DELL Technologies

Ataki ransomware: wzmocnienie cyberbezpieczeństwa i odporności dzięki rozwiązaniom Dell Technologies

Co to jest ransomware?

Ransomware to rodzaj złośliwego oprogramowania, które blokuje dostęp do systemu komputerowego lub danych do momentu zapłacenia okupu. Jest to jeden z najbardziej destrukcyjnych typów cyberataków. Pięćdziesiąt procent organizacji na całym świecie zostało dotkniętych oprogramowaniem ransomware co najmniej raz w ciągu ostatniego roku, a średni czas przestoju po ataku ransomware wynosi trzy tygodnie, co prowadzi do poważnych zakłóceń operacyjnych

Rosnące zagrożenie atakami ransomware

Ransomware to rodzaj złośliwego oprogramowania, które blokuje dostęp do systemu komputerowego lub danych do momentu zapłacenia okupu. Jest to jeden z najbardziej destrukcyjnych typów cyberataków. Pięćdziesiąt procent organizacji na całym świecie zostało dotkniętych oprogramowaniem ransomware co najmniej raz w ciągu ostatniego roku, a średni czas przestoju po ataku ransomware wynosi trzy tygodnie, co prowadzi do poważnych zakłóceń operacyjnych.

Jak działa ransomware

Ransomware zwykle infekuje organizacje, gdy ktoś kliknie złośliwy link, otworzy zainfekowany załącznik lub odwiedzi naruszoną witrynę. Następnie przechodzi do systemów w celu zaszyfrowania plików, co czyni je nieczytelnymi. Następnie program ransomware zazwyczaj wyświetla komunikat z żądaniem okupu (często w kryptowalucie) w zamian za klucz deszyfrujący. Jeśli okup nie zostanie zapłacony, atakujący może grozić usunięciem danych lub ich publicznym wyciekiem. Typowym przykładem ataku ransomware, który pojawił się w 2017 roku, był WannaCry — wirus, który szybko rozprzestrzenił się na całym świecie, dotykając szpitale, przedsiębiorstwa i instytucje państwowe oraz powodując ogromne straty finansowe. Globalne konsekwencje ekonomicznego wirusa WannaCry wyniosły od 4 mld USD do 8 mld USD według Cyber Risk Management (CyRiM) i Lloyd's of London, przy czym w ciągu kilku dni ponad 200 000 systemów w 150 krajach zostało zaatakowanych.

Dwie z największych zaatakowanych korporacji na świecie to FedEx, który zgłosił straty w wysokości 300 milionów dolarów z powodu zakłóceń w świadczeniu usług i czyszczenia sprzętu, oraz Renault-Nissan, który musiał tymczasowo wstrzymać produkcję w kilku zakładach. Może być wiele ukrytych kosztów ataku ransomware, na przykład:

- Przestoje firmy i utrata produktywności
- Uszczerbek na reputacji
- Koszt odzyskania i poprawek systemu
- Grzywny określone w przepisach i regulacjach

W przypadku ataku ransomware firmy powinny podjąć następujące kroki:

- Nie płać, chyba że jest to bezwzględnie konieczne — nie ma gwarancji, że atakujący przywróci dostęp.
- Przywróć z kopii zapasowej, jeśli jest dostępna.
- Zgłoś atak do władz.
- Wzmocnienie zabezpieczeń w celu zapobiegania przyszłym infekcjom (np. aktualizowanie oprogramowania, szkolenie personelu, ochrona punktów końcowych).

Przeciwdziałanie atakom ransomware z pomocą firmy Dell Technologies

Firma Dell Technologies wyposaża organizacje w kompleksowe, przyszłościowe narzędzia zaprojektowane z myślą o zapobieganiu zagrożeniom ransomware, zanim spowodują one szkody.

Poprawione bezpieczeństwo punktów końcowych dzięki Dell Trusted Devices

Punkty końcowe są często głównymi punktami wejścia dla ataków ransomware, co sprawia, że bezpieczeństwo punktów końcowych jest kluczowym obszarem zainteresowania. Dell Trusted Devices integruje sprzętowe funkcje zabezpieczeń, które chronią systemy bez uszczerbku dla wydajności. Rozwiązania, takie jak Dell SafeBIOS i SafeID, wzmacniają urządzenia końcowe przed nieautoryzowanym dostępem, podczas gdy Dell SafeData szyfruje dane w celu ochrony poufnych informacji nawet poza zaporą firmową. Dzięki wbudowaniu zabezpieczeń bezpośrednio w urządzenia firmy uzyskują ochronę na poziomie sprzętowym, ograniczając możliwości atakujących.

Proaktywne wykrywanie dzięki CrowdStrike

Można uniknąć ataków, jeśli organizacje używają odpowiednich narzędzi do wykrywania zagrożeń i reagowania na nie w czasie rzeczywistym. CrowdStrike, w ramach oferty rozwiązań firmy Dell, zapewnia platformę ochrony punktów końcowych nowej generacji opartą na sztucznej inteligencji i analizie behawioralnej. Technologia ta identyfikuje i neutralizuje podejrzaną aktywność, zanim przekształci się w atak. Dzięki bezproblemowej integracji z infrastrukturą firmy Dell CrowdStrike umożliwia zespołom IT utrzymanie widoczności w całym środowisku, zapewniając natychmiastową i skuteczną reakcję na zagrożenia.

Kompleksowa ochrona danych dzięki Dell PowerProtect

Rozwiązania Dell PowerProtect stanowią podstawę odporności na ataki ransomware. Te zaawansowane narzędzia do ochrony danych zostały zaprojektowane z myślą o zabezpieczeniu danych przedsiębiorstwa przed zagrożeniami wewnętrznymi i zewnętrznymi. Funkcje takie jak niezamienne kopie zapasowe dają gwarancję, że dane nie mogą być zmieniane, usuwane ani szyfrowane przez oprogramowanie ransomware, zapewniając niezawodną siatkę bezpieczeństwa nawet w obliczu zaawansowanych ataków. Na przykład Dell PowerProtect Cyber Recovery Vault izoluje krytyczne dane z sieci przy użyciu odizolowanej technologii, zapewniając, że pozostają nietknięte nawet podczas najbardziej zaawansowanych naruszeń. Dzięki zautomatyzowanemu wykrywaniu anomalii i inteligentnym przepływom pracy organizacje zyskują możliwość wczesnego wykrywania złośliwej aktywności i reagowania, zanim ransomware się rozprzestrzeni.

Zaawansowane zabezpieczenia sieciowe i mikrosegmentacja dzięki rozwiązaniom Dell PowerSwitch Networking i SmartFabric OS

Wzmocnij ochronę przed atakami typu zero-day, zapewniając zaawansowaną segmentację sieci, ścisłą kontrolę dostępu i analizę ruchu w czasie rzeczywistym w całej infrastrukturze.

Odzyskiwanie na dużą skalę dzięki usługom Dell Data Protection Services

Firma Dell wie, że choć zapobieganie jest kluczowe, równie ważnym aspektem gotowości na ransomware jest odzyskiwanie danych. Usługi Dell Data Protection Services zapewniają nie tylko zautomatyzowane rozwiązania do tworzenia kopii zapasowych i odzyskiwania danych, ale także specjalistyczne doradztwo, które zapewnia firmom szybkie odzyskiwanie danych i minimalizację przestojów. Usługi takie jak zdalne odzyskiwanie danych i reagowanie na incydenty zapewniają organizacjom wsparcie, którego potrzebują w szczytowych momentach kryzysu. To kompleksowe podejście gwarantuje zachowanie integralności danych i skrócenie czasu odzyskiwania, co zapobiega zakłóceniom działania.

To tylko kilka przykładów rozwiązań firmy Dell, które mogą pomóc w walce ze złośliwymi zagrożeniami wewnętrznymi.

Siła we współpracy

Oparte na współpracy podejście firmy Dell rozszerza ochronę poza technologię wyłącznie firmy Dell. Dzięki współpracy z czołowymi firmami zajmującymi się cyberbezpieczeństwem, takimi jak CrowdStrike i Secureworks, firma Dell oferuje ekosystem zintegrowanych rozwiązań, które uwzględniają każdy możliwy wektor ataków. Rozwiązania te zapewniają kompleksowe zabezpieczenia, umożliwiając firmom tworzenie wielowarstwowych zabezpieczeń dostosowanych do ich unikalnych profili ryzyka.

Dlaczego warto wybrać firmę Dell?

Dell Technologies to nie tylko dostawca technologii — to zaufany partner w walce z oprogramowaniem ransomware. Łącząc innowacje, ekspercką wiedzę i zaangażowanie w zwiększanie możliwości firm, firma Dell wyposaża organizacje w narzędzia i pewność potrzebne do stawienia czoła zmieniającym się zagrożeniom. Niezależnie od tego, czy zabezpieczamy punkty końcowe, chronimy krytyczne dane, czy umożliwiamy szybkie odzyskiwanie, produkty i usługi firmy Dell zapewniają ciągłość działania i święty spokój.

Budowanie odpornej przyszłości

Ataki ransomware nadal ewoluują, ale dzięki Dell Technologies firmy mogą wyprzedzać zagrożenia. Korzystając z zaawansowanego sprzętu, oprogramowania i usług, organizacje mogą zbudować platformę cyberbezpieczeństwa, która jest odporna, elastyczna i niezawodna. Chroń swoje dane, zabezpiecz swoje operacje i swoją firmę na przyszłość już dziś dzięki kompleksowym rozwiązaniom firmy Dell przeciwko ransomware.

Aby zapewnić odporność firmy, trzeba zrozumieć obecny krajobraz zagrożeń i być na bieżąco z pojawiającymi się zagrożeniami. Eksperci ds. cyberbezpieczeństwa firmy Dell Technologies stale monitorują nowe wektory ataków (jak to nazywamy?) i pracują nad proaktywnym eliminowaniem potencjalnych luk w naszych produktach i usługach. Dzięki temu możemy zapewnić najbardziej aktualną ochronę przed stale zmieniającymi się zagrożeniami ransomware.

Oprócz bycia na bieżąco firmy muszą również wdrożyć wielowarstwowe podejście do bezpieczeństwa. Oznacza to wdrożenie szeregu zabezpieczeń, takich jak zapory sieciowe, oprogramowanie chroniące przed złośliwym oprogramowaniem, systemy wykrywania włamań i kopie zapasowe danych. Poprzez zróżnicowanie strategii obronnych możesz zminimalizować wpływ każdego ataku i zapewnić firmie działanier nawet w przypadku udanej próby ataku ransomware.

Ważne jest również, aby regularnie testować i aktualizować zabezpieczenia (zarówno poprawki systemów, jak i aktualizacje zasad). Hakerzy nieustannie znajdują nowe sposoby na ominięcie tradycyjnych środków bezpieczeństwa, więc ważne jest, aby firmy wyprzedziły konkurencję, regularnie testując swoje zabezpieczenia i aktualizując je w razie potrzeby. Obejmuje to regularne oceny luk w zabezpieczeniach, testy penetracyjne i zarządzanie poprawkami.

Innym kluczowym aspektem ochrony firmy przed oprogramowaniem ransomware jest edukacja pracowników w zakresie najlepszych praktyk dotyczących cyberbezpieczeństwa. Wiele ataków ransomware jest inicjowanych za pomocą technik inżynierii społecznej, takich jak phishingowe wiadomości e-mail lub złośliwe linki. Poprzez uczenie pracowników, jak wykrywać i unikać tych zagrożeń, można znacznie zmniejszyć prawdopodobieństwo udanego ataku.

Ponadto posiadanie planu awaryjnego może znacznie ograniczyć skutki ataku ransomware. Plan ten powinien obejmować regularne kopie zapasowe ważnych danych i systemów, a także jasną procedurę reagowania na atak i odzyskiwanie danych.

Oprócz tych proaktywnych działań ważne jest również posiadanie silnego planu reagowania na incydenty. Obejmuje to jasno określone role i obowiązki w zakresie obsługi ataku ransomware, a także protokoły komunikacji w celu powiadamiania zainteresowanych stron i ograniczania szkód.

Wreszcie bycie na bieżąco z najnowszymi trendami i rozwojem ataków ransomware może pomóc Ci wyprzedzić potencjalne zagrożenia. Regularnie przeglądając raporty branżowe i aktualizacje od ekspertów ds. bezpieczeństwa, możesz aktywnie wdrażać nowe środki bezpieczeństwa, aby chronić swoją firmę.

Pamiętaj, że żadna firma nie jest odporna na ataki ransomware, ale dzięki odpowiednim strategiom i narzędziom możesz zminimalizować ryzyko i konsekwencje takich ataków. Dzięki proaktywnemu podejściu do cyberbezpieczeństwa nie tylko chronisz swoją firmę, ale także budujesz zaufanie wśród klientów i interesariuszy.

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

Więcej informacji na temat rozwiązań firmy Dell

Skontaktuj się z ekspertem firmy Dell Technologies

Zobacz więcej zasobów

Dołącz do rozmowy, stosując #hasztag

DELL Technologies