DELL Technologies

Ataki typu Man-in-the-Middle (MITM): wzmacnianie cyberbezpieczeństwa i odporności z firmą Dell Technologies

Rosnące zagrożenie atakami typu Man-in-the-Middle (MITM)

Ataki typu Man-in-the-Middle (MITM) pozostają jednym z najbardziej zaawansowanych i niebezpiecznych wyzwań związanych z cyberbezpieczeństwem. Ataki te, w których hakerzy przechwytują i modyfikują prywatną komunikację bez wykrycia, są wymierzone w przedsiębiorstwa każdej wielkości we wszystkich branżach. Od platform e-commerce po instytucje finansowe, żadna organizacja nie jest odporna na to ryzyko. Ataki MITM często otwierają drogę do kradzieży danych, oszustw finansowych i szkód reputacji, co czyni je poważnym zagrożeniem w coraz bardziej cyfrowym świecie.

Dell Technologies rozumie wyjątkowe wyzwania, przed którymi stają firmy, chroniąc się przed tymi zaawansowanymi zagrożeniami. Dzięki innowacyjnym, skalowalnym rozwiązaniom w zakresie zabezpieczeń firma Dell umożliwia organizacjom neutralizowanie zagrożeń MITM, ochronę zasobów i utrzymanie integralności biznesowej.

Co to jest atak typu Man-in-the-Middle Attack (MITM)?

Atak typu Man-in-the-Middle (MITM) ma miejsce, gdy cyberprzestępca potajemnie przechwytuje komunikację między dwiema stronami, np. między pracownikiem a serwerem korporacyjnym lub klientem a witryną firmową. Cel atakującego może się różnić — od kradzieży wrażliwych danych po manipulowanie komunikacją w złośliwych celach — ale wynik jest taki sam: naruszenie zaufania i bezpieczeństwa.

Typowe techniki MITM

Niektóre z najbardziej rozpowszechnionych metod, których używają atakujący, obejmują następujące elementy:

Podsłuchiwanie sieci Wi-Fi: cyberprzestępcy wykorzystują niezabezpieczone lub naruszone publiczne sieci Wi-Fi do przechwytywania komunikacji.

Zatruwanie DNS: atakujący przekierowują użytkowników na fałszywe strony internetowe poprzez manipulowanie rekordami DNS, gromadząc w ten sposób poufne informacje bez wiedzy użytkowników.

Przechwytywanie sesji: przechwytując aktywne poświadczenia sesji, atakujący uzyskują nieautoryzowany dostęp do kont prywatnych.

Rozdzielanie SSL: ta technika powoduje obniżenie poziomu bezpiecznych połączeń HTTPS do zagrożonych połączeń HTTP, ujawniając poufne informacje.

Taka elastyczność sprawia, że ataki MITM są szczególnie niebezpieczne, ponieważ wykorzystują codzienne transakcje biznesowe i interakcje, które na pierwszy rzut oka wydają się uzasadnione.

Wpływ na firmy

Skutki ataku MITM wykraczają daleko poza bezpośredni incydent. Niektóre z najbardziej szkodliwych skutków obejmują:

Utracone przychody

Kradzież danych uwierzytelniających i naruszenia operacji często prowadzą do obciążeń finansowych, które obejmują bezpośrednie straty i koszty odzyskiwania.

Niepowodzenia operacyjne

Czas i zasoby wykorzystane na rozwiązanie ataku zmniejszają krytyczne funkcje biznesowe, wpływając na produktywność i rozwój.

Erozja zaufania

Zaufanie klientów może szybko ulec pogorszeniu w przypadku naruszenia ich danych osobowych, co prowadzi do długoterminowego uszkodzenia reputacji.

Konsekwencje prawne

Firmy działające w branżach, w których obowiązują ścisłe wymagania dotyczące zgodności z przepisami, mogą zostać ukarane grzywnami lub sankcjami po naruszeniu danych.

Autentyczny przykład

Jednym z niepokojących przypadków była sytuacja globalnej firmy detalicznej, której niezaszyfrowana platforma płatności internetowych padła ofiarą ataku typu rozdzielanie SSL. Osoba atakująca przechwytywała informacje o kartach kredytowych klientów podczas realizacji transakcji. Dzięki szybkiemu wykrywaniu i strategicznym środkom bezpieczeństwa, w tym narzędziom ochrony punktów końcowych firmy Dell, firma była w stanie powstrzymać atak i ograniczyć długoterminowe szkody. W tym scenariuszu przedstawiono bezpośrednie zagrożenia i krytyczną potrzebę warstwowej ochrony.

35,9 mld

znanych przypadków naruszenia bezpieczeństwa danych na całym świecie

Źródło: Maj 2024 r. raport PureWL

Przeciwdziałanie atakom MITM z pomocą firmy Dell Technologies

Dell Technologies wyposaża organizacje w kompleksowe, przyszłościowe narzędzia zaprojektowane z myślą o ograniczeniu ryzyka związanego z atakami MITM, zanim spowodują one szkody.

Zabezpiecz punkty końcowe za pomocą rozwiązania Dell Trusted Devices

Punkty końcowe są często źródłem zagrożeń MITM, co czyni je priorytetem ochronnym. Dell oferuje zaufane urządzenia, w których najnowocześniejsze zabezpieczenia są wbudowane bezpośrednio w sprzęt. Na przykład:

- **System Dell SafeBIOS** zapewnia ochronę integralności systemu przed nieautoryzowanymi manipulacjami w sekwencji rozruchu.
- **SafeID** dodaje kolejną warstwę ochrony, zabezpieczając dane uwierzytelniające użytkownika, tworząc twierdzę przed kradzieżą poświadczeń.
- **Dell SafeData** zapewnia kompleksowe szyfrowanie, które chroni poufne informacje wewnątrz i na zewnątrz firmowych zapór sieciowych, co sprawia, że przechwycone dane są nieczytelne.

Funkcje te zostały wdrożone w globalnych przedsiębiorstwach w celu zapewnienia bezpieczeństwa systemów punktów końcowych. Na przykład międzynarodowa firma produkcyjna wykorzystała rozwiązanie Dell Trusted Devices do ochrony pracowników zdalnych przed wymierzonymi w firmowe notebooki atakami MITM, zapewniając bezpieczne połączenie nawet podczas podróży o wysokim ryzyku.

Zaawansowane wykrywanie za pomocą narzędzia CrowdStrike

Wykrywanie zagrożeń MITM i reagowanie na nie w czasie rzeczywistym ma kluczowe znaczenie. Oprogramowanie CrowdStrike, zintegrowane z ekosystemem firmy Dell, wykorzystuje sztuczną inteligencję i analizę behawioralną do monitorowania i neutralizowania podejrzanej aktywności. Ciągłe monitorowanie zapewnia ochronę w środowiskach hybrydowych, w których zagrożenia często się ukrywają. Proaktywnie identyfikując anomalie, firmy mogą wyeliminować potencjalne próby ataków MITM przed wystąpieniem uszkodzeń.

Na przykład, korzystając z zaawansowanego wykrywania, instytucja finansowa pomyślnie wykryła i ograniczyła włamanie do swojego portalu dla klientów. Sztuczna inteligencja platformy zidentyfikowała nietypową aktywność sieci wskazującą na rozdzielanie SSL, umożliwiając natychmiastowe działania naprawcze.

Wzmocniona ochrona danych dzięki rozwiązaniu Dell PowerProtect

Nawet organizacje z zaawansowanymi zabezpieczeniami mogą doświadczać naruszeń. W tym momencie wkracza rozwiązanie Dell PowerProtect. Dzięki takim funkcjom, jak niezmienność danych i odizolowana pamięć masowa, chroni krytyczne dane biznesowe przed zmianami, zniszczeniem lub nieautoryzowanym dostępem podczas ataku. PowerProtect Cyber Recovery Vault zapewnia dodatkowe bezpieczeństwo, izolując poufne dane z sieci podstawowych, zapewniając, że nawet w najgorszym przypadku wrażliwe informacje pozostają nienaruszone i można je odzyskać.

Technologia ta miała kluczowe znaczenie dla organizacji opieki zdrowotnej, która stanęła w obliczu ataku z zatruwaniem DNS. Dzięki wykorzystaniu niezmiennych kopii zapasowych i sejfu do odzyskiwania danych PowerProtect organizacja szybko przywróciła operacje bez utraty danych.

Usługi szybkiego reagowania na incydenty i odzyskiwania danych

Usługi Dell w zakresie ochrony danych uzupełniają swoje technologie, oferując szybkie, prowadzone przez ekspertów odzyskiwanie danych w przypadku naruszenia bezpieczeństwa. Rozwiązania te ograniczają przestoje i minimalizują zakłócenia operacyjne — od zdalnego odzyskiwania danych po reagowanie na incydenty. Gdy liczy się każda sekunda, posiadanie zaufanego partnera zapewnia organizacjom możliwość odzyskania sprawności bez obaw.

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.

Wzmacnianie bezpieczeństwa dzięki wielowarstwowemu podejściu

Aby w pełni zwalczać ataki MITM, organizacje muszą wdrożyć wieloaspektową strategię bezpieczeństwa. Dell Technologies podkreśla następujące działania:

- **Zastosowanie zasad modelu „zero trust”:** weryfikuj wszystkie działania i dostęp użytkowników w każdym punkcie, niezależnie od tego, czy pochodzą z sieci korporacyjnej, czy spoza niej.
- **Użycie zaawansowanego szyfrowania:** szyfrowanie od końca do końca dla całej komunikacji sprawia, że przechwycone dane stają się niezdatne do użytku dla atakujących.
- **Wdrożenie uwierzytelniania wieloskładnikowego (MFA):** MFA dodaje warstwy uwierzytelniania do systemów, znacznie zmniejszając luki w zabezpieczeniach nieautoryzowanego dostępu.
- **Edukacja pracowników:** zwiększ czujność pracowników, podkreślając zagrożenia, takie jak schematy phishingu, podejrzane korzystanie z sieci Wi-Fi i niezweryfikowane łącza.
- **Regularne testowanie systemu:** częste testy penetracyjne i aktualizacje pomagają zidentyfikować luki w zabezpieczeniach i zapewnić aktualność zabezpieczeń.

Kompleksowa oferta zabezpieczeń firmy Dell w połączeniu z tymi praktykami tworzy potężną, elastyczną ochronę przed zmieniającymi się zagrożeniami.

Wartość partnerstwa strategicznego

Współpraca Dell Technologies z czołowymi firmami zajmującymi się cyberbezpieczeństwem, takimi jak CrowdStrike i Secureworks, jeszcze bardziej wzmacnia jej ofertę. Integracja wiedzy eksperckiej w ramach tych partnerstw pozwala firmie Dell zająć się każdym możliwym wektorem ataku. Na przykład CrowdStrike zwiększa ochronę punktów końcowych, wzbogacając platformy firmy Dell o analizę zagrożeń, a Secureworks zapewnia przydatne informacje na temat zmieniających się zagrożeń, zapewniając ciągłe przygotowanie i adaptację.

Przewaga Dell Technologies

Wybór firmy Dell Technologies oznacza współpracę z zaufanym liderem w dziedzinie innowacji w zakresie cyberbezpieczeństwa. Kompleksowe rozwiązania firmy Dell pozwalają organizacjom wyprzedzić osoby atakujące, niezależnie od tego, czy chodzi o ochronę punktów końcowych, odzyskiwanie danych czy współpracę partnerską.

Zabezpiecz swoją firmę, utrzymuj zaufanie klientów i przygotuj swoją działalność na przyszłość dzięki kompleksowym rozwiązaniom MITM firmy Dell. Skontaktuj się z nami już dziś, aby rozpocząć tworzenie odpornej, bezpiecznej przyszłości dla swojej firmy.

Współpracując z firmą Dell Technologies, podejmujesz aktywne stanowisko wobec cyberzagrożeń, budując trwałe zaufanie wśród klientów i interesariuszy oraz zapewniając sukces operacyjny w coraz bardziej niezabezpieczonym cyfrowym świecie. Bezpieczniejsze jutro 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