DATENSICHERHEIT: EINE BESTANDSAUFNAHME

Messung Ihres DATENRISIKOS

Rubrik Zero Labs

INHALT

Dies ist eine Geschichte über

Es geht um verschiedene Datenarten, wie Daten sich ändern und um eine pragmatische Sichtweise auf Datenbedrohungen.

Es ist auch eine Geschichte über Risiken. Wie wir sie messen, inwieweit wir sie einplanen können, wie sie sich ändern und warum sie nie ganz verschwinden.

Doch zuerst möchten wir erklären, ***wer wir sind und was wir tun.***

DATEN UND METHODOLOGIE

Rubrik Zero Labs bietet praxistaugliche, anbieterunabhängige Einblicke und Empfehlungen zur Minderung von Datensicherheitsrisiken. Dazu kombinieren wir hauptsächlich Ergebnisse aus vier Quellen:

RUBRIK TELEMETRIE = ◆
Wir nutzen Telemetriedaten von Rubrik, um uns ein Bild vom Datenbestand eines typischen Unternehmens und den damit einhergehenden Risiken zu machen.

WAKEFIELD RESEARCH = ▲
Ansichten von über 1.600 IT- und Sicherheitsmanagern

RUBRIK PARTNER = ●
Forschungsergebnisse und Empfehlungen von zwei unserer Partnerorganisationen

BEITRAGENDE ORGANISATIONEN = ■
Forschungsergebnisse renommierter Cyber-Sicherheitsunternehmen und -institutionen

RUBRIK TELEMETRIE ◆

Wir bei Rubrik Zero Labs sind der Meinung, dass wir allen Organisationen, die uns ihre Daten anvertrauen, Transparenz bezüglich der Rückschlüsse schulden, die wir aus ihren Daten ziehen. Apropos Transparenz: Unten sehen Sie, woher unsere Telemetriedaten stammen und wie sie unsere Perspektive beeinflussen.

Hinweis: In diesem Bericht verwenden wir erstmals Daten von Laminar. Laminar ist eine führende Datensicherheitsmanagementplattform, die 2023 von Rubrik übernommen wurde.

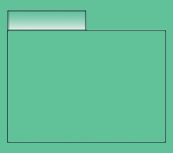
RUBRIK TELEMETRIEDATEN UMFASSEN:

> 6.000 Kunden

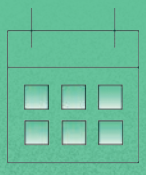
68 Länder

42 EB gesichert mit über 38,4 Mrd. sensiblen Datensätzen

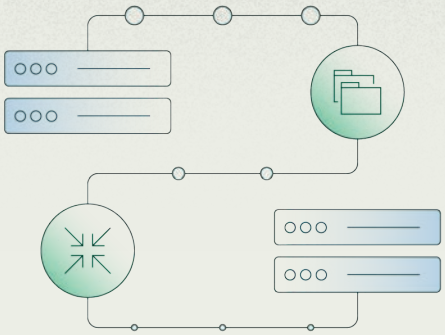
Gesamtvolumen der gesicherten Daten:
- 42 Exabyte logischer Speicher
- 963 Backend-Petabyte (BEPB) physischer Speicher



> 38,4 Mrd. sensible Datensätze



Daten für den Zeitraum von 1.1.2023 bis 31.12.2023



EB und BEPB

Eine Anmerkung von den Datengurus: Wenn Sie das Wort „Daten“ hören, denken Sie wahrscheinlich (wie die meisten anderen Menschen) an logischen oder auch Frontend-Speicher. Wir hier im Datensektor konzentrieren uns jedoch auf Backend-Speicher. Rubrik nimmt sämtliche Daten eines Unternehmens und reduziert das Volumen dieses Frontend-Speichers mit einer Reihe verschiedener Methoden (wie Deduplizierung und Komprimierung) zum sogenannten Backend-Speicher. In diesem Bericht nutzen wir durchweg Backend-Speicher.

Wie viel sind 42 EB?

Stellen Sie sich Ihre Patientenakte mit sämtlichen Formularen, Bildern (Röntgen-, MRT- und sonstigen Aufnahmen), Notizen und allen anderen Daten vor. Wenn Sie diesbezüglich irgendwo im Mittelfeld liegen, enthält Ihre elektronische Patientenakte rund 80 MB Daten.

Wenn die 42 EB der von Rubrik gesicherten Daten nur aus elektronischen Patientenakten bestehen würden, wären das fünf solcher Akten für jeden der 117 Milliarden Menschen, die während der gesamten Geschichte der Menschheit auf der Erde gelebt haben. Also ... eine Menge

WAKEFIELD RESEARCH

Wir haben mit Wakefield Research zusammengearbeitet, um zusätzliche Informationen von IT- und Sicherheitsmanagern zu erlangen. Die Ergebnisse dieser Studie ergänzen unsere Telemetriedaten, sodass wir nun sowohl die Meinungen dieser Führungskräfte als auch die von ihnen beobachtete Realität analysieren können. Im Interesse der größtmöglichen Objektivität sind in diesem Datensatz keine Kunden von Rubrik enthalten.

> 1.600 IT- und Sicherheitsmanager

10 Länder

> 50 % CIOs oder CISOs

1.625

Entscheidungsträger in Unternehmen mit mindestens 500 Angestellten in zehn Ländern (Deutschland, USA, Frankreich, Italien, Niederlande, Vereinigtes Königreich, Japan, Australien, Singapur, Indien) in drei Regionen (Amerika, EMEA und APAC)

50 % CIOs oder CISOs

50 % IT-Entscheidungsträger

50 % Direktoren oder VPs

50 % Sicherheitsentscheidungsträger

RUBRIK PARTNER

Zwei unserer Partner haben uns mit Datensätzen und Empfehlungen zur kontinuierlichen Verbesserung der Datenresilienz unterstützt.

Microsoft

Von Microsoft haben wir Daten aus dem Microsoft Digital Defense Report 2023[1] erhalten, insbesondere zu Datenausschleusungsraten und Empfehlungen zur Resilienzsteigerung.

AON

Aon hat Daten aus dem 2023 Aon Cyber Resilience Report[2] beigesteuert, insbesondere zu Backups in der Praxis und den langfristigen Konsequenzen von Angriffen.

BEITRAGENDE ORGANISATIONEN

Verschiedene Organisationen haben wichtige Daten beigesteuert, die eine andere Perspektive bieten als die Telemetriedaten von Rubrik und das Gesamtbild damit objektiver gestalten.

MANDIANT
NOW PART OF Google Cloud

Mandiant hat Untersuchungsergebnisse zur Verweildauer aus seinen Incident-Response- und MDR-Einsätzen im gesamten Verlauf des Jahres 2023[3] mit uns geteilt.

UNIT 42
BY PALO ALTO NETWORKS

Palo Alto Networks Unit 42 hat uns Informationen über Lösegeldforderungen und -zahlungen bei Ransomware-Angriffen zur Verfügung gestellt, die 2023 zu Incident-Response- oder MDR-Einsätzen geführt haben.

proofpoint.

Von Proofpoint haben wir Informationen aus dem 2023 Human Factors Threat Report[4] zu gezielten Cloud-Angriffen erhalten.

Recorded Future®

Recorded Future hat uns über öffentlich bekanntgegebene Ransomware-Trends 2023[5] informiert.

UNIVERSITY OF MINNESOTA

Die University of Minnesota Twin Cities - School of Public Health hat Informationen über die Auswirkungen von Ransomware-Angriffen auf Einrichtungen des Gesundheitswesens bereitgestellt. Diese beruhen auf dem vor Kurzem veröffentlichten Forschungsbericht „Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients“[6], der sich derzeit in der abschließenden Peer-Review-Phase befindet.

1 https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
2 https://www.aon.com/2023-cyber-resilience-report/
3 https://www.mandiant.com/m-trends
4 https://www.proofpoint.com/us/resources/threat-reports/human-factor
5 https://therecord.media/ransomware-tracker-the-latest-figures
6 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292

ZUM THEMA: RISIKO

Einige grundsätzliche Anmerkungen zum Ansatz dieser Studie

ERSTENS

Wir haben die „Risikomathematik“ vereinfacht:

Wie wahrscheinlich ist es, dass externe Akteure an Ihre Daten gelangen? + Welche Risiken schlummern derzeit in Ihren Daten? + Welche Konsequenzen könnte das haben? + Wie reagieren Sie auf diese Auswirkungen? = Unsere Risikomathematik

MEHR MATHE BRAUCHEN WIR NICHT!

ZWEITENS

Wir konzentrieren uns auf Daten
Als Datensicherheitsunternehmen kennen wir uns erheblich besser mit den Daten von Organisationen aus als zum Beispiel mit ihrer Infrastruktur oder Architektur. Deshalb konzentrieren wir uns in diesem Bericht auf die Risiken in Ihren Daten und für Ihre Daten.

Schwerpunktbereiche
Seien wir ehrlich. Sie haben genug zu tun. Niemand von uns hat Zeit, sich detailliert mit jedem Aspekt der Datensicherheit zu befassen. Deshalb haben wir uns bei dieser Untersuchung bewusst auf einige wichtige Themen beschränkt:

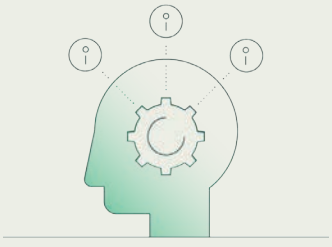
Cloud
Kommerzielle Cloud-Angebote gibt es mittlerweile seit mehreren Jahrzehnten. Trotzdem besteht vielerorts noch Unklarheit bezüglich der Datensicherheit in Clouds. Cloud-Umgebungen werden häufiger – und erfolgreicher – angegriffen als vergleichbare On-Premises-Umgebungen. Und sie enthalten tote Winkel, die ihren Schutz erschweren.

Ransomware
Vor nicht allzu langer Zeit sagten Experten einen Niedergang der Ransomware voraus. Dieser blieb jedoch aus und Ransomware verursacht weiterhin großen Schaden in Organisationen aller Art.

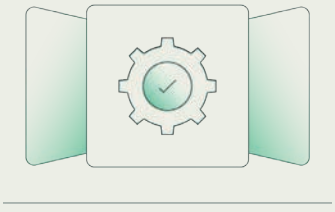
Gesundheitswesen
Sehr wenige andere Organisationen generieren und speichern so viele sensible Daten wie Einrichtungen des Gesundheitswesens und werden dabei so intensiv gesetzlich reguliert und überwacht. Ein positiver Nebeneffekt sind die vergleichsweise großen Mengen öffentlich verfügbarer Daten aus dieser Branche, die wir analysieren können.

DRITTENS

An wen richtet sich diese Studie?



Informationen sollten die richtigen Entscheidungsträger erreichen und Entscheidungen zu Risiken werden gewöhnlich von Managern in gehobenen Positionen getroffen.



Unser Ziel ist daher, diese Entscheidungsträger (ob in den Geschäftsbereichen, der Cyber-Sicherheit oder der IT) zu informieren und zu unterstützen.

Wir möchten eine Ausgangsbasis schaffen, von der aus diese Entscheidungsträger Risken gemeinsam angehen können.

EIN KURZER BLICK AUF DIE MENSCHLICHE SICHTWEISE AUF RISIKEN

Menschen kommen mit Ungewissheit nur schwer zurecht. Wenn wir hören, dass etwas geschehen könnte, denken wir gern entweder in die eine oder in die andere Richtung:

Eine Regenwahrscheinlichkeit von 52 %
im Wetterbericht heißt weder
„Ja, es wird regnen“ noch „Nein, es wird nicht regnen.“

Dabei wüssten wir eigentlich gern viel mehr: Wie viel Regen? Ein paar Tropfen oder ein Wolkenbruch? Sollte ich lieber zuhause bleiben? Weil ich sowieso keine Lust auf Büro hatte.

Diese Entscheidungen können nur Sie allein treffen.

Es wäre schön, wenn Sie diese Entscheidungen wenigstens ein für alle Mal treffen könnten.

Aber ... so funktioniert es nicht.

Unsere Reaktion auf die Regenwahrscheinlichkeit für heute beeinflusst, wie wir den Wetterbericht von morgen interpretieren und wird zum Teil des Erfahrungsschatzes, den wir für den zukünftigen Umgang mit Regen nutzen.

Das Zusammenspiel all dieser Faktoren verändert die Ausgangsbedingungen für unsere Reaktion auf den nächsten Sturm. Das trifft auf Regen und auf Cyber-Risiken zu.

Sehen wir uns nun die externen Bedrohungen an, die Sie im Auge behalten sollten.

Ist Ihr Datenbestand

DURCH ANGREIFER GEFÄHRDET?

Beginnen wir mit einer einfachen Frage:

Ist es wahrscheinlich, dass Angreifer es auf ***meine Daten*** abgesehen haben?

Will Ihr vernetzter Kühlschrank Sie umbringen?

Ransomware auf ESXi ist eine riesige neue Gefahr

WELCHE SCHLAGZEILEN SOLLTEN SIE ERNST NEHMEN UND WAS IST NUR PANIKMACHE?

Wie Angreifer KI wirklich nutzen

Ist dies das neue Solarwinds?

Der Super-GAU: größter Datenverlust aller Zeiten

Warum Strawberry Tempest schlimmer ist als Lapsus$

Niemand kann Ihnen mit 100%iger Gewissheit sagen, ob Sie von einem Cyber-Angriff betroffen sein werden oder nicht, aber wir können Ihnen sagen, womit Sicherheitsprofis wie Sie im vergangenen Jahr konfrontiert waren.

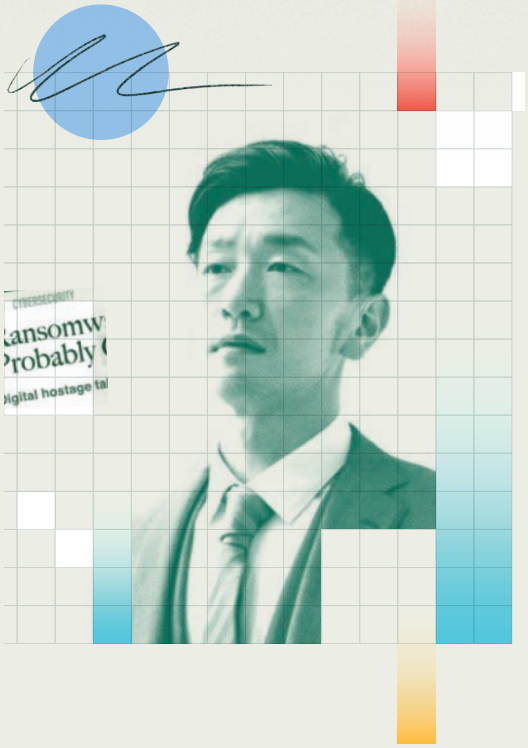
Fast alle mussten etwa jede zweite Woche einen Cyber-Angriff abwehren.

So sah das vergangene Jahr für IT- und Sicherheitsmanager aus: ▲

94 % erlebten mindestens einen schwerwiegenden Angriff auf ihre Organisation.

30 böswillig verursachte schädliche Ereignisse wurden Managern in gehobenen Positionen 2023 im Schnitt gemeldet

93 % der externen Organisationen meldeten zuständigen Behörden offiziell Datenverluste.



Cyber-Angriffe sind weitaus wahrscheinlicher als *physischer Diebstahl oder Feuer.*

Zur objektiven Beurteilung der Wahrscheinlichkeit von Cyber-Angriffen verglich eine europäische Versicherungsgesellschaft[1] Cyber-Angriffe mit herkömmlichen Bedrohungen im selben Zeitraum und fand:

67 % Organisationen werden mit 67 % größerer Wahrscheinlichkeit einen Cyber-Angriff als einen physischen Diebstahl erleiden.

5 x Ein Cyber-Angriff ist fünfmal wahrscheinlicher als ein Feuer.

20 % der Organisationen wissen nicht, was sie bei einem Cyber-Angriff tun sollten.

1 https://www.aviva.com/newsroom/news-releases/2023/12/One-in-five-businesses-have-been-victims-of-cyber-attack-in-the-last-year/

Angreifer nehmen gern *hybride Umgebungen* ins Visier.

Wenn Sie mit einem Angriff rechnen müssen, sollten Sie wissen, was wo geschehen könnte. In vielen der 94 % der von Cyber-Angriffen betroffenen externen Organisationen wurden gleichzeitig mehrere Arten von Umgebungen angegriffen: ▲

67 %
SaaS

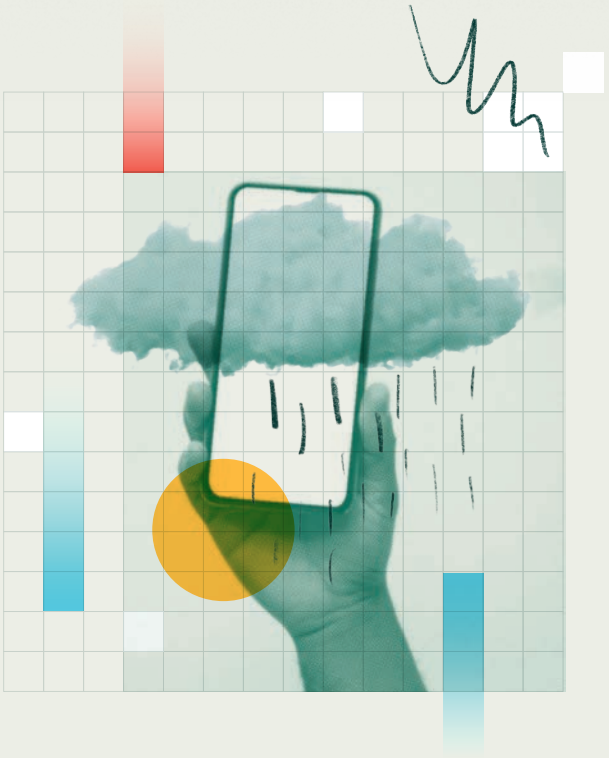
66 %
Cloud

51 %
On-Premises

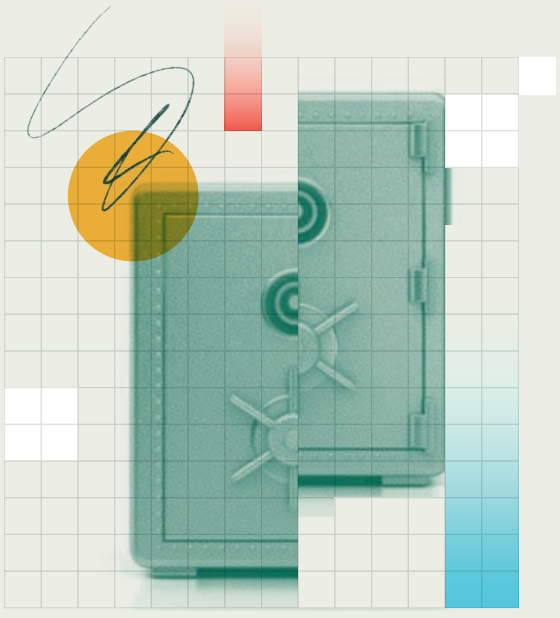
Die beiden häufigsten Angriffsarten in diesen Umgebungen sind: ▲

38 %
der Organisationen erlitten mindestens einen Cyber-Angriff mit Datenschutzverletzung.

33 %
der Opfer erlitten mindestens einen Ransomware-Angriff.



Fast alle Cloud-Mandanten wurden angegriffen und zwei Drittel wurden 2023 infiltriert.



Das geht nicht nur aus unseren eigenen Forschungsergebnissen hervor. Proofpoint zufolge[1]: ■

94 %
der Cloud-Mandanten wurden im vergangenen Jahr jeden Monat angegriffen.

62 %
der angegriffenen Cloud-Mandanten wurden erfolgreich infiltriert.

1 https://www.proofpoint.com/us/resources/threat-reports/human-factor

Angreifer haben tagelang *Zugang zu Ihren Daten*, bevor sie enttarnt werden.

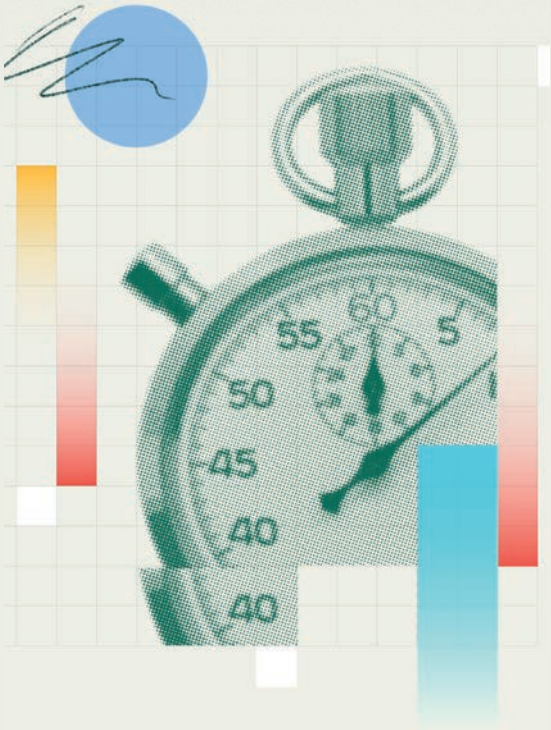
Mandiant misst die Verweilzeit[1] als die Anzahl der Tage, während derer ein Angreifer unbemerkt Zugang zur Umgebung seines Opfers hat.

10 TAGE

Die mittlere globale Verweilzeit aller Vorfälle betrug im vergangenen Jahr 10 Tage.

5 TAGE

Die mittlere globale Verweilzeit für Ransomware-Vorfälle betrug 5 Tage.



DIE GUTE NACHRICHT:

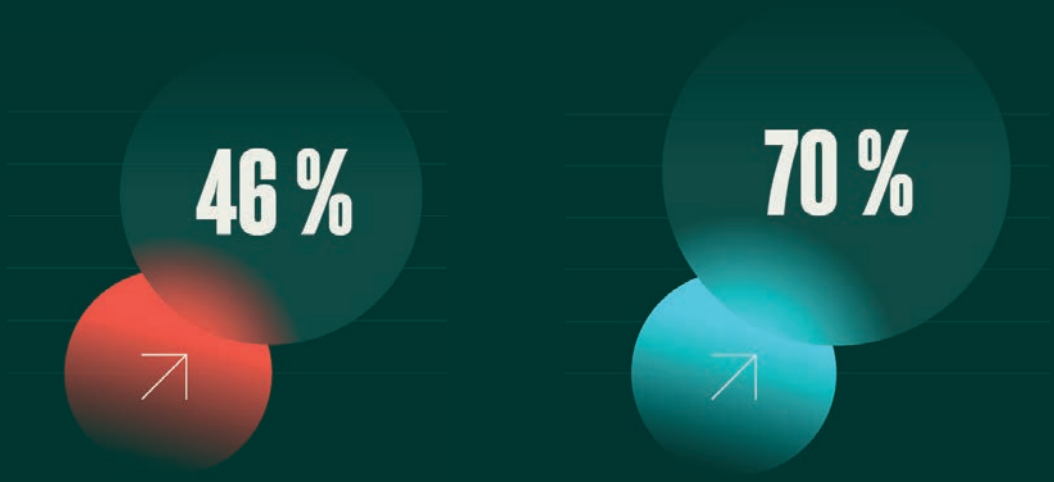
Dies sind die kürzesten Verweilzeiten, die Mandiant je beobachtet hat.

DIE SCHLECHTE NACHRICHT:

Sie geben Angreifern immer noch zu viel Zeit, ihre Ziele zu erreichen.

SIE BILDEN ES SICH NICHT NUR EIN. ES GIBT MEHR RANSOMWARE (70 % MEHR).

Recorded Future verfolgt öffentlich bekanntgegebene Ransomware-Angriffe und hat im letzten Jahr einen erheblichen Anstieg verzeichnet:



358 gemeldete Ransomware-Angriffe im Gesundheitswesen (46 % mehr als im Vorjahr)

4.399 gemeldete Angriffe in allen Branchen (70 % mehr als im Vorjahr)

Wenden wir uns nun Ihren Daten zu.

1 https://www.mandiant.com/m-trends

Lauern

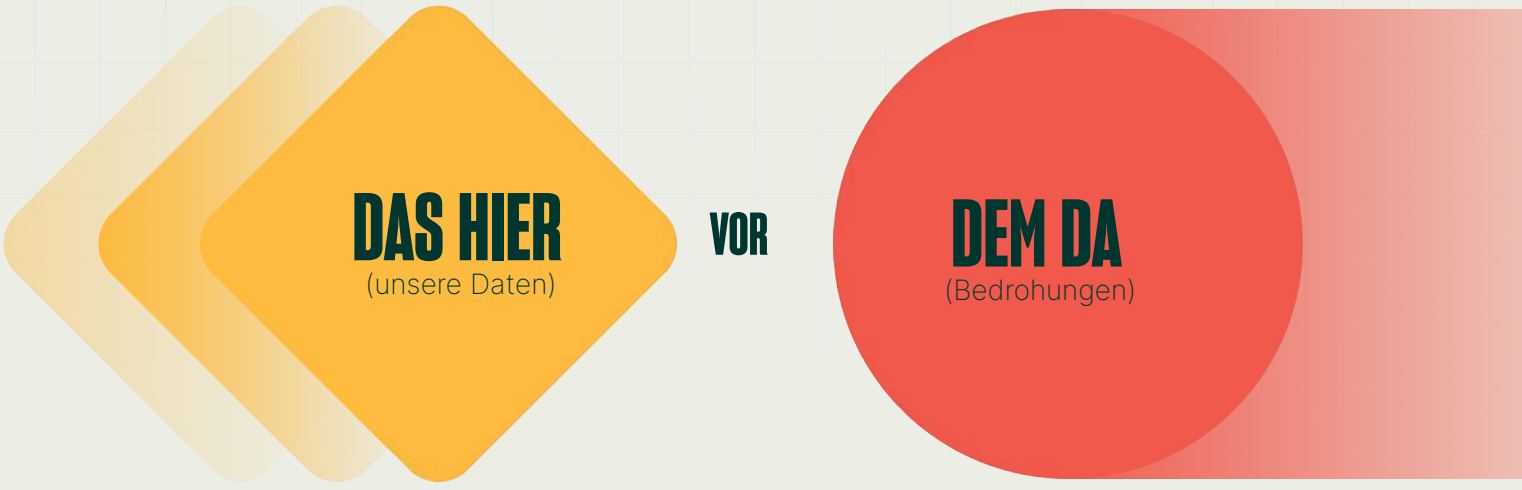
RISIKEN IN IHREN DATEN?

Vor dem oben beschriebenen (beunruhigenden) Hintergrund sind Organisationen gut beraten, zwei Faktoren nach Kräften zu reduzieren:

DIE WAHRSCHEINLICHKEIT EINES ERFOLGREICHEN ANGRIFFS

DIE FOLGEN EINES ANGRIFFS

Letztendlich haben wir ein (theoretisch) sehr einfaches Ziel. Wir wollen



schützen. Dazu müssen wir uns beides genauer ansehen. Sehen wir uns nun an, was Betriebsexperten von Sicherheitsprofis erwarten.

DATEN

werden in immer größerer Menge generiert –
und müssen geschützt werden.

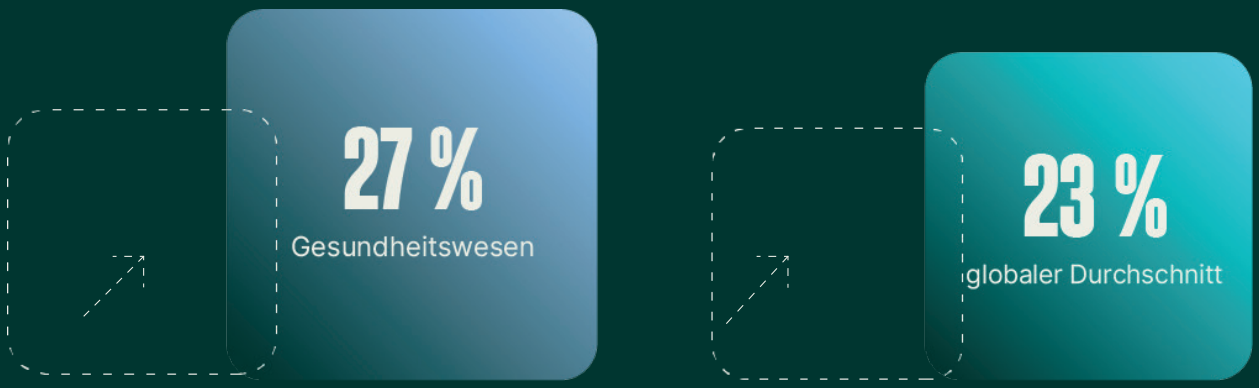
Sicherheitsprofis im Gesundheitswesen sind für den Schutz immer größerer Datenspeicher verantwortlich, die immer mehr sensible Daten enthalten und weltweit im Vergleich zu anderen Branchen überdurchschnittlich schnell wachsen. ◆

Einrichtungen des Gesundheitswesens sichern 22 % mehr Daten als der weltweite Durchschnitt aller Organisationen.

WAS WAR BETB NOCHMAL?

Frontend/Backend
Die Datengurus erinnern uns: Wenn Sie das Wort „Daten“ hören, denken Sie wahrscheinlich (wie die meisten anderen Menschen) an logischen oder auch Frontend-Speicher. Wir hier im Datensektor konzentrieren uns jedoch auf Backend-Speicher. Rubrik nimmt sämtliche Daten eines Unternehmens und reduziert das Volumen dieses Frontend-Speichers mit einer Reihe verschiedener Methoden (wie Deduplizierung und Komprimierung) zum sogenannten Backend-Speicher. In diesem Bericht nutzen wir durchweg Backend-Speicher.

In einer typischen Einrichtung des Gesundheitswesens ist das Datenvolumen allein im vergangenen Jahr um 27 % gewachsen (der Durchschnitt aller Branchen war 23 %).



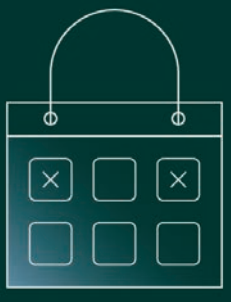
Eine typische Einrichtung des Gesundheitswesens hat 50 % mehr sensible Daten als der globale Durchschnitt.

Die Anzahl der sensiblen Datensätze im Gesundheitswesen ist 2023 um mehr als 63 % gestiegen – weitaus stärker als in jeder anderen Branche und fünfmal so stark wie der globale Durchschnitt (13 %).

ORGANISATIONEN MUSSTEN 2023 EINE REKORDZAHL VON HERAUSFORDERUNGEN STEMMEN

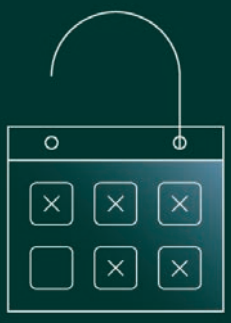
Schwachstellen sind zwar kein perfektes Maß für die Anfälligkeit, bieten aber einen guten Anhaltspunkt für den Umfang und das Ausmaß des Risikos, das Hersteller an ihre Kunden weitergeben.

2022 wurde ein neuer Rekord für die Anzahl der in einem Jahr gemeldeten Schwachstellen aufgestellt:



25.083
Schwachstellen aufgedeckt

2023 wurde dieser Rekord um 16 % überboten.

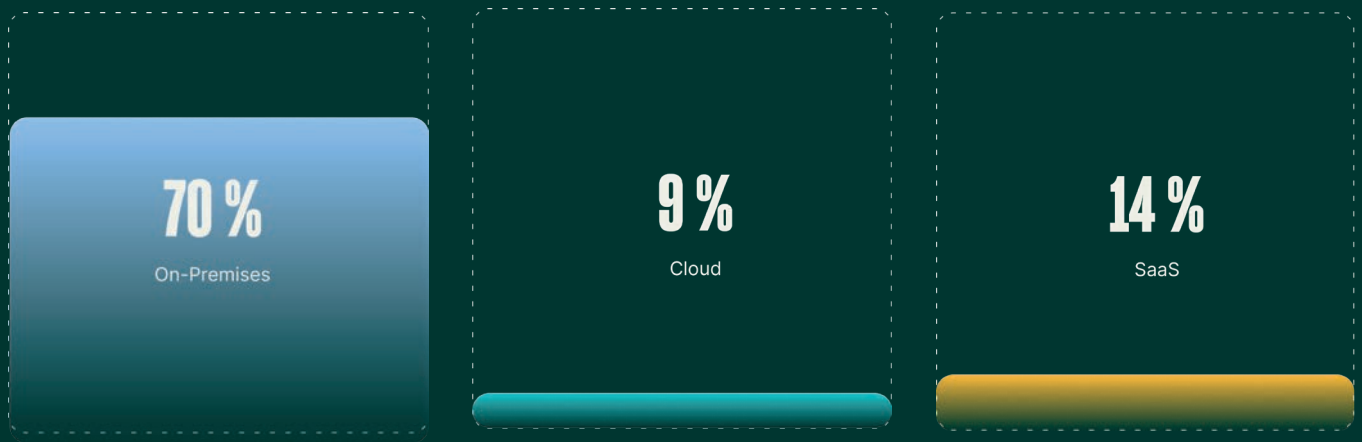


29.065
Schwachstellen aufgedeckt

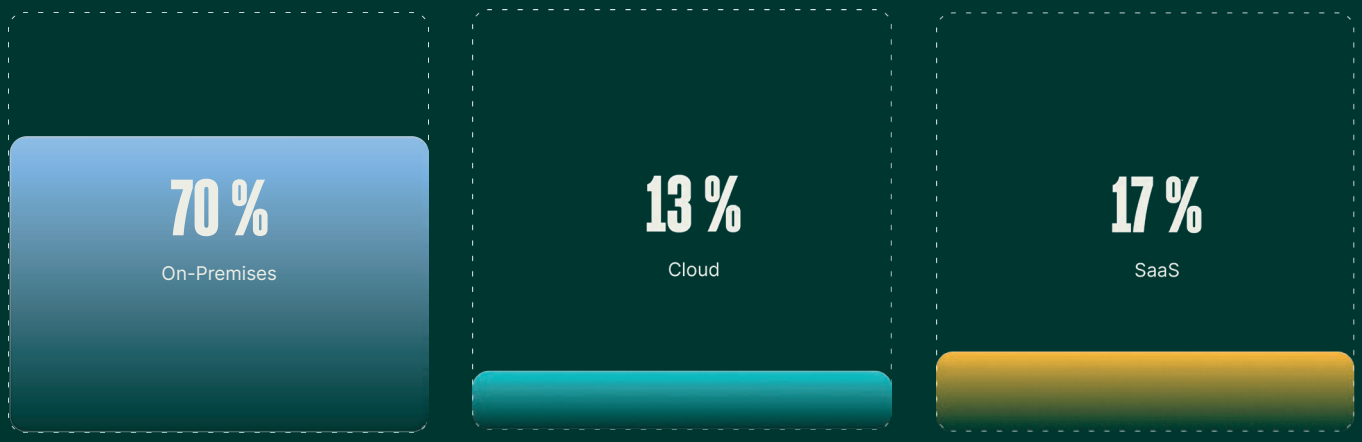
ORGANISATIONEN SIND IMMER STÄRKER AUF CLOUDS UND SAAS ANGEWIESEN ◆

An moderne Unternehmen werden Anforderungen gestellt, die ohne eine steigende Cloud-Nutzung kaum zu bewältigen sind. Daher machen Cloud- und SaaS-Umgebungen einen steigenden Anteil von Hybrid-Umgebungen aus, während On-Premises-Architekturen an Bedeutung verlieren.

2022:



2023:



CLOUDS HABEN TOTE WINKEL

Cloud-Datensicherheit

TOTER WINKEL NR. 1:

70 % der Daten in einem typischen Cloud-Speicher sind in Objektspeichern.

Die meisten Sicherheitsvorkehrungen basieren auf Technologie, die Objektinhalte weder maschinell lesen noch inspizieren kann.

Cloud-Datensicherheit

TOTER WINKEL NR. 2:

88 % der Daten in Objektspeichern sind entweder Textdateien oder halbstrukturierte Dateien in Formaten wie CSV, JSON oder XML.

Nehmen wir einmal an, dass Ihre Tools und Prozesse in Objektspeicher hineinsehen können. Dort wartet die nächste Herausforderung auf Sie: Ob (und wenn ja, welche) unstrukturierten oder halbstrukturierten Daten maschinell gelesen oder anderweitig abgedeckt werden können, variiert zwischen den führenden Sicherheitstechnologien und -diensten so stark, dass von Transparenz insgesamt keine Rede sein kann.

Cloud-Datensicherheit

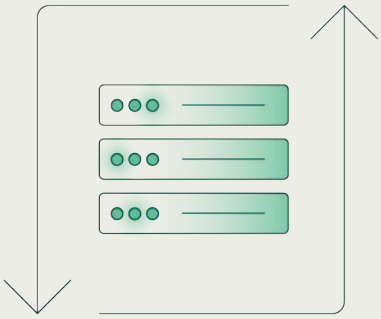
TOTER WINKEL NR. 3:

Mehr als 25 % aller Objektspeicher enthalten Daten, die gesetzlichen oder anderen offiziell bindenden Vorschriften unterliegen. Das können zum Beispiel geschützte Gesundheitsdaten (PHI) oder personenbezogene Daten (PII) sein.

Einfach ausgedrückt ist die Cloud-Nutzung von Haus aus risikobehaftet, weil Organisationen einerseits auf sie angewiesen sind, in Cloud-Umgebungen aber andererseits weniger Sicherheitsfunktionen und Transparenz zum Schutz regulierter Daten vorfinden als in ihren On-Premises-Umgebungen.

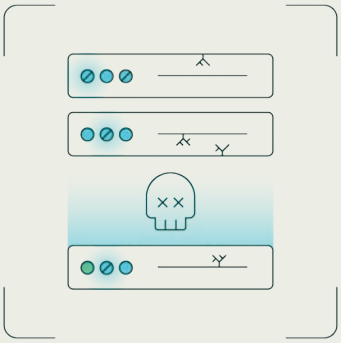
DIE MEISTEN BACKUP-LÖSUNGEN SIND DER AUFGABE NICHT GEWACHSEN

Technologien für Backups und Wiederherstellung gehören zu den kritischen Komponenten praktisch aller professionell genutzten Infrastrukturen. Sie werden seit Jahrzehnten zur Disaster Recovery und zur Einhaltung von Compliance-Vorgaben genutzt. Das geschieht vielerorts allerdings nicht reibungslos.



99 %

Eine frühere Untersuchung von Rubrik Zero Labs[1] ergab, dass über 99 % der externen Organisationen eine Backup-Lösung haben. ◆

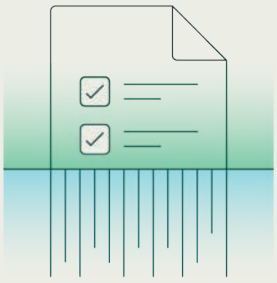


> 93 %

Mehr als 93 % dieser Organisationen hatten allerdings erhebliche Probleme mit ihren vorhandenen Lösungen. ◆

70 %

Aon zufolge[2] werden Backups in 70 % der Organisationen allerdings nicht an mehreren Standorten gelagert oder sind nicht unveränderlich. ●



40 %

Fast 40 % der von Rubrik untersuchten Organisationen hatten keine Compliance-Richtlinien für ihre Daten-Backups definiert. ◆

1 https://www.rubrik.com/zero-labs/2023-spring
2 https://www.aon.com/2023-cyber-resilience-report/

DIE SCHLECHTE NACHRICHT:

Cyber-Kriminelle wissen, wie wichtig Backups sind und nehmen sie routinemäßig ins Visier.

Sie versuchen bei fast jedem Angriff, Backups und Wiederherstellungsmechanismen lahmzulegen.
Aus Berichten von erfolgreich angegriffenen externen Organisationen geht hervor: ▲

96 %

Bei 96 % der Angriffe wurde versucht, Backups zu manipulieren.

74 %

74 % dieser Versuche waren zumindest teilweise erfolgreich.

Cyber-Kriminelle schützen sich vor erfolgreicher Wiederherstellung.

Ransomware-Angreifer kennen gängige Sicherheitsmaßnahmen und entwickeln ihre Ansätze entsprechend weiter. Statt Daten nur zu verschlüsseln, stehlen sie diese nun und drohen, sie zu veröffentlichen. Damit können sie auch Organisationen erpressen, die die Verschlüsselung durch eine schnelle Wiederherstellung rückgängig machen konnten.

2 x

Microsoft hat ermittelt, dass die Anzahl der Angriffe, bei denen nach dem Eindringen in die Umgebung eventuell Daten ausgeschleust wurden, sich seit November 2022 verdoppelt hat. ●

12 %

Eine Bewertung von Aon ergab, dass eine Datenschutzverletzung insgesamt 12 % größere Auswirkungen hat als Ransomware allein. ●

93 %

93 % der externen Organisationen, die einem Ransomware-Angriff zum Opfer gefallen waren, zahlten ein Lösegeld und 58 % von ihnen nannten die angedrohte Offenlegung gestohlener Daten als Hauptgrund für die Zahlung. ▲

So viel zur Wahrscheinlichkeit – wenden wir uns nun den Auswirkungen zu.

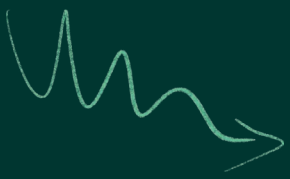
Wie schlimm
WIRD ES?

Viele Menschen halten einen Cyber-Angriff für das Ende der Geschichte.

Doch die Geschichte geht noch weiter.

Kommen wir noch einmal auf das Beispiel mit dem Wetterbericht zurück: Ihr Tag *endet nicht, wenn es regnet.*

Das Leben geht weiter. Aber jetzt müssen Sie sich an neue Bedingungen anpassen. Wie bleiben Sie trocken? Gehen Sie trotzdem mit dem Hund spazieren? Was passiert, wenn Sie vom Regen erwischt werden?



Auf ähnliche Weise löst ein Cyber-Angriff eine ganze Reihe von Bemühungen zur Schadensbehebung, Wiederherstellung und Berichterstellung aus.

Wie mühselig dies alles ist, hängt wesentlich davon ab, wie gut Sie auf eine solche Situation vorbereitet waren.

Sehen wir uns nun genauer an, welche Folgen Cyber-Angriffe – insbesondere mit Ransomware – im vergangenen Jahr im Gesundheitswesen hatten.

ÄHNLICH IST ES NACH EINEM CYBER-ANGRIFF

Bei Cyber-Angriffen auf das Gesundheitswesen wurden allein im vergangenen Jahr persönliche Daten von einem Drittel aller US-Amerikaner gestohlen.[1]

> 244.000

Personen waren (im Durchschnitt) bei jedem dieser Cyber-Angriffe betroffen.

186 %

mehr als 2022

> 133 Mio.

Patientenakten waren im vergangenen Jahr von Cyber-Angriffen auf das Gesundheitswesen der USA betroffen.

1 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Von einem Ransomware-Angriff im Gesundheitswesen sind fast fünfmal mehr sensible Daten betroffen als beim globalen Durchschnitt aller Angriffe. ◆

Rubrik misst sowohl das Ausmaß der Ransomware-Verschlüsselung als auch die Menge der davon betroffenen sensiblen Daten. Als „betroffen" betrachten wir Daten in verschlüsselten, gelöschten und ausgeschleusten Dateien.

Bei einem typischen Verschlüsselungsanschlag mit Ransomware auf eine Produktionsumgebung im Gesundheitswesen sind das:

16,8 MIO.
betroffene Dateien
pro Verschlüsselung

8,4 MIO. der Daten in den betroffenen Dateien sind sensible Datensätze.

20 % aller sensiblen Daten einer typischen Einrichtung des Gesundheitswesens sind pro erfolgreicher Verschlüsselung mit Ransomware betroffen.

Im Durchschnitt aller Branchen sind weitaus weniger sensible Daten betroffen:

13,7 MIO.
betroffene
Dateien pro
Verschlüsselung

1,7 MIO. betroffene sensible Datensätze pro Verschlüsselung

6 % der sensiblen Daten der betroffenen Organisation

Virtualisierung ist bei Ransomware-Angriffen im Gesundheitswesen ein wichtiger Aspekt. ◆

Sehen wir uns nun an, wo die Ransomware-Verschlüsselung stattfindet.

97 %

der verschlüsselten Daten befinden sich in virtualisierten Architekturen. (Gesundheitswesen)

83 %

der verschlüsselten Daten befinden sich in virtualisierten Architekturen. (Durchschnitt aller Branchen)

Das ist vermutlich auf zwei Faktoren zurückzuführen.

1. Virtualisierte Architekturen sind meist durch weniger Sicherheitsvorkehrungen geschützt als herkömmliche Endpunkte. Dadurch entstehen Einfallstore, die von Angreifern ausgenutzt werden können.

2. Wenn Angreifer sich Zugang zu einem Dashboard für die Verwaltung virtualisierter Umgebungen verschafft haben, benötigen sie oft nur gestohlene Anmeldedaten, um von dort aus sehr schnell sehr große Bereiche der Infrastruktur zu infiltrieren.

GROSSE UNTERSCHIEDE BEI RANSOMWARE-ZAHLUNGEN

Ransomware-Angreifer fordern anfänglich oft mehr Lösegeld, als sie letztendlich erhalten. Palo Alto Networks Unit 42 hat im vergangenen Jahr die folgenden Lösegeldzahlungen beobachtet: ■

	ALLE BRANCHEN:	GESUNDHEITSWESEN:
Mittlere Forderung	800.000 $	200.000 $
Mittlere Zahlung	275.000 $	100.000 $
Dritthöchste Zahlung	25.000.000 $	297.000 $

Backups und Datendiebstahl haben einen großen Einfluss auf die Wahrscheinlichkeit einer Lösegeldzahlung.

An der niederländischen Universiteit Twente[1] wurde untersucht, welche Faktoren einerseits die Entscheidung für oder gegen eine Lösegeldzahlung und andererseits die Höhe der Zahlung beeinflussen. Die Ergebnisse:

Organisationen mit wiederherstellbaren Backups waren

27,5x

WENIGER ZU EINER LÖSEGELDZAHLUNG BEREIT

1 https://databreaches.net/university-of-twente-maps-decision-making-process-for-ransomware-victims/

Datenausschleusung steigerte sowohl die Wahrscheinlichkeit einer Lösegeldzahlung als auch die Höhe der Zahlung.

40 %

zahlten ein Lösegeld, wenn Daten ausgeschleust worden waren.

25 %

zahlten ein Lösegeld, wenn keine Daten ausgeschleust worden waren.

5,5 x

höhere Lösegelder wurden gezahlt, wenn Daten ausgeschleust (und nicht nur verschlüsselt) worden waren.

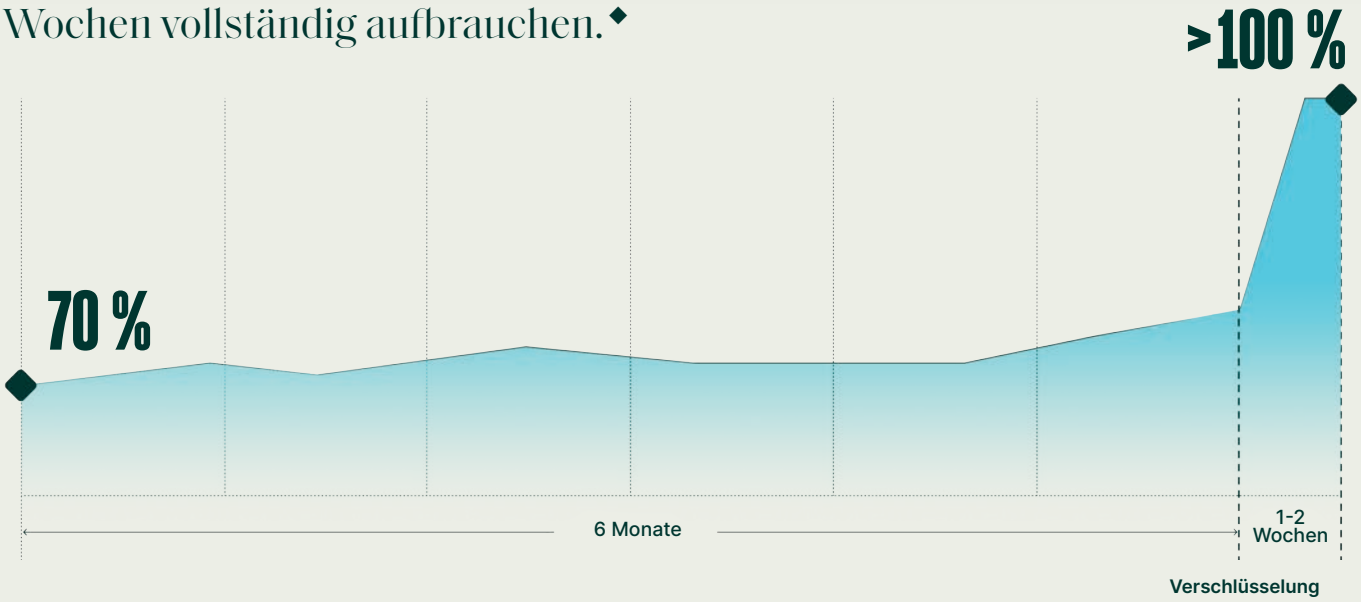
Speicherüberlastung: Die böse Überraschung bei der Wiederherstellung

Ein Unglück kommt selten allein. Nur wenige Organisationen sind auf die Datenflut vorbereitet, die mit Ransomware einhergeht.

Wenn bei einem Ransomware-Angriff im Gesundheitswesen 16,8 Millionen Dateien verschlüsselt werden, werden für die betroffene Organisation 16,8 Millionen „neue“ Dateien angelegt (im Vergleich zu 13,7 Millionen im globalen Durchschnitt). ◆

Für diese „neuen“ Dateien werden dann Backups angelegt, die zum Zeitpunkt der Verschlüsselung riesige Mengen Speicherplatz beanspruchen.

Wenn die verfügbare Speicherkapazität einer Organisation vor einem Ransomware-Angriff zu mehr als 70 % ausgelastet ist, könnten diese „neuen" Daten die zur Wiederherstellung erforderliche Speicherkapazität innerhalb von einer oder zwei Wochen vollständig aufbrauchen.◆



Erschwerend kommt hinzu, dass von einem Ransomware-Angriff betroffene Organisationen oft selbst „neue Daten" generieren müssen, zum Beispiel forensische Images für die Analyse und unveränderliche Kopien für juristische Zwecke. Oft müssen auch im Rahmen der Angriffsabwehr und der Wiederherstellung Daten dupliziert werden. Einfach ausgedrückt muss die betroffene Organisation sofort noch mehr neue Daten generieren, wenn sie auf das Generieren großer Mengen neuer Daten seitens der Angreifer reagiert.

Bei den über 200 Wiederherstellungseinsätzen, die das Rubrik Ransomware Response Team inzwischen hinter sich hat, führte dies meistens zu einer der folgenden beiden Situationen. Die Organisation musste entweder:

1. ihre Datenkapazität schnell vergrößern, wozu finanzielle Investitionen und ein erheblicher Arbeitsaufwand erforderlich waren.

2. die Wiederherstellungskapazität reduzieren, um das Datenwachstum zu drosseln, wodurch allerdings die Wiederherstellungsoptionen in kritischen Zeitabschnitten eingeschränkt wurden.

RANSOMEWARE-FOLGEN WAREN FÜR MINDESTENS 42 TODESFÄLLE IN DEN USA MITVERANTWORTLICH

Jeder Ransomware-Angriff hat Folgen für die Daten. Das tatsächliche, damit einhergehende Risiko wird – besonders im Gesundheitswesen – an den Auswirkungen auf den Betrieb und auf Menschenleben gemessen. ▪

Die University of Minnesota Twin Cities - School of Public Health hat die tatsächlichen Konsequenzen von Ransomware-Vorfällen zwischen 2016 und 2021 für Krankenhäuser und die Patientenbetreuung untersucht.[1] Das Ergebnis:

20 %

Der Durchsatz bei der Patientenbetreuung fiel in der ersten Woche eines Ransomware-Angriffs um 20 %.

Diese Angriffe wirken sich nicht mehr nur auf Daten, Unternehmen oder die Privatsphäre von Personen aus. Es gibt direkte Beweise dafür, dass Cyber-Angriffe lebensbedrohlich sein können.

1 von 4

Obwohl nur 5 % der Krankenhäuser in den USA während des Untersuchungszeitraums selbst einem Ransomware-Angriff zum Opfer fielen, wurden weitere 20 % durch die Verlegung oder Umleitung von Patienten aus den direkt betroffenen in umliegende Krankenhäuser ebenfalls in Mitleidenschaft gezogen.

0,5–1 %

Ein typisches Krankenhaus büßte als direkte Folge eines einzigen Ransomware-Angriffs zwischen 0,5 % und 1 % seines Jahresumsatzes ein.

2–3 Wochen

Im Durchschnitt erreichte die Patientenbetreuung erst zwei bis drei Wochen nach einem Ransomware-Angriff wieder ihr normales Niveau.

42–67 Todesfälle

Die Folgen von Ransomware-Angriffen trugen direkt zum Tod von zwischen 42 und 67 Patienten bei.[2]

1 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292
2 https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/

Wiederherstellung und NEUBEGINN

Selbst wenn die erste Reaktion abgeschlossen und der Normalbetrieb größtenteils wiederhergestellt ist, machen die Folgen eines Ransomware-Angriffs sich weiterhin bemerkbar.

DIESE KÖNNEN NEGATIV, ABER AUCH POSITIV SEIN.

Cyber-Angriffe ***verändern*** Organisationen und Menschen.

Aon zufolge führte ein schwerwiegender Sicherheitsvorfall zu: ●

9 %

Fall des Aktienkurses pro Vorfall

Externe Organisationen nannten die folgenden direkten Auswirkungen von Cyber-Angriffen: ▲

44 %

erzwungene Änderungen der Führungsriege

43 %

Negativschlagzeilen bzw. Reputationsverlust

37 %

Umsatzverlust

36 %

Kundenabwanderung

Für 96 % der IT- und Sicherheitsmanager in gehobenen Positionen hatten Cyber-Angriffe zudem emotionale bzw. psychologische Auswirkungen: ▲

53 %

größere Sorge bezüglich der eigenen Stellung

41 %

Vertrauensverlust zwischen Kollegen und Teammitgliedern

38 %

Sorgen über die Job-Sicherheit

33 %

Schlaflosigkeit oder Schlafstörungen

Die Führungsriege wird Beweise dafür sehen wollen, dass die Organisation ***den nächsten Angriff überstehen*** kann.

60 % der IT- und Sicherheitsmanager sind extrem oder sehr besorgt über die Fähigkeit ihres Unternehmens, den Geschäftsbetrieb während eines Cyber-Angriffs aufrechtzuerhalten. ▲

28 % der Vorstände oder Führungsriegen externer Organisationen haben nach Meinung der Befragten wenig oder kein Vertrauen in die Fähigkeit der Organisation, kritische Daten und Anwendungen nach einem Cyber-Angriff wiederherzustellen. ▲

CYBER-ANGRIFFE WERFEN VORHERSEHBARE PROBLEME AUF

Hier ist eine Übersicht über die gängigsten Probleme bei einem Cyber-Angriff und die am häufigsten auftretenden Veränderungen, auf die Organisationen sich nach einem Cyber-Angriff vorbereiten sollten:

Externe Organisationen beantworteten die Frage nach der größten Herausforderung, mit der sie bei einem Cyber-Angriff konfrontiert waren, wie folgt: ▲

- **19 %** bereichsübergreifende Arbeit in Hybrid-Umgebungen
- **18 %** fehlende Abstimmung zwischen Teams
- **18 %** ineffektive Backup- und Wiederherstellungslösungen
- **17 %** fehlende Einbindung der Führungsriege
- **16 %** mangelnde Transparenz

Die häufigsten durch Cyber-Angriffe verursachten Änderungen in externen Organisationen waren: ▲

- **24 %** stärkere Überwachung durch die Führungsriege
- **20 %** Änderungen der Cyber-Sicherheitstechnologie
- **19 %** Überarbeitung der Cyber-Sicherheitspläne und -prozeduren
- **19 %** stärkerer Fokus auf Rechenschaftslegung
- **18 %** Verschlechterung der Stimmung in IT- oder Cyber-Sicherheitsteams

Cyber-Angriffe können auch positive Konsequenzen haben.

Wenn Organisationen dazu bereit sind, können sie diese Krisen nutzen, um ihre Zukunft neu zu gestalten.

Aon zufolge stiegen die Aktienkurse von Unternehmen, die einen Cyber-Angriff erfolgreich bewältigt hatten, um

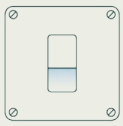
18 % stärker

an als die vergleichbarer Unternehmen. ●

Nach einem Cyber-Angriff beschlossen externe Organisationen Folgendes: ▲

55 %

haben mehr in neue Technologien oder Services investiert.



42 %

haben Anbieter oder externe Partner gewechselt.

37 %

haben zusätzliches Personal eingestellt.

Sie können nicht alle Risiken vollständig eliminieren, aber Sie können den Risikozyklus und Ihr neues Grundrisiko beeinflussen.

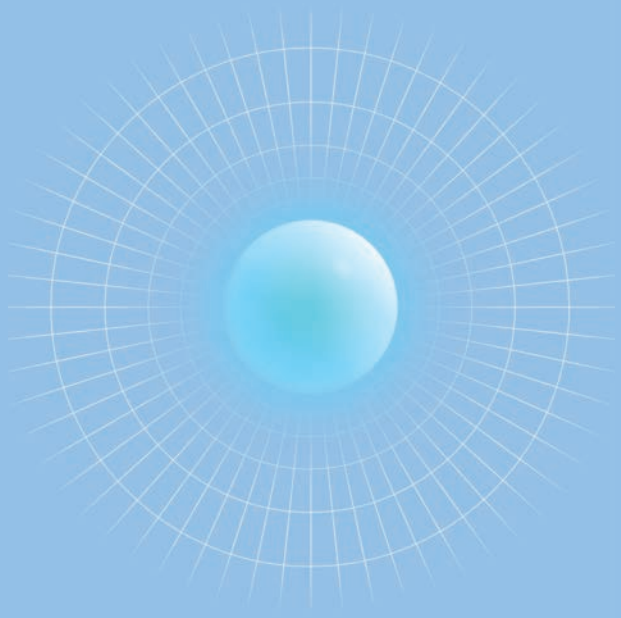
Neubestimmung des DATENRISIKOS

Wir würden sehr gern sagen, dass die Geschichte mit diesen Reaktionen endet.

Tatsächlich beginnt damit jedoch ein neues Kapitel.

SIE HABEN EINEN STURM ÜBERSTANDEN. DOCH DAS NÄCHSTE UNWETTER KOMMT BESTIMMT.

Und der nächste Sturm wird Sie höchstwahrscheinlich mit neuen Risiken konfrontieren, auf die Sie möglicherweise nicht vorbereitet sind.



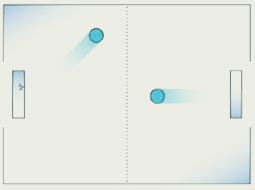
Wir würden auch gern sagen, dass es Möglichkeiten gibt, die Risikofaktoren zu beeinflussen, die vom Angreiferverhalten abhängig sind. Doch unsere Analysen zeigen, dass dies fast genauso aussichtslos ist, als wollten wir das Wetter ändern.

Wie in fast allen Lebensbereichen entziehen sich die Ereignisse um Sie herum Ihrer Kontrolle. Dennoch können Sie durch die Neubestimmung der Risiken deren Konsequenzen beeinflussen.

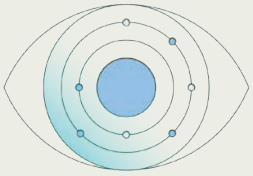
Sehen wir uns nun an, was die Daten zur erfolgreichen Bewältigung dieser Neuausrichtung zu sagen haben. Jede unserer Risikoempfehlungen basiert auf den Ergebnissen von Untersuchungen zu Cyber-Angriffen sowie deren Auswirkungen oder erwarteten Auswirkungen auf Daten.

WOVON HÄNGT IHR NEUES DATENRISIKO WIRKLICH AB?

Hier sind einige besonders wirksame Maßnahmen, mit denen Sie Ihr Datenrisiko erheblich reduzieren können:



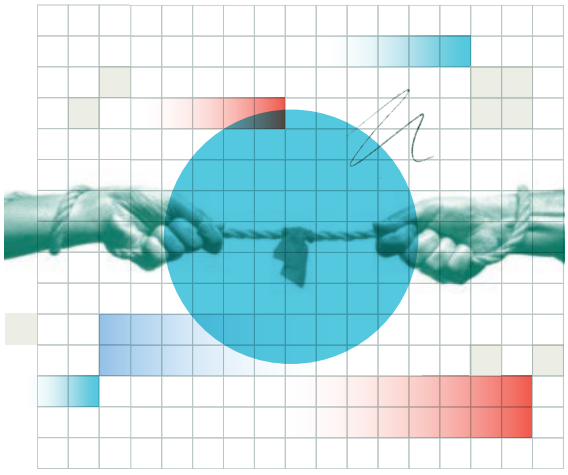
Bereiten Sie sich auf die Angriffsabwehr in allen Bereichen einer Hybrid-Infrastruktur vor. Angreifer nutzen Hybrid-Umgebungen bereits erfolgreich aus und Sicherheitsprofis müssen nachziehen.



Verbessern Sie Ihre ***Datentransparenz***, insbesondere:

- Verschaffen Sie sich eine Übersicht über alle Bereiche von Hybrid-Umgebungen.
- Ermitteln Sie, wo sich sensible Daten befinden und welchen Vorschriften die einzelnen Datenelemente unterliegen.
- Bereiten Sie sich darauf vor, Fragen neuer Führungskräfte zu beantworten und zu zeigen, wie Ihre jüngsten Investitionen die erwarteten Vorteile bieten werden.

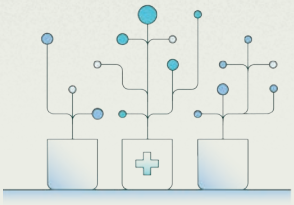
Erwarten Sie ein stärkeres Interesse seitens der Führungsriege und informieren Sie sie nach einem Cyber-Angriff proaktiv über Ihre Bemühungen.



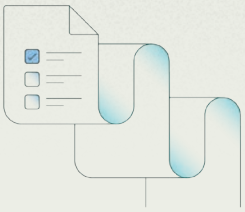
Bereiten Sie sich auf die Wiederherstellung und auf die *Störung der Wiederherstellung* durch die Angreifer vor.

Dazu sollten Sie:

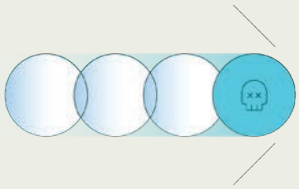
- sicherstellen, dass Backups vollständig unveränderlich und auch während eines Cyber-Angriffs verfügbar sind.
- einen möglichst großen Teil des Wiederherstellungsprozesses automatisieren.
- die Ergebnisse der Wiederherstellung in allen Bereichen Ihrer Hybrid-Umgebung testen.
- vorhandene Sicherheitsdienste und -technologien nutzen, um die Unveränderlichkeit der Backups und die Verzahnung der Backup-Technologien zu überprüfen.



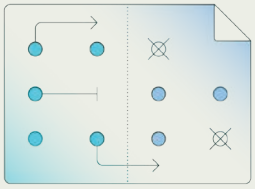
Seien Sie sich bewusst, dass das Volumen Ihrer Daten (insbesondere das Ihrer sensiblen Daten) wächst. Finden Sie Wege, dieses Wachstum zu kontrollieren und dem Schutz der kritischen Daten Priorität einzuräumen.



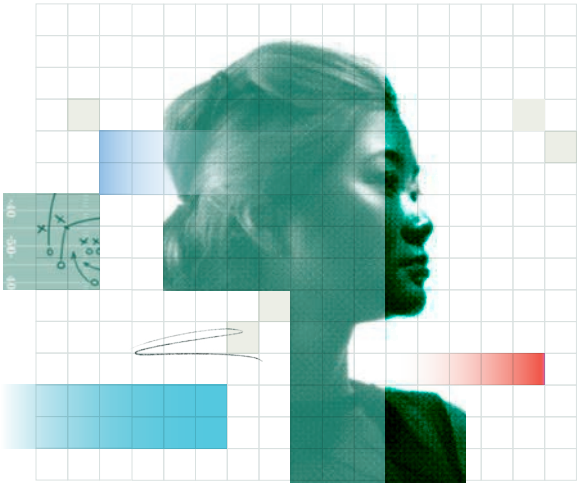
Bereiten Sie sich darauf vor, Compliance- und Rechtsfragen zu beantworten, während ein Ransomware-Angriff im Gange ist, Teile Ihre Umgebung verschlüsselt sind und Angreifer die Veröffentlichung gestohlener Daten androhen.



Seien Sie sich bewusst, dass Cyber-Angriffe oft zu Investitionen in neue Technologien und zusätzliches Personal oder zum Anbieter- oder Partnerwechsel führen. Bereiten Sie sich darauf vor, diese Perioden größerer Änderungsbereitschaft optimal zu nutzen.



Informieren Sie Ihre gesamte Organisation regelmäßig über Ihre Pläne und den Fortschritt bei deren Umsetzung, um die durch den Cyber-Angriff gedrückte Stimmung zu verbessern und allen Teams wieder Vertrauen zu vermitteln.



Fördern Sie vor, bei und nach Cyber-Angriffen die *Zusammenarbeit verschiedener Teams*.

Dazu sollten Sie:

- gemeinsam genutzte Playbooks erstellen und Planübungen durchführen.
- ermitteln, welche Teams am besten in der Lage sind, bestimmte Risikoentscheidungen zu treffen.
- die beste Methode zur Übermittlung der erforderlichen Daten an diese Entscheidungsträger finden.
- dafür sorgen, dass alle Teams dieselben Daten vor Augen haben, damit Entscheidungen schneller getroffen und Konflikte, die durch verschiedene Sichtweisen entstehen könnten, vermieden werden.

EINE ANDERE PERSPEKTIVE

Wir bei Rubrik Zero Labs betrachten Risiken normalerweise aus einer datengestützten Perspektive. Hier möchten wir unseren Blickwinkel jedoch erweitern, indem wir auch die Empfehlungen zur Verbesserung der Resilienz aus dem Microsoft Digital Defense Report 2023[1] miteinbeziehen. Microsoft hat eine völlig andere Sichtweise als Rubrik, von der wir uns neue Impulse für die Risikominderung erhoffen.

99 % Microsoft zufolge schützen grundlegende Sicherheitshygienemaßnahmen Daten vor 99 % aller Angriffe.•

Einige spezifische Empfehlungen: •

- Aktivieren Sie die Multi-Faktor-Authentifizierung.
- Wenden Sie das Zero-Trust-Prinzip an, insbesondere für Assets, mit denen kritische Daten und Funktionen gesichert werden.
- Schützen Sie kritische Bereiche Ihrer Hybrid-Umgebungen mit erweiterten Bedrohungs- und Malware-Erkennungsfunktionen.
- Spielen Sie auf wichtigen Systemen und Anwendungen zeitnah die neuesten Patches ein.
- Schützen Sie Ihre Daten, indem Sie kritische Daten und deren Speicherorte identifizieren und geeignete Sicherheitsmaßnahmen für diese Bereiche implementieren.

Wenn wir eine Ebene tiefer in die Sicht von Microsoft auf Ransomware eintauchen, finden wir „Die fünf Grundlagen" zur Reduzierung der Auswirkungen von Ransomware: •

1 moderne Authentifizierung mit gegen Phishing resistenten Anmeldedaten

2 Anwendung des Least-Privilege-Prinzips auf den gesamten Technologie-Stack

3 bedrohungs- und risikofreie Umgebungen

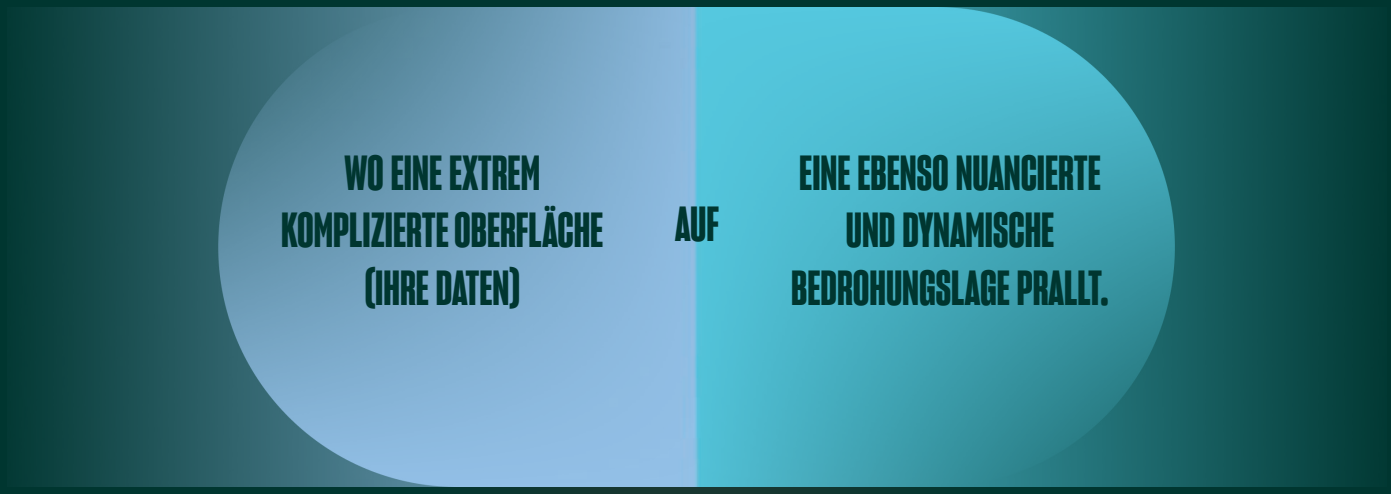
4 Management des Sicherheitsniveaus für Compliance und zur Überwachung des Zustands von Geräten, Services und Assets

5 automatische Cloud-Backups und Datei-Synchronisierung für benutzer- und geschäftskritische Daten

1 https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Wir haben diesen Bericht mit der Vereinfachung unserer Risikomathematik begonnen: Wir müssen DAS HIER vor DEM DA schützen.

In der Praxis sind Risiken ein unglaublich komplexes Feld,



RISIKO

Da buchstäblich Millionen von Variablen und Faktoren Ihr Risiko beeinflussen, werden Sie es nie exakt ermitteln oder vollständig eliminieren können. Sie können jedoch die Maßnahmen identifizieren und ergreifen, die es am stärksten reduzieren, sich auf vorhersehbare Situationen vorbereiten und sich so einen Vorsprung verschaffen.

Wir hoffen, dass wir Ihnen mit diesem Bericht einige Anregungen zur Risikominderung und zur Vorbereitung auf den dynamischen Risikozyklus geben konnten.

DANKSAGUNG

Rubrik möchte allen Organisationen danken, die diese Studie durch die Bereitstellung der Ergebnisse ihrer sorgfältigen und aufwendigen Datenanalysen unterstützt haben.

- Unsere Partner bei Microsoft und Aon haben sowohl strategische Empfehlungen als auch die Datenbasis, auf der diese beruhen, mit uns geteilt.
- Die folgenden Organisationen haben es uns gestattet, ihre Analysen zu nutzen und haben unterstützende Materialien zu deren richtiger Einordnung bereitgestellt:
  - Proofpoint
  - Recorded Future (Allan „Ransomware Sommelier“ Liska)
  - Mandiant (Kirstie „Swiftie“ Failey)
  - Palo Alto Networks Unit 42 (Ingrid Parker)
- Die University of Minnesota Twin Cities School of Public Health (Hannah Neprash, Claire McGlave und Sayeh Nikpay) hat uns die Nutzung ihrer Forschungsergebnisse gestattet, uns diese Ergebnisse im Detail erklärt und mit uns zusammengearbeitet, um ihre akademische Forschung mit der Branchenforschung von Rubrik Zero Labs abzustimmen.

Wie alle Projekte von Rubrik Zero Labs verdankt auch diese Studie ihren Erfolg zahlreichen Helfern. Wakefield Research hat externe Daten beigesteuert, um unsere Untersuchung so objektiv wie möglich zu gestalten. Shaped By ist es gelungen, die Daten anschaulich zu präsentieren. Und nicht zuletzt haben viele Rubrikianer Fachwissen, Kontextinformationen und Empfehlungen beigesteuert. Wir möchten uns besonders bei Amanda „Danger“ O’Callaghan, Linda „Taskmaster“ Nguyen, Lynda „Go Niners“ Hall, Ben Long, Peter „I’m the Law“ Chang, Ajay Kumar Gaddam, Ryan Goss, Derek Morefield, Josh Burns, Gunakar Goswami, Prasath Mani, Ethan Hagan, Kevin Nguyen, Caleb „Social King“ Tolin, Kelly Cooper, Hannah Battillo, Sindhu Nagendra, Caitlin „Plz stop letting Steve talk to reporters“ O’Malley und Fareed Fityan bedanken.