DELL Technologies

Zero Day: wzmocnienie cyberbezpieczeństwa i odporności dzięki rozwiązaniom Dell Technologies

Rosnące zagrożenie atakami typu zero day

Ataki typu zero day szybko stały się jednym z największych wyzwań w dzisiejszym środowisku cyberbezpieczeństwa. Ataki te wykorzystują luki w zabezpieczeniach, które nie są znane dostawcom oprogramowania i ekspertom ds. bezpieczeństwa, pozostawiając firmy nieprzygotowane i narażone. Organizacje we wszystkich branżach, od opieki zdrowotnej po finanse, są narażone na takie naruszenia, co często skutkuje poważnymi konsekwencjami finansowymi i operacyjnymi.

Tempo transformacji cyfrowej przyspiesza, a ataki typu zero-day stają się coraz częstsze i bardziej zaawansowane. Potrzeba solidnych zabezpieczeń nigdy nie była większa. Firma Dell Technologies rozumie krytyczny charakter tego zagrożenia i zapewnia firmom innowacyjne, skalowalne zabezpieczenia, które skutecznie zwalczają ataki typu zero day i umożliwiają odzyskiwanie danych po atakach typu zero day.

Czym są ataki typu zero day?

Atak zero day polega na wykorzystaniu nieujawnionej luki w zabezpieczeniach oprogramowania lub sprzętu przed udostępnieniem poprawki lub rozwiązania. Atakujący wykorzystują lukę w zabezpieczeniach, często powodując poważne zakłócenia, zanim luka zostanie wykryta i naprawiona.

Jak działają ataki typu zero day

1. **Odkrywanie luk w zabezpieczeniach:** Hakerzy wykrywają błędy w kodowaniu lub ukryte furtki w aplikacjach bądź systemach **oprogramowania.**
2. **Przygotowywanie ataków:** Złośliwe oprogramowanie jest tworzone w celu wykorzystania luk w zabezpieczeniach. Atakujący mogą wykorzystać ukierunkowane kampanie phishingowe lub strony internetowe zawierające złośliwe oprogramowanie do użycia luk.
3. **Wykonanie ataku:** wykorzystywane są luki, co naraża system i potencjalnie umożliwia kradzież danych lub zakłócenia operacyjne.

Typowe techniki

- Niechciane pobrania nakłaniają użytkowników do nieświadomej instalacji złośliwego oprogramowania.
- E-maile phishingowe rozsyłają złośliwe linki lub załączniki w celu wykorzystania luk w zabezpieczeniach.
- Ataki bezplikowe unikają wykrycia, wykonując operacje całkowicie w pamięci systemu.

Te wysoce zaawansowane wektory ataków sprawiają, że ataki typu zero-day są szczególnie niebezpieczne, ponieważ tradycyjne narzędzia do wykrywania na podstawie sygnatur często ich nie rozpoznają.

Konsekwencje dla firm

Ataki typu zero-day wiążą się ze znacznym ryzykiem ze względu na nieprzewidywalność i opóźnienie w wykrywaniu. Konsekwencje mogą być katastrofalne na wielu frontach.

Straty finansowe

Udany atak typu zero-day może skutkować wysokimi kosztami, od grzywien regulacyjnych po utratę przychodów w czasie przestoju. Na przykład nieidentyfikowana luka w platformie e-commerce może uniemożliwić proces płatności, bezpośrednio wpływając na sprzedaż.

Konsekwencje dla reputacji

Publiczne postrzeganie firmy może zostać nieodwracalnie naruszone. Klienci tracą zaufanie w przypadku ujawnienia poufnych informacji lub awarii usług.

Zakłócenia operacyjne

Nierozwiązane luki w zabezpieczeniach często paraliżują systemy, co prowadzi do obniżenia produktywności, opóźnień projektów i utraty możliwości biznesowych.

Przykład z życia

Główny dostawca opieki zdrowotnej padł ofiarą ataku typu zero-day, który był ukierunkowany na nieaktualizowane oprogramowanie urządzeń medycznych. Atak zakłócił kluczowe operacje, ujawnił dane pacjentów i kosztował organizację **miliony** w opłatach za odzyskanie danych, jednocześnie podkopując zaufanie pacjentów.

Alarmujące statystyki

Badania wskazują, że według raportu Ponemon z 2023 roku około 80% naruszeń bezpieczeństwa wiąże się z wykorzystaniem luk typu zero-day

Ataki typu zero-day stale stanowią ponad **70%** przypadków wykorzystania luk w zabezpieczeniach

Źródło: 2024: IMandiant „M-Trends”

Przeciwdziałanie atakom typu zero day dzięki firmie Dell Technologies

Firma Dell Technologies oferuje najlepsze w branży rozwiązania, które pomagają firmom aktywnie chronić się przed atakami typu zero-day, jednocześnie promując szybkie odzyskiwanie danych po takich naruszeniach.

Rozwiązania w zakresie bezpieczeństwa serwerów i pamięci masowej

Rozwiązania firmy Dell w zakresie zabezpieczeń serwerów i pamięci masowej zapewniają dodatkowe warstwy ochrony:

- Bezpieczne serwery monitorują i blokują próby nieautoryzowanego dostępu.
- Systemy tworzenia kopii zapasowych i odzyskiwania danych dają pewność, że nawet w najgorszym przypadku informacje o znaczeniu krytycznym pozostają dostępne i nienaruszone.

Wzmocnione punkty końcowe dzięki zaufanym urządzeniom firmy Dell

Punkty końcowe są kluczowym miejscem wejścia dla atakujących. Urządzenia Dell Trusted Devices wprowadzają zaawansowane środki bezpieczeństwa, zapewniając ochronę punktów końcowych przed niewykrytymi zagrożeniami.

- **SafeBIOS** chroni oprogramowanie wewnętrzne przed manipulacją, zapewniając integralność systemu od podstaw.
- **SafeID** chroni poświadczenia użytkownika, zabezpieczając procesy uwierzytelniania.
- **SafeData** szyfruje wrażliwe dane w spoczynku i w ruchu, czyniąc je bezużytecznymi w przypadku przechwycenia lub wykorzystania.

Proaktywne wykrywanie zagrożeń dzięki CrowdStrike

CrowdStrike wykorzystuje zaawansowaną analizę i sztuczną inteligencję do monitorowania aktywności punktów końcowych, wykrywając nietypowe zachowania, które mogą wskazywać na wykorzystanie luk typu zero-day. Proaktywne wykrywanie zagrożeń zapewnia szybką reakcję, zanim luki w zabezpieczeniach zdołają spowodować rozległe uszkodzenia.

Na przykład dostawca telekomunikacyjny korzystający z narzędzia CrowdStrike był w stanie wcześnie wykryć anomalie w ruchu sieciowym, łagodząc potencjalne wykorzystanie luk typu zero-day na serwerach klienta.

Rozwiązania Dell PowerProtect

Dell PowerProtect zapewnia solidne, niezmienne kopie zapasowe i izolowane opcje odzyskiwania. Firmy mogą szybko i skutecznie przywracać operacje po ataku typu zero-day, zachowując ciągłość biznesową i chroniąc ważne dane klientów.

Na przykład duża sieć sprzedaży detalicznej wykorzystała rozwiązanie PowerProtect do odzyskiwania zaszyfrowanych plików, które zostały naruszone przez atak ransomware wynikający z luki w zabezpieczeniach typu zero-day, unikając długotrwałych przestojów.

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.

Znaczenie wielowarstwowego podejścia do zabezpieczeń

Prawdziwe bezpieczeństwo wymaga więcej niż jednego rozwiązania. Wielowarstwowa strategia łączy technologię, procesy i ludzi w celu utworzenia kompleksowej struktury ochrony.

Kluczowe działania na rzecz wzmocnienia obronności

- **Zastosuj zasady zero zaufania:** Weryfikuj każdą osobę i urządzenie próbujące uzyskać dostęp do sieci.
- **Implementacja zaawansowanego szyfrowania:** Wykorzystaj protokoły szyfrowania, aby chronić dane w ruchu i w spoczynku.
- **Edukuj pracowników:** przeprowadzaj szczegółowe sesje szkoleniowe, aby nauczyć pracowników rozpoznawania prób phishingu i taktyk inżynierii społecznej.
- **Regularnie testuj systemy:** Przeprowadzaj spójne testy penetracyjne i skanowanie pod kątem luk w zabezpieczeniach, aby zapewnić dostosowanie zabezpieczeń do nowych zagrożeń.

Firma Dell Technologies łączy te praktyki z zaawansowanymi rozwiązaniami zabezpieczającymi, zapewniając organizacjom gotowość do skutecznego zwalczania luk w zabezpieczeniach typu zero-day.

Partnerstwa wzmacniające cyberbezpieczeństwo

Współpraca firmy Dell z liderami branży **Microsoft**, **CrowdStrike**i **Secureworks** zapewnia klientom dostęp do najnowocześniejszych danych i narzędzi bezpieczeństwa.

- **Firma Microsoft** bezproblemowo integruje się z rozwiązaniami firmy Dell, aby zapewnić zgodność całego systemu i proaktywne mechanizmy ochrony
- **CrowdStrike** oferuje zaawansowaną analizę zagrożeń punktów końcowych Threat Intelligence w celu wykrywania potencjalnych ataków typu zero-day.
- **SecureWorks** zapewnia ciągłe monitorowanie i specjalistyczne środki zaradcze w celu reagowania na ataki w czasie rzeczywistym.

Wykorzystanie Dell Professional Services

Usługi Dell Professional Services obejmują kompleksowy zakres doradztwa, wdrażania i pomocy w odzyskiwaniu danych, które pomagają firmom w radzeniu sobie z zagrożeniami typu zero-day i ich ograniczeniu. Od reagowania na incydenty po planowanie planu cyberbezpieczeństwa — firma Dell pomaga organizacjom osiągnąć długoterminową odporność.

Buduj odporną przyszłość

Inwestowanie w firmę Dell Technologies oznacza posiadanie partnera, który oferuje nie tylko doskonałą technologię, ale także święty spokój. Dzięki najnowocześniejszym rozwiązaniom, strategicznym partnerstwom i niezrównanej wiedzy firma Dell umożliwia organizacjom przewidywanie, wykrywanie i odzyskiwanie danych nawet po najbardziej zaawansowanych atakach typu zero-day.

Skontaktuj się z firmą Dell Technologies już dziś, aby zabezpieczyć swoją firmę, ochronić swoją reputację i rozwijać się w nieprzewidywalnym środowisku cyfrowym. Zaufaj firmie Dell, która zabezpieczy Twoją przyszłość przed zagrożeniami jutra.

Firma Dell Technologies wzbudza zaufanie, umożliwiając firmom wyprzedzanie o krok ewoluujących wyzwań związanych z atakami typu zero-day dzięki rozwiązaniom i usługom bezpieczeństwa zaprojektowanym z myślą o ochronie tego, co najważniejsze.

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

Więcej informacji na temat rozwiązań Dell

Skontaktuj się z ekspertem firmy Dell Technologies

Zobacz więcej materiałów

Dołącz do rozmowy, stosując #hasztag

DELL Technologies