

01

Die Risiken eines  
Cyberangriffs verstehen

02

Das Risiko eindämmen

03

Erfahren Sie mehr über die  
Wiederherstellung nach einem  
Ransomware-Angriff

04

Szenarien für die Wiederherstellung  
nach einem Cyberangriff

05

Lernen Sie praktische  
Anwendungen kennen

06

Gehen Sie proaktiv vor

**Zerto**

a Hewlett Packard  
Enterprise company

# CYBER ATTACK SURVIVAL KIT

Cyber-Resilienz dank schneller  
Wiederherstellung



DEMO ANFORDERN

WEITER



01

Die Risiken eines  
Cyberangriffs verstehen

02

Das Risiko eindämmen

03

Erfahren Sie mehr über die  
Wiederherstellung nach einem  
Ransomware-Angriff

04

Szenarien für die Wiederherstellung  
nach einem Cyberangriff

05

Lernen Sie praktische  
Anwendungen kennen

06

Gehen Sie proaktiv vor

# CYBER-RESILIENZ:

## Schützen Sie Ihr Unternehmen vor finanziellen Folgen und Rufschädigung

### Ransomware... Nicht ob, sondern wann und wie schwerwiegend?

Ransomware-Angriffe eskalieren seit Jahren und nehmen in Umfang und Schwere weiter zu. Cyberkriminelle nutzen bösartige Codes, um Schaden in Unternehmen anzurichten, und erfinden ständig neue und unerwartete Methoden, um Malware zu verbreiten und wichtige Daten zu verschlüsseln. Wenn Ihr Unternehmen angegriffen wird, werden wichtige Daten verschlüsselt, und die Behebung des Angriffs kann durch Rufschädigung und Umsatzeinbußen Millionen kosten. Die Kosten für Erpressungen steigen weiter, und die Angriffe werden immer spezifischer. Kein Unternehmen ist gegen einen Ransomware-Angriff gefeit.

Wie verbreitet ist das Problem der Ransomware in Unternehmen?

Im Jahr 2023 waren 66 % der Unternehmen von Ransomware betroffen<sup>1</sup>

Es wird erwartet, dass Ransomware bis zum Jahr 2031<sup>2</sup> alle zwei Sekunden ein Unternehmen, einen Verbraucher oder ein Gerät angreifen wird.

Angesichts der alarmierenden Statistiken und Schlagzeilen über Ransomware-Angriffe stellt sich nicht die Frage, ob es zu einem Angriff kommen wird, sondern wann und wie schwerwiegend er sein wird.

Noch erschreckender wird es, wenn man sich die Kosten dieser Angriffe ansieht.

Die durchschnittliche Lösegeldzahlung hat sich fast verdoppelt, von 812.380 US-Dollar im Jahr 2022 auf 1.542.333 US-Dollar im Jahr 2023<sup>1</sup>

Die Gesamtkosten für Ransomware werden sich im Jahr 2031 auf 265 Milliarden US-Dollar belaufen<sup>4</sup>

Eines ist klar: Ransomware wird nicht nur immer häufiger, sondern auch immer kostspieliger.

Unternehmen wie das Ihre konzentrieren sich seit langem darauf, Cyberangriffe auf ihre Rechenzentren und Benutzer zu verhindern. Da sich die Geschäftswelt jedoch rasant entwickelt, befinden sich Ihre Daten heute an unterschiedlichen Orten (vor Ort und in der Cloud), in verschiedenen Workloads und in den Händen von mehr Benutzern als je zuvor. Um in dieser sich wandelnden Bedrohungslandschaft anspruchsvollere Service-Levels zu erfüllen, muss Ihre Strategie die Wiederherstellung von Daten ebenso ernst nehmen wie die Prävention.

Wenn Sie wissen, dass ein Angriff erfolgen wird, brauchen Sie mehrere Verteidigungsschichten, zu denen auch die Wiederherstellung Ihrer Daten gehört.

<sup>1,3</sup> *Ransomware-Bericht 2023: Sophos-Bericht „State of Ransomware“*

<sup>2,4</sup> *Globale Kosten aufgrund von Schäden durch Ransomware werden bis 2031 voraussichtlich mehr als 265 Mrd. US-Dollar betragen (cybersecurity.ventures.com)*



DEMO ANFORDERN

ZURÜCK



WEITER



01

Die Risiken eines  
Cyberangriffs verstehen

02

Das Risiko eindämmen

03

Erfahren Sie mehr über die  
Wiederherstellung nach einem  
Ransomware-Angriff

04

Szenarien für die Wiederherstellung  
nach einem Cyberangriff

05

Lernen Sie praktische  
Anwendungen kennen

06

Gehen Sie proaktiv vor

# RANSOMWARE IN ECHTZEIT ERKENNEN

## Bei Ransomware- Angriffen kommt es auf Schnelligkeit an

Wenn Sie von einem Ransomware-Angriff betroffen sind, ist eine schnelle Reaktion entscheidend, um die Auswirkungen des Angriffs zu verringern. Aber wie kann man reagieren, wenn man nicht weiß, dass der Angriff bereits begonnen hat? Wenn Sie erkennen können, wann ein Angriff beginnt und Daten verschlüsselt werden, haben Sie die Möglichkeit, schnell zu handeln. Wenn Sie lange brauchen, um ein Backup zu scannen, sind Ihre Daten möglicherweise bereits verschlüsselt, und die Reichweite der Malware wird immer größer.

Die Erkennung von Verschlüsselungen in Echtzeit kann dazu beitragen, das Ausmaß oder den Radius der Auswirkungsphase von Ransomware zu minimieren. Einige Unternehmen unterschätzen möglicherweise, wie viel und wie schnell Ransomware in der Regel verschlüsselt, aber die Zahlen sprechen eine deutliche Sprache.

## Analyse

Eine interne Analyse von 116 weltweit verteilten Ransomware-Angriffen, die 43 verschiedene Ransomware-Varianten umfassten, ergab, dass im Durchschnitt 183,5 GB an Daten kompromittiert wurden. Eine separate Studie von Splunk mit dem Titel *Eine empirisch vergleichende Analyse von Ransomware-Binärdateien* ergab, dass die durchschnittliche Ransomware ein Gigabyte an Daten in 47,7 Sekunden verschlüsseln kann. Das bedeutet, dass bei einem typischen Angriff die vollständige Detonation der Verschlüsselung schätzungsweise 2 Stunden und 26 Minuten dauern würde.

Leider bedeutet das Warten auf die Ausführung eines nächtlichen Backups und das anschließende Scannen dieser Kopien, dass die durchschnittliche Ransomware den gesamten Datensatz bereits 12 bis 24 Stunden vorher verschlüsselt hat – in einem Wettlauf mit der Zeit sind die Angreifer bereits meilenweit entfernt, bevor überhaupt ein Alarm auf ein Problem aufmerksam macht.

## Mit Zerto

Zerto hingegen kann Angriffe innerhalb von Sekunden erkennen und Sie entsprechend alarmieren. Wenn Ransomware beispielsweise innerhalb von 15 Sekunden erkannt wird, ist die durchschnittliche Ransomware nicht nur noch nicht fertig mit der Verschlüsselung, sondern hat es auch nur geschafft, etwa 300 MB der 183,5 GB zu verschlüsseln – das entspricht einer Einsparung von 99,8 % bei der Menge der gesperrten Daten.

Je eher Sie etwas erkennen, desto eher können Sie Maßnahmen ergreifen: Deshalb hat die Erkennung von Verschlüsselung in Echtzeit Auswirkungen auf die reale Welt.

**Lesen Sie das Datenblatt – [Erkennung von Ransomware in Echtzeit](#)**

**Lesen Sie den Gorilla-Leitfaden zur Erkennung von Ransomware in Echtzeit und zur Wiederherstellung [Gorilla-Leitfaden zur Erkennung von Ransomware in Echtzeit und zur Wiederherstellung](#)**



DEMO ANFORDERN

ZURÜCK



WEITER



01

Die Risiken eines  
Cyberangriffs verstehen

02

Das Risiko eindämmen

03

Erfahren Sie mehr über die  
Wiederherstellung nach einem  
Ransomware-Angriff

04

Szenarien für die Wiederherstellung  
nach einem Cyberangriff

05

Lernen Sie praktische  
Anwendungen kennen

06

Gehen Sie proaktiv vor

# SICHERUNG IN EINEM VAULT

## Isolieren und Sperren von Daten mit Unveränderlichkeit und Air Gapping

Ein wesentlicher Unterschied zwischen einer Cyberattacke wie Ransomware und einem typischen Katastrophenszenario besteht darin, dass ein Ransomware-Angreifer aktiv versucht, eine Wiederherstellung zu verhindern. Die Angreifer haben es auf die Verschlüsselung oder Löschung von Wiederherstellungsdaten abgesehen, so dass die einzige Möglichkeit zur Wiederherstellung die Zahlung des Lösegelds ist. Die Sicherung von Wiederherstellungsdaten ist von entscheidender Bedeutung, um im schlimmsten Fall, wenn Angreifer Ihre Wiederherstellungstools kompromittiert haben, die Wiederherstellung sicherzustellen.

Eine Möglichkeit, Daten zu schützen, besteht darin, sie unveränderlich zu machen, so dass Angreifer sie nicht ändern oder löschen können. Unveränderlichkeit wird häufig bei statischen Datenkopien verwendet, die in einem unveränderlichen Zustand an entfernten

Orten wie Cloud-Speichern gespeichert werden. Dennoch haben Angreifer Wege gefunden, unveränderliche Datenkopien anzugreifen, indem sie die Richtlinien, die sie unveränderlich machen, ändern oder die Systemzeiten künstlich verändern. Für einen besseren Schutz ist ein Cyber-Vault erforderlich.

### Was ist ein Cyber-Vault?

Ein gut konzipierter Cyber-Vault kann Wiederherstellungsdaten schützen, indem er sie mithilfe von Air Gapping und Unveränderlichkeit aufbauend auf einer Zero-Trust-Architektur für Angreifer unzugänglich macht. Im Idealfall kann der Vault nur durch direkten physischen Zugriff innerhalb des Rechenzentrums verwaltet werden, so dass er vollständig vor Netzwerkeingriffen geschützt ist. Die Cyber-Vault-Architektur soll einen luftdichten Reinraum bieten, in dem die Wiederherstellung während der forensischen Phase nach einem Ransomware-Angriff schnell und sicher beginnen kann.

Der Zerto Cyber Resilience Vault kombiniert Zerto mit HPE Alletra Storage, HPE Proliant Compute und HPE Aruba Networking und

bietet so eine vollständig isolierte Zero-Trust-Architektur. Diese Architektur ermöglicht jede Ebene der Wiederherstellung, von einzelnen Dateien bis hin zu ganzen Standorten, wobei der isolierte Tresor die ultimative Ausfallsicherung darstellt. Mit Zerto können Benutzer die meisten Arten von Angriffen innerhalb von Minuten oder Stunden abwehren. Mit dem Zerto Cyber Resilience Vault sind Sie vor allen Arten von Cyberangriffen geschützt – mit isolierten, luftdichten und unveränderlichen Kopien Ihrer Daten in einer produktionsgerechten Rechen- und Speicherumgebung.

**Erfahren Sie mehr über den Zerto Cyber Resilience Vault – [Cyber Resilience Vault](#)**

**Sehen Sie sich ein kurzes Video an – [Den Zerto Cyber Resilience Vault auf Vimeo verstehen](#)**



DEMO ANFORDERN

ZURÜCK



WEITER



01

Die Risiken eines  
Cyberangriffs verstehen

02

Das Risiko eindämmen

03

Erfahren Sie mehr über die  
Wiederherstellung nach einem  
Ransomware-Angriff

04

Szenarien für die Wiederherstellung  
nach einem Cyberangriff

05

Lernen Sie praktische  
Anwendungen kennen

06

Gehen Sie proaktiv vor

# SZENARIEN FÜR DIE WIEDERHERSTELLUNG NACH EINEM CYBERANGRIFF

## Wiederherstellen, was benötigt wird

Cyberangriffe wie Angriffe durch Ransomware können in vielen Formen und Größen auftreten. Sie können nur Dateien und Ordner oder virtuelle Maschinen betreffen, aber auch ganze Standorte oder gleich mehrere Standorte. Auch wenn ein Tresor Ihnen Sicherheit bei der Wiederherstellung gibt, können viele Angriffe wieder ausgeglichen werden. Diese fünf Videos zeigen einige der vielfältigen Wiederherstellungsmöglichkeiten mit Zerto.

## Wiederherstellung nach Dateiverschlüsselung durch Ransomware

Dieses Video zeigt einen kleinen Angriff, bei dem Dateien und Ordner auf einer VM verschlüsselt wurden, und erläutert, wie Zerto eine sofortige Wiederherstellung von Dateien ermöglichen kann.

[Wiederherstellung nach Dateiverschlüsselung durch Ransomware \(v2 bei Vimeo\)](#)

## Ransomware nach VM-Verschlüsselung

Dieses Video betrachtet einen Angriff, bei dem eine ganze VM kompromittiert wurde, und erläutert, wie Zerto eine sofortige VM-Wiederherstellung ermöglichen kann.

[Wiederherstellung nach VM-Verschlüsselung durch Ransomware \(v2 bei Vimeo\)](#)

## Wiederherstellung bei durch Ransomware infizierter Anwendung

Dieses Video zeigt einen Angriff, der alle VMs eines Multi-VM-Anwendungsstapels infiziert hat, und wie Zerto mithilfe von orchestrierten Ausfallsicherungen für einen Peer-Standort die Wiederherstellung durchführen kann.

[Wiederherstellung bei durch Ransomware infizierter Anwendung \(v2 bei Vimeo\)](#)

## Wiederherstellung bei durch Ransomware infiziertem Standort

Dieses Video zeigt einen Angriff, der die

Infrastruktur aller Vorrichtungen vor Ort kompromittiert hat, und wie Zerto mithilfe von orchestrierten Ausfallsicherungen für einen DR-Standort die Wiederherstellung durchführen kann.

[Wiederherstellung bei durch Ransomware infiziertem Standort \(v2 bei Vimeo\)](#)

## Wiederherstellung bei mehreren durch Ransomware infizierten Standorten

Dieses Video zeigt einen Angriff, der die gesamte Infrastruktur vor Ort und in der Cloud infiziert hat, und wie Zerto mit portablen, unveränderlichen Kopien, die an jede neue oder bestehende Zerto-Installation angeschlossen werden können, die Wiederherstellung durchführen kann.

[Wiederherstellung bei mehreren durch Ransomware infizierten Standorten \(v2 bei Vimeo\)](#)

ZURÜCK



DEMO ANFORDERN

WEITER



01

Die Risiken eines  
Cyberangriffs verstehen

02

Das Risiko eindämmen

03

Erfahren Sie mehr über die  
Wiederherstellung nach einem  
Ransomware-Angriff

04

Szenarien für die Wiederherstellung  
nach einem Cyberangriff

05

Lernen Sie praktische  
Anwendungen kennen

06

Gehen Sie proaktiv vor

# EINE GESCHICHTE VON ZWEI RANSOMWARE-ANGRIFFEN

## Vorher und Nachher

Über TenCate: Dieses multinationale Textilunternehmen mit Sitz in den Niederlanden war zweimal von Ransomware-Angriffen betroffen. Der erste Angriff fand vor der Implementierung von Zerto statt, der zweite nach der Implementierung von Zerto. Die Erfahrungen des Unternehmens mit der Wiederherstellung nach Ransomware-Angriffen mit Hilfe von Backups beim ersten Mal und mit Zerto beim zweiten Mal zeigen die Leistungsfähigkeit von Zerto bei der schnellen, unterbrechungsfreien Wiederherstellung nach einem Ransomware-Angriff.

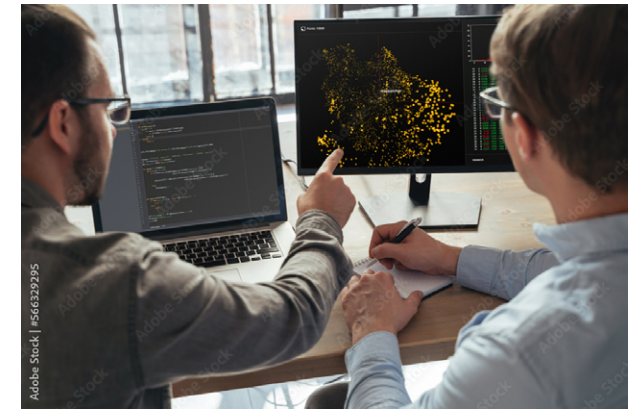
TenCate benötigte nach dem ersten Angriff mit der eigenen Sicherungslösung des Unternehmens Wochen für die Wiederherstellung. Nach der Einführung von Zerto waren nach dem zweiten Angriff nur 10 Minuten für die Wiederherstellung nötig – und es gingen nahezu keine Daten verloren.

### Vorher

Eine der Produktionsstätten von TenCate wurde mit CryptoLocker angegriffen. Alle Dateiserver waren infiziert. Zu diesem Zeitpunkt bestand die einzige Wiederherstellungsmethode von TenCate in der Wiederherstellung von der Festplatte. Infolge dieses Angriffs erlitt TenCate einen Datenverlust von 10 Stunden und war zwei Wochen lang nicht in der Lage, die Daten wiederherzustellen.

### Nachher

Verzeichnisse auf einem Dateiserver in einer Produktionsstätte wurden von einer weiterentwickelten Form von CryptoLocker angegriffen. TenCate erlebte nur 10 Sekunden Datenverlust und konnte die Daten in weniger als 10 Minuten wiederherstellen.



*Nach der Einführung von Zerto waren nach dem zweiten Ransomware-Angriff nur 10 Minuten für die Wiederherstellung nötig, wobei nahezu keine Daten verloren gingen.*



DEMO ANFORDERN

ZURÜCK



WEITER



01

Die Risiken eines  
Cyberangriffs verstehen

02

Das Risiko eindämmen

03

Erfahren Sie mehr über die  
Wiederherstellung nach einem  
Ransomware-Angriff

04

Szenarien für die Wiederherstellung  
nach einem Cyberangriff

05

Lernen Sie praktische  
Anwendungen kennen

06

Gehen Sie proaktiv vor

# AUFBAU EINER CYBER- RESILIENZ-STRATEGIE

## Nehmen Sie jetzt eine proaktive Haltung ein

Die Verhinderung von Cyberangriffen ist nicht immer möglich, aber die Eindämmung der Bedrohung schon. Mit Zerto können Sie Ihr Unternehmen vor den nachhaltigen Auswirkungen von Cyberangriffen wie Angriffen durch Ransomware schützen. Wenn Sie die Kontrolle über Ihre Geschäftsdaten haben, sind Sie den Forderungen der Hacker nicht mehr ausgeliefert. Vergessen Sie die Zahlung des Lösegelds und die Wiederherstellung der verlorenen Arbeit. Mit der Erkennung von Verschlüsselung in Echtzeit, Unveränderbarkeit, Air Gapping in einem sicheren Tresor und flexibler, orchestrierter Wiederherstellung trägt Zerto dazu bei, Datenverluste und Ausfallzeiten im Falle eines Ransomware-Angriffs zu minimieren.

Testen Sie Zerto  
Recovery from  
Ransomware mit  
einem auf Abruf  
verfügbaren,  
praktischen  
Laboratorium –  
myZerto Labs:  
MyZerto

**ERKUNDEN SIE  
UNSER LABOR**

Lesen Sie ein  
technisches  
Whitepaper –  
Technisches  
Whitepaper  
zu Ransomware

**WHITEPAPER**

Erfahren Sie mehr  
über Zerto for  
Cyber Resilience –  
Wiederherstellung  
bei Angriffen  
durch Malware &  
Ransomware

**MEHR ERFAHREN**

Sehen Sie sich  
ein On-Demand-  
Webinar an –  
Aufbau eines  
Cyber Resilience  
Vault mit Zerto

**DAS WEBINAR ANSEHEN**

Kontaktieren Sie  
uns für weitere  
Informationen

**KONTAKT**



**DEMO ANFORDERN**

ZURÜCK

