DELL Technologies

Infiltracja kopii zapasowych: Wzmacnianie cyberbezpieczeństwa i odporności dzięki Dell Technologies

Streszczenie dla zarządu

Infiltracja kopii zapasowych stanowi rosnące zagrożenie dla firm w każdym sektorze. Wykorzystuje luki w zabezpieczeniach systemów, które mają na celu ochronę informacji o znaczeniu krytycznym. Ataki te naruszają bezpieczeństwo systemów odzyskiwania danych, podważają zaufanie i zagrażają operacjom. Od znacznych strat finansowych po wydłużone przestoje i szkody na reputacji — konsekwencje mogą być poważne.

Firma Dell Technologies zapewnia kompleksowy pakiet zabezpieczeń w celu ochrony wrażliwych danych i zapobiegania tym atakom, w tym urządzenia Dell Trusted Device, infrastrukturę Dell Trusted Infrastructure i rozbudowane funkcje zabezpieczeń zintegrowane ze wszystkimi naszymi rozwiązaniami. Dzięki współpracy strategicznej i usługom profesjonalnym firma Dell pomaga organizacjom ustanowić odporne, wielowarstwowe struktury zabezpieczeń w celu skutecznego wykrywania, niszczenia i odzyskiwania danych po incydentach infiltracji kopii zapasowych.

Dzięki wdrożeniu innowacyjnych rozwiązań i specjalistycznej pomocy technicznej firmy Dell przedsiębiorstwa będą lepiej przygotowane do zabezpieczenia infrastruktury i utrzymania ciągłości działania.

Rosnące zagrożenie infiltracją kopii zapasowych

Systemy kopii zapasowych są niezbędne do ciągłości prowadzenia działalności biznesowej, co ma kluczowe znaczenie dla odzyskiwania danych po zdarzeniach cybernetycznych, takich jak ransomware czy awarie sprzętu. Niestety właśnie te istotne filary bezpieczeństwa coraz częściej stają się celem cyberprzestępców. Infiltracja kopii zapasowych powoduje uszkodzenie lub usunięcie danych z kopii zapasowych, co sprawia, że są one niedostępne, gdy są najbardziej potrzebne.

Te ewoluujące zagrożenia wymagają proaktywnych działań. Brak ochrony systemów kopii zapasowych naraża operacje i dane wrażliwe. Potencjalnymi celami są przedsiębiorstwa każdej wielkości, od małych po międzynarodowe korporacje, a szczególnie zagrożone są branże takie jak opieka zdrowotna, finanse i produkcja.

Firma Dell Technologies dostrzega pilną potrzebę wzmocnienia środowisk tworzenia kopii zapasowych, w związku z czym oferuje zaawansowane narzędzia i wskazówki w celu przeciwdziałania tym zaawansowanym atakom.

Ataki infiltracyjne na kopie zapasowe

Infiltracja kopii zapasowych występuje, gdy cyberprzestępcy wykorzystują luki w zabezpieczeniach systemów kopii zapasowych w celu naruszenia, zniszczenia lub zaszyfrowania krytycznych danych odzyskiwania. Te wyrafinowane ataki mogą zbiegać się w czasie lub następować po innych incydentach, takich jak instalacja oprogramowania typu ransomware lub złośliwego oprogramowania, co zwiększa straty operacyjne i finansowe.

Jak działają ataki na kopie zapasowe

1. **Pierwsze naruszenie:** Atakujący uzyskują nieautoryzowany dostęp do sieci, często poprzez phishing, słabe poświadczenia lub nienaprawione luki w zabezpieczeniach.
2. **Ruch boczny:** Po dostaniu się do sieci atakujący wykorzystują narzędzia do niepostrzeżonego przemieszczania się, atakując repozytoria kopii zapasowych i krytyczne zbiory danych.
3. **Naruszenie bezpieczeństwa kopii zapasowych:** Podstawowe taktyki obejmują szyfrowanie plików kopii zapasowych, usuwanie punktów odtwarzania oraz uszkadzanie danych.

Typowe techniki

- **Kradzież poświadczeń** narusza konta administracyjne, aby umożliwić pełny dostęp do systemów kopii zapasowych.
- **Instalacja oprogramowania typu ransomware** szyfruje zarówno dane w czasie rzeczywistym, jak i kopie zapasowe, żądając zapłaty za odszyfrowanie.
- **Niszczenie rozłożone w czasie** stopniowo niszczy kopie zapasowe, pozostając niewykryte. Naraża firmę na straty i pozostawia ją bez możliwości odzyskania danych.

Takie techniki podkreślają wyrafinowanie i powagę tych zagrożeń, co wymaga działań wyprzedzających.

Konsekwencje dla firm

Straty finansowe

Infiltracja kopii zapasowych zwiększa koszty odzyskiwania danych i wydłuża czas przestoju, często podwajając lub potrajając koszty reakcji. Odzyskiwanie danych z zaszyfrowanych lub zagrożonych kopii zapasowych może wymagać płatności dla atakujących, nowej infrastruktury lub drogich konsultantów.

Zakłócenia operacyjne

Bez odpowiednich kopii zapasowych organizacje muszą liczyć się z długimi czasami odzyskiwania, co prowadzi do zakłóceń w usługach, opóźnień w projektach i zatrzymania kluczowych funkcji.

Konsekwencje reputacji

Trwała utrata danych lub wydłużony czas przestoju osłabia zaufanie interesariuszy, co może potencjalnie zaszkodzić długoterminowej rentowności firmy.

Autentyczne przykłady

Globalny dostawca opieki zdrowotnej wykrył, że jego kopie zapasowe zostały uszkodzone podczas ataku typu ransomware. Pomimo zapłacenia okupu trzytygodniowe dane pacjentów zostały trwale utracone, opóźniając operacje i wywołując procesy sądowe. Całkowite koszty odzyskiwania przekroczyły **50 mln USD.**

Alarmujące statystyki

Ostatnie badania szacują, że średni spadek finansowy spowodowany udanym atakiem na system tworzenia kopii zapasowych przekracza **4,45 mln USD**[1], licząc kary, przestoje i wydatki na odzyskiwanie danych. Szczególnie alarmująca jest rosnąca częstotliwość takich incydentów, a globalne raporty pokazują wzrost zagrożeń związanych z kopiami zapasowymi **o 39%** rok do roku.

57%
ataków ukierunkowanych na tworzenie kopii zapasowych skutecznie infiltruje repozytoria kopii zapasowych

Źródło: 2024: Index Engines

Przeciwdziałanie infiltracji kopii zapasowych dzięki firmie Dell Technologies

Firma Dell Technologies oferuje rozbudowany pakiet narzędzi i usług, które sprostają unikalnym wyzwaniom związanym z atakami infiltracji kopii zapasowych, umożliwiając firmom skuteczne zapobieganie atakom, wykrywanie i odzyskiwanie danych.

Rozwiązania w zakresie bezpieczeństwa serwerów i pamięci masowej

Rozwiązania serwerowe i pamięci masowej firmy Dell zapewniają wyjątkową odporność na ataki ukierunkowane na tworzenie kopii zapasowych. Wbudowane funkcje zapewniają bezpieczeństwo kopii zapasowych i nie naruszają migawek.

- **Niezmienne kopie zapasowe/migawki** tworzą punkty przywracania odporne na manipulacje.
- **Funkcja Air-Gapped Recovery** izoluje dane z aktywnych sieci, aby zapobiegać uszkodzeniu.

[1]Ponemon — Cost of a Data Breach Report, 2024 r.

Wzmacnianie urządzeń Dell Data Protection

Urządzenia do ochrony danych Dell są wyposażone w funkcje takie jak Dell SafeBIOS zapewniający integralność oprogramowania układowego i SafeData do bezpiecznego szyfrowania, aby pomóc chronić przed atakami na kopie zapasowe. Ponadto rozwiązania te mają takie możliwości jak uwierzytelnianie wieloskładnikowe (MFA), kontrola dostępu oparta na rolach (RBAC) i podwójne uwierzytelnianie, aby zapobiec zagrożeniom.

Zaawansowane wykrywanie zagrożeń za pomocą narzędzia CrowdStrike

Integracja między CrowdStrike i Dell Data Protection koncentruje się na zwiększeniu bezpieczeństwa i poprawie monitorowania środowisk ochrony danych za pomocą zestawu zaawansowanych funkcji.

1. **Ochrona punktów końcowych i danych:** Firma Dell integruje zabezpieczenia punktów końcowych CrowdStrike oraz rozszerzone wykrywanie i reagowanie (EDR/XDR) z rozwiązaniami do ochrony danych. Obejmuje to gromadzenie danych telemetrycznych z programów PowerProtect Data Manager i PowerProtect Data Domain firmy Dell, a także informacji o zabezpieczeniach z konsoli CrowdStrike Falcon i oprogramowania SIEM nowej generacji
2. **Monitorowanie i reagowanie:** Usługa Dell Managed Detection and Response (MDR) zarządza oprogramowaniem CrowdStrike na rzecz klientów, gromadząc dzienniki i badając wszelkie wskaźniki naruszenia bezpieczeństwa (IoC) lub wykryte anomalie. Ta integracja umożliwia firmie Dell ciągłe monitorowanie i współpracę z SOC klienta w celu zapewnienia szybkiego i skutecznego usuwania zagrożeń
3. **Widoczność i kontrola ruchu danych w czasie rzeczywistym:** Platforma CrowdStrike Falcon Data Protection zapewnia wgląd w ruch danych w czasie rzeczywistym między różnymi źródłami i kanałami, klasyfikując dane zarówno według treści, jak i kontekstu. Pomaga to zapobiegać kradzieży danych i zapewnić skuteczne egzekwowanie zasad ochrony danych poprzez połączenie zawartości z analizą kontekstową
4. **Ujednolicone zarządzanie i uproszczone wdrażanie:** Integracja umożliwia zarządzanie zarówno punktami końcowymi, jak i ochroną danych za pomocą jednej platformy i agenta, co zmniejsza złożoność i obciążenie operacyjne. Dodatkowym ułatwieniem jest proste i natywne dla chmury podejście platformy CrowdStrike Falcon, które pozwala na szybkie wdrożenie i minimalne zakłócenia

Integracja między CrowdStrike i Dell Data Protection wykorzystuje zaawansowane funkcje EDR/XDR, monitorowanie w czasie rzeczywistym i kompleksowe zarządzanie danymi w celu zwiększenia ogólnego bezpieczeństwa i odporności środowisk ochrony danych.

Czołowa instytucja finansowa niedawno wdrożyła rozwiązanie PowerProtect Cyber Recovery, uniemożliwiając atakującym dostęp do 90% krytycznych kopii zapasowych podczas naruszenia, umożliwiając bezproblemowe przywracanie bez płatności okupu.

Rozwiązania Dell PowerProtect dla integralności kopii zapasowych

Dell PowerProtect zapewnia kompleksową ochronę kopii zapasowych, wykorzystując niezmienność, izolację i kompresję, aby zapobiec naruszeniom systemu kopii zapasowych. Dzięki integracji z narzędziami do wykrywania ransomware rozwiązanie PowerProtect daje pewność, że podejrzane zmiany są natychmiast sygnalizowane, co pozwala na podjęcie natychmiastowych działań.

Wielowarstwowe podejście do zabezpieczeń

Ochrona danych wymaga skoordynowanych, wieloaspektowych strategii bezpieczeństwa. Firma Dell pomaga firmom wdrażać najlepsze praktyki branżowe w celu zbudowania odpornego środowiska tworzenia kopii zapasowych.

Najważniejsze kroki w celu wzmocnienia obrony

- **Wprowadź zasady modelu „zero trust”:** Stale weryfikuj wszystkich użytkowników, wszelkie urządzenia i procesy, zmniejszając ryzyko nieautoryzowanego dostępu.
- **Zapewnij szyfrowanie wszystkich kopii zapasowych:** Miej pewność, że dane pozostają nieczytelne w przypadku naruszenia bezpieczeństwa, zarówno w trakcie transmisji, jak i w stanie spoczynku.
- **Edukuj pracowników:** Zapoznaj pracowników z metodami wykrywania prób oszustw typu phishing i innych taktyk inżynierii społecznej, które prowadzą do pierwotnych naruszeń bezpieczeństwa.
- **Regularne testowanie luk w zabezpieczeniach:** Częste testy pomagają organizacjom identyfikować i naprawiać słabe obszary, zanim atakujący je wykorzystają.

Firma Dell łączy te praktyki z najnowocześniejszymi rozwiązaniami, tworząc solidną i responsywną infrastrukturę gotową do sprostania pojawiającym się wyzwaniom.

Strategiczne partnerstwa, które zwiększają bezpieczeństwo

Firma Dell współpracuje z liderami ds. cyberbezpieczeństwa, takimi jak Microsoft, CrowdStrike i Secureworks. Każde partnerstwo doskonali rozwiązania firmy Dell, oferując klientom niezrównane możliwości ochrony, takie jak zaawansowana analiza zagrożeń, monitorowanie punktów końcowych i kompleksowe strategie reagowania.

Wykorzystanie usług Dell Professional Services

Usługi profesjonalne firmy Dell Technologies wykorzystują wiedzę ekspercką i wskazówki, aby pomóc firmom skutecznie sprostać złożonym wyzwaniom związanym z cyberbezpieczeństwem. Od tworzenia planów reagowania na incydenty po wdrażanie architektur modelu „zero-trust” — specjaliści firmy Dell dbają o to, aby środowiska klientów były odporne na współczesne zagrożenia, takie jak infiltracja kopii zapasowych.

Zbuduj odporność biznesową dzięki firmie Dell

Wybór firmy Dell Technologies pozwala firmom wyprzedzić wyrafinowanych atakujących przy zachowaniu ciągłości działania. Dzięki innowacjom, partnerstwu i wiedzy eksperckiej firma Dell zapewnia organizacjom zapobieganie, wykrywanie i odzyskiwanie danych nawet po najpoważniejszych atakach związanych z infiltracją kopii zapasowych.

Dalsze działania

Skontaktuj się z firmą Dell Technologies już dziś, aby chronić swoją firmę. Wspólnie zabezpieczymy najważniejsze zasoby, ochronimy Twoją reputację i zbudujemy odporną przyszłość.

Firma Dell nadal dba o zaufanie w erze cyfrowej, zapewniając organizacjom narzędzia, wiedzę i wsparcie, których potrzebują do bezpiecznego działania i rozwoju.

Odporność kopii zapasowych zaczyna się od firmy Dell Technologies. Działaj już teraz, aby zabezpieczyć przyszłość Twojej działalności i wzmocnić pozycję w zakresie cyberbezpieczeństwa.

Więcej informacji o tym, jak radzić sobie z największymi wyzwaniami związanymi z cyberbezpieczeństwem, znajdziesz na stronie **Dell.com/SecuritySolutions**

Dowiedz się więcej o Rozwiązania firmy Dell

Skontaktuj się z ekspertem firmy Dell Technologies

Zobacz więcej materiałów

Dołącz do rozmowy, stosując #hasztag

DELL Technologies