Rubrik Zero Labs

Der Stand der Datensicherheit:

DIE BITTERE WAHRHEIT

Inhalt

Datenquellen

(RT) **TELEMETRIEDATEN VON RUBRIK**

(WR) **WAKEFIELD RESEARCH**

(ER) **DATEN ZUR REAKTION AUF VORFÄLLE**

ÜBER DEN BERICHT

Rubrik Zero Labs hat es sich zur Aufgabe gemacht, umsetzbare, herstellerunabhängige Erkenntnisse zu liefern, um Datensicherheitsrisiken zu reduzieren. Wir haben Erkenntnisse aus verschiedenen Quellen einbezogen. Diese Daten umfassen den Zeitraum zwischen dem 1. Januar und dem 31. Dezember 2022.

TELEMETRIEDATEN VON RUBRIK:

Wir verwenden Telemetriedaten von Rubrik, um der Alltagsrealität in Unternehmen nahezukommen und gleichzeitig etwaige systeminhärente Verzerrungen erkennbar zu machen.

5000+
Kunden

3
Regionen

22
Branchen

57
Länder

Gesamtvolumen der gesicherten Daten:

28
Exabyte (EB)
an logischem Speicher

659
Backend-
Petabyte (BEPB)

Sensible Daten in:

8,7+ Milliarden
Dateien

1 von 38
Dateien enthält
sensible Daten

19+ Milliarden
sensibler Datensätze
innerhalb der Dateien

Ein Ein Gefühl für die Größenordnung:

Es gibt Schätzungen, die besagen, dass alle Wörter, die jemals in der Geschichte der Menschheit in allen Sprachen gesprochen wurden, 5 EB entsprechen … Das sind nur 18 % des Datenvolumens, das Rubrik im Jahr 2022 geschützt hat.[1,2,3,4]

28 EB vs 659 BEPB

Wenn die meisten Menschen „Daten“ hören, denken sie an logischen Speicher, auch „Frontend-Speicher“ genannt. Diejenigen von uns, die in der Datenbranche arbeiten, legen den Fokus auf den Backend-Speicher.

Rubrik wendet verschiedene Funktionen auf die Gesamtheit der Daten eines Unternehmens an – einschließlich Deduplizierung und Komprimierung –, um die Datenmenge im Backend-Speicher zu reduzieren. Deshalb konzentrieren wir uns im Rest dieses Berichts auf den Backend-Speicher.

Fallstudie
Wir haben uns einen Angriff auf eine der in der Rubrik Telemetrie erfassten Organisationen näher angesehen. Der Name des Unternehmens wurde aus Datenschutzgründen geändert.

1 https://www.space.com/18383-how-far-away-is-jupiter.html
2 https://www.sizes.com/tools/filing_cabinets.htm
3 https://www.zmescience.com/science/how-big-data-can-get/
4 https://www.backblaze.com/blog/what-is-an-exabyte/

WAKEFIELD RESEARCH:

Wir haben eine Umfrage bei Wakefield Research in Auftrag gegeben, um unsere Rubrik-Telemetrie durch einen umfassenderen Blick auf die Datensicherheitslandschaft abzurunden.

Wir haben IT- und Sicherheitsverantwortliche befragt, um die Unterschiede in ihren Standpunkten zu untersuchen.

1600+
IT- und Sicherheitsverantwortliche

49 %
CIOs und CISOs

3 Regionen
USA, EMEA und APAC

16 %
VPs

38 %
leitende Direktoren oder Vorstandsmitglieder

10 Länder
Vereinigte Staaten, Vereinigtes Königreich, Frankreich, Deutschland, Italien, Niederlande, Japan, Australien, Singapur, Indien

DATEN ZUR REAKTION AUF VORFÄLLE:

Wir haben andere angesehene Cybersicherheitsorganisationen hinzugezogen, um einen ganzheitlicheren Überblick über die Datensicherheitslandschaft zu erhalten. Wir bedanken uns dafür, dass wir ihre Erkenntnisse nutzen durften.

Mandiant:
Mittlere globale Verweilzeiten und Ransomware-Untersuchungsquoten aus M-Trends 2023

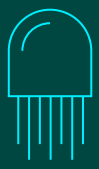
Palo Alto Networks Unit 42:
Lösegeldforderungen im Jahr 2022 aus dem Bericht 2023 von Unit 42 zu Ransomware und erpresserischen Drohungen

Expel:
Ransomware-Vorläuferaktivitäten und Zunahme von Angriffen auf Public Clouds aus „Great Expeltations 2022“

Permiso:
Unerlaubte Nutzung von Zugangsdaten bei Angriffen auf Clouds und Zugriffsebenen aus „Permiso 2022 - End of Year Observations“

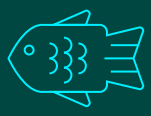
DIE DATENMEER-LANDSCHAFT

Unternehmen schwimmen auf einem Meer an Daten.
An der Oberfläche sieht der Ozean riesig, aber unbewegt aus.



Aber jeder, der in seine Tiefen eintaucht, weiß, dass es dort nur so wimmelt.

Die Sicht ist begrenzt, aber je mehr man sucht, desto mehr Daten findet man – in Höhlen, unter Steinen, fast überall. Die Strömung ist schnell. Man sieht die gleiche Szene nie zweimal.



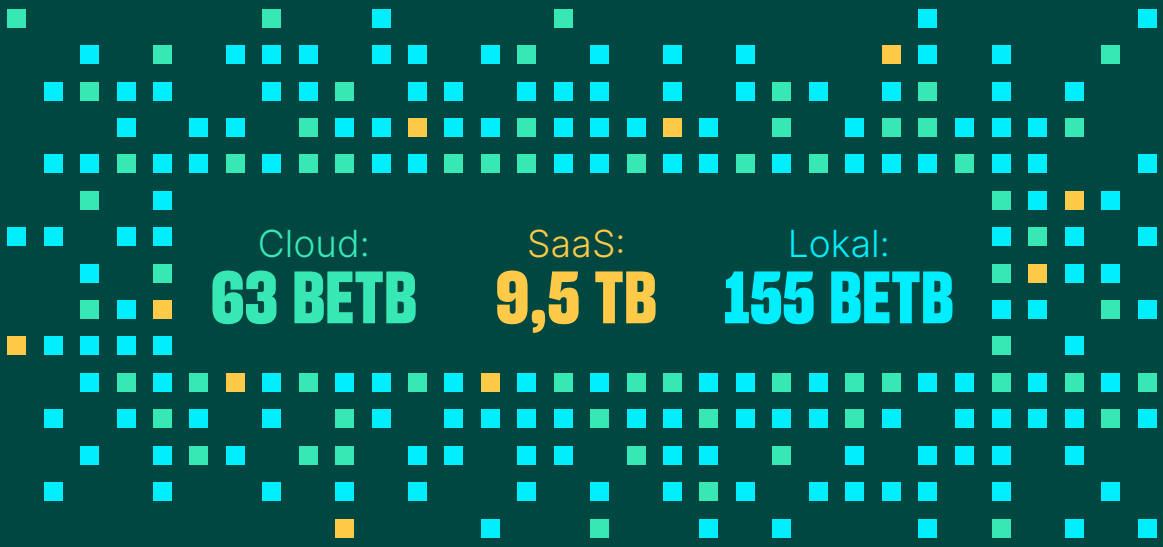
Und die ganze Zeit über fragt man sich:

„LAUERN HIER RAUBTIERE IN FINSTEREN ECKEN UND WARTEN NUR DARAUF, ANZUGREIFEN?"

Daten wachsen schneller und an mehr Orten, als man denkt ®

In einer typischen Umgebung gesicherte Daten

GESAMT: 227 BETB



Durchschnittliches Wachstum gesicherter Daten im Jahr 2022:

Gesamt:	Cloud:	SaaS:	Lokal:
25 %	61 %	236 %	19 %

Das Datenvolumen eines typischen Unternehmens wird sich in den nächsten fünf Jahren verdreifachen und

545 BETB AN SPEICHER ERFORDERN,

wenn die Wachstumsraten gleich bleiben.

45 %

der Unternehmen weltweit sichern ihre Daten in einer Mischung aus lokalen, Cloud- und SaaS-Lösungen.

36 %

der Unternehmen weltweit nutzen mehrere Cloud-Anbieter gleichzeitig.

Für jede Datensicherheitslösung gibt es neue Herausforderungen ®

Die letzte Verteidigungslinie während einer Krise sind die Daten-Backup- und Wiederherstellungssysteme und die damit verbundenen Prozesse. Unternehmen stellen jedoch fest, dass es nicht ausreicht, einfach nur eine Backup-Lösung zu haben.

99 %

der externen Unternehmen gaben an, dass sie über eine Backup- und Wiederherstellungslösung verfügen.

Allerdings hatten 93 %

erhebliche Probleme mit ihrer Lösung. Die häufigsten Probleme sind Personalmangel, Bandbreitenbeschränkungen, Infrastrukturlücken und das Fehlen von vorab abgestimmten Plänen oder Prioritäten.

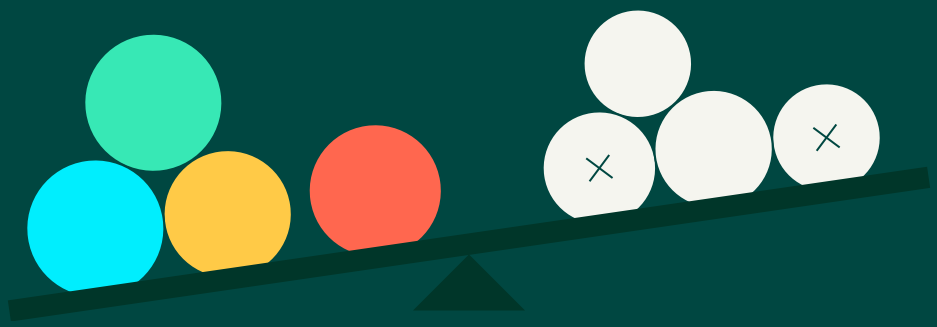
93 %

der externen Unternehmen berichteten, dass Angreifer während eines Cyberangriffs versuchten, Datensicherungen zu beschädigen.

73 %

gaben an, dass Versuche zumindest teilweise erfolgreich waren.

Jeder **„tut etwas“”** für die Datensicherheit, aber 2022 waren die Datensicherheitsinitiativen noch kaum aufeinander abgestimmt ®



56 %

aller Unternehmen haben mindestens eine Zero-Trust-Initiative durchgeführt.

56 %

haben einen Reaktionsplan aufgestellt oder überarbeitet.

54 %

haben Backup- und Wiederherstellungsoptionen getestet.

52 %

haben Datenwiederherstellungsprozesse erstellt oder ihre Ausführung optimiert.

Die Fallstudie

2024

Eine in den USA ansässige Bildungseinrichtung hat 2022 die harte Realität, was Datensicherheit angeht, selbst erlebt. Anhand ihrer Geschichte werden wir untersuchen, wie verbreitet ihre Erfahrung tatsächlich ist.

Die Fakten in dieser Fallstudie sind wahr, aber der tatsächliche Name der Organisation wurde anonymisiert, um Kundendaten zu schützen.

Die Umgebung der Stone University

2,9 PB
logischer Speicher

64 BETB
physisch gespeicherte Daten

Daten in zwei
getrennten Umgebungen

155 %
Datenwachstum im Jahr 2022

WAS SIE NICHT WISSEN,

WIRD IHNEN SCHADEN

Angreifer verschafften sich Zugriff auf das System der Stone University mittels einer Log4j-Sicherheitslücke, die bewirkte, dass der Server des Helpdesk-Ticketsystems anfällig für Angriffe war.

Log4j

Ende 2021 sorgte eine Sicherheitslücke in weithin eingesetzter Open-Source-Software, der Log4j-Softwarebibliothek von Apache, für Aufruhr in der IT-Branche. Innerhalb von 12 Stunden begannen Cyberkriminelle, diese Sicherheitslücke, die jetzt als „Log4Shell" bezeichnet wird, auszunutzen, und tun das bis heute.[5].

5 Laut The Guardian ist die vor Kurzem erkannte Software-Schwachstelle „die kritischste Sicherheitslücke des letzten Jahrzehnts".

Durch den Zugriff auf diesen Server gelang es den Angreifern, die Sicherheitsmaßnahmen an den Grenzen der Infrastruktur zu umgehen.

Die Angreifer setzten eine Mischung aus legitimen Tools ein, um illegale Zugangsdaten zu erstellen, ihren Zugriff zu erweitern, sich in der gesamten Umgebung weitere Standbeine zu schaffen und Active Directory zu kompromittieren.

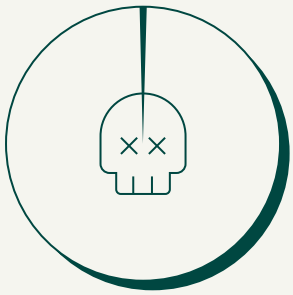
Die Cyberkriminellen bewegten sich durch die gesamte Stone University und verschafften sich Zugang zu fünf verschiedenen Rechnern in der VMware-Umgebung der Universität. Dabei sammelten sie wichtige Informationen – ohne dass die Stone University dies bemerkte.

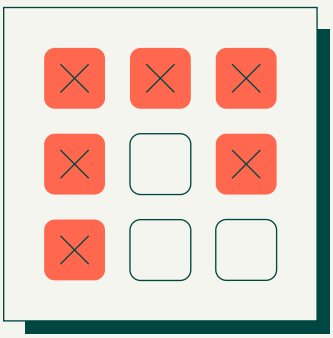
1 2 3 4 5

Was der Stone University passiert ist, ist zwar besorgniserregend, aber wenn man sich an dem orientiert, was viele andere Unternehmen im letzten Jahr erlebt haben, ist es keineswegs außergewöhnlich. ®

99 %

der IT- und Sicherheitsverantwortlichen wurden im Jahr 2022 auf mindestens einen Cyberangriff auf ihr Unternehmen aufmerksam gemacht. Im Durchschnitt mussten sich **Verantwortliche im Jahr 2022 52-mal mit Angriffen auseinandersetzen.**





61 %

dieser Angriffe betrafen SaaS-Anwendungen, die Umgebung, die am häufigsten das Ziel eines Angriffs ist.

DATEN-DEEP-DIVE:

Alle Arten von Umgebungen waren von böswilligen Aktivitäten betroffen, zu folgenden Anteilen:

61 % SaaS

62 % Cloud

50 % Lokal

Nach Angaben von Expel stieg 2022 die Anzahl der bösartigen Vorfälle in den drei großen Public Clouds gegenüber 2021 um 70 %.

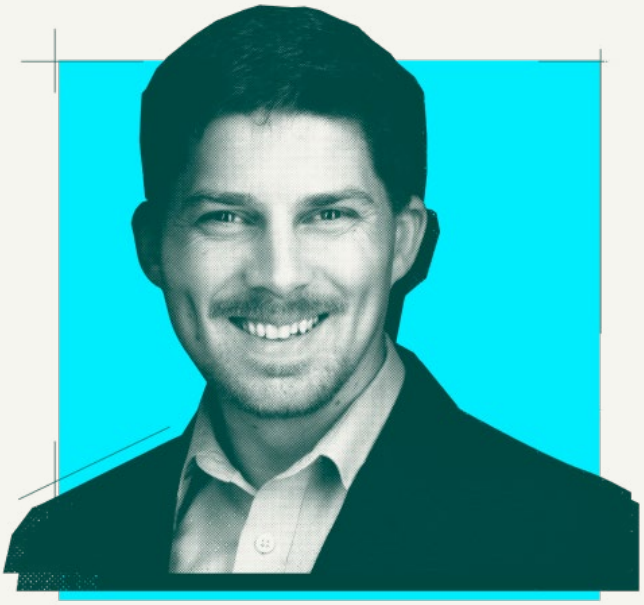
Hinweis: Die drei genannten Public Clouds sind Amazon Web Services (AWS), Google Cloud Platform (GCP) und Microsoft Azure (Azure).[6]

Nachdem sich die Cyberkriminellen über die Sicherheitslücke Zugang zur Umgebung der Stone University verschafft hatten, gingen sie schnell dazu über, Anmeldedaten böswillig einzusetzen. Permiso meldete, dass 100 % der Cloud-Eingriffe, die von Permiso erkannt wurden und auf die Permiso reagiert hatte, das Ergebnis von kompromittierten Zugangsdaten waren.[7]

Darüber hinaus gewährten diese Zugangsdaten zu mehr als 90 % viel zu hohe Berechtigungen, d. h. in der Regel wurden nur 5 bis 10 % der zugewiesenen Berechtigungen tatsächlich genutzt.[8]

„Die meisten Unternehmen haben wenig bis gar keinen Einblick in die Nutzung ihrer IDs … Diese werden weder überwacht, noch überprüft und es ist nicht leicht zu erkennen, wenn sie kompromittiert werden. Mit dem Wachstum von API-gesteuerten Ökosystemen werden diese geheimen Daten in rasantem Tempo weitergegeben und verbreitet, wodurch die Anzahl der kompromittierten Schlüssel, Tokens und Zertifikate drastisch ansteigt."

Ian Ahl, VP und Head of P0 Labs, Permiso



6 https://expel.com/blog/2023-great-expeltations-report-top-six-findings/
7 https://permiso.io/blog/s/permiso-2022-end-of-year-observations
8 https://permiso.io/blog/s/permiso-2022-end-of-year-observations

TAG 4:
VORBEREITUNG DER RANSOMWARE

KLOPF, KLOPF

Unternehmen wissen oft erst, dass sie angegriffen werden, wenn der Angreifer es ihnen mitteilt.

Die noch immer unentdeckten Angreifer der Stone University **bereiteten sich darauf vor, ihre Anwesenheit bekannt zu machen.**

Sie sorgten dafür, dass sie über mehrere Zugangspunkte über die Systeme der Stone University verfügen, damit ...

DIE STONE UNIVERSITY DAS FORTSCHREITEN DES ANGRIFFS NICHT DURCH DAS SCHLIESSEN EINER EINZELNEN TÜR AUFHALTEN KONNTE.

Sie verschafften sich auch Zugang zu einem alten Daten-Backup-Server, um **die Reaktion der Stone University zu beobachten.**

Ironischerweise war die Stone University zuvor zu einem anderen Backup-Anbieter und einer anderen Backup-Technologie gewechselt, hatte diesen Server aber beibehalten, obwohl er nicht mehr gebraucht wurde.

Zuletzt
exfiltrierten die Cyberkriminellen acht Gigabyte (GB) an Daten aus der gesamten Stone University.

Die Cyberkriminellen

BLIEBEN WÄHREND DIESES

gesamten Vorgangs UNBEMERKT.

Wie häufig sind Ransomware-Angriffe? ®

40 %

40 % der befragten externen Unternehmen meldeten einen erfolgreichen Ransomware-Angriff.

11 %

Expel berichtete, dass 11 % aller bösartigen Vorfälle, auf die das SOC gestoßen ist, mit Ransomware-Aktivitäten in Zusammenhang stehen.[9]

18 %

Mandiant meldete, dass 18 % seiner Einsätze Ransomware-Ereignisse betrafen.[10]

DATEN-DEEP-DIVE:

Wie häufig sind Cyberangriffe?
Arten von Angriffen auf Unternehmen im Jahr 2022:

- 59 % Datenklau
- 54 % Kompromittierung von Geschäfts-E-Mails oder betrügerischer Datentransfer
- 41 % durch Insider ausgelöste Vorfälle
- 40 % Ransomware

Die Handlungsweise der Angreifer der Stone University entsprechen Mandiants Daten zu mittleren globalen Verweilzeiten von Angreifern:

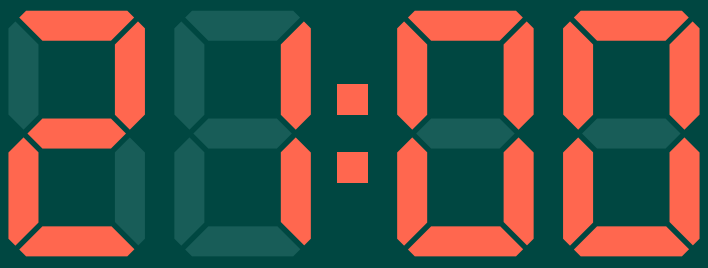
- Mittlere globale Verweilzeit
- 16 Tage – Alle Untersuchungen
  (Spionage, finanzieller Gewinn, unbekannter Ausgang usw.)
- 9 Tage – Ransomware-Untersuchungen
  (18 % aller Mandiant-Untersuchungen)
- Die Verweildauer bei Ransomware-Untersuchungen ist in der Regel kürzer, da der Angreifer sich selbst zu erkennen gibt, indem er die Lösegeldforderung sendet oder eine Umgebung verschlüsselt.[11]

9https://expel.com/blog/2023-great-expeltations-report-top-six-findings/
10https://www.mandiant.com/m-trends
11https://www.mandiant.com/m-trends

TAG 5:
AKTIVIERUNG DER RANSOMWARE

OH NEIN!

Die Angreifer der Stone University begannen am Sonntagabend gegen 21 Uhr mit der Lösegeldphase ihres Angriffs.



Sie verwendeten AvosLocker, um Dateien innerhalb der VMware ESXi-Infrastruktur auf 150 VMs zu verschlüsseln, darunter auch die ersten fünf für den Angriff verwendeten VMs.

AvosLocker fuhr außerdem die Tools zum Verwalten der virtuellen Maschinen kurz vor dem Verschlüsseln der Dateien herunter, um zu verhindern, dass die Stone University effektiv reagieren konnte.

AvosLocker

„AvosLocker" bezeichnet sowohl eine Malware-Familie als auch eine Bedrohungsgruppe. Es handelt sich hierbei um „Ransomware-as-a-Service" als „Geschäftsmodell", bei dem Partner einen Service zum Installieren von Ransomware und zum Fordern von Lösegeld abonnieren. Im Fall von AvosLocker umfasst das Abonnement die direkte Abwicklung von Lösegeldverhandlungen, die Veröffentlichung exfiltrierter Daten von Opfern sowie den tatsächlichen Einsatz eines speziellen Ransomware-Tools.[12]

12https://www.cisa.gov/news-events/alerts/2022/03/22/fbi-and-fincen-release-advisory-avoslocker-ransomware

Zuletzt machten die Angreifer ihre Forderung bekannt:

in der Mitte Ransomware **SCHLÄGT** der Geschichte zu, nicht am Anfang oder am Ende.

Viele Menschen glauben, dass das Verschlüsselungsereignis das Ende der Ransomware-Geschichte ist, aber das ist fast nie der Fall. So hatten die Cyberkriminellen beispielsweise tagelang unbemerkt ungehindert Zugang zu den Systemen der Universität. Und es wird noch einige Tage dauern, bis diese Ransomware-Geschichte zu Ende erzählt ist.

DATEN-DEEP-DIVE:

Ransomware ist eine Art von Bedrohung, bei der Dateneigentümern der Zugriff auf ihre Daten unmöglich gemacht wird.

Bei einem Angriff mit dem Ziel, Daten unzugänglich zu machen, können Ransomware, Wiper, Datenlöschungen über gültige Zugangsdaten und Dienstverweigerung (Denial of Service) zum Einsatz kommen. Darüber hinaus exfiltrieren Cyberkriminelle routinemäßig Daten für eine ganze Reihe von Zielen vor Verschlüsselungsvorgängen.

Im Jahr 2022 hat das Ransomware Response Team von Rubrik Dutzenden von Organisationen bei der Wiederherstellung von Daten geholfen.

Am häufigsten ging es bei diesen Reaktionen um folgende Ransomware-Familien:

- LOCKBIT2.0
- BLACKCAT/ALPHV
- AVOSLOCKER
- META
- PLAY
- HIVE
- SPARTA
- BLACK BASTA
- SPIDER
- VICE Society

GEWINNEN SIE DIE KONTROLLE ZURÜCK

Ob Sie einen Angriff abwehren können, hängt davon ab, wie schnell Sie reagieren können

Die Stone University begann schnell damit, auf den Vorfall zu reagieren, wurde aber durch den Umfang der Verschlüsselung in ihren Möglichkeiten eingeschränkt.

Um dieses Problem zu lösen, stellten die zuständigen Experten Daten in forensischen Umgebungen und Testumgebungen wieder her, um sie zu untersuchen und die nächsten Maßnahmen zu priorisieren.

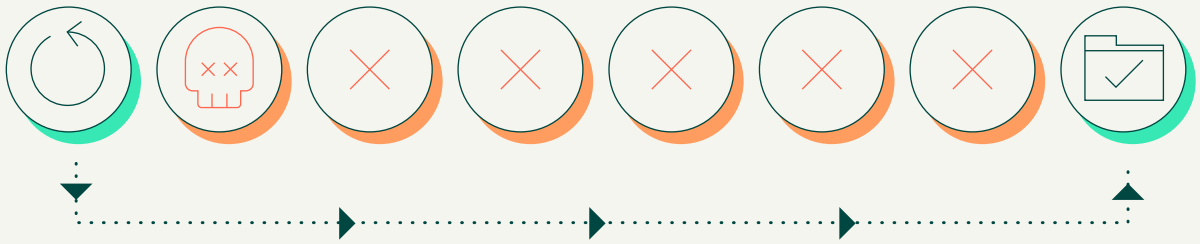
Die Stone University analysierte außerdem ihre Offline-Daten-Backups, entdeckte einen mutmaßlich kompromittierten Server und band diesen Server per LiveMount zur Detailanalyse in die forensische Umgebung ein.

Dann stieß das Team auf den JACKPOT

Es fand die Notizen der Angreifer mitsamt ihrem Kompromittierungsplan, einer Liste aller kompromittierten Konten und einem Zeitplan. Weitere forensische Untersuchungen brachten sieben weitere kompromittierte Server und den ersten Kompromittierungspunkt zutage.

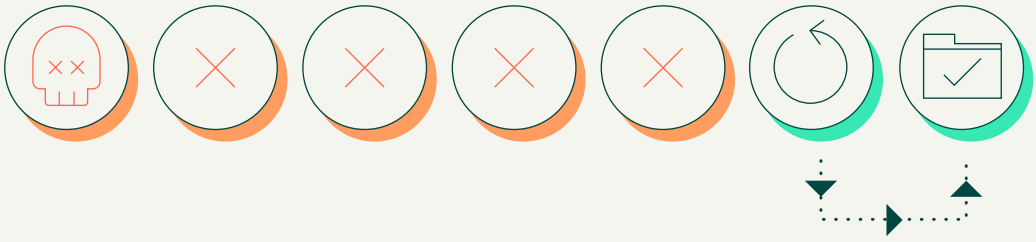
Hoffnungsvoll begann die Stone University mit dem raschen Wiederaufbau der Umgebung in zwei Wellen:

Zuerst die tatsächlich kompromittierten Server aus dem ersten Zugriff.



Das Team der Stone University stellte die acht kompromittierten Server, die sich in fünf VMs befanden, auf einen Zeitpunkt wieder her, der einen Tag vor dem Eindringen der Angreifer lag. Dadurch gingen insgesamt sechs Tage an Daten verloren.

Anschließend die Server, die mit Ransomware verschlüsselt, aber nicht Teil der ursprünglichen Kompromittierung waren.



Damit blieben noch 145 VMs übrig. Für diese war eine weniger intensive Reaktion allein auf der Grundlage der Verschlüsselungsaktion erforderlich. Diese 145 VMs wurden aus Backups wiederhergestellt, die nur einen Tag vor der Aktivierung der Ransomware erstellt worden waren, wodurch fünf zusätzliche Tage Datenverlust auf diesen 145 VMs vermieden wurden.

Der gesamte Wiederherstellungsvorgang erforderte außerdem neue ESXi-Hosts, ein neues vCenter und einen Neuaufbau von Active Directory.

Von allen möglichen Ergebnissen war dies so ziemlich das beste, was sich die Stone University erhoffen konnte. Das Team der Stone University war optimistisch und entschlossen, das Lösegeld nicht zu zahlen.

Es kann leicht passieren, dass man die erste große Hürde bei einem Verschlüsselungsereignis übersieht:

Wie kann man etwas, das verschlüsselt ist, diagnostizieren und analysieren? Hilft es, das Lösegeld zu bezahlen? Wer sich durch das Erstellen sauberer Kopien seiner Daten auf diesen ersten Verschlüsselungsmoment vorbereitet, hat bessere Erfolgschancen. Die Stone University war vorbereitet, aber was gehört dazu, um auf diesen Moment vorbereitet zu sein?

Hilft es, Lösegeld zu bezahlen? ®

46 %

Externe Unternehmen, die ein Lösegeld gezahlt haben, konnten mit den von den Angreifern bereitgestellten Entschlüsselungslösungen nur begrenzte Erfolge erzielen: 46 % konnten die nur Hälfte ihrer Daten oder weniger auf diese Art wiederherstellen.

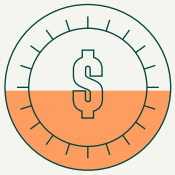
16 %

Nur 16 % aller externen Unternehmen konnten ihre Daten mithilfe der Entschlüsselungstools der Angreifer wiederherstellen.

Telemetriedaten von Rubrik offenbarten die Prävalenz von Ransomware-Vorläufern und Verschlüsselungsraten. ®

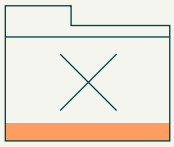
75 %

der Unternehmen haben ein gewisses Maß an anomalen Aktivitäten beobachtet.



48 %

der Unternehmen weltweit haben versuchte Ransomware-Angriffe in der einen oder anderen Form gegen sie festgestellt.



15 %

der Unternehmen weltweit haben eine Form von erfolgreicher Verschlüsselung in ihren Umgebungen festgestellt, die eine Datenwiederherstellung erforderlich macht.

Weniger als **0,004 %** der gesicherten Daten waren von einem Verschlüsselungsereignis betroffen. ®

REFERENZTERMINOLOGIE:

Erkennung anomalen Verhaltens
Die Erkennung von anomalem Verhalten ist die erste Phase in einem zweistufigen Prozess zur Identifizierung von Ransomware. Während dieses Prozesses analysiert Rubrik die Metadaten des Dateisystems auf anomales Verhalten, z. B. eine ungewöhnliche Anzahl von Dateien, die hinzugefügt, gelöscht oder repliziert wird. Bei den meisten anomalen Aktivitäten handelt es sich nicht um Ransomware, sie müssen jedoch weiter untersucht werden.

Erkennung verdächtiger Dateien
Die zweite Phase des zweistufigen Ransomware-Erkennungsprozesses ist die Erkennung verdächtiger Dateien. Mit einer Kombination aus künstlicher Intelligenz und maschinellem Lernen werden in dieser Phase die zuvor identifizierten Dateien auf Datenentropie, Dateierweiterungen, Komprimierung, bekannte bösartige Ransomware-Aktivitäten und eine Vielzahl anderer Faktoren untersucht, die auf Ransomware hindeuten.

Snapshot-Analyse
Ein Snapshot ist eine Kopie des Offline-Daten-Backups und erfolgt in der Regel in einem automatisierten, wiederkehrenden Muster
oder in Ad-hoc-Aufgaben. Anhand der fertigen Snapshots können dann Analysen durchgeführt werden.

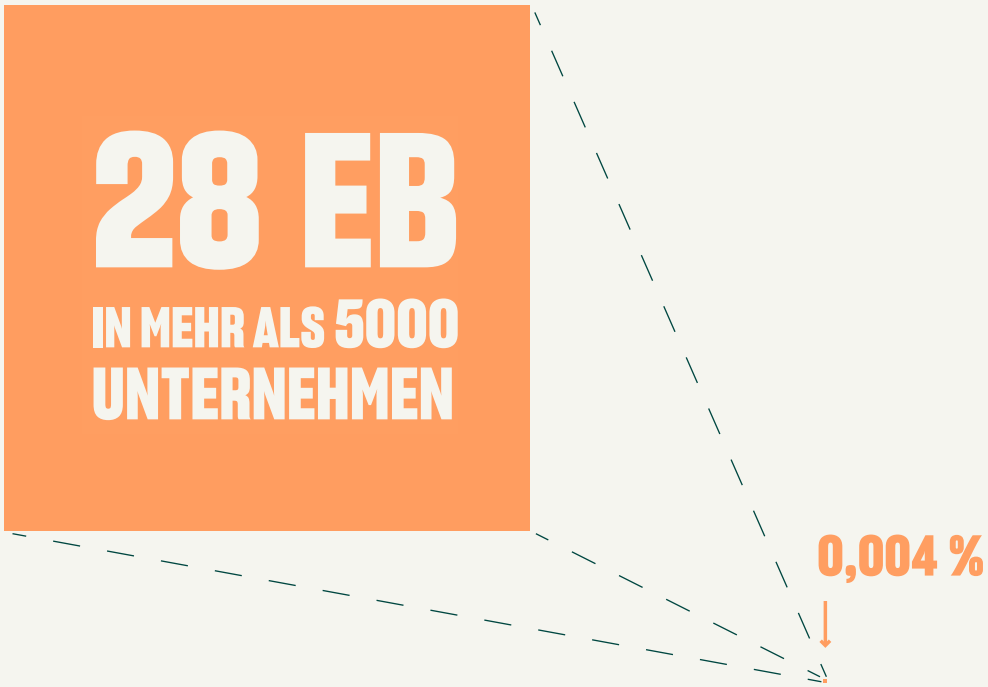
- 27.266.649 Snapshots von allen Rubrik-Kunden wurden auf Ransomware-Aktivitäten untersucht
- 20.692 Snapshots, das sind 0,07 % aller Snapshots, enthielten anomale Aktivitäten.
- 1.198 der anomalen Snapshots, also 6 % aller anomalen Aktivitäten, zogen ein Verschlüsselungsereignis nach sich, das die Fertigstellung des Snapshots verhinderte.
- Nur bei 0,004 % aller ausgewerteten Snapshots lag ein Verschlüsselungsproblem vor.
- Alle Verschlüsselungsvorgänge wurden zuvor als anomale Aktivitäten identifiziert.
- 100 % der Verschlüsselungsvorfälle waren auf eine fehlende Multi-Faktor-Authentifizierung zurückzuführen.

Bei allen Rubrik-Kunden im Jahr 2022 ®

erforderten weniger als 0,004 % aller gesicherten Daten eine weiterführende Analyse oder wiesen auf Ransomware-Aktivitäten hin.

Dies bietet eine Momentaufnahme davon, wie ein Unternehmen die Kontrolle über seine Bedrohungslage erlangen kann.

Es ist praktisch unmöglich, Ihr Unternehmen komplett aus der Schusslinie zu nehmen, aber Sie können Ihre Angriffsfläche stark verkleinern.



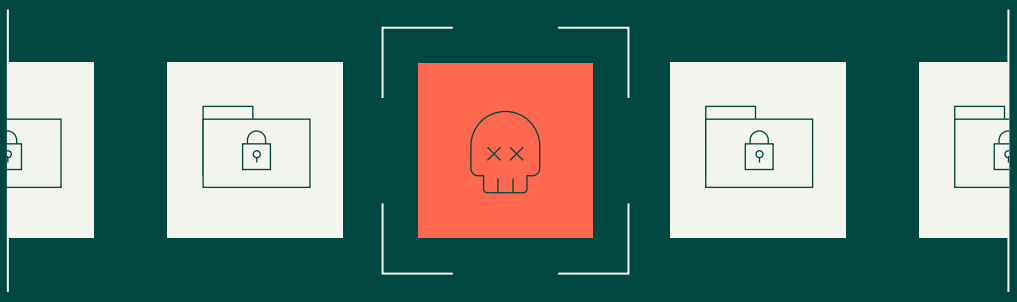
TAG 8:
ZWEITE LÖSEGELDFORDERUNG

MOMENT... WAS?

Verschlüsselung ist nicht die einzige (oder bevorzugte) Waffe von Angreifern

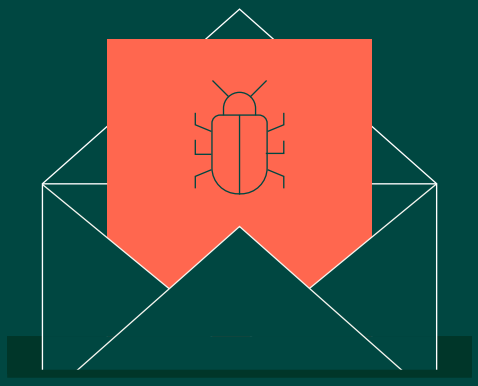
3 TAGE NACH

der ersten Lösegeldforderung schickten die Angreifer eine zweite. Darin drohten sie damit, die 8 GB an exfiltrierten Daten an eine von AVOSLOCKER kontrollierte Leak-Site weiterzuleiten, wenn das Lösegeld nicht innerhalb von vier Tagen gezahlt würde.



Die Angreifer versuchten auch, weitere Teile der Umgebung der Stone University zu kompromittieren, um die Gegenmaßnahmen zu überstehen.

Nach einem hoffnungsvollen Start warf diese unerwartete Wendung die Stone University zurück an den Anfang und stellte das Unternehmen vor eine weitere schwierige Entscheidung:



das Lösegeld zu zahlen oder zu erleben, wie interne Daten online veröffentlicht werden.

72 %

der nicht durch Rubrik geschützten Unternehmen meldeten, dass sie auf eine Lösegeldforderung eingegangen sind.[WR]

DATEN-DEEP-DIVE:

Für nicht durch Rubrik geschützte Unternehmen, die ein Lösegeld zahlten, gilt: (WR)

40 %

gingen wegen Verschlüsselungsereignissen auf eine Lösegeldforderung ein.

37 %

gingen aufgrund der Drohung, dass andernfalls Daten veröffentlicht werden, auf eine Lösegeldforderung ein.

Von Palo Alto Networks Unit 42 als Reaktion auf Vorfälle beobachtete Lösegeldzahlungen im Jahr 2022: (ER)

+50 Mio. USD

Höchste Lösegeldforderung

+7 Mio. USD

Höchstes gezahltes Lösegeld[13]

13https://start.paloaltonetworks.com/2023-unit42-ransomware-extortion-report

UND TIEF DURCHATMEN

Datentransparenz schafft Entscheidungsmöglichkeiten

Die Stone University setzte auf drei verschiedene Maßnahmen, um auf die Lösegeldforderung zu reagieren.

1

Zunächst wurden Erkennungs- und Reaktionsmaßnahmen durchgeführt, um nachfolgende Angriffsversuche zu erkennen und dagegen vorzugehen. Dazu mussten mehrere Server ausgetauscht, mehrere Firewalls ersetzt und andere Absicherungsmaßnahmen ergriffen werden.

2

Zweitens wurde der Einsatz zur Datenwiederherstellung fortgesetzt, indem Teile der wiederhergestellten Umgebungen getestet und diese Teile dann in die Produktionsumgebung übernommen wurden.

NEW
3

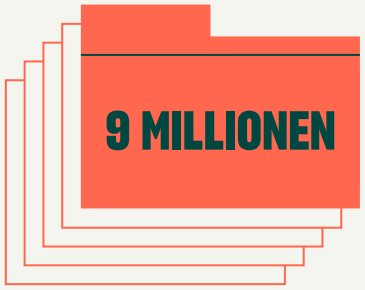
Drittens begann die Stone University damit, abzuschätzen, welche Auswirkungen es hätte, sollte der Angreifer die exfiltrierten Daten online stellen.

Aber ...

Die Stone University konnte aufgrund der anhaltenden Datenverschlüsselung nicht feststellen, ob die Angreifer tatsächlich 8 GB Daten gestohlen hatten oder welche Daten genau gestohlen wurden.

Also ...

Stattdessen legte die Stone University den Fokus bei der Erkennung von Datenauswirkungen auf das letzte Daten-Backup.

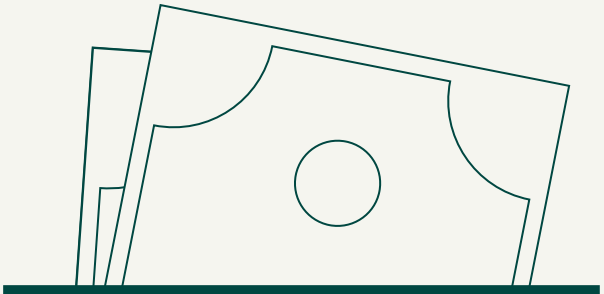


Die gute Nachricht

Die Stone University fand innerhalb von 24 Stunden Antworten und hatte nun drei Tage Zeit, fundierte Entscheidungen zu treffen.

Die schlechte Nachricht

Die Angreifer hatten 8 GB an Daten mit mehr als 9 Millionen sensiblen Datensätzen von 2013 bis heute gestohlen.



DIE STONE UNIVERSITY ENTSCHIED SICH DAFÜR, AUCH DAS ZWEITE LÖSEGELD NICHT ZU ZAHLEN, UM ZU VERMEIDEN, DASS GELD IN DIE TASCHEN VON KRIMINELLEN FLIESST.

Die Veröffentlichung der sensiblen Daten im Internet wäre zwar ein schwerer Schlag für die Stone University, aber dafür war die Stone University um eine bittere Erkenntnis reicher: Es gibt keine Garantie dafür, dass keine sensiblen Daten veröffentlicht werden, **selbst wenn das Lösegeld gezahlt wird.**

Stattdessen
nutzte die Stone University die drei Tage, um die betroffenen Personen und Organisationen proaktiv zu informieren.

Bis die Daten veröffentlicht wurden, hatte die Stone University alle mühsamen, aber notwendigen und wichtigen Maßnahmen ergriffen und

- ✓ die Regulierungs- und Compliance-Organisationen benachrichtigt
- ✓ die betroffenen Personen kontaktiert
- ✓ den Fokus auf langfristige Verbesserungen und andere erforderliche Datenleck-Maßnahmen gesetzt

Der Dominoeffekt

Der Großteil der Stone University ging nach Beendigung des Angriffs wieder zum Normalbetrieb über. Die zwei Wochen, in denen sich das Ransomware-Ereignis abspielte, hatten jedoch Nachwirkungen, deren Behebung Wochen bis Monate an Bemühungen und Entscheidungen erfordern würde.

Schnell wechselnde und verstreute Daten stellen ein echtes Risiko für Unternehmen dar.[RT]

Ein typisches Unternehmen besitzt

Dateien mit sensiblen Daten

sowie

Datensätze, die in ihrer Gesamtheit sensibel sind.

Dateien und sensible Datensätze: Dateien enthalten Datensätze. Manche dieser Datensätze können sensibel sein. So kann beispielsweise eine Tabellenkalkulationsdatei Hunderte von sensiblen Datensätzen enthalten, während andere Dateien möglicherweise keine sensiblen Daten enthalten.

Ein typisches Unternehmen verfügt über genügend sensible Daten, um hohe finanzielle Strafen zahlen zu müssen.

DATEN-DEEP-DIVE:

Jedes globale Unternehmen verfügt nicht nur über eine riesige Menge an Daten, sondern einige dieser Daten könnten einen erheblichen Schaden verursachen, wenn sie plötzlich nicht mehr zur Verfügung stünden oder kompromittiert würden.

Ein Beispiel dafür sind sensible Daten. Welche Daten als sensibel gelten, hängt von verschiedenen Industriestandards oder -vorschriften ab, z. B. PII, HIPAA, DSGVO und CPAA.[14,15,16,17]

Bei der Bewertung der Auswirkungen von Daten auf Verbraucher sowie Unternehmen gibt es zahlreiche Herausforderungen. Finanzielle Sanktionen für sensible Daten sind eine Option.[18,19,20]

HIER EIN PAAR BEISPIELE:

DSGVO
Geldstrafe für die Offenlegung sensibler Daten: Bis zu 20 Mio. Euro oder 4 % des weltweiten Unternehmensumsatzes bei schweren Verstößen, je nachdem, welcher Betrag höher ist.

In einer typischen Umgebung würde eine Geldstrafe von weniger als zwei Euro pro Datensatz reichen, um auf 20 Mio. Euro zu kommen.

HIPAA
Geldstrafe für die Preisgabe sensibler Daten: 50 bis 50.000 USD pro Verstoß, mit einem Höchstbetrag von 1,5 Mio. USD.

Wenn man nur die typische Datei-Durchschnittsanzahl heranzieht, würde die Gesamtsumme den Höchstbetrag von 1,5 Mio. USD ohne Weiteres übersteigen und bei der niedrigsten Geldstrafe von 50 USD insgesamt 28 Mio. USD betragen.

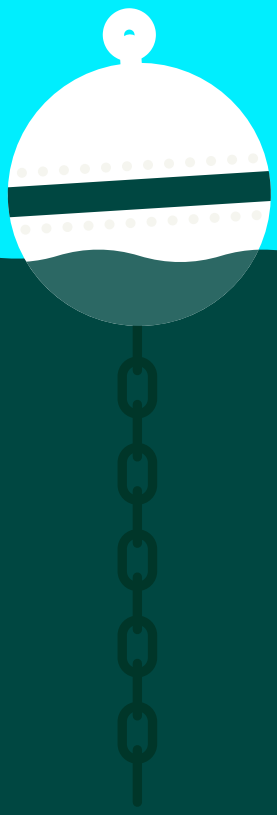
CPRA
Strafe für die Offenlegung sensibler Daten: Bis zu 2.500 USD pro Verstoß oder bis zu 7.500 USD für jeden vorsätzlichen Verstoß. Die Strafsumme ist nach oben offen.

Schon die Dateianzahl eines typischen Unternehmens könnte 1,1 Mrd. USD an Geldbußen nach sich ziehen.

14https://gdpr-info.eu/art-4-gdpr/
15https://www.cdc.gov/phlp/publications/topic/hipaa.html
16https://www.dol.gov/general/ppii
17https://oag.ca.gov/privacy/ccpa#:~:text=The%20right%20to%20limit%20the,personal%20information%20collected%20about%20them.
18https://gdpr-info.eu/issues/fines-penalties/#:~:text=83(5)%20GDPR%2C%20the,fiscal%20year%2C%20whichever%20is%20higher.
19https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/north-america/united-states/topics/penalties-for-non-compliance
20https://cppa.ca.gov/

AUSWIRKUNGEN

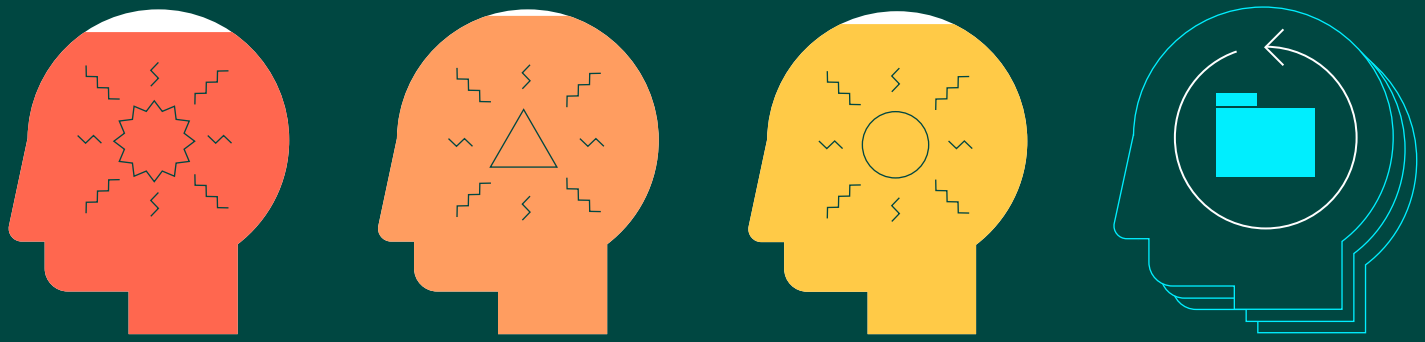
Jeder Angriff endet irgendwann. Allerdings sollte man sich dann nicht entspannt zurücklehnen. Stellen wir uns stattdessen vor, dass wir von unserem Tauchgang in die Tiefe an die Meeresoberfläche zurückgekehrt sind.



Was sollten wir aus diesem Fall lernen?
Was werden wir anders machen?

Angriffe haben Auswirkungen auf Unternehmen und Menschen

Diese Angriffe haben noch lange nach Abschluss der forensischen Untersuchungen und IT-Maßnahmen Auswirkungen auf unsere Unternehmen und auf uns Menschen. Sie bewirken, dass wir unsere eigene Handlungsfähigkeit anzweifeln.



93 %

der Unternehmen, die im Jahr 2022 Opfer eines Cyberangriffs wurden, hatten mit negativen Auswirkungen zu kämpfen.

98 %

der IT- und Sicherheitsverantwortlichen berichteten über erhebliche emotionale oder psychische Auswirkungen von Cyberangriffen.

96 %

Die allermeisten Verantwortlichen befürchten, dass ihre Unternehmen nicht in der Lage sein werden, die Geschäftskontinuität aufrechtzuerhalten, wenn sie Opfer eines Cyberangriffs werden.

39 %

Mehr als ein Drittel der Führungskräfte ist der Ansicht, dass der Vorstand oder die Führungsetage wenig bis gar kein Vertrauen in die Fähigkeit des eigenen Unternehmens hat, kritische Daten und Geschäftsanwendungen im Falle eines Cyberangriffs wiederherzustellen.

der externen Unternehmen werden wahrscheinlich einer Lösegeldforderung nachgeben.

93 % der Unternehmen, die im Jahr 2022 Opfer eines Cyberangriffs wurden, hatten mit negativen Auswirkungen zu kämpfen: ®

49 %
Verlust von Kunden

45 %
Verlust von Einnahmen

44 %
negative Schlagzeilen und/ oder Rufschädigung

42 %
erzwungene Veränderungen in der Führungsetage

5 %
negative Auswirkungen auf den Aktienkurs

Diese Angriffe belasten Führungskräfte. 98 % der Befragten berichteten, dass Cyberangriffe im vergangenen Jahr erhebliche emotionale und/oder psychische Auswirkungen auf sie hatten:

53 %
vermehrt Angst in Bezug auf die eigenen Aufgaben

46 %
Sorgen um den Arbeitsplatz

43 %
Vertrauensverlust unter Kollegen und Teammitgliedern

41 %
Schlaflosigkeit oder Schlafstörungen

Nachwirkungen kommen zu bereits vor dem Angriff bestehenden Problemen hinzu ®

Angriffe sind keine isolierten Ereignisse. Herausforderungen gab es schon vor dem Angriff, und zu diesen bereits bestehenden Problemen kommen nun vorhersehbare Nachwirkungen hinzu:

47 %

Fast die Hälfte (47 %) der IT- und Sicherheitsverantwortlichen ist der Meinung, dass ihr Cybersicherheitsbudget für 2023 nicht ausreichend ist, um notwendige Investitionen zu ermöglichen.

27 %

derselben Führungskräfte gehen davon aus, dass ihre Budgets für IT und Cybersicherheit im Jahr 2023 geringer ausfallen werden.

4 %

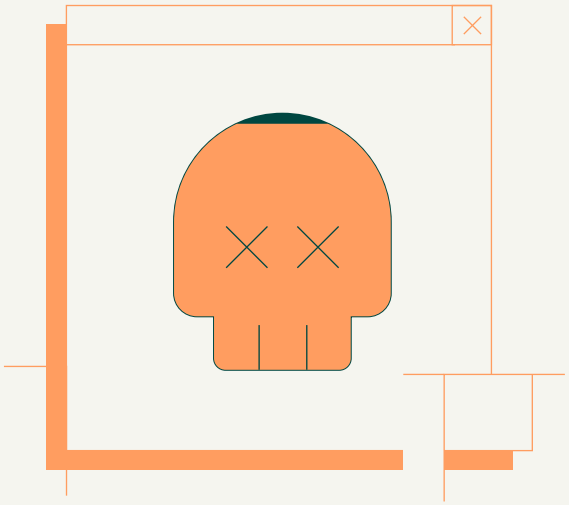
IT- und Sicherheitsverantwortliche müssen daran arbeiten, ihre Teams richtig aufzustellen. Nur 4 % geben an, dass es keine Faktoren gibt, die die Abstimmung von IT- und Sicherheitsteams einschränken.

Die fünf wichtigsten Probleme, die zu einer mangelnden Abstimmung zwischen IT- und Sicherheitsteams beim Schutz ihrer Unternehmen vor Cyberangriffen führen, sind: ®

1. **52 %** Unterschiedliche Tools
2. **51 %** Unterschiede in der Transparenz
3. **50 %** Kollidierende Prioritäten
4. **47 %** Fehlende formale Planung bzw. fehlende formale Prozesse
5. **45 %** Schlecht abgestimmte Führungsstrukturen

Angriffe können auch eine Chance sein ®

Es gibt Licht in der Dunkelheit: Ihr Unternehmen kann die unvermeidlichen Bedrohungen überstehen und gestärkt daraus hervorgehen. Gerade diese Angriffe bieten Gelegenheit für Verbesserungen und wichtige Veränderungen.



99 %

der Unternehmen, die 2022 Opfer eines Cyberangriffs wurden, haben neue Maßnahmen ergriffen:

48 %

sind zu einem anderen Anbieter gewechselt oder andere Partnerschaften eingegangen, um bessere Ergebnisse zu erzielen

54 %

höhere Ausgaben für neue Technologien oder Dienstleistungen

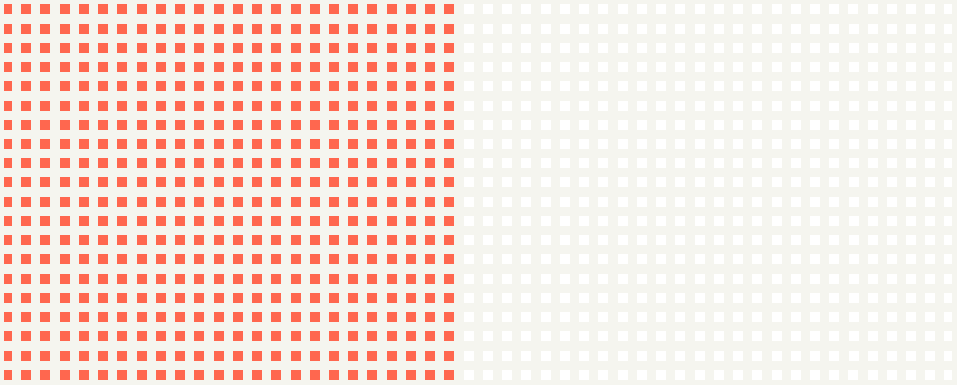
43 %

Einstellung zusätzlicher Mitarbeiter

Trotz all dieser Herausforderungen wird der Sicherheitsstatus von Unternehmen insgesamt besser ®

Aber Veränderungen gehen nicht immer nur auf Cyberangriffe zurück. Wenn wir bereit sind, Chancen zu nutzen, die sich aus Krisen und systematischen Bemühungen um Resilienz ergeben, können wir Erfolg haben.

Obwohl **48 %** der Rubrik-Kunden in irgendeiner Form von einem Ransomware-Vorfall betroffen waren ...



... waren weniger als **0,004 %** der gesicherten Daten von einem Verschlüsselungs-ereignis betroffen.

Rubrik Zero Labs hat beobachtet, dass Unternehmen im Laufe des Jahres 2022 Maßnahmen zur Verbesserung der Lage ergriffen haben, und erwartet, dass sich dieser Trend 2023 fortsetzen wird. Diese Verbesserung ist in allen Branchen und Regionen spürbar.

16 %

Diese Veränderungen haben bewirkt, dass Unternehmen ihren Sicherheitsstatus im Jahr 2022 um durchschnittlich 16 % verbessert haben.

97 %

Expel merkt an, dass 97 % der Ransomware-Angriffe gestoppt wurden, bevor die Ransomware aktiviert werden konnte.[21]

21https://expel.com/blog/2023-great-expeltations-report-top-six-findings/

PERSPEKTIVE ZUR DATENSICHERHEIT VON EXPEL: (ER)

11 % aller von Expel im Jahr 2022 beobachteten Vorfälle hätten eine Aktivierung von Ransomware zur Folge haben können.

97 % dieser Vorfälle konnten gestoppt werden, bevor die Ransomware aktiviert wurde. Wenn Verteidiger den Angriffszyklus der Ransomware-Akteure erkennen und darauf reagieren können, besteht eine große Chance, ihre Angriffspläne zu vereiteln.[22]

Rubrik bietet seinen Kunden die Berechnung eines kumulativen Data Security Score an und erkennt einen kontinuierlichen, positiven Trend bei der organisatorischen Verbesserung. Der Data Security Score wird alle 24 Stunden basierend auf den folgenden Kategorien berechnet:

1. Plattformsicherheit: Misst die Wirksamkeit der Sicherheitsmaßnahmen für die Infrastruktur, in der Daten gespeichert sind, und umfasst Themen wie Benutzerkontrollen, Administrator-Authentifizierung, Prüfprotokolle usw.
2. Datenschutz und Wiederherstellung: Analysiert, wie gut die Backup-Daten gesichert sind, ob eine saubere Kopie des letzten Backups verfügbar ist, und andere damit zusammenhängende Faktoren.
3. Ransomware-Untersuchung: Bestimmt die Qualität und Häufigkeit der Überwachung im Hinblick auf Ransomware-Bedrohungen und auch, ob diese Daten nach einem Verschlüsselungsereignis wiederhergestellt werden können.
4. Erkennung sensibler Daten: Misst, wie gut sensible Daten geschützt werden, wie gut die Zugriffskontrollen für diese Daten funktionieren und ob sensible Daten für die Wiederherstellung priorisiert werden.
5. Die Punktzahlen (Scores) sind wie folgt zu lesen:
   - 0 bis 50: Mangelhaft
   - 51 bis 75: Es sind Verbesserungen nötig
   - 76 bis 90: Zufriedenstellend
   - 91+: Ausgezeichnet

Typischerweise stieg dieser Wert für globale Unternehmen im Jahr 2022 von **51,2** auf **59,47** was einer **Steigerung von 16 % entspricht**.

Durchschnittswerte bei der Gesamtbewertung: 59,47

Verbesserungsrate im Jahr 2022: 16,2 %

„Es muss immer bedacht werden, dass Sicherheit nicht in einem Vakuum existiert. Wenn Unternehmen versuchen, mit weniger Mitteln mehr zu erreichen, ist es dringend nötig, sich auf skalierbare, effiziente Technologien wie Cloud-Optionen zu stützen. Eine schnelle Einführung, insbesondere für Unternehmen, die nicht von Anfang an Cloud-basiert sind, ist jedoch mit einem gewissen Risiko verbunden. Da Unternehmen weiterhin stetig neue Technologien einsetzen, um mit den sich wandelnden Märkten Schritt zu halten, können Sicherheitsteams mit einer Zunahme von Sicherheitsvorfällen rechnen, die in der Regel auf leicht zu übersehende, leicht auszunutzende Fehlkonfigurationen oder ungeschützte Zugangsschlüssel zurückzuführen sind."

Jonathan Hencinski, VP, Security Operations, Expel

22https://expel.com/blog/2023-great-expeltations-report-top-six-findings/

Je mehr unsere Communitys von Cyberkriminalität betroffen sind, desto mehr stehen wir gegenseitig in der Verantwortung.

Wir können bessere Produkte entwickeln und uns für bewährte Verfahren einsetzen, wir müssen unser Wissen aber auch austauschen. Jede gewonnene Erkenntnis ist ein Schritt nach vorne.

MIT JEDEM SCHRITT VERBESSERT SICH UNSERE SICHERHEIT.

Daher möchte Rubrik Zero Labs mit derselben Aussage enden, mit der wir begonnen haben: Wir danken den vier Organisationen, die uns erlaubt haben, ihre Daten zu nutzen, und wir danken Wakefield Research für die geleistete Arbeit und Shaped By für den Einsatz beim Zusammenstellen dieses Berichts. Außerdem möchten wir die Beiträge der folgenden Rubrik-Mitarbeiter mit Dank für ihre Arbeit an diesem Projekt hervorheben Amanda O'Callaghan, Ajay Kumar Gaddam, Sham Reddy, Kumar Subramanian, Linda Nguyen, Lynda Hall, Kelsey Shively und Kelley Cooper sowie die Kreativ- und Entwicklungsteams von Rubrik.

Rubrik Zero Labs