Streszczenie dla zarządu

Zwiększ cyberodporność i chroń dane przed zagrożeniami typu cyber ransomware, korzystając m.in. z odizolowanego sejfu i oprogramowania do analizy bazującego na uczeniu maszynowym opartym na sztucznej inteligencji

Dzięki rozwiązaniu PowerProtect Cyber Recovery z CyberSense firmy Dell Technologies

W miarę wzrostu częstotliwości zagrożeń cybernetycznych i ewoluowaniu metod ataków plany ochrony danych muszą uwzględniać podejście, które zapewnia bezpieczeństwo i analizowanie wszystkich komponentów IT: od najmniej ważnych do najistotniejszych. Dell PowerProtect Cyber Recovery może pomóc w ochronie najbardziej poufnych danych o znaczeniu krytycznym, a zarazem zapewnić prawidłowe odzyskiwanie danych w obliczu cyberataku lub innego zakłócającego zdarzenia.

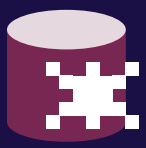
Dell PowerProtect Cyber Recovery to rozwiązanie do zarządzania danymi oraz ich ochrony i odzyskiwania, które pomaga organizacjom chronić dane i aplikacje przed atakami ransomware, niszczycielskimi cyberatakami i nieoczekiwanymi zdarzeniami. W rozwiązaniu tym stosuje się metodę wielokrotnego kopiowania, która polega na tym, że po utworzeniu kopii zapasowych kopiuje się je do izolowanej pamięci masowej w celu ochrony i analizy. Rozwiązanie PowerProtect Cyber Recovery składa się z wielu komponentów, w tym z co najmniej jednego sejfu pamięci masowej znajdującego się potencjalnie lokalnie w urządzeniu PowerProtect DD (nazywanym wcześniej Data Domain) lub w chmurze za pośrednictwem zdefiniowanej programowo pamięci masowej Dell APEX Protection Storage for Public Cloud (nazywanej wcześniej DD Virtual Edition). W obu przypadkach sejf jest fizycznie i operacyjnie odizolowany, tj. oddzielony od środowiska produkcyjnego — potencjalnie fizycznie oddzielony w przypadku środowiska lokalnego i logicznie oddzielony w przypadku środowiska APEX. To sprawia, że złośliwym podmiotom i nieupoważnionym użytkownikom niezwykle trudno jest się zalogować i naruszyć kopie zapasowe.

PowerProtect Cyber Recovery obejmuje też CyberSense, czyli w pełni zautomatyzowany i zintegrowany silnik inteligentnej analizy zabezpieczeń, który automatycznie skanuje dane, pliki, bazy danych i obrazy w sejfie w poszukiwaniu oznak uszkodzenia w wyniku ataku ransomware. CyberSense zapewnia pełną analizę treści, przyjmuje obserwacje z plików, które służą jako dane wejściowe dla modelu uczenia maszynowego (ML) opartego na sztucznej inteligencji (SI) oraz wykrywa złośliwe działania obejmujące masowe usuwanie, szyfrowanie i wprowadzanie innych podejrzanych zmian w infrastrukturze podstawowej (w tym w usłudze Active Directory i DNS), plikach użytkowników oraz produkcyjnych bazach danych o znaczeniu krytycznym, które mogą wskazywać na atak ransomware lub niszczycielski. Gdy CyberSense wykryje wzorce uszkodzenia, generuje na pulpicie nawigacyjnym PowerProtect Cyber Recovery alert, który zawiera dodatkowe informacje na temat skali i wpływu ataku.[1]

PowerProtect Cyber Recovery pomaga organizacjom łagodzić skutki cyberataków, zwiększać odporność danych dzięki ich wielu kopiom zapasowym z osobnych lokalizacji, skracać przestoje i utrzymywać ciągłość prowadzenia działalności biznesowej. W niniejszym raporcie wykorzystano dostępne publicznie informacje w celu podkreślenia kluczowych cech i funkcji w zakresie ochrony danych oraz przedstawiono nasze wnioski z analizy porównawczej silnika CyberSense.

Ochrona poufnych danych

Szyfrowanie niezmiennych danych w locie podczas replikacji kopii zapasowych do fizycznie i logicznie odizolowanych sejfów



Wykrywanie uszkodzenia strony programu SQL Server

Silnik CyberSense wykrył zarażenie, którego nie zgłosiło konkurencyjne rozwiązanie

Wykrywanie nieuszkodzonych kopii zapasowych

Silnik CyberSense wykrył najnowszą niezarażoną kopię zapasową na potrzeby odzyskiwania danych

zabezpieczenia

Dell PowerProtect Cyber Recovery udostępnia kilka funkcji zabezpieczeń, które pomagają chronić dane o znaczeniu krytycznym przed atakami ransomware i innymi wyrafinowanymi zagrożeniami, uniemożliwiają nieupoważnionym użytkownikom uzyskanie dostępu do poufnych informacji oraz przyspieszają odzyskiwanie danych, dzięki czemu organizacje mogą szybko wznowić normalne działanie.

Cechy i funkcjonalność urządzeń PowerProtect DD mogą mieć kluczowe znaczenie dla działań w zakresie bezpieczeństwa, integralności i odzyskiwania danych, które realizują rozwiązania PowerProtect Cyber Recovery. Te funkcje obejmują m.in. blokadę przechowywania, DDBoost, kontrolę dostępu opartą na rolach (RBAC) i podwójną autoryzację.

Izolacja

Izolacja danych odnosi się do odseparowywania danych i ograniczania dostępu do nich dzięki barierom lub granicom, które zapobiegają nieupoważnionemu dostępowi. Izolacja używa często tymczasowych połączeń sieciowych zamiast połączeń trwałych.

Izolacja danych zapewnia brak styczności danych o znaczeniu krytycznym z zarażoną siecią, w której złośliwy podmiot mógłby podjąć próbę zmiany konfiguracji, usunięcia danych, modyfikacji zasad lub podsłuchiwania ruchu sieciowego w poszukiwaniu danych uwierzytelniających użytkowników. Izolacja pomaga też zmniejszyć obszar narażony na ataki, ograniczając złośliwym podmiotom możliwości uzyskania dostępu i kontroli. Ponadto organizacje mogą ograniczać krąg użytkowników, którzy mają dostęp, tylko do autoryzowanego personelu, co pomaga zapobiegać nadpisywaniu danych przez nieupoważnione osoby.

Oprócz wspomnianych już funkcji PowerProtect Cyber Recovery może zapewniać fizyczną i logiczną izolację, aby pomagać w ochronie danych. Odizolowane fizycznie lokalne urządzenie PowerProtect DD może działać jako sejf, w którym użytkownicy ani systemy ze środowiska produkcyjnego nie mogą uzyskiwać dostępu do komponentów. Sam sejf jest fizycznie odłączony od sieci produkcyjnej.[2] Dzięki eliminacji dostępu z sieci produkcyjnej do środowiska odzyskiwania danych organizacja może zmniejszyć obszar narażony na ataki.

Niezmienność*

Dzięki skonfigurowaniu kopii zapasowych jako niezmiennych, czyli przeznaczonych tylko do odczytu, organizacja może z pełnym zaufaniem używać tych kopii do odzyskiwania danych. Pod względem operacyjnym niezmienność pomaga zachować autentyczność i niezawodność danych. Systemy DD, w tym te wchodzące w skład rozwiązań PowerProtect Cyber Recovery, mogą zapewnić niezmienność sposobu przechowywania danych przy użyciu partycji logicznych systemu plików o nazwie MTrees. Rozwiązania te korzystają również z replikacji MTree do kopiowania niezmiennych kopii danych z produkcyjnego urządzenia DD na inne urządzenie DD w sejfie za pośrednictwem protokołu DDBoost.[3]

* Produkty firmy Dell zostały zaprojektowane z myślą o wspieraniu wysiłków klientów na rzecz zabezpieczenia ich danych o znaczeniu krytycznym. Podobnie jak w przypadku każdego produktu elektronicznego w produktach z zakresu ochrony danych, pamięci masowej i innych elementów infrastruktury mogą występować luki w zabezpieczeniach. Ważne jest, aby klienci instalowali aktualizacje zabezpieczeń zaraz po ich udostępnieniu przez firmę Dell.

CyberSense

Skuteczna ochrona danych wymaga kompleksowej strategii, która zapewnia bezpieczeństwo na każdym poziomie. Pomimo wszystkich mechanizmów autonaprawy, zabezpieczeń, niezmienności i funkcji izolacji, jakie udostępnia rozwiązanie Dell PowerProtect Cyber Recovery, mniej oczywiste ataki mogłyby nadal wnikać głębiej w infrastrukturę przedsiębiorstwa, np. na poziom zapasowych kopii danych, i potencjalnie pozostawać niewykryte do czasu naruszenia bezpieczeństwa danych produkcyjnych lub całej grupy użytkowników. Rozwiązania Dell PowerProtect Cyber Recovery stanowią ostatnią linię obrony przed cyberatakami i skuteczny środek przyspieszający odzyskiwanie danych dzięki funkcji CyberSense.

Przetestowaliśmy CyberSense i podobnie działające narzędzie z platformy do zarządzania danymi oferowanej przez naszego konkurenta (którego nazywamy „Dostawcą X"), a przeznaczonej do urządzenia o podobnej wielkości. Z naszych testów wynika, że rozwiązanie PowerProtect Cyber Recovery wykryło zarażenie na stronach bazy danych SQL — rozwiązanie Dostawcy X nie było w stanie tego zrobić. PowerProtect Cyber Recovery wymagało też mniejszej liczby kopii zapasowych niż rozwiązanie Dostawcy X w celu wykrycia uszkodzenia danych.

1. Dell, „CyberSense® for PowerProtect Cyber Recovery", dostęp 8 września 2023 r., https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
2. Dell, „MTree replication" (Replikacja MTree), dostęp 11 września 2023 r., https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.
3. Principled Technologies, „Dell EMC Cyber Recovery protected our test data from a cyberattack" (Rozwiązanie Dell EMC Cyber Recovery ochroniło nasze dane testowe przed cyberatakiem), dostęp 21 sierpnia 2023 r., http://facts.pt/rkew01n.

▶ Zobacz oryginalną wersję tego podsumowania w języku angielskim

Przeczytaj raport ▶

Principled Technologies®

Facts matter.®