Trek2Summit

veeam

5 SPOSOBÓW
na zwiększenie bezpieczeństwa
TWOJEJ KOPII ZAPASOWEJ W CHMURZE

www.trek2summit.com

Trek2Summit

veeam

Czy jesteś gotowy na atak ransomware?

Rozwój i ewolucja oprogramowania ransomware to jeden z najbardziej destrukcyjnych trendów ostatniej dekady, który z przestępstwa gospodarczego przekształcił się w przestępstwo o ogromnych konsekwencjach dla bezpieczeństwa.

Aby skutecznie odeprzeć atak ransomware potrzeba sprawnej i wielowarstwowej obrony.

- **Czy masz rozwiązanie zabezpieczające, które nie skupia się tylko na jednym wektorze ataku, który z łatwością cyberprzestępcy mogą ominąć?**
- **Czy Twój personel ma odpowiednią, wyspecjalizowaną wiedzę w zakresie bezpieczeństwa Twoich danych?**

Pamiętaj!

Twoje dane są łatwiej dostępne niż kiedykolwiek wcześniej dla wyrafinowanych cyberprzestępców.

Trek2Summit

veeam

Korzyści z bezpieczeństwa w chmurze Amazon Web Services

1. Zaawansowa zabezpieczenia

Infrastruktura AWS zapewnia silne zabezpieczenia, które pomagają chronić Twoją prywatność. Wszystkie dane są przechowywane w wysoce bezpiecznych centrach danych AWS.

2. Spełnij wymagania dotyczące zgodności

Infrastruktura AWS spełnia wymogi norm bezpieczeństwa i ochrony informacji kluczowych organizacji zajmujących się bezpieczeństwem.

Dzięki temu Twoje dane są bezpieczne.

Oznacza to, że segmenty Twojej zgodności zostały już spełnione.

3. Oszczędność pieniędzy

Obniż koszty, korzystając z centrów danych AWS. Zachowaj najwyższy standard bezpieczeństwa bez konieczności zarządzania własnych obiektem.

4. Szybkie skalowanie

Bezpieczeństwo skaluje się wraz z wykorzystanie chmury AWS. Bez względu na wielkość Twojej firmy infrastruktura AWS została zaprojektowana tak, aby zapewnić bezpieczeństwo Twoich danych.

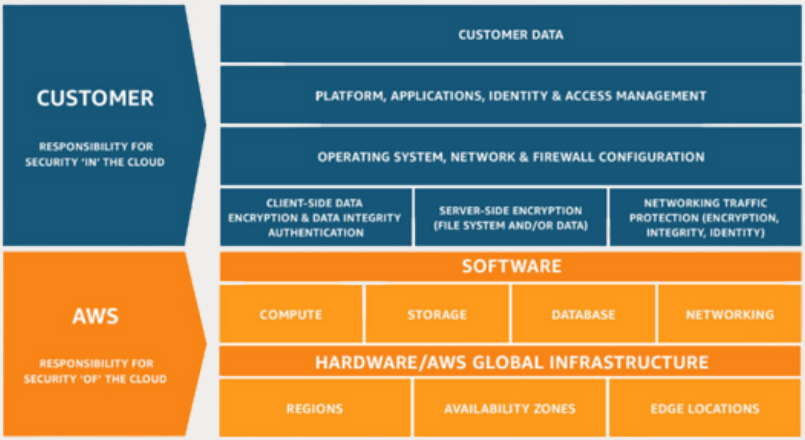
Trek2Summit

veeam

Model współdzielonej odpowiedzialności

W zależności od wybranej formy usług chmurowych (PaaS, IaaS) zakres odpowiedzialności za bezpieczeństwo Twoich danych jest zarówno po stronie AWS, jak i Twojej.

Poniższy diagram dokładnie pokazuje (w przypadku IaaS), o który zakres odpowiedzialności powinieneś zadbać.



Źródło: Shared Responsibility Model - Amazon Web Services (AWS)

Pamiętaj, że nie jesteś z tym sam! Wybierając nas jako Twojego partnera usług AWS możesz zadbać o bezpieczeństwo Twoich danych.

Przejdźmy zatem do sposobów na zwiększenie bezpieczeństwa kopii zapasowej w chmurze AWS

1. Bezpieczna kopia zapasowa to twoja ostatnia linia obrony

Wdrożone rozwiązanie do ochrony danych powinno być w stanie bezpiecznie chronić szeroki zakres wszystkich obciążeń o znaczeniu krytycznym, niezależnie od tego, czy są to tradycyjne obciążenia w centrum danych, takie jak maszyny fizyczne i wirtualne, czy też obciążenia natywne w chmurze i konteneryzowane w AWS.

Niezależnie od tego, czy obciążenia są wdrażane lokalnie, czy w chmurze, dane muszą być przenośne, aby uwzględnić niepewność i przyszłe wymagania.

Ta przenośność przybiera różne formy, ale ma kluczowe znaczenie w Twojej obronie. Na przykład wykorzystanie bezpiecznej pamięci AWS jako celu dla lokalnych kopii zapasowych, migracja obciążeń do AWS w przypadku udanego ataku, odzyskiwanie obciążeń z jednego konta AWS na drugie itp.).

O czym więc należy pamiętać wybierając rozwiązanie do tworzenia kopii zapasowych?

O możliwości przechwytywania danych wieloma metodami, na przykład natywnymi migawkami, kopiami zapasowymi opartymi na obrazach, replikacją itp. Wykorzystując technologie i usługi bezpieczeństwa AWS takie jak AWS S3 Object Lock czy zarządzanie kluczami AWS (KMS) zwiększamy pewność, że dane kopii zapasowej pozostaną nienaruszone w przypadku ataku, a to pozwala na bezpieczne i pozbawione wirusów odzyskanie danych.

2. Postępuj zgodnie z zasadą 3-2-1-1-0

Czyli złotą zasadą ochrony danych!

To podstawa każdej strategii bezpiecznego tworzenia kopii zapasowych, pomagająca organizacjom radzić sobie z ryzykiem ataku ransomware lub innego rodzaju incydentami wpływającymi na bezpieczeństwo danych.

Znasz regułę 3-2-1? Uzupełnij ją o 1-0.

Co więc oznaczają poszczególne liczby?

3 **Zachowaj co najmniej trzy egzemplarze swoich danych**

Ryzyko, że coś pójdzie nie tak w przypadku trzech zestawów danych jednocześnie, jest znacznie mniejsze niż w przypadku pojedynczego urządzenia do tworzenia kopii zapasowych, zwłaszcza gdy główna kopia zapasowa często znajduje się blisko podstawowych danych.

2 **Przechowuj kopie na dwóch różnych nośnikach**

W przypadku danych lokalnych dobrym rozwiązaniem jest przechowywanie jednej kopii na dysku w centrum danych, a drugiej w chmurze, takiej jak Amazon S3. I odwrotnie, w przypadku obciążeń natywnych w chmurze, opcje przechowywania

danych ochronnych obejmują migawki w Amazon Elastic Block Storage(Amazon EBS) i kopie zapasowe na Amazon S3, w różnych regionach lub kontach, a nawet kopie zapasowe lokalnie.

1 **Przechowuj co najmniej jedną kopię w innym miejscu**

Zdecydowanie zaleca się trzymanie co najmniej jednej wersji kopii zapasowej poza lokalizacją fizyczną, w której znajdują się podstawowe dane i podstawowa kopia zapasowa. Jak omówiono powyżej, AWS oferuje wiele typów i regionów przechowywania na całym świecie, aby zapewnić geograficzne oddzielenie kopii zapasowych produkcyjnych, podstawowych i wtórnych. Nie zapomnij o zaszyfrowaniu tych danych!

1 **Jedna kopia jest w trybie offline lub jest niezmienna**

Gdy haker uzyska dostęp do Twojego środowiska, może to mieć wpływ na wszystko, co ma połączenie internetowe. Chociaż w chmurze trudno jest uzyskać nośniki działające w trybie offline lub z przerwami powietrznymi ze względu na stałe połączenie, niezmienność dzięki Amazon S3 Object Lock oferuje funkcję zapisu wielu plików jako jednokrotnie zapisanych (WORM - Write-Once-Read-Many), dzięki czemu po zapisaniu kopii zapasowych w pamięci masowej nie można ich zmieniać ani usuwać do czasu upływu czasu określonego na podstawie zasad.

0

Regularnie sprawdzaj czy kopie nie zawierają błędów

Kopie zapasowe muszą być stale monitorowane i weryfikowane. Monitorowanie zmniejsza ryzyko wystąpienia jakichkolwiek błędów. Weryfikacja natomiast obejmuje częste testy odzyskiwania danych oraz sprawdzania ich czystości, tak aby ich czystości, tak aby bezbłędna kopia zapasowa została odzyskała w rzeczywistym scenariuszu.

3. Skorzystaj z blokady obiektów Amazon S3

Możliwość wykorzystania obiektowej pamięci masowej Amazon S3 to niezwykle trwałe, skalowalne i ekonomiczne repozytorium.

Jednak jedna funkcja jest niezwykle istotna. Jaka? Blokada obiektu S3 i jej gwarancja niezmienności. Niezmienność to skuteczny sposób nie tylko na ochronę przed zdarzeniami związanymi z cyberbezpieczeństwem, jak ransomware czy nieuczciwi administratorzy, lecz również znacznie łagodniejsze zdarzenia, jak przypadkowe usunięcia, zmiany.

Niezmienność może być nawet wymagana w celu zapewnienia zgodności z wymogami regulacyjnymi.

S3 Object Lock zapewnia niezmienność poprzez model WORM. Dane nie mogą być zmienione, usunięte bądź zastąpione przez wcześniej określony okres czasu.

Dlaczego ta funkcjonalność jest tak istotna?
W przypadku ataku ransomware masz pewność, że istnieje czysta, niezmieniona kopia zapasowa Twoich danych, która pozwoli na przywrócenie działania firmy bez potrzeby płatności okupu.

Pamiętaj!

Blokada obiektu S3 i jej gwarancja niezmienności to istotna funkcją Amazon S3. To sposób zarówno na większe ataki, jak i łagodniejsze zdarzenia. Dzięki temu w przypadku ataku, możesz odzyskać dane i przywrócić działanie firmy, bez potrzeby płatności okupu.

4. Izoluj dane na oddzielnych kontach

Wyobraź sobie, że Twoje środowisko produkcyjne jest zagrożone w wyniku ataku brute-force.

Jeśli dane produkcyjne i dane kopii zapasowej znajdują się na tym samym koncie AWS, osoba atakująca ma dostęp nie tylko do danych produkcyjnych o znaczeniu krytycznym, ale także do danych kopii zapasowych.

Konto AWS to granica bezpieczeństwa, która ma między innymi własne uprawnienia, konto użytkowników i podsieci IP. Tworząc oddzielne konta AWS dla obciążeń takich jak produkcja, tworzenie/testowanie i tworzenie kopii zapasowych, tworzysz wiele bezpiecznych środowisk, które chronią przed atakiem na indywidualne obciążenie.

W przypadku konieczności przeprowadzenia przywracania dane można skopiować z konta kopii zapasowej i odzyskać na konto produkcyjne, mając pewność, że dane nie zostały naruszone w wyniku ataku.

5. Najmniejsze uprawnienia dostępu

Ważne!

Uprawnienia dostępu należy poddawać ciągłemu i regularnemu audytowi, w szczególności usuwanie wszelkich niepotrzebnych poświadczeń, a także monitoring okresową rotację poświadczeń.

Najlepszą praktyką jest używanie ról AWS Identity and Access Management (IAM) do tymczasowego nadawania poświadczeń umożliwiających dostęp tylko do zasobów potrzebnych do wykonywania pracy.

Skonfiguruj jednokrotne logowanie AWS, aby umożliwić użytkownikom z zewnętrznego źródła dostęp do zasobów AWS na Twoich kontach.

AWS IAM zapewnia metody, które pomogą Ci zrozumieć, jaki dostęp jest potrzebny:

- Stosuj grupowanie poziomów dostępu – stwórz odpowiednią politykę
- Zweryfikuj swoje zasady – możesz sprawdzić poprawność zasad za pomocą narzędzia IAM Access Analizer podczas tworzenia i edytowania zasad JSON
- Wygeneruj politykę na podstawie aktywności związanej z dostępem – możesz wygenerować politykę IAM opartą o aktywność związaną z dostępem dla danej jednostki IAM (użytkownika lub roli)
- Użyj ostatnio używanych informacji – kolejna funkcja, która umożliwia pomoc z najniższymi uprawnieniami to dane o ostatnio uzyskiwanym dostępie do danej informacji. Dostępne a karcie Doradca dostępu na stronie szczegółów konsoli IAM dla użytkownika, grupy, roli lub zasady uprawnień. Informacje o ostatnim dostępie obejmują również informacje o ostatnio wykonywanych akcjach w przypadku takich usług jak Amazon EC2, IAM, Lambda i S3.
- Przeglądaj zdarzenia na koncie w AWS CloudTrail – aby jeszcze bardziej ograniczyć uprawnienia, możesz przeglądać zdarzenia na swoim koncie w historii zdarzeń CloudTrail.

Trek2Summit

veeam

Przyspiesz wdrożenie nowoczesnej ochrony danych dzięki Veeam i AWS!

Veeam to pięciokrotny lider Gartner Magic Quadrant, ponad 400 tys. Klientów – od 82% firm z listy Fortune 500 po małe i średnie firmy – ufa firmie Veeam w zakresie swoich danych.

Niezależnie od tego, czy już dziś korzystasz z AWS, czy dopiero zaczynasz, Veeam może pomóc Ci chronić, zarządzać i zabezpieczać wszystko z łatwością, od natywnych aplikacji i usług chmurowych w AWS po tradycyjne obciążenia lokalne w chmurze hybrydowej środowiska.

Trek2Summit

veeam

Skontaktuj się z nami i razem zadbajmy o bezpieczeństwo Twoich danych!

Monika Szeja
Business Development Manager
+48 793 931 063
monika.szeja@trek2summit.com

Tomasz Sochacki
CEO
+48 787 939 123
tomasz.sochacki@trek2summit.com