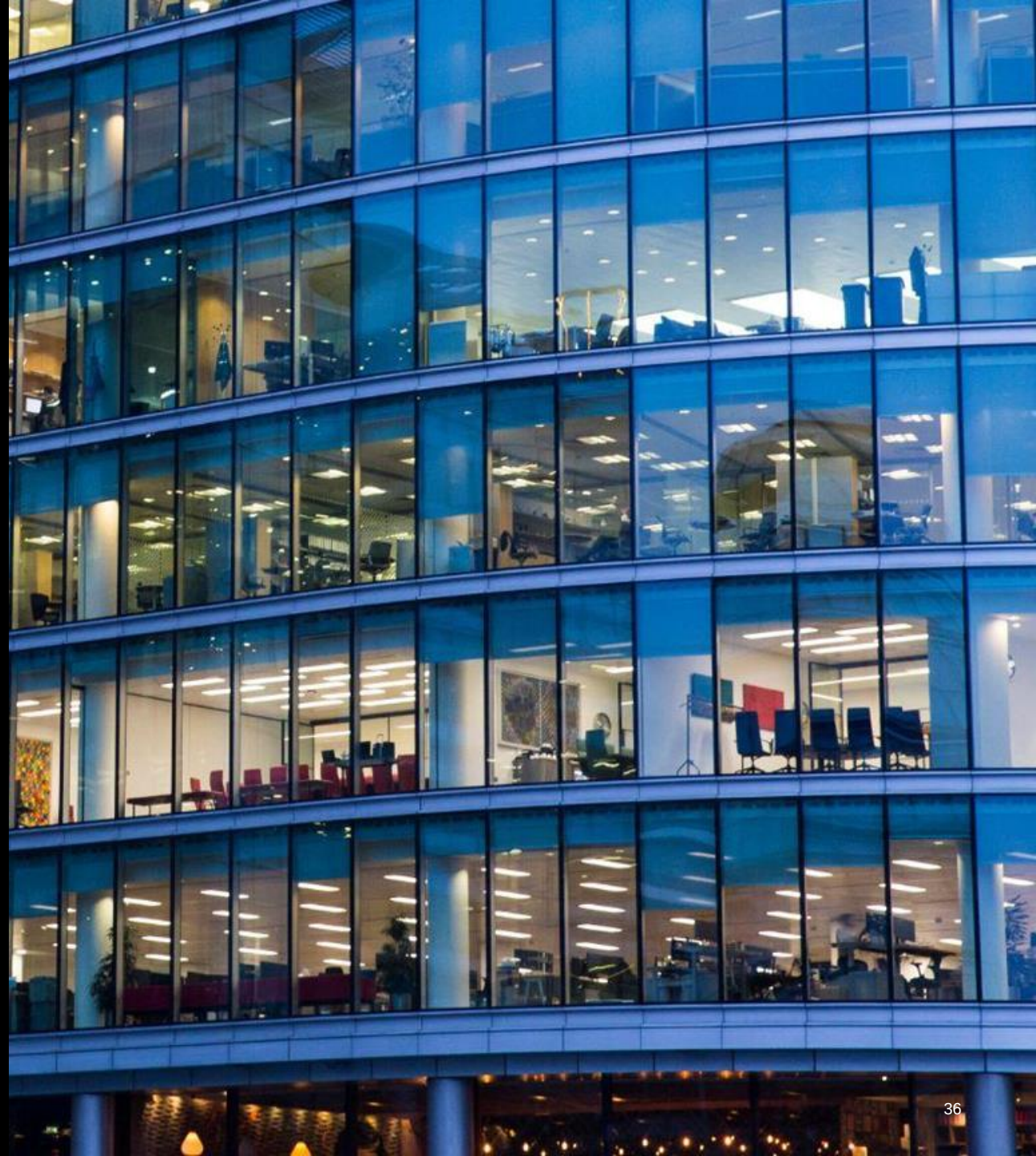
52 Prozent der Befragten sind Führungskräfte in grossen Unternehmen (Umsatz von 1 Milliarde Dollar und mehr); 16% sind in Unternehmen mit einem Umsatz von 10 Milliarden Dollar oder mehr tätig.

Die Befragten sind in einer Reihe von Branchen tätig: industrielle Fertigung (24%), Technologie, Medien, Telekommunikation (21%), Finanzdienstleistungen (20%), Einzelhandel und Verbrauchermärkte (18%), Energie, Versorgungsunternehmen und Ressourcen (9%), Gesundheit (5%) sowie Regierung und öffentliche Dienste (3%).

Die Befragten sind in verschiedenen Regionen ansässig: Westeuropa (31%), Nordamerika (28%), Asien-Pazifik (18%), Lateinamerika (12%), Osteuropa (5%), Afrika (4%) und Naher Osten (3%).

Der Global Digital Trust Insights Survey ist formell als Global State of Information Security Survey (GSISS) bekannt.

PwC Research, das globale Kompetenzzentrum von PwC für Marktforschung und Einblicke, führte diese Umfrage durch.



Kontaktieren Sie uns

Urs Küderli

Partner
Leiter Cybersecurity und Privacy,
PwC Schweiz

Tel: +41 58 792 42 21
urs.kuederli@pwc.ch

Johannes Dohren

Partner
Head of Cyber Resilience and Defence,
PwC Schweiz

Tel: +41 58 792 22 20
johannes.dohren@pwc.ch

Yan Borboën

Partner
Digital Assurance & Cybersecurity und Privacy,
PwC Schweiz

Tel: +41 58 792 84 59
yan.borboen@pwc.ch

Danke
www.pwc.ch/dti2023

pwc.com