Zerto
a Hewlett Packard Enterprise company

Jak ograniczać straty powodowane przez „ransomware”

Przygotuj się na atak „ransomware” z Zerto

Oprogramowanie złośliwe, tzw. ransomware to jedno z największych zagrożeń dla firm i organizacji na całym świecie. Przy tym zarówno samo zagrożenie, jak i koszty ataków „ransomware” stale rosną. Jeśli nie jesteś przygotowany na atak, jesteś narażony na trwające długie godziny czy nawet dni przestoje, utratę danych i dotkliwe straty reputacji „ w mediach. Zachowanie konkurencyjności, a nawet samo przetrwanie biznesu w następnej dekadzie, wymaga potraktowania „ransomware” nie tylko jako kolejnego cyberzagrożenia, ale jako potencjalnej prawdziwej katastrofy.

Zapobieganie skutkom ataków „ransomware” jest ważne, ale niezależnie od liczby zastosowanych środków zapobiegawczych, powszechność „ransomware” oznacza, że atak jest nieunikniony. Przygotowanie i wybór odpowiedniego rozwiązania do odtwarzania danych po ataku ma w przypadku „ransomware” kluczowe znaczenie.

Eksperci ds. cyberbezpieczeństwa przewidują, że do 2031 r. częstotliwość ataków „ransomware” i wynikające z nich koszty będą rosły w całej światowej gospodarce.

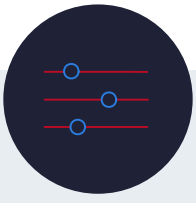
265 miliardów USD
koszt ataków „ransomware”

2 sekundy
wystąpienie ataku “ransomware”

Źródło: David Braue, „Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031.” Cybercrime Magazine. 3 czerwiec 2021.

Odtwórz systemy i odzyskaj dane w ciągu kilku minut od momentu ataku

Jednym z największych kosztów ataku „ransomware” jest przestój spowodowany utratą dostępu do kluczowych danych i systemów. Skrócenie przestoju do czasu liczonego w minutach praktycznie eliminuje te koszty.



Przywróć dane do stanu na kilka sekund przed atakiem

Utrata danych może bezpośrednio przekładać się na utratę własności intelektualnej, produktywności i przychodów. Zapobiegaj utracie danych z okresu liczonego w dniach czy godzinach, umożliwiając przywrócenie ich do stanu na kilka sekund przed atakiem.

Niższe ryzyko dzięki natychmiastowym, nieprzerwanym testom

Plan odtwarzania po ataku jest tak dobry, jak zdolność do jego pomyślnej realizacji. Testowanie planów odtwarzania po ataku bez zakłócania funkcjonowania środowiska produkcyjnego pozwala wykonywać testy często, w dowolnym momencie. Zyskaj pewność, że wszystko zadziała, dzięki szybkiemu testowaniu zarówno przełączania awaryjnego, jak i samego odtwarzania.

Zerto Disaster Recovery pozwala walczyć ze skutkami „ransomware”

Zerto, firma należąca do Hewlett Packard Enterprise, zapewnia firmom i organizacjom na całym świecie najlepsze wskaźniki RTO (Recovery Time Objective) i RPO (Recovery Point Objective), bez względu na skalę działalności. Zerto wyróżnia się na tle innych rozwiązań do odtwarzania danych tym, że zapewnia ciągłą replikację danych. Jest to możliwe dzięki użyciu unikalnej technologii opartej na dzienniku zmian, dostosowaniu odtwarzania do poszczególnych aplikacji, niezmiennym kopiom danych, automatyzacji odtwarzania, wieloplatformowej elastyczności, możliwości nieinwazyjnego testowania DR, raportowaniu i analityce.

Funkcje odtwarzania po ataku „ransomware” oferowane przez Zerto

Ciągła ochrona danych – Zerto replikuje w czasie rzeczywistym wszystkie zmiany zachodzące w danych do dziennika, w którym co pięć sekund tworzone są punkty kontrolne na potrzeby odtwarzania. Ten dziennik odtwarzania może być umiejscowiony lokalnie, w ośrodku zdalnym lub przechowywany w obydwu miejscach. Umożliwia to szybkie odtwarzanie pojedynczych plików, maszyn wirtualnych, kontenerów, całych aplikacji i witryn do stanu na kilka sekund przed atakiem „ransomware”.

Odtwarzanie dopasowane do aplikacji – Zerto logicznie grupuje maszyny wirtualne i kontenery, żeby połączyć wszystkie obciążenia aplikacji, jednostki biznesowej, lokalizacji czy dowolnej wymaganej kombinacji. Grupa VPG (Virtual Protection Group) zapewnia spójność danych we wszystkich aplikacjach w grupie, dzięki czemu można bez obaw odzyskiwać aplikacje po ataku „ransomware” bez żadnych problemów.

Niezmienne kopie danych – celem ataków „ransomware” są często kopie migawkowe i kopie zapasowe, ponieważ uniemożliwia to łatwe odtwarzanie danych i zwiększa prawdopodobieństwo zapłaty okupu. Przy pomocy Zerto można zablokować wprowadzanie zmian do kopii dziennika. W ten sposób chronimy go przed zaszyfrowaniem przez „ransomware” i zapewniamy możliwość użycia do odtworzenia danych.

Wieloplatformowa elastyczność – ataki „ransomware” często wymierzone są w określone systemy operacyjne lub platformy wirtualizacyjne. Zerto zapewnia dodatkową ochronę przed zaszyfrowaniem przez „ransomware” danych potrzebnych do odtworzenia po ataku. Jest to realizowane poprzez wsparcie dla całych środowisk składających się platform lokalnych i chmurowych, jak też i replikację między nimi.

Automatyzacja przełączania awaryjnego i odtwarzania – odtwarzanie danych w ciągu kilku minut za pomocą kilku kliknięć, niezależnie od tego, czy odzyskuje się pojedynczy plik, jedną lub więcej aplikacji, czy cały ośrodek. Mechanizmy automatyzacji i orkiestracji Zerto umożliwiają odtwarzanie maszyn wirtualnych i kontenerów oraz ich danych w wirtualnych grupach ochrony (VPG). Dzięki temu po ataku aplikacje można szybko przywrócić do działania przy minimalnej interwencji ręcznej.

Nieinwazyjne testowanie DR – scenariusze odtwarzania można testować często i bez zakłócania pracy środowiska produkcyjnego. Możesz przetestować możliwości odtworzenia pojedynczych aplikacji lub całych ośrodków. Wbudowane mechanizmy raportowania oznaczają, że w ten sposób można nie tylko przygotować się na atak „ransomware”, ale spełnić wymagania związane ze zgodnością z regulacjami. A kiedy już dojdzie do ataku, można przenieść testy odtwarzania do izolowanego środowiska. Dzięki temu upewnimy się, zanim przywrócimy odzyskane dane z powrotem do środowiska produkcyjnego, że są one wolne od „ransomware”.

Raportowanie i analityka Zerto – Wbudowana w rozwiązanie analityka Zerto zapewnia jeden, kompletny widok całego środowiska obejmującego wiele ośrodków, również w chmurze publicznej. Raportowanie Zerto daje pewność, że jesteś przygotowany na atak „ransomware”. Jednocześnie może nawet pomóc w ustaleniu, kiedy atak się rozpoczął.

Atak „ransomware” na TenCate

PRZECZYTAJ PRZYKŁAD ZASTOSOWANIA

PRZED ZERTO:

2 tygodnie

odtwarzanie

12 godzin

utrata danych

PO WDROŻENIU ZERTO:

<10 minut

czas odtwarzania

sekundy

utrata danych

„Szczerze mówiąc, po ostatnim ataku, nawet się uśmiechnąłem, kiedy zacząłem odtwarzanie. Wiedziałem, że z Zerto sytuacja jest pod kontrolą. Byłem spokojny i pewny, że się uda. Wybrałem punkt przywracania na kilka minut przed infekcją, przetestowałem czy maszyna wirtualna jest czysta i podłączyłem vNIC – a potem wróciłem do normalnej pracy. Do domu nie wracałem zmartwiony, zestresowany czy przygnębiony”.

Jayme Williams
Starszy Inżynier systemowy, TenCate

WYPRÓBUJ ZERTO TERAZ

Uwolnij się od strachu przed ransomware. Zapewnij ochronę dla 10 maszyn wirtualnych teraz, za darmo.

WYPRÓBUJ ZA DARMO

PRZECZYTAJ PRZEWODNIK JAK PRZETRWAĆ CYBERATAK

O Zerto

Zerto, firma należąca do Hewlett Packard Enterprise, umożliwia klientom prowadzenie nieprzerwanej działalności biznesowej poprzez uproszczenie ochrony, odtwarzania i mobilności aplikacji lokalnych oraz chmurowych. Platforma chmurowa Zerto do ochrony i zarządzania danymi eliminuje ryzyko i złożoność związane z modernizacją i wdrażaniem chmury w środowiskach prywatnych, publicznych i hybrydowych. Prosta, czysto programowa platforma zapewnia ciągłą ochronę danych bez względu na skalę łącząc funkcje odtwarzania po awarii albo ataku, wykonywania kopii zapasowych oraz związane z mobilnością danych. Zerto cieszy się zaufaniem ponad 9500 klientów na całym świecie wspierając rozwiązania dla Microsoft Azure, IBM Cloud, AWS, Google Cloud, Oracle Cloud i ponad 350 dostawców usług zarządzanych. **www.zerto.com**