CYBERRESILIENZ:

Die Strategie gegen Ransomware heißt rasche Wiederherstellung

Nicht ob, sondern wann

[illegible]

[illegible]

[illegible] m 300 [illegible] % zugenommen [illegible]

[illegible]

[illegible]

[illegible]

$ 11,5 Milliarden [illegible]
$ 1,4 Millionen [illegible]

[illegible] Sie [illegible]

RETTENDE RESILIENZ

[illegible] gefasst zu sein, sodass Sie im Ernstfall reagieren und den Betrieb aufrechterhalten können. Dies erfordert ein Umdenken: Es geht bei Ransomware nicht darum, Attacken abzuwehren, sondern darum, [illegible] geht darum, eine Kultur zu entwickeln, die darauf ausgerichtet ist, Störungen zu [illegible] Außerdem brauchen Sie eine Wieder- [illegible] Ihre Daten behalten – ohne Lücken, ohne Verluste. Dann können Sie den Betrieb ohne Verzögerung wieder aufnehmen. Voraussetzung ist die Umstellung auf kontinuierliche Datensicherung (Continuous Data protection/CDP).

WIEDERHERSTELLUNG NACH RANSOMWARE IN SEKUNDEN

Wie nutzen Kunden die Zerto-Plattform zur Wiederherstellung ihrer Systeme?

Dieses On-demand-Webinar zeigt, wie Zerto, ein Unternehmen von Hewlett Packard Enterprise, einem Kunden geholfen hat, seine Systeme nach einem Angriff schnell wiederherzustellen. Sie erfahren, wie der operative Betrieb nahtlos fortgesetzt werden konnte – und wie Sie selbst auf eine solche Strategie der Datensicherung umstellen können.

HINTERGRUNDWISSEN

Ransomware: Der Bedrohung durch Cyberangriffe begegnen

WAS IST RANSOMWARE?

Dieser Typ Schadsoftware erlangt Zugriff auf Ihre Dateien und verschlüsselt sie. Eine Entschlüsselung ist nur mit dem privaten Schlüssel möglich, den der Angreifer einbehält und erst nach Zahlung eines Lösegelds freizugeben verspricht.

Cyberresilienz: Kostspielige Ausfallrisiken minimieren

WAS IST CYBERRESILIENZ?

Unter Cyberresilienz versteht man die Vorbereitung und Reaktion auf Cyberangriffe sowie die Wiederherstellung nach einer Attacke. Das ist mehr als reine Prävention. Es geht darum, die Integrität Ihrer kritischen Daten konsequent sicherzustellen.

> *Die meisten Ransomware-Attacken lassen sich durch gute Cyberhygiene und effektive, regelmäßige Datensicherung inklusive regelmäßiger Wiederherstellungstests verhindern. Wir empfehlen Unternehmen den proaktiven Ansatz, denn auch wenn Sie Lösegeld zahlen, bekommen Sie nicht immer die Freigabeschlüssel. Eine proaktive Strategie ist außerdem meist leichter umzusetzen und kostengünstiger.*
>
> **— Raj Samani, CTO Europe bei Intel Security**

ZWEI RANSOMWARE-ANGRIFFE IM VERGLEICH

TenCate Textiles

Vorher und nachher

TenCate ist ein multinationales Textilunternehmen mit Sitz in den Niederlanden, das Opfer zweier Ransomware Attacken wurde. Die erste geschah vor der Implementierung von Zerto, die zweite danach. Ein Vergleich der Erfahrungen des Unternehmens mit der Wiederherstellung nach der ersten Attacke ohne und nach der zweiten mit der Zerto IT Resilience Platform™ zeigt eindrucksvoll die Vorteile unserer Lösung.

Ohne Zerto

Eine TenCate-Produktionsanlage wurde mit CryptoLocker-Schadsoftware angegriffen. Alle Dateiserver wurden infiziert. TenCate hatte nur die Möglichkeit einer Wiederherstellung von Festplatte. Das Unternehmen hatte zwölf Stunden keine Daten und brauchte zwei Wochen für die Wiederherstellung.

Mit Zerto

Die Verzeichnisse eines Fileservers einer Produktionsanlage wurden mit einer fortgeschrittenen Version von CryptoLocker infiziert. Der Zugriff auf die TenCate-Daten war gerade einmal zehn Sekunden lang blockiert, die Wiederherstellung nahm nicht einmal zehn Minuten in Anspruch.

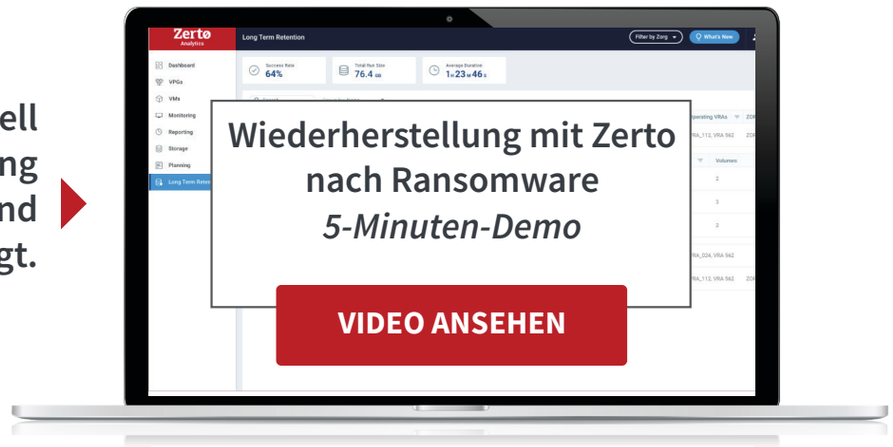
ZURÜCK
WEITER

DEMO: WIEDERHERSTELLUNG NACH RANSOMWARE IN AKTION

CDP (Continuous Data Protection) von Zerto schützt Ihre Daten in Echtzeit. Mit wenigen Klicks können Sie genau auf den Moment kurz vor dem Angriff zurücksetzen und so Ihre Daten vollständig und granular wiederherstellen. Zertos Journal-basierte Lösung ist so flexibel, dass sie nur diejenigen Daten und Komponenten wiederherstellt, die Sie tatsächlich benötigen, ob ausgewählte Dateien, virtuelle Maschinen oder komplette Anwendungsstacks.

> *Wir konnten die letzte Ransomware-Attacke in 15 Minuten stoppen und unsere Systeme nach drei Stunden wieder in Betrieb nehmen!*
>
> *Ohne Zerto hätten wir Lösegeld zahlen müssen – und zwar ohne die Garantie, unsere Daten zurückzubekommen.*
>
> — **Rubyanne O'Bryan**
> **Systemadministrator, ClearPath Mutual**

Sehen Sie selbst, wie schnell und leicht die Wiederherstellung nach Ransomware-Attacken und anderen Angriffen gelingt.



PROAKTIV HANDELN, KONTINUIERLICH SICHERN

Angriffe zu verhindern, ist nicht immer möglich, die **Minimierung der Risiken aber sehr wohl.** Mit Zerto schützen Sie Ihr Unternehmen vor den Folgen von Cyberbedrohungen wie Malware oder Ransomware.

Lösegeldzahlungen können Sie vergessen, ebenso verlorene Daten, die Sie neu erarbeiten müssten. Dank voll automatisiertem Failover und Failback **stellen Sie kompromittierte Anwendungen und Daten in Minuten wieder her** – mit nur drei Mausklicks.

Zerto schützt Ihre Systeme mit Continuous Data Protection, sodass Sie bei Malware- und Ransomware-Angriffen **nur minimale Datenverluste und Ausfallzeiten** erleiden. Eine Wiederherstellung bzw. Zurücksetzung auf beliebige Zeitpunkte ist in Sekunden möglich.

Cyberresilienz mit Zerto entdecken

Schutzfunktionen-Management mit Zerto

ZURÜCK