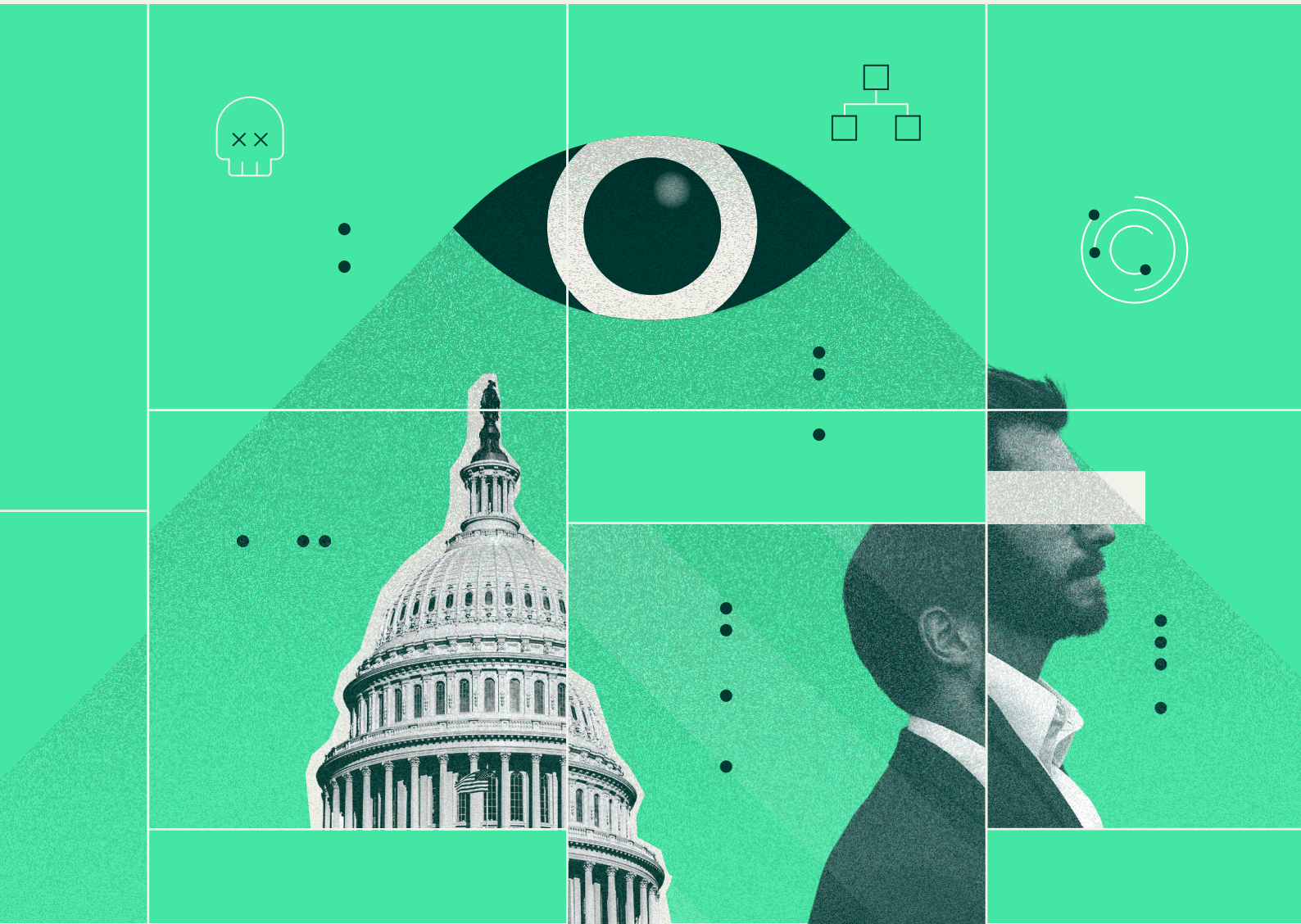
Rubrik Zero Labs

WHITEPAPER

Der Stand der Datensicherheit

Die Auswirkungen von Cyberkriminalität auf Menschen



Inhalt

Dies ist eine Geschichte über Daten und darüber, was auf dem Spiel steht, wenn sie bedroht sind. Es ist auch eine Geschichte über Menschen: die Menschen, die Daten für ihre Arbeit benötigen, die Kriminellen, die diese Daten bedrohen, und die Menschen, welche die Daten schützen.

In diesem ersten von Rubrik in Auftrag gegebenen und von Wakefield Research durchgeführten Bericht von Rubrik Zero Labs erforschen wir auch, wie sich Datensicherheit auf die Menschen auswirkt, die täglich damit zu tun haben.

Rubrik Zero Labs hat es sich zur Aufgabe gemacht, umsetzbare, herstellerunabhängige Erkenntnisse zum Reduzieren von Datensicherheitsrisiken zu liefern. Wir fördern Zero-Trust-Datensicherheit auf Basis realer Bewertungen von Cyberbedrohungen und bewährter Verfahren für Cyberresilienz. Unsere Arbeit legt den Fokus auf drei Hauptpfeiler:

1

Operationalisieren besorgniserregender Befunde
Erstellung proaktiver, umsetzbarer Entscheidungspunkte aus datengestützten Beobachtungen und Trendanalysen.

2

Risikoverringerung
Verringerung und Begrenzung der Bedrohungsmöglichkeiten durch Forschung, öffentliches Engagement, Partnerschaftsbemühungen und technische Änderungen an zentralen Datensicherheitstechnologien oder -verfahren.

3

Verbessern unserer Community
Wir möchten durch detaillierte Recherchen zu Sicherheitsthemen, Modellen und externen Veröffentlichungen als vertrauenswürdiger Berater im Bereich der Datensicherheit agieren.

„Erst zuhören. Dann sprechen.“

Peter Drucker, der Vater modernen Managements, sagte einmal: „Erst zuhören. Dann sprechen.“ In diesem Sinne wollten wir die Rubrik Zero Labs damit eröffnen, dass wir den Menschen zuhören, die sich jeden Tag auf Cyberkriminalität vorbereiten und dagegen vorgehen.

Um ein vollständiges, unvoreingenommenes Bild zu erhalten, haben wir bewusst Meinungen von außerhalb unseres eigenen Kundenkreises eingeholt. Wir haben mit mehr als 1.600 Führungskräften im Bereich der IT und Sicherheit, von denen die Hälfte CIOs und CISOs sind, aus 10 Ländern gesprochen, um zu erfahren, wie sie den Stand der Datensicherheit einschätzen. Anschließend haben wir einige der klügsten Köpfe im Bereich der Cybersicherheit gebeten, diese Antworten einzuordnen, und sie gefragt, was Unternehmen tun können, um ihre Daten besser zu schützen. Unten erfahren Sie mehr über die Daten und die Standpunkte.

1.600+
IT- und Sicherheits-verantwortliche

819
CIOs und CISOs

10
Länder weltweit

Aufschlüsselung der Befragten

Die weltweite Umfrage wurde von Rubrik in Auftrag gegeben und von Wakefield Research unter 1.625 Entscheidungsträgern aus den Bereichen IT und Sicherheit (Vorstandsmitglieder, VPs, CIOs und CISOs) in Unternehmen mit mindestens 500 Mitarbeitern durchgeführt. Die Untersuchung wurde vom 18. bis zum 27. Juli 2022 in den USA, dem Vereinigten Königreich, Frankreich, Deutschland, Italien, den Niederlanden, Japan, Australien, Singapur und Indien durchgeführt.

Stellenebene	241 VP	565 Geschäftsführer	408 CISO	411 CIO
Region	500 USA	625 EMEA	500 APAC	
Unternehmens-größe	366 2500+	505 1000-2499	754 500-999	

1.0 Die Landschaft

1.1
Umfang und Auswirkungen von Cyberangriffen nehmen weiter zu

1.2
Unternehmen verlieren das Vertrauen in ihre Fähigkeit, Angriffen zu widerstehen

1.3
Bekannte Bedrohungen sind nach wie vor die größte Herausforderung

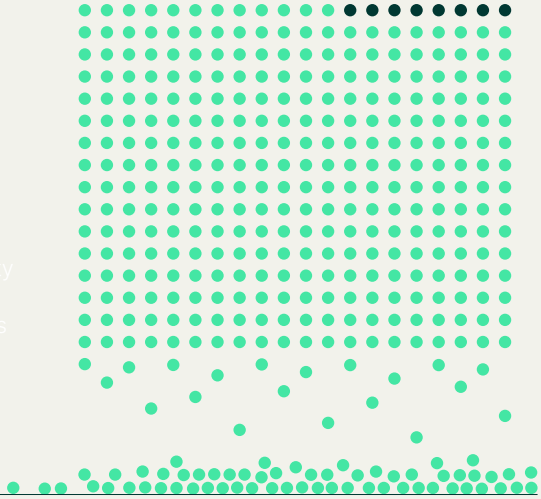
1.1

Umfang und Auswirkungen von Cyberangriffen nehmen weiter zu

Trotz jahrzehntelanger Bemühungen und Investitionen in die Cybersicherheit bleibt es dabei: Die Cyberbedrohungen nehmen nicht ab. Im Gegenteil, sie werden immer schlimmer.

98 %

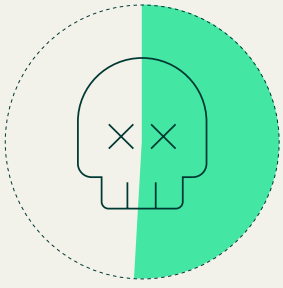
der mehr als 1.600 Führungskräfte in den Bereichen IT und Sicherheit haben angegeben, dass sie im letzten Jahr von einem Cyberangriff erfahren haben.



Im Durchschnitt wurden IT- und Sicherheitsverantwortliche im letzten Jahr 47-mal auf Angriffe aufmerksam gemacht

52 %

der Befragten mussten sich mit einer Datenschutzverletzung auseinandersetzen.



51 %

hatten im gleichen Zeitraum mit Ransomware zu kämpfen.

> Datenschutzverletzungen sind nicht mehr nur die Sache kleiner, interner Teams. Leitende Führungskräfte, ganze Organisationen und die breite Öffentlichkeit wissen inzwischen um derartige Ereignisse und ihre Auswirkungen.

1.2

Unternehmen verlieren das Vertrauen in ihre Fähigkeit, Angriffen zu widerstehen

Sowohl IT- und Sicherheitsverantwortliche als auch die Führungsetage von Unternehmen scheinen an ihrer Fähigkeit zu zweifeln, Bedrohungen zu bekämpfen, während sich die Angriffsfläche vergrößert, Cyberkriminelle immer gewiefter werden und ständig über den neuesten Hacker-Trick berichtet wird.

33 %

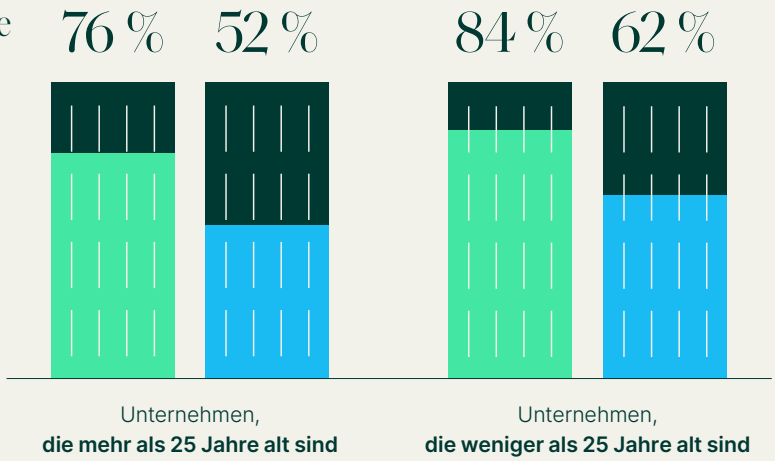
der IT- und Sicherheitsverantwortlichen sind der Ansicht, dass ihr Vorstand und ihre Geschäftsleitung wenig bis gar kein Vertrauen in die Fähigkeit des Unternehmens haben, kritische Daten und Geschäftsanwendungen im Falle eines Cyberangriffs wiederherzustellen.

92 %

der IT- und Sicherheitsverantwortlichen befürchten, dass sie nicht in der Lage sein werden, die Geschäftskontinuität aufrechtzuerhalten, wenn sie Opfer eines Cyberangriffs werden.

Im Hinblick auf Ransomware gaben die Befragten Folgendes an:

- Sie würden in Betracht ziehen, zu bezahlen
- Sie würden mit großer oder sehr großer Wahrscheinlichkeit bezahlen



Wie zuversichtlich ist Ihr Vorstand bzw. Ihre Geschäftsführung in Bezug auf die Fähigkeit des Unternehmens, kritische Daten und Geschäftsanwendungen im Falle eines Cyberangriffs wiederherzustellen?

27 %

Absolut zuversichtlich

40 %

Meist zuversichtlich, aber manchmal skeptisch

33 %

Kaum oder gar nicht zuversichtlich

1.3 Bekannte Bedrohungen sind nach wie vor die größte Herausforderung

Obwohl in der Cybersicherheitsbranche viel von Zero-Day-Angriffen die Rede ist, gab nur etwa ein Drittel der Befragten an, im letzten Jahr einen solchen Angriff erlebt zu haben, und nur wenige sehen darin die größte Bedrohung für das kommende Jahr.

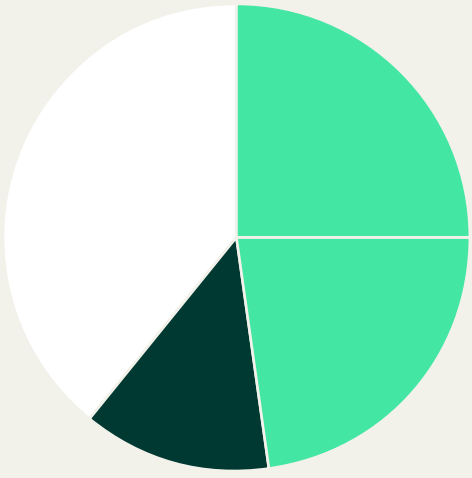
Nur 39 %

der Cyberangriffe auf Ebene der IT- und Sicherheitsverantwortlichen betrafen im letzten Jahr einen Zero-Day-Exploit, was bedeutet, dass bei fast zwei Dritteln der Ereignisse bekannte Schwachstellen ausgenutzt wurden.

11 %

der IT- und Sicherheitsverantwortlichen gaben an, dass sie Schwachstellen aus früheren Ereignissen nicht angemessen behoben haben.

48 % der IT- und Sicherheitsverantwortlichen sehen als größte Bedrohung für nächstes Jahr:



25 %
Datenschutzverletzungen

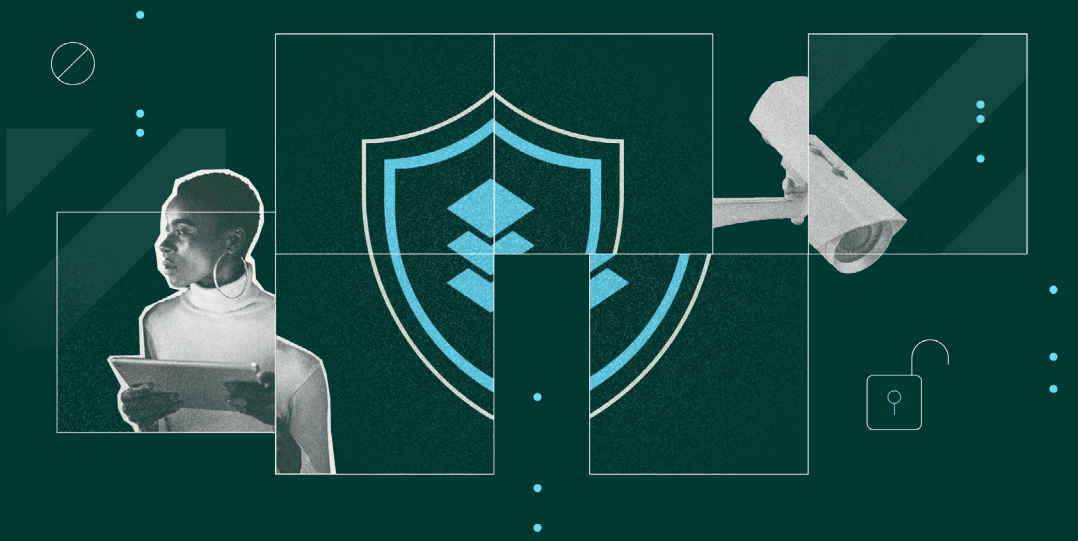
23 %
Ransomware Veranstaltungen

verglichen mit nur

13 %
Zero-Day-Exploits

> Die Kombination aus der zunehmenden Zahl und der wachsenden Bekanntheit von Cyberangriffen, neu auftretenden Bedrohungen und Problemen bei der Lösung bekannter Probleme stellt erhebliche Anforderungen an Mitarbeiter in IT- und Sicherheitsteams.

2.0
Die Realität



2.1
IT- und Sicherheitsverantwortliche benötigen immer noch wichtige Ressourcen zum Sichern ihrer Daten

2.2
Der Druck durch Cyberkriminalität fordert seinen Tribut

2.3
Führungskräfte tun sich schwer mit der umfassenden Umsetzung von Sicherheitsstrategien

2.1

IT- und Sicherheitsverantwortliche benötigen immer noch wichtige Ressourcen zum Sichern ihrer Daten

Die Cybersicherheitsbranche hat seit Jahren mit einem hinlänglich bekannten Fachkräftemangel zu kämpfen. Nach Angaben von Cybersecurity Ventures ist die Zahl der offenen Stellen im Bereich Cybersicherheit um 350 % von 1 Million im Jahr 2013 auf 3,5 Millionen im Jahr 2021 gestiegen. Es überrascht nicht, dass die von Rubrik Zero Labs Befragten den Fachkräftemangel als größte Herausforderung beim Schutz ihrer Organisationen nannten, gefolgt von Tools, Budget und Unterstützung durch die Führungsebene oder den Vorstand.

Welches sind die fünf größten Herausforderungen beim Schutz Ihres Unternehmens vor Cyberangriffen?

1

Fachkräftemangel in den IT- oder SecOps-Teams

2

Fehlen von Instrumenten und Lösungen für die Cybersicherheit

3

Unzureichende Finanzmittel für die Datensicherheit

4

Fehlende Priorisierung der Datensicherheit durch die Führungsebene/den Vorstand

5

Uneinigkeit zwischen verschiedenen Teams darüber, wie man sich vor Cyberangriffen schützen kann

Seit jeher

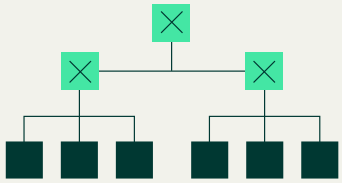
sind Ressourcenknappheiten in kleineren Organisationen stärker ausgeprägt. Kleinere Einrichtungen müssen mit weniger Personal und begrenzten Mitteln gegen dieselben Bedrohungen kämpfen.

2.2 Der Druck durch Cyberkriminalität fordert seinen Tribut

Jahrelanger zunehmender Druck in Verbindung mit einem Mangel an Ressourcen scheint nicht nur Führungskräfte in IT und Cybersicherheit samt ihren Teams zu belasten, sondern auch Unternehmen als Ganzes.

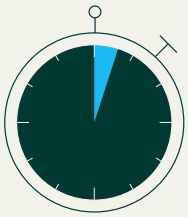
96 %

der IT- und Sicherheitsverantwortlichen berichteten über erhebliche emotionale oder psychische Auswirkungen durch die Sorge um die Sicherheit ihres Arbeitsplatzes und den Vertrauensverlust ihrer Kollegen in sie oder ihr Unternehmen.



Bei 36 %

der Unternehmen, die an unserer Studie teilnahmen, kam es im letzten Jahr aufgrund eines Cyberangriffs und der darauf folgenden Reaktion zu einem Wechsel in der Führungsetage.



Nur 5 %

der Unternehmen konnten innerhalb einer Stunde nach der Erkennung eines Cyberangriffs zur Geschäftskontinuität oder zum normalen Betrieb zurückkehren.

96 % der befragten Unternehmen hatten mit den negativen Folgen eines Cyberangriffs zu kämpfen. Welche Auswirkungen hatte ein Cyberangriff auf Ihr Unternehmen?

42 %
Negative Schlagzeilen und/oder Rufschädigung

41 %
Verlust von Kunden

40 %
Entgangene Einnahmen

36 %
Es kam zu erzwungenen Änderungen in der Führungsetage

5 %
Negative Auswirkungen auf den Aktienkurs

> Burnout von Mitarbeitern, zunehmende Komplexität und eine höchst unbeständige Bedrohungslage belasten die Abläufe und den ohnehin schon kleinen Pool an Fachpersonal erheblich. Da immer mehr Fälle unberechtigten Eindringens bekannt werden, sind die negativen Auswirkungen einer einzelnen Sicherheitsverletzung im gesamten Unternehmen spürbar.

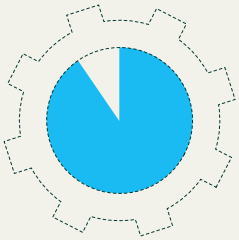
2.3 Führungskräfte tun sich schwer mit der umfassenden Umsetzung von Sicherheitsstrategien

IT- und Sicherheitsverantwortliche haben betont, wie wichtig es ist, IT- und SecOps-Teams besser aufeinander abzustimmen, um effektiv auf Ereignisse zu reagieren und proaktive Verbesserungen vorzunehmen. Branchenführer haben auch Partnerschaften zwischen öffentlichem und privatem Sektor gefordert, um zur Lösung globaler Cybersicherheitsprobleme beizutragen. Die Daten von Rubrik Zero Labs zeigen jedoch, dass es in der Praxis schwieriger ist, im Hinblick auf diese Vorschläge Fortschritte zu erzielen.

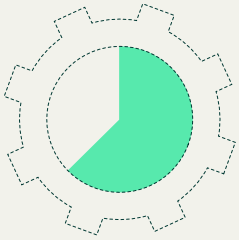
---

31 % der befragten Führungskräfte gaben an, dass ihre IT- und SecOps-Teams entweder nur wenig oder gar nicht aufeinander abgestimmt sind, wenn es um die Verteidigung ihres Unternehmens geht.

der Befragten sind der Ansicht, dass Partnerschaften zwischen öffentlichem und privatem Sektor

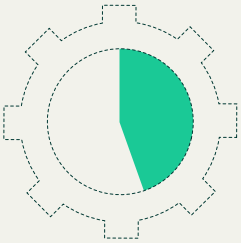


89 %
von Vorteil sind



64 %
von großem Vorteil sind

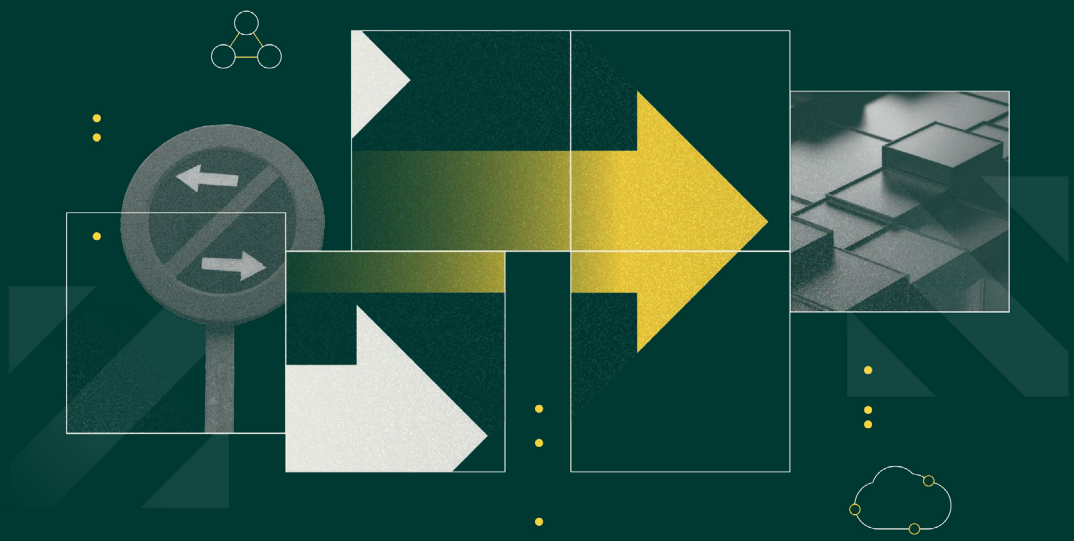
Allerdings gaben weniger als die Hälfte der Befragten an, dass sie an Partnerschaften zwischen privatem und öffentlichem Sektor zum Verbessern der Cybersicherheit beteiligt sind.



44 %
an Partnerschaften zwischen privatem und öffentlichem Sektor beteiligt

> Trotz erheblicher Anstrengungen und Investitionen haben Unternehmen nach wie vor Probleme bei der Umsetzung. Grundlegende Änderungen an Architektur und Prozessen bringen den größten Nutzen, sind aber oft schwer zu bewerkstelligen.

3.0 Die Lösung



3.1 Was sind die nächsten Schritte für IT- und Sicherheitsverantwortliche?

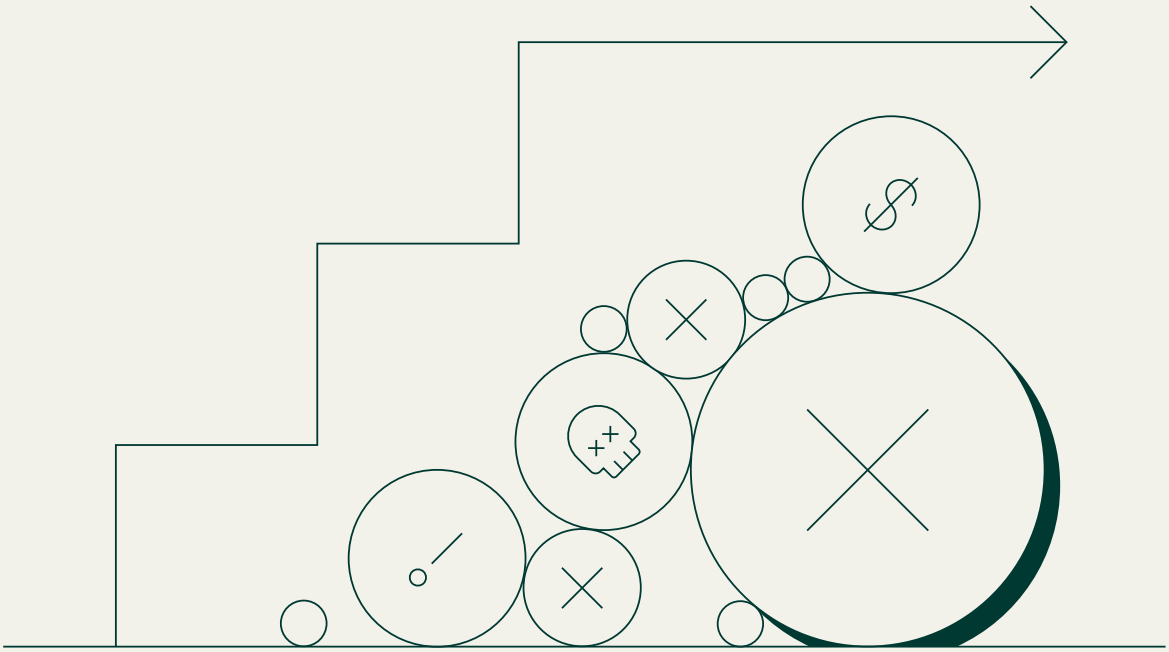
3.2 Best Practices

3.1 Was sind die nächsten Schritte für IT- und Sicherheitsverantwortliche?

Die Untersuchungen von Rubrik Zero Labs zeigen, dass IT- und Sicherheitsverantwortliche weiterhin mit einer wachsenden Liste von Herausforderungen konfrontiert sind, wenn es darum geht, die Daten ihres Unternehmens vor Cyberangriffen zu schützen.

Was können sie tun (falls sie überhaupt etwas tun können), um die Herausforderungen zu bewältigen, mit denen sie konfrontiert sind?

Vorreiter und Koryphäen auf dem Gebiet der Cybersicherheit gaben ihre fachlichen Empfehlungen zur Bewältigung der Bedrohungslage ab. Sie bestätigten, wie ernst die Lage ist, und schlugen drei wichtige Best Practices vor, die Unternehmen anwenden können, um sich und ihre Daten zu schützen.



3.2 Best Practices

1 Die Reaktionsfähigkeit im Hinblick auf Datenschutzverletzungen muss *wöchentlichen* Angriffen standhalten

IT- und Sicherheitsverantwortliche haben gemeldet, dass sie letztes Jahr im Durchschnitt auf 47 Cyberangriffe auf ihr Unternehmen aufmerksam gemacht wurden. Das ist fast ein Angriff pro Woche. Da es unwahrscheinlich ist, dass diese Häufigkeit abnimmt, müssen diese IT- und Sicherheitsverantwortlichen jede Woche in der Lage sein, diese Ereignisse zu bewältigen. Nach jedem Vorfall sollten Unternehmen ihre Pläne für die Cyber-Reaktionsfähigkeit und das Krisenmanagement schnell überarbeiten, um die Cyberresilienz im Laufe der Zeit zu verbessern. Diese Verbesserungen werden die jeweiligen Teams in die Lage versetzen, den Betrieb schneller und zuverlässiger wiederherzustellen und dafür zu sorgen, dass jede folgende Sicherheitsverletzung weniger negative Folgen hat.

An der Schaffung eines kollaborativen Prozesses, bei dem die gewonnenen Erkenntnisse aus jeder Sicherheitsverletzung zum Verbessern der Reaktion auf die nächste genutzt werden, müssen sich nicht nur das IT- und das Sicherheitsteam beteiligen, sondern auch andere Teams. Die Rechtsabteilung, die Personalabteilung und das Kommunikationsteam, um nur einige zu nennen, müssen Zeit und Mühe aufwenden, damit diese Art der Zusammenarbeit funktioniert.

> Die Frage lautet nicht mehr, ob ein Cyberangriff Ihr Unternehmen treffen wird, sondern wann. Gute Vorbereitung kann Ihre Geheimwaffe sein. Führungskräfte müssen nicht nur eine Reaktionsstrategie entwickeln, sondern diese auch in die Praxis umsetzen, damit im Falle eines Angriffs das richtige Team sowie die richtigen Lösungen und Prozesse eingesetzt werden, um ihr Unternehmen schnell wieder Betriebsbereit zu machen."
>
> **John W. Thompson**
> ehemaliger Vorstandsvorsitzender bei Microsoft, ehemaliger CEO bei Symantec

> Um auf einen Cyberangriff zu reagieren, müssen nicht nur das IT- und das Sicherheitsteam zusammenarbeiten, sondern auch Führungskräfte aus allen Abteilungen. Um auf einen Cyberangriff vorbereitet zu sein, ist jedoch nicht nur Zusammenarbeit, sondern auch ständige Schulung und Übung nötig. Sicherzustellen, dass ein gut durchdachter Plan für die Datensicherheit und -wiederherstellung vorhanden ist, ist ein grundlegender Schritt, um das Unternehmen widerstandsfähig zu machen und dafür zu sorgen, dass der Betrieb uneingeschränkt aufrechterhalten werden kann."
>
> **Michael Mestrovich**
> CISO von Rubrik, ehemaliger CISO der Central Intelligence Agency (CIA)

3.2 Best Practices

2 Führungskräfte müssen *mehr von ihren Daten erwarten*

Daten werden bei einem Cybervorfall oft als passives Opfer behandelt. Durch den Einsatz von Technologien zur Datenbeobachtung können Unternehmen jedoch selbst Datenbestände nutzen, um ihr Cyberrisiko zu senken und die Reaktionszeiten auf Vorfälle zu verkürzen.

Zu den wichtigsten Fragen, die sich IT- und Sicherheitsverantwortliche stellen sollten, gehören:

- Wie viele Daten erstellt und verwaltet mein Unternehmen?
- Welche Daten sind sensibel oder enthalten personenbezogene Informationen (PII)?
- Wo sind diese Daten gespeichert?
- Wer kann darauf zugreifen?
- Welche Daten haben die stärksten Auswirkungen auf das Unternehmen?
- Verfügt mein Unternehmen über die richtigen Technologien und Prozesse, um Richtlinien auf Basis von Datenvolumen, Wichtigkeit, Sensibilität und Zugriff umzusetzen?
- Welche unterstützenden Systeme sind für den Zugang zu diesen Daten entscheidend und in welcher Reihenfolge kommen sie zum Einsatz?
- Wie schnell können Sie Antworten auf Ihre Datenfragen finden?

Diese Fragen können in einem Geschäftsumfeld, in dem Mitarbeiter weiterhin remote arbeiten und Unternehmen immer mehr zu hybriden Umgebungen übergehen, schwer zu beantworten sein. Sie helfen Unternehmen aber auch, auf Datenschutzverletzungen zu reagieren und die Widerstandsfähigkeit in einer Vielzahl von Situationen zu verbessern, z. B. bei Katastrophen, böswilligen Insidern und versehentlichen Datenverlusten.

> Um sich gegen moderne Cyberbedrohungen zu verteidigen, müssen IT- und Sicherheitsverantwortliche ihre Daten genau kennen und wissen, wer Zugang zu ihnen hat, wo sie sich befinden und ob sie sensible Informationen enthalten. Böswillige Akteure sind darauf spezialisiert, aus blinden Flecken Kapital zu schlagen, und IT- und Sicherheitsteams sind ihren Kunden gegenüber verpflichtet, solchen Akteuren immer einen Schritt voraus zu sein."
>
> **Asheem Chandna**
> Partner, Greylock Partners

> Der Schutz Ihres Unternehmens und Ihrer Daten ist eine Frage der grundlegenden Resilienz. Und Resilienz entsteht durch die Sicherung Ihrer Daten. Sollten bei einem Cyberangriff herkömmliche Verteidigungslinien durchbrochen werden, haben Sie, wenn Ihre Daten sicher sind, die Möglichkeit, Ihre Unternehmensdaten schnell wiederherzustellen und erfolgreich aus der Situation hervorzugehen."
>
> **Shay Reddy**
> CISO, Hanna Andersson

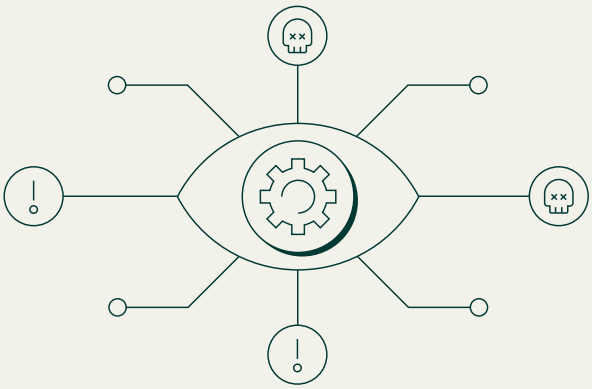
3.2 Best Practices

3 Teilen Sie Erkenntnisse über Cyberrisiken und Bedrohungen *teamübergreifend*

Die Daten von Rubrik Zero Labs zeigen, dass die Mehrheit der Befragten davon ausgeht, dass ihnen in Zukunft weniger Ressourcen zur Verfügung stehen werden, was auf eine Reihe von Faktoren zurückzuführen ist, darunter wirtschaftliche Unsicherheit, knappere Budgets, konkurrierende Prioritäten und globale geopolitische Faktoren.

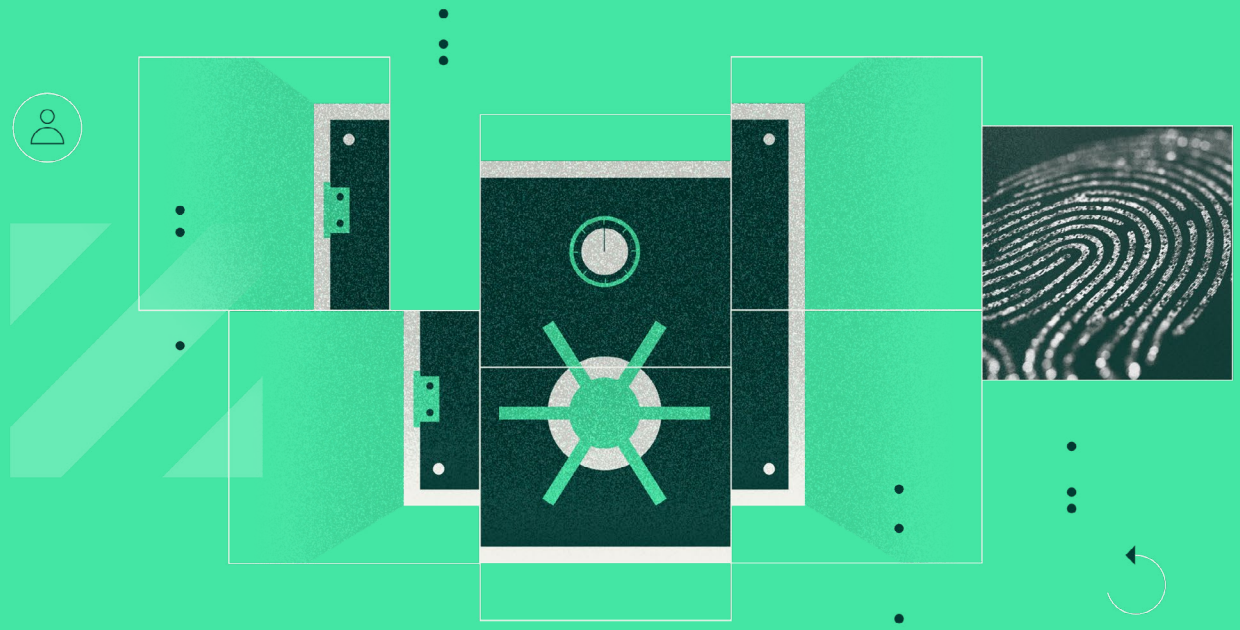
Diese zunehmenden Stressfaktoren machen es wichtiger denn je, dass Teams funktionsübergreifend agieren und eine gemeinsame Sicht auf ihre Daten haben. Bessere Zusammenarbeit, die durch teamübergreifende Transparenz ermöglicht wird, ist besonders wichtig bei einem Cybervorfall, bei dem eine schnellere Reaktion und Wiederherstellung notwendig ist, um die Kontinuität des Geschäftsbetriebs sicherzustellen, aber auch um Routinearbeiten zu erledigen.

Je mehr Teams in einem Unternehmen dieselben Tools, dieselben Prozesse und dieselbe Transparenz anwenden, desto besser können entsprechende Entscheidungen getroffen und in großem Umfang angewendet werden.



> Wir übersehen oft die psychologische Dimension von Cyberangriffen und vom Chaos, das oft auf die Entdeckung eines Vorfalls folgt. Die Angreifer allerdings sind sich darüber völlig im Klaren. Sowohl Kriminelle als auch von Staaten beauftragte Akteure versuchen gleichermaßen, bei ihren Angriffen emotionale Reaktionen hervorzurufen, wie die Zunahme krimineller Erpressungsversuche und von Hacking- und Datenleck-Kampagnen zeigt. Letztendlich wird die Schuld für diese Cyberangriffe meist IT- und Sicherheitsverantwortlichen gegeben. Eine der wirksamsten Techniken zur Vorbereitung auf diese Art von Angriffen, die ich bisher gesehen habe, besteht darin, zu akzeptieren, dass Sie irgendwann einen schlimmen Tag erleben werden, und Ihre Aufgabe darin zu sehen, dafür zu sorgen, dass dieser Tag nicht zu einem „noch schlimmeren Tag" wird. Deshalb müssen Verteidiger aus allen Bereichen zusammenkommen und sich über bewährte Verfahren, Erfahrungen aus Angriffen, Simulationen und Frameworks austauschen, damit wir gemeinsam unsere Abwehr stärken und die psychologischen Auswirkungen eines Angriffs minimieren können."
>
> **Chris Krebs**
> ehemaliges Vorstandsmitglied von CISA und Gründungspartner der Krebs Stamos Group

Zusammenfassung



Sichern Sie Ihre Daten im **Kampf gegen Cyberkriminalität**

Cyberkriminalität stellt für viele Unternehmen eine ständige Bedrohung dar, obwohl viel Zeit und Ressourcen für den Schutz von Daten, Anwendungen und Infrastruktur aufgewendet werden. IT- und Sicherheitsverantwortliche brauchen Unterstützung in Form von Aufmerksamkeit und Unterstützung durch die Geschäftsleitung, finanziellen Mitteln und Mitarbeitern.

All dies reicht jedoch noch nicht aus.
Unternehmen müssen ihre eigenen Datenbestände im Kampf gegen Cyberkriminelle nutzen, um ihre Daten verwertbar zu machen, sie zu schützen und sie einfacher, sicherer und schneller wiederherzustellen.

Rubrik Zero Labs