DELL Technologies

Złośliwe ataki wewnętrzne: wzmacnianie cyberbezpieczeństwa i odporności dzięki firmie Dell Technologies

Rosnące zagrożenie ze strony złośliwych ataków wewnętrznych

Złośliwe ataki wewnątrz organizacji stały się jednym z najpoważniejszych zagrożeń dla bezpieczeństwa w dzisiejszym świecie biznesu. W przeciwieństwie do zagrożeń zewnętrznych złośliwi użytkownicy mają już pewien stopień zaufania i dostępu w organizacji, co sprawia, że ich działania są szczególnie szkodliwe i trudniejsze do wykrycia. Od dostępu do wrażliwych danych po sabotaż systemów — ataki wewnętrzne mogą zakłócać krytyczne operacje i powodować poważne konsekwencje finansowe i utratę reputacji.

Firma Dell Technologies dostrzega rosnące zagrożenie związane z tego typu atakami i opracowuje innowacyjne, skalowalne rozwiązania, które ułatwiają firmom identyfikowanie, zapobieganie i ograniczanie ryzyka związanego z złośliwymi atakami wewnętrznymi. Łącząc najnowocześniejszą technologię z usługami eksperckimi, firma Dell pomaga organizacjom wyprzedzić te wewnętrzne zagrożenia.

Czym są złośliwe ataki wewnętrzne?

Złośliwy atak wewnętrzny ma miejsce, gdy osoba w organizacji wykorzystuje swoje uprawnienia do naruszenia danych, zakłócenia działalności lub pozyskania poufnych informacji w celu osiągnięcia osobistych, finansowych lub konkurencyjnych celów. Osoba ta może być pracownikiem, wykonawcą, partnerem lub osobą posiadającą uzasadniony dostęp do systemów i sieci firmy.

Jak działają złośliwe ataki wewnętrzne

Użytkownicy, którzy wywołują ataki wewnętrzne wykorzystują swoją zaufaną pozycję, aby ominąć standardowe zabezpieczenia. Do typowych technik należą:

1. **Kradzież danych:** eksfiltracja poufnych danych klienta, własności intelektualnej lub dokumentacji finansowej.
2. **Sabotaż:** celowe uszkodzenie systemów IT w celu zakłócenia działalności biznesowej lub osłabienia reputacji.
3. **Nadużywanie poświadczeń:** używanie skradzionych lub niewłaściwie używanych poświadczeń do eskalacji uprawnień dostępu lub tworzenia fałszywych kont.
4. **Współpraca z zewnętrznymi atakującymi:** dzielenie się dostępem lub wrażliwą wiedzą z zewnętrznymi cyberprzestępcami w zamian za korzyści finansowe.

Ta podwójna przewaga, jaką stanowią zaufanie i wewnętrzna wiedza, sprawia, że złośliwi pracownicy są wyjątkowo niebezpieczni w porównaniu z zewnętrznymi atakującymi.

Wpływ na firmy

Skutki złośliwych ataków wewnętrznych są długofalowe i powodują szkody wykraczające poza straty finansowe. Firmy mogą napotkać różne konsekwencje, takie jak:

Straty finansowe

Kradzież poufnych informacji, oszustwa lub sabotaż mogą prowadzić do strat finansowych i kosztów odzyskiwania sięgających milionów dolarów.

Zakłócenia operacyjne

Sabotaż systemu lub zniszczenie danych może spowodować wstrzymanie działalności, co prowadzi do opóźnień, utraty możliwości i spadku wydajności.

Uszkodzenie reputacji

Naruszenie lub atak ze strony osób wewnętrznych osłabia zaufanie klientów i interesariuszy, wpływając na lojalność klientów i postrzeganie rynku.

Naruszenie zgodności z przepisami

W zależności od branży ataki wewnętrzne mogą prowadzić do wysokich kar i grzywien, jeśli dotyczą danych wrażliwych, takich jak dane medyczne lub finansowe.

Autentyczny przykład

W 2020 roku kontrahent IT pracujący w dużej instytucji finansowej celowo usunął krytyczne konfiguracje systemów, powodując awarie sieci przez ponad **10 godzin**. Ten akt sabotażu spowodował straty finansowe w wysokości wielu **milionów** dolarów, wysokie koszty napraw i uszczerbek na reputacji. Takie incydenty ilustrują destrukcyjny potencjał zagrożeń wewnętrznych i podkreślają pilną potrzebę solidnych środków wykrywania i zapobiegania.

Szacowane koszty

Według badania przeprowadzonego przez Ponemon Institute w 2024 r. średni koszt incydentu związanego z atakiem wewnętrznym szacowany jest na **4,99 mln USD** i stanowi prawie **55%** wszystkich naruszeń bezpieczeństwa. Kwota ta obejmuje koszty wykrycia, odzyskania danych i złagodzenia skutków, co wskazuje na pilną potrzebę inwestowania przez organizacje w prewencyjne zabezpieczenia przed ryzykiem związanym z atakami wewnętrznymi.

83%

organizacji zgłosiło co najmniej jeden atak wewnętrzny w ciągu ostatniego roku.

Źródło: 2024: Cybersecurity Insiders' Report

Zwalczanie złośliwych ataków wewnętrznych z wykorzystaniem rozwiązań firmy Dell Technologies

Dell Technologies oferuje kompleksowy ekosystem narzędzi i usług do walki ze złośliwymi zagrożeniami wewnętrznymi, dzięki czemu Twoja organizacja jest przygotowana na nieoczekiwane sytuacje.

Zabezpiecz punkty końcowe za pomocą rozwiązania Dell Trusted Devices

Punkty końcowe często służą jako punkty wejścia dla zagrożeń wewnętrznych. Dell Trusted Devices integruje najnowocześniejsze funkcje zabezpieczeń ze sprzętem, aby wzmocnić punkty końcowe i chronić wrażliwe dane.

- **System Dell SafeBIOS** zapewnia integralność oprogramowania wewnętrznego, zapobiegając próbom manipulowania działaniem systemu na poziomie sprzętu.
- **SafeID** chroni dane poświadczeń, zapobiegając nieautoryzowanemu dostępowi i nadużywaniu poświadczeń.
- **SafeData** szyfruje wrażliwe dane od końca do końca, zapewniając, że przechwycone lub wyodrębnione informacje pozostają nieczytelne dla złośliwych osób.

Wdrażając te rozwiązania, organizacje mogą zapewnić ochronę swoich punktów końcowych niezależnie od tego, czy zagrożenie pochodzi wewnętrznie, czy zewnętrznie.

Proaktywne wykrywanie zagrożeń dzięki CrowdStrike

Identyfikacja zagrożeń wewnętrznych wymaga widoczności i monitorowania zachowań użytkowników. Oprogramowanie CrowdStrike, zintegrowane z rozwiązaniami firmy Dell, wykorzystuje sztuczną inteligencję i analizę behawioralną do wykrywania anomalii wskazujących na zagrożenia wewnętrzne.

Na przykład nietypowe przesyłanie danych poza godzinami pracy lub nieautoryzowany dostęp do krytycznych obszarów sieci są natychmiast oznaczane, co ułatwia szybką reakcję. Amerykańska organizacja opieki zdrowotnej niedawno wykorzystała proaktywne wykrywanie zagrożeń, aby zidentyfikować i zakończyć próbę eksfiltracji danych pacjentów przez pracownika, zapobiegając kosztownemu naruszeniu.

Ulepszona ochrona danych dzięki Dell PowerProtect

Dell PowerProtect zapewnia solidną linię obrony dzięki bezpiecznym kopiom zapasowym, odizolowanej pamięci masowej i niezmiennym kopiom danych o znaczeniu krytycznym. Zapewniając ochronę poufnych informacji przed modyfikacją lub usunięciem, ataki wewnętrzne ukierunkowane na integralność danych mogą być nieskuteczne.

Przykładem może być firma produkcyjna, która miała do czynienia z niezadowolonym pracownikiem próbującym sabotować pliki projektowe. Sejf do odzyskiwania danych Dell PowerProtect pozwolił firmie przywrócić działalność w ciągu kilku godzin, unikając zakłóceń i utrzymując ciągłość prowadzenia działalności biznesowej.

Szybkie odzyskiwanie danych dzięki usługom Dell Professional Services

Gdy zagrożenie wewnętrzne przekształca się w incydent, niezbędne jest szybkie odzyskiwanie danych. Usługi Dell Professional Services, w tym zdalne odzyskiwanie danych i reagowanie na incydenty, zapewniają firmom szybkie odzyskiwanie danych i systemów. Eksperci firmy Dell kierują procesem, aby zminimalizować przestoje i ograniczyć skutki.

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

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

Wzmacnia 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

Skuteczna ochrona przed zagrożeniami wewnętrznymi wymaga więcej niż jednej warstwy ochrony. Wdrożenie wielowarstwowej strategii bezpieczeństwa gwarantuje, że żadna luka w zabezpieczeniach nie stanie się słabym punktem. Najważniejsze kroki:

Najważniejsze kroki w celu wzmocnienia obrony

- **Zasady modelu „zero trust”:** ciągła weryfikacja wszystkich żądań dostępu i założenie, że żaden podmiot nie jest z zasady godny zaufania, nawet jeśli działa w obrębie obszaru chronionego.
- **Kontrola dostępu oparta na rolach (RBAC):** ograniczenie dostępu pracowników tylko do systemów i danych niezbędnych do pełnienia ich ról.
- **Zaawansowane rozwiązania w zakresie szyfrowania:** szyfrowanie danych w stanie spoczynku i podczas transmisji, skutecznie neutralizujące kradzież danych.
- **Świadomość pracowników i szkolenia:** wprowadzenie częstych programów podnoszących świadomość w zakresie bezpieczeństwa, aby zapobiegać przypadkowemu udziałowi w złośliwych działaniach.
- **Regularne testowanie systemu:** przeprowadzanie testów penetracyjnych i skanowania luk w zabezpieczeniach w celu zapewnienia niezawodności zabezpieczeń.

Praktyki te, wspomagane przez rozwiązania firmy Dell, tworzą potężne, kompleksowe ramy ochrony przed złośliwymi informatorami.

Wzmacnianie obrony poprzez partnerstwa strategiczne

Dell współpracuje z czołowymi w branży dostawcami cyberbezpieczeństwa, w tym z firmami **CrowdStrike** i **Secureworks**, aby jeszcze bardziej wzmacniać swoje rozwiązania. CrowdStrike zwiększa bezpieczeństwo punktów końcowych i zapewnia cenne informacje o zagrożeniach na podstawie wskaźników naruszenia bezpieczeństwa, a Secureworks oferuje zaawansowane usługi wykrywania zagrożeń i reagowania na nie. Współpraca ta zapewnia klientom firmy Dell korzyści z ekosystemu zintegrowanych i najnowocześniejszych technologii.

Dlaczego warto wybrać rozwiązania Dell Technologies w zakresie cyberbezpieczeństwa

Firma Dell Technologies nadal wyznacza złoty standard w zakresie wielowarstwowych rozwiązań w zakresie cyberbezpieczeństwa. Firmy korzystają z wiodącej w branży wiedzy specjalistycznej firmy Dell, ścisłej współpracy partnerskiej oraz innowacyjnego zestawu produktów, które dostosowują się do obecnie ewoluujących zagrożeń. Od zabezpieczeń punktów końcowych, przez wykrywanie ataków wewnętrznych, po usuwanie skutków incydentów — firma Dell zapewnia kompletną strukturę odporności, która jest godna zaufania i umożliwia rozwój.

Zbuduj odporną przyszłość dzięki Dell Technologies

Chroń swoją firmę przed złośliwymi zagrożeniami wewnętrznymi dzięki kompleksowym, skalowalnym rozwiązaniom firmy Dell Technologies. Współpracując z firmą Dell, nie tylko zabezpieczasz swoje operacje, ale także zapewniasz ciągłość prowadzenia działalności, wspierasz zaufanie klientów i chronisz swoją organizację na przyszłość. Skontaktuj się z nami, aby dowiedzieć się więcej na temat wdrażania proaktywnej ochrony już dziś.

Dell Technologies jest zaufanym sojusznikiem w walce z zagrożeniami wewnętrznymi, ochronie najważniejszych zasobów i umożliwieniu firmie rozwoju w dynamicznym środowisku cyfrowym. Przyszłość bezpieczeństwa to przyszłość sukcesu, a wszystko zaczyna się od firmy Dell.

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

Więcej informacji na temat rozwiązań Dell

Skontaktuj się z ekspertem firmy Dell Technologies

Zobacz więcej zasobów

Dołącz do rozmowy, stosując #hasztag

DELL Technologies