DELL Technologies

Ochrona przed cyberatakami w łańcuchu dostaw dzięki firmie Dell Technologies

Streszczenie dla zarządu

Coraz bardziej globalny charakter operacji biznesowych i ich wzajemne powiązania narażają organizacje na rosnące zagrożenia związane z cyberatakami w łańcuchu dostaw. Te zaawansowane ataki wykorzystują luki w zabezpieczeniach cyklu życia sprzętu, od produkcji po wdrożenie, a także oprogramowanie innych firm, umożliwiając złośliwym podmiotom naruszenie bezpieczeństwa całych systemów poprzez zaufane aplikacje lub aktualizacje. Takie incydenty są nie tylko katastrofalne finansowo, ale mogą również pogorszyć reputację oraz zakłócić działalność na ogromną skalę.

Konsekwencje tych zagrożeń są bardzo poważne. Ataki w łańcuchu dostaw często pozostają niewykryte do momentu wystąpienia poważnych szkód, co sprawia, że niezbędne jest stosowanie proaktywnych strategii obrony. Dzięki zaawansowanej ochronie punktów końcowych, proaktywnemu monitorowaniu oraz kompleksowym rozwiązaniom w zakresie bezpieczeństwa serwerów i danych firma Dell umożliwia firmom zabezpieczenie całego łańcucha dostaw. Dzięki technologii, partnerom i wiedzy eksperckiej organizacje mogą budować odporność i chronić się przed lukami w zabezpieczeniach nieodłącznie związanymi z ich ekosystemami.

Rosnące zagrożenie cyberatakami w łańcuchu dostaw

W ostatnich latach liczba ataków w łańcuchach dostaw znacznie wzrosła. Manipulując urządzeniami fizycznymi podczas produkcji, wysyłki lub wdrażania lub znajdując słabe punkty u dostawców oprogramowania, atakujący uzyskują środki do wprowadzania złośliwych komponentów lub kodu, uszkodzenia systemów lub pozyskania wrażliwych danych. Ofiarami są zarówno małe firmy, jak i globalne przedsiębiorstwa, skutkiem czego doznają poważnych strat finansowych, obniżenia poziomu zaufania klientów i konsekwencji prawnych. Firma Dell Technologies dostrzega to rosnące zagrożenie i wspiera prace nad środkami zapobiegawczymi w celu złagodzenia katastrofalnych skutków takich ataków.

Zrozumienie cyberataków w łańcuchu dostaw

Jak działają ataki na łańcuch dostaw sprzętu

1. **Etap produkcji:** Atakujący wprowadzają złośliwe elementy podczas montażu sprzętu, często wykorzystując zainfekowanych poddostawców.
2. **Faza wysyłki:** Urządzenia są przechwytywane podczas transportu i modyfikowane w celu szkodliwego zmodyfikowania oprogramowania wewnętrznego lub sprzętu.
3. **Wdrożenie i aktywacja:** gdy zainfekowany sprzęt dostanie się do sieci organizacji, atakujący uzyskują dostęp do poufnych danych lub możliwość na działania typu backdoor.

Jak działają ataki na łańcuch dostaw oprogramowania

1. **Pierwsze naruszenie:** Dostawca oprogramowania innego producenta jest zagrożony, często poprzez phishing, niepoprawione luki w zabezpieczeniach lub zagrożenia wewnętrzne.
2. **Manipulacja kodem:** Cyberprzestępcy wdrażają szkodliwe komponenty, takie jak złośliwe oprogramowanie lub wirusy typu backdoor do oprogramowania przeznaczonego do dystrybucji.

3. **Rozpowszechnienie wśród użytkowników końcowych:** Firmy instalujące lub aktualizujące oprogramowanie nieumyślnie pobierają złośliwe składniki.

Typowe techniki — sprzęt

- **Manipulacja oprogramowaniem wewnętrznym:** Osadzanie złośliwego kodu aktywującego się po wdrożeniu.
- **Implantacja sprzętu:** Integracja ukrytych elementów w celu monitorowania lub pozyskania danych.
- **Wykorzystanie zaufanych dostawców:** Wykorzystanie dostawców zewnętrznych przy użyciu mniej bezpiecznych procesów.

Typowe techniki — oprogramowanie

- **Kradzież elementów:** Infekowanie bibliotek lub modeli innych producentów złośliwym kodem.
- **Wstrzyknięcie aktualizacji:** zmiana oficjalnych aktualizacji oprogramowania w celu wykorzystania luk w zabezpieczeniach.
- **Metoda „dependency confusion”:** wykorzystanie uzależnienia organizacji od niezabezpieczonych zależności pakietów.

Wpływ na firmy

Konsekwencje finansowe

Ataki ukierunkowane na łańcuchy dostaw często powodują koszty związane z karami finansowymi, wydatkami na odzyskiwanie systemów i rekompensaty dla klientów. Jeden głośny incydent z udziałem globalnej firmy zarządzającej IT spowodował straty przekraczające 70 milionów dolarów, co ilustruje ogromną skalę szkód finansowych, jakie mogą powodować takie naruszenia.

Zakłócenia operacyjne

Uszkodzone lub wyłączone systemy spowodowane przez infiltrację złośliwego oprogramowania często prowadzą do rozległych przestojów, obniżając produktywność organizacyjną i opóźniając realizację projektu.

Konsekwencje dla reputacji

Zaufanie do partnerów w zakresie oprogramowania ma dla nowoczesnych firm znaczenie kluczowe. Naruszenie łańcucha dostaw związanego z oprogramowaniem oferowanym przez organizację może osłabić reputację i obniżyć lojalność klientów.

Rzeczywiste przykłady — sprzęt/oprogramowanie

Globalny producent elektroniki wykrył uszkodzone komponenty w swoim łańcuchu dostaw, co doprowadziło do powszechnych awarii systemu. Koszty ataku przekroczyły **45 milionów dolarów** i obejmowały działania naprawcze, opłaty związane z obsługą prawną oraz nieodwracalne szkody w relacjach z dostawcami.

Naruszenie w firmie SolarWinds jest jednym z najbardziej znanych ataków w łańcuchu dostaw oprogramowania. Zainfekowanie produktów z serii Orion spowodowało zainfekowanie różnych organizacji na całym świecie, w tym agencji rządowych i firm z listy Fortune 500. Szacunki dotyczące szkód przekroczyły **90 milionów dolarów**, a naruszenie uwidoczniło daleko idące konsekwencje luk w zabezpieczeniach łańcucha dostaw.

Specjalistyczna wiedza firmy Dell Technologies w zakresie zwalczania ataków w łańcuchu dostaw

Szeroka oferta rozwiązań firmy Dell Technologies w zakresie zabezpieczeń pozwala firmom wyprzedzić zmieniające się zagrożenia cybernetyczne.

Dell Secured Component Verification (SCV)

Secure Component Verification (SCV) jest integralną częścią strategii bezpieczeństwa łańcucha dostaw firmy Dell Technologies zaprojektowaną w celu zapewnienia autentyczności i integralności elementów sprzętowych w różnych rozwiązaniach firmy Dell. SCV zapewnia kryptograficzną walidację elementów systemu od momentu produkcji aż po dostawę i wdrożenie. Firma Dell Technologies zapewnia solidne zabezpieczenia łańcucha dostaw, gwarantując, że systemy są odporne na manipulacje i bezpieczne od momentu opuszczenia fabryki aż po wdrożenie. Zwiększa to ogólne bezpieczeństwo, rzetelność i wydajność klientów firmy Dell.

Zabezpieczanie punktów końcowych za pomocą rozwiązania Dell Trusted Workspace

Dell Trusted Devices integruje zabezpieczenia na poziomie sprzętu i oprogramowania wewnętrznego w celu tworzenia systemów odpornych na manipulacje.

- **SafeBIOS** zapewnia integralność oprogramowania wewnętrznego podczas rozruchu, zapobiegając nieautoryzowanym zmianom konfiguracji oraz weryfikuje integralność oprogramowania wewnętrznego podczas rozruchu, zapobiegając uruchamianiu zainfekowanych systemów.
- **SafeID** zabezpiecza poświadczenia uwierzytelniania na poziomie sprzętowym, zapobiegając nieautoryzowanemu dostępowi oraz chroni poświadczenia logowania, zabezpieczając klucze uwierzytelniania, blokując nieautoryzowanych użytkowników.
- **SafeData** umożliwia kompleksowe szyfrowanie wrażliwych plików biznesowych, blokując próby pozyskania danych.

Proaktywne wykrywanie zagrożeń za pomocą CrowdStrike

CrowdStrike integruje się z technologiami firmy Dell, aby w czasie rzeczywistym uzyskiwać wgląd w zachowanie złośliwego oprogramowania.

- **Analiza w celu wykrywania zagrożeń opartych na zachowaniu:** Monitorowanie zachowania sprzętu i oprogramowania wewnętrznego pod kątem oznak manipulacji oraz wykrywanie nietypowej aktywności oprogramowania, aby zapobiec wdrożeniu złośliwego oprogramowania.
- **Narzędzia do natychmiastowej reakcji:** Sztuczna inteligencja izoluje zagrożone systemy, zapobiegając ruchowi bocznemu w sieci.
- **Eliminacja zagrożeń oparta na sztucznej inteligencji:** Aktywnie identyfikuje i izoluje zagrożenia, zapobiegając ich poprzecznemu rozprzestrzenianiu się w systemach korporacyjnych.
- **Możliwości integracji:** Środowiska hybrydowe i wielochmurowe są holistycznie chronione za pomocą narzędzi Dell i CrowdStrike.

Większe bezpieczeństwo dzięki rozwiązaniom serwerowym i pamięci masowej firmy Dell

Rodzina serwerów Dell PowerEdge obejmuje zaawansowaną ochronę w celu zabezpieczenia platform oprogramowania o znaczeniu krytycznym. Systemy pamięci masowej, takie jak Dell PowerStore, oferują najlepsze w branży szyfrowanie aplikacji i danych.

- **Bezpieczne oprogramowanie wewnętrzne serwerów:** Monitoruje i blokuje nieautoryzowane zmiany na poziomie sprzętu.
- **Monitorowanie sieci izolowanej:** Wykrywa anomalie wskazujące na ingerencję w łańcuch dostaw.
- Niezmienne kopie zapasowe: Zabezpieczają punkty odtwarzania nawet w przypadku naruszenia głównej pamięci masowej.
- **Sejfy odzyskiwania:** Izolowane środowiska chronią przed awariami kaskadowymi inicjowanymi przez zainfekowane systemy.

Wielowarstwowe podejścia do ograniczania ryzyka

Firma Dell zachęca firmy do przyjęcia kompleksowych strategii łączących technologię, praktyki personelu i aktualizację procesów.

Działania strategiczne

- **Poprawa widoczności łańcucha dostaw:** Wymaga od wszystkich dostawców przestrzegania rygorystycznych standardów bezpieczeństwa i certyfikacji sprzętu na każdym etapie.
- **Wdrożenie zaawansowanego szyfrowania:** Zabezpiecza dane na każdym poziomie przy użyciu zaawansowanych protokołów, co ogranicza dostępność nawet w przypadku naruszenia zabezpieczeń sprzętu.
- **Wprowadzenie zasad modelu „zero trust”:** Żadne urządzenie, aplikacja ani użytkownik nie zyskują zaufania automatycznie i bez weryfikacji.
- **Standardy bezpiecznego kodowania:** Współpraca z partnerami w zakresie oprogramowania, egzekwowanie rygorystycznych wytycznych dotyczących wtyczek, interfejsów API i integracji.
- **Regularne monitorowanie aktywności i audyty:** częste audyty zapewniają integralność usług oferowanych przez inne firmy.
- **Przeprowadzanie regularnych testów:** Wdrażanie testów penetracyjnych i ocen oprogramowania wewnętrznego w celu ciągłej weryfikacji integralności urządzenia.
- **Kształcenie pracowników:** Szkolenie zespołów, aby rozpoznawały elementy lub pakiety, które wykazują podejrzane zachowania.

W jaki sposób usługi Dell Professional Services zapewniają firmom odporność

Usługi Dell Professional Services kierują firmami w zakresie wdrażania solidnych zabezpieczeń łańcucha dostaw. Zespoły doświadczonych ekspertów ds. cyberbezpieczeństwa zapewniają analizy, szkolenia i strategie reagowania na zagrożenia dostosowane do unikalnych potrzeb danej organizacji.

- **Wytyczne dotyczące wdrażania:** strategiczne dostosowanie praktyk opartych na modelu „zero trust” i weryfikacja dostawców spośród różnych środowisk.
- **Reagowanie na incydenty:** Zapewnij firmom szybkie odzyskiwanie danych po złośliwych atakach.

Przyszłościowe systemy dla przedsiębiorstw firmy Dell

Cyberataki w łańcuchu dostaw są przykładem wyrafinowania nowoczesnych zagrożeń. Firmy potrzebują ochrony, która nie tylko zapobiega naruszeniom, ale także zapewnia szybkie odzyskiwanie danych w przypadku wystąpienia incydentów. Współpraca z firmą Dell Technologies oznacza dostęp do najnowocześniejszych narzędzi, strategicznej specjalistycznej wiedzy i sieci zaufanych współpracowników.

Dalsze działania

Chroń wrażliwe zasoby i zwiększ niezawodność operacyjną, wdrażając najlepsze praktyki opracowane przez Dell Technologies. Skontaktuj się już dziś, aby uzyskać spersonalizowaną konsultację w ramach przygotowań do zabezpieczenia najważniejszych systemów przedsiębiorstwa.

Firma Dell Technologies reprezentuje zaufanie, zdolność adaptacji i innowacyjność w miarę rozwoju cyberbezpieczeństwa łańcucha dostaw. Dzisiejsze zaangażowanie zabezpiecza jutrzejszy sukces.

Bezpieczniejsza przyszłość zaczyna się od firmy Dell Technologies. Chronimy to, co najważniejsze.

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