ZAMÓW DEMO

JAK PRZETRWAĆ CYBERATAK?
- PRZEWODNIK

Obawiasz się „ransomware”? Postaw na „**recoverware**”.

DALEJ

ZAMÓW DEMO

CYBERODPORNOŚĆ:

Najwyższy czas wziąć na cel Twoją strategię odtwarzania po ataku „ransomware”

„ransomware”… Nie czy, ale kiedy

Ataki „ransomware” nasilały się powoli od lat. Cyberporywacze danych wykorzystując złośliwy kod sieją spustoszenie zarówno wśród prywatnych użytkowników komputerów, jak i firm. Kiedy wezmą na cel Twoją organizację zaszyfrują kluczowe dane a powrót do normalności po ataku może kosztować utratę reputacji i przychodów liczoną w milionach.

Czy ryzyko ataku jest duże? Na ile powszechne jest to zjawisko?

> Czy wiesz, że zagrożenie „ransomware” **wzrosło** w ubiegłym roku **o 300%**?

Ataki na firmy takie jak Travelex, największe na świecie biuro wymiany walut, nie ustają. Departament Bezpieczeństwa Wewnętrznego USA wydał ostrzeżenie w 2020 roku dla amerykańskich firm, żeby „rozważyły i oceniły” możliwe konsekwencje i zagrożenie cyberatakiem na ich organizacje w następstwie wzrostu napięcia z Iranem. Te alarmujące statystyki i wiadomości w mediach nie pozostawiają wątpliwości czy Twoja firma zostanie zaatakowana. Właściwe pytanie brzmi: kiedy.

Sprawa stają się jeszcze bardziej przerażająca, kiedy przyjrzymy się kosztom tych ataków.

> **11,5 miliarda USD** = szacowany koszt ataków „ransomware” (2019)
>
> **1,4 miliona USD** = średni koszt odtwarzania danych / ataku

Jasne jest, że ataki „ransomware” są nie tylko coraz częstsze, ale także bardziej kosztowne. Biorąc pod uwagę wzrastającą nieuchronność ataku „ransomware”, firmy nie mogą po prostu uznać, że zapobiec będą mu w stanie rozwiązania cyberbezpieczeństwa — w końcu jeden z ataków przebije się przez te zabezpieczenia. Nie wystarczy jednak plan „disaster recovery”. Konieczna jest zmiana podejścia. Zamiast tradycyjnego planu odtwarzania po awarii trzeba zapewnić organizacji cyberodporność, która zagwarantuje ciągłość świadczenia usług.

CYBERODPORNOŚĆ NA RATUNEK

Cyberodporność to zdolność przygotowania się do, zareagowania na i przywrócenia normalnej działalności po ataku. Wymaga to zmiany sposobu myślenia o „ransomware”: od zapobiegania atakom do bycia przygotowanym na ewentualny atak. Nabywanie cyberodporności polega na rozwijaniu procesu i budowaniu kultury skoncentrowanej na odporności, a nie ograniczającej się do zapobiegania. Potrzebne jest również rozwiązanie do odtwarzania po ataku, które gwarantuje dostęp do wszystkich danych, bez jakiejkolwiek ich utraty. Tylko w ten sposób Twoja działanośćpowróci do normy bez opóźnień. Oznacza to przejście na CDP (Continuous Data Protection), czyli ciągłą ochronę danych.

PRZECZYTAJ WIĘCEJ

ZAMÓW DEMO

ODTWARZANIE PO ATAKU „RANSOMWARE” LICZONE W SEKUNDACH

Jak klienci używają platformy Zerto do odtwarzania swoich systemów?

Obejrzyj webinarium, żeby zobaczyć jak Zerto, firma należąca do Hewlett Packard Enterprise, pomogła klientowi szybko odtworzyć systemy po cyberataku. Posłuchaj jak szybko i bezpieczeństwowo wznowili działalność i dowiedz się jak zmienić podejście do ochrony danych.

ZAMÓW DEMO

BROSZURY INFORMACYJNE

„ransomware”: ograniczanie zagrożenia związanego z cyberatakami

CO TO JEST „RANSOMWARE”?

Złośliwe oprogramowanie, które służy do zdobywania dostępu do plików i szyfrowania danych poprzez generowanie pary kluczy prywatny--publiczny. Odszyfrowanie danych jest niemożliwe bez klucza prywatnego, który jest przechowywany – dopóki nie zostanie zapłacony okup – na serwerze przestępców.

ZOBACZ BROSZURĘ

Cyberodporność: ograniczaj i zarządzaj wysokimi kosztami związanymi z cyberzagrożeniami przy pomocy Zerto

CZYM JEST CYBERODPORNOŚĆ?

Cyberodporność to przygotowanie się do, reagowanie na i przywracanie normalnej działalności po ataku. Samo zapobieganie już nie wystarcza. Trzeba raczej podejmować konsekwentne działania mające na celu zapewnienie integralności najważniejszych danych. Cyberodporność obejmuje swoim zakresem pracowników, procesy i technologię.

ZOBACZ BROSZURĘ

Większości ataków „ransomware” można uniknąć dzięki dobrej cyberhigienie i efektywnemu, regularnemu tworzeniu kopii zapasowych danych, które są stale testowane w celu zapewnienia, że będzie można je przywrócić w razie potrzeby. Rekomendujemy wszystkim firmom proaktywność, ponieważ klucze odszyfrowujące nie zawsze są dostarczane, po zapłacie okupu. Proaktywne działanie jest często łatwiejsze i mniej kosztowne niż podejście reaktywne.

— Raj Samani, CTO w regionie Europy, Intel Security

ZAMÓW DEMO

TENCATE Textiles

OPOWIEŚĆ O DWÓCH ATAKACH „RANSOMWARE”

Przed i po

Informacje o firmie Tencate: Tencate, międzynarodowa firma z branży tekstylnej z siedzibą w Holandii, dwukrotnie doświadczyła ataków „ransomware”. Pierwszy atak miał miejsce przed wdrożeniem Zerto, a drugi po wdrożeniu Zerto. Doświadczenia firmy w zakresie odtwarzania po ataku „ransomware” przy użyciu kopii zapasowych za pierwszym razem w porównaniu do użycia za drugim razem Zerto, pokazują moc platformy IT Resilience Platform™ firmy Zerto, która pomogła Tencate szybko odzyskać dane.

Przed wdrożeniem

Jeden z zakładów produkcyjnych Tencate padł ofiarą CryptoLockera. Wszystkie serwery plików zostały zainfekowane. W tej sytuacji jedyną metodą odtwarzania dla TenCate było odtwarzanie z dysku. W wyniku tego ataku firma zanotowała utratę danych z okresu 12 godzin i nie była w stanie odzyskać danych przez dwa tygodnie.

Po wdrożeniu

Katalogi na serwerze plików w zakładzie produkcyjnym zostały zaatakowane przez bardziej zaawansowaną formę Cryptolockera. TenCate odnotowała utratę danych zaledwie z okresu 10 sekund i była w stanie odzyskać dane w mniej niż 10 minut.

WSTECZ
DALEJ

ZAMÓW DEMO

DEMO: ODTWARZANIE PO ATAKU „RANSOMWARE”

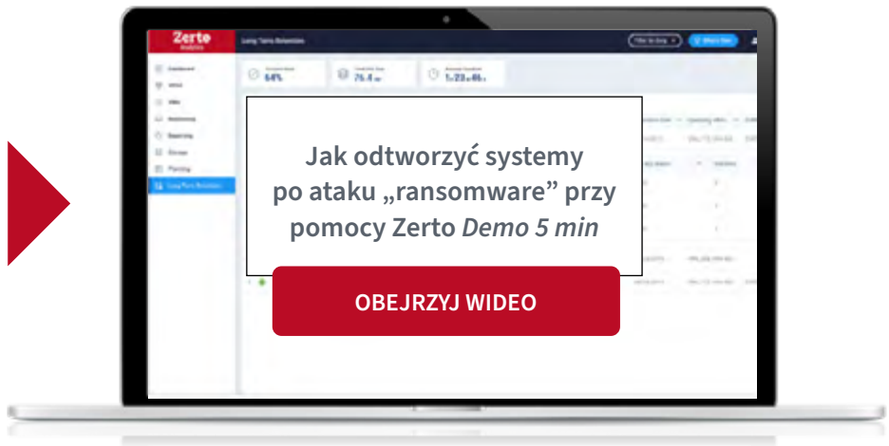
Ciągła ochrona danych firmy Zerto zapewnia ochronę Twoich danych w czasie rzeczywistym. Wystarczy kilka kliknięć, żeby odtworzyć wszystkie dane do punktu w czasie na sekundy przed atakiem. Technologia odtwarzania Zerto oparta na dzienniku jest wystarczająco elastyczna, żeby odzyskać tylko to, czego potrzebujesz: niezależnie od tego, czy mówimy o kilku plikach, maszynach wirtualnych czy całym stosie aplikacyjnym.

Podczas ostatniego ataku “ransomware”, jakiego doświadczyliśmy byliśmy w stanie zatrzymać go w ciągu 15 minut i przywrócić działanie w ciągu 3 godzin!

Bez Zerto musielibyśmy zapłacić okup i nadal nie wiedzielibyśmy, czy będziemy w stanie odzyskać nasze dane.

— Rubyanne O’Bryan Administrator systemów, ClearPath Mutual

Zobacz, jak szybko i łatwo możesz powrócić do normalnej działalności po ataku „ransomware” i odtwarzać systemy w przypadku innych zagrożeń



ZAMÓW DEMO

DZIAŁAJ PROAKTYWNIE

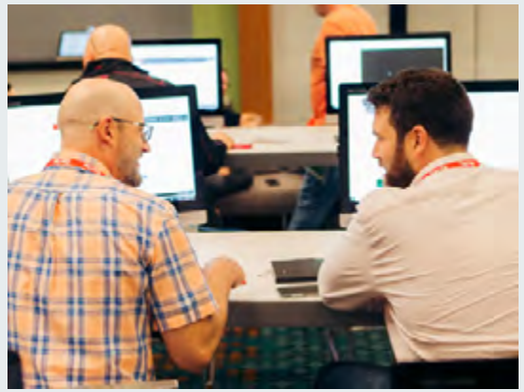
Zapobieganie cyberatakom nie zawsze jest możliwe, ale **ograniczanie zagrożenia z pewnością tak**. Zerto umożliwia ochronę Twojej firmy przed trwałymi skutkami cyberzagrożeń, takich jak złośliwe oprogramowanie czy “ransomware”.

Zapomnij o płaceniu okupu i odtwarzaniu utraconych efektów pracy. W pełni zautomatyzowane przełączanie awaryjne i powrót do normalnej działalności po ataku umożliwia **odzyskanie uszkodzonych aplikacji i danych w ciągu kilku minut** — za pomocą zaledwie 3 kliknięć.

Zerto chroni Twoje systemy zapewniając CDP - ciągłą ochronę danych. Pomaga to **zminimalizować ilość utraconych danych i przestoje** w przypadku ataku złośliwego oprogramowania lub “ransomware”. Zarazem możliwe jest powrót i odtworzenie danych z dowolnego punktu w czasie — nawet na kilku sekund przed atakiem.

Dowiedz się więcej o cyberodporność osiąganej dzięki Zerto

ZOBACZ BROSZURĘ



Zarządzanie ochroną z Zerto

POZNAJ NASZE LABORATORIA

WSTECZ