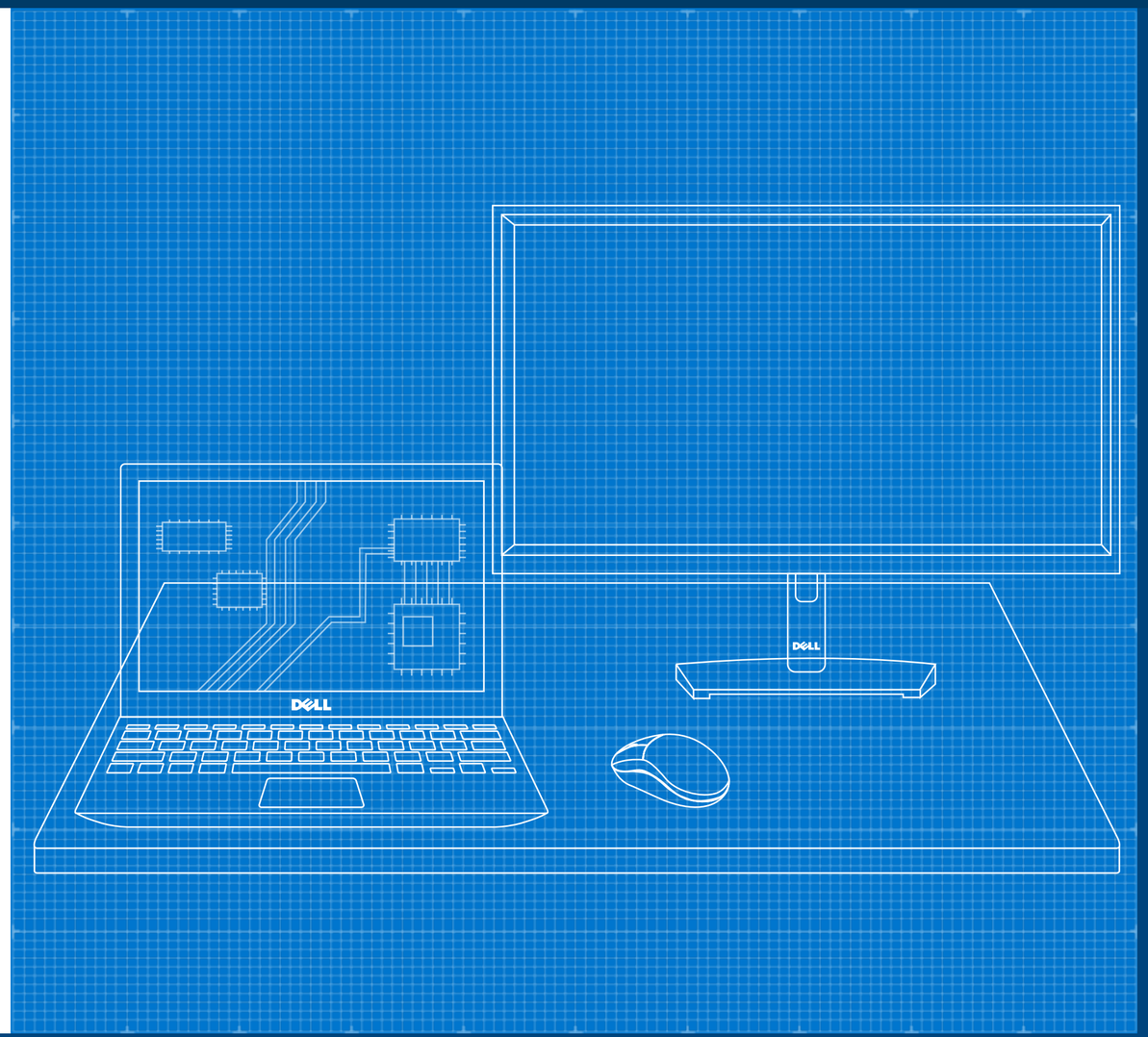
DELL Technologies

Zaufana przestrzeń robocza

Zwiększ bezpieczeństwo swojej floty urządzeń dzięki wielu warstwom zabezpieczeń



Streszczenie dla kierownictwa

Cyberataki są nieuniknione, a ich natężenie i stopień zaawansowania stale rosną. Urządzenia końcowe, sieci i środowiska chmurowe stały się głównymi celami.

Niniejszy e-book zawiera wytyczne dla osób podejmujących decyzje w zakresie IT i bezpieczeństwa dotyczące elementów niezbędnych do najskuteczniejszej ochrony punktów końcowych w obliczu zmieniającego się krajobrazu zagrożeń.

Spis treści

Krajobraz zagrożeń

Wprowadzenie modelu pracy hybrydowej spowodowało zwiększenie złożoności systemów i pojawienie się nowych celów ataków.**Punkty końcowe, sieci i chmury stanowią coraz częstsze cele dla cyberprzestępców.**

Co więcej, atakujący stosują coraz bardziej zaawansowane techniki, które za cel obierają różne warstwy stosu obliczeniowego, ukrywając się w prawidłowych procesach systemowych. Niektóre metody pozwalają nawet uzyskać uprzywilejowany dostęp i wyłączyć mechanizmy zabezpieczające oprogramowania*, unikając przy tym wykrycia*.

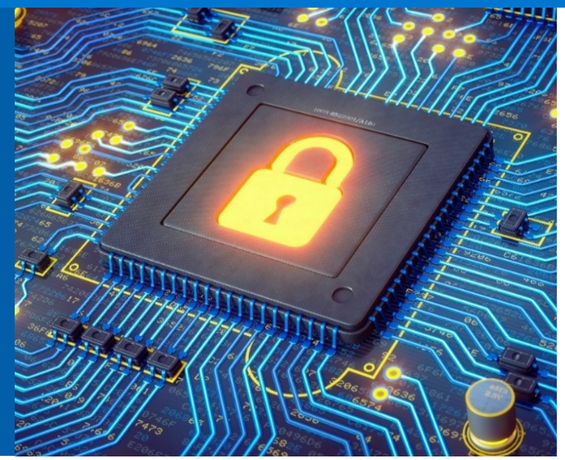
Aby przeciwdziałać tego typu zagrożeniom, wiele organizacji rozpoczęło wdrażanie modelu „zero trust”. Warunkiem powodzenia tej operacji jest utrzymanie zaufania do urządzeń.

Jak jednak to zrobić, gdy częstotliwość ataków się nasila, a zaawansowana technologia stwarza im nowe cele?

[1]CrowdStrike Global Threat Report, 2024.
[2]Dell Innovation Index, 2023.

Czy wiesz, że...

75% ataków przeprowadzonych w 2023 r. nie było spowodowanych złośliwym oprogramowaniem[1]



Zaledwie 41% badanych organizacji może z pełnym przekonaniem stwierdzić, że ich technologie i aplikacje są bezpieczne[2]

Chcesz zgłębić model „zero trust”, aby zwiększyć swoją świadomość w zakresie cyberbezpieczeństwa? Zapoznaj się z naszym e-bookiem: *Bezpieczeństwo punktów końcowych to istotny element realizacji strategii „zero trust”*.

Wyzwania

Skuteczne zabezpieczenie punktów końcowych wymaga zrozumienia przeciwnika i poznania sposobu jego działania.

Mając na uwadze potencjalne korzyści płynące z udanego ataku, **cyberprzestępcy często podejmują wiele prób włamania do tej samej organizacji, wykorzystując przy tym różne metody i punkty wejścia, co zwiększa ich szanse.** Na przykład w całym cyklu eksploatacji jednego urządzenia atakujący mogą próbować wykorzystać luki w zabezpieczeniach, stosując różne kierunki ataku.

Starsze mechanizmy zabezpieczające nie wystarczają do skutecznej ochrony punktów końcowych. Gdy organizacje wzmacniają jeden obszar narażony na atak, cyberprzestępcy po prostu wybierają łatwiejsze cele. W miarę ewolucji modelu hybrydowego atakujący opracowali nowe kierunki ataków na punkty końcowe, co doprowadziło do katastrofalnych skutków.

Zobacz przykłady ataków

Atak na łańcuch dostaw: Celem są dostawcy i uzyskanie dostępu do ich systemów, danych i/lub sieci, a co za tym idzie, do ich klientów. **PRZYKŁAD: atak na łańcuch dostaw sprzętu komputerowego, którego źródłem jest ingerencja w podzespoły:**

Atakujący przechwytują przesyłkę z komputerem i dokonują podmiany dysków twardych.

Dział IT wprowadza zainfekowane urządzenia do użytku w firmie.

Atakujący instaluje złośliwe oprogramowanie, aby uzyskać dane uwierzytelniające podczas logowania użytkowników.

Atak socjotechniczny: użytkownicy końcowi są nakłaniani do przekazania poufnych informacji, które można wykorzystać do uzyskania dostępu do urządzenia i sieci. **PRZYKŁAD: atak spoofingowy zainicjowany przez wiadomość e-mail typu phishing:**

Użytkownik końcowy nie jest świadomy zagrożenia i podaje dane uwierzytelniające na sfałszowanej stronie internetowej.

Atakujący używa prawidłowych danych uwierzytelniających, aby uzyskać zdalny dostęp do sieci.

Atakujący wykrada informacje za pośrednictwem usługi sieciowej, szyfruje skradzione dane i żąda okupu za ich odzyskanie.

Spis treści

Zabezpieczenie nowoczesnej przestrzeni roboczej

Do zapewnienia właściwej ochrony punktów końcowych niezbędne jest wdrożenie mechanizmów prewencji, wykrywania i reagowania oraz przywracania działania i środków zaradczych na różnych etapach w całym cyklu eksploatacji urządzenia — od pozyskiwania i produkcji komputerów, poprzez wysyłkę, wprowadzenie do użytku i użytkowanie, po wycofanie z eksploatacji. Wyobraźmy sobie rozmiar takiego obszaru ataku!

Optymalna strategia cyberbezpieczeństwa uwzględnia najgorszy scenariusz. Zakłada, że atak może się wydarzyć i przewiduje wiele warstw zabezpieczeń, aby powstrzymywać zagrożenia jak najszybciej i jak najczęściej. Uwzględnia również środki zaradcze, aby minimalizować ryzyko ponownego wystąpienia ataku.

[3]Dell Innovation Index, 2023.

PREWENCJA

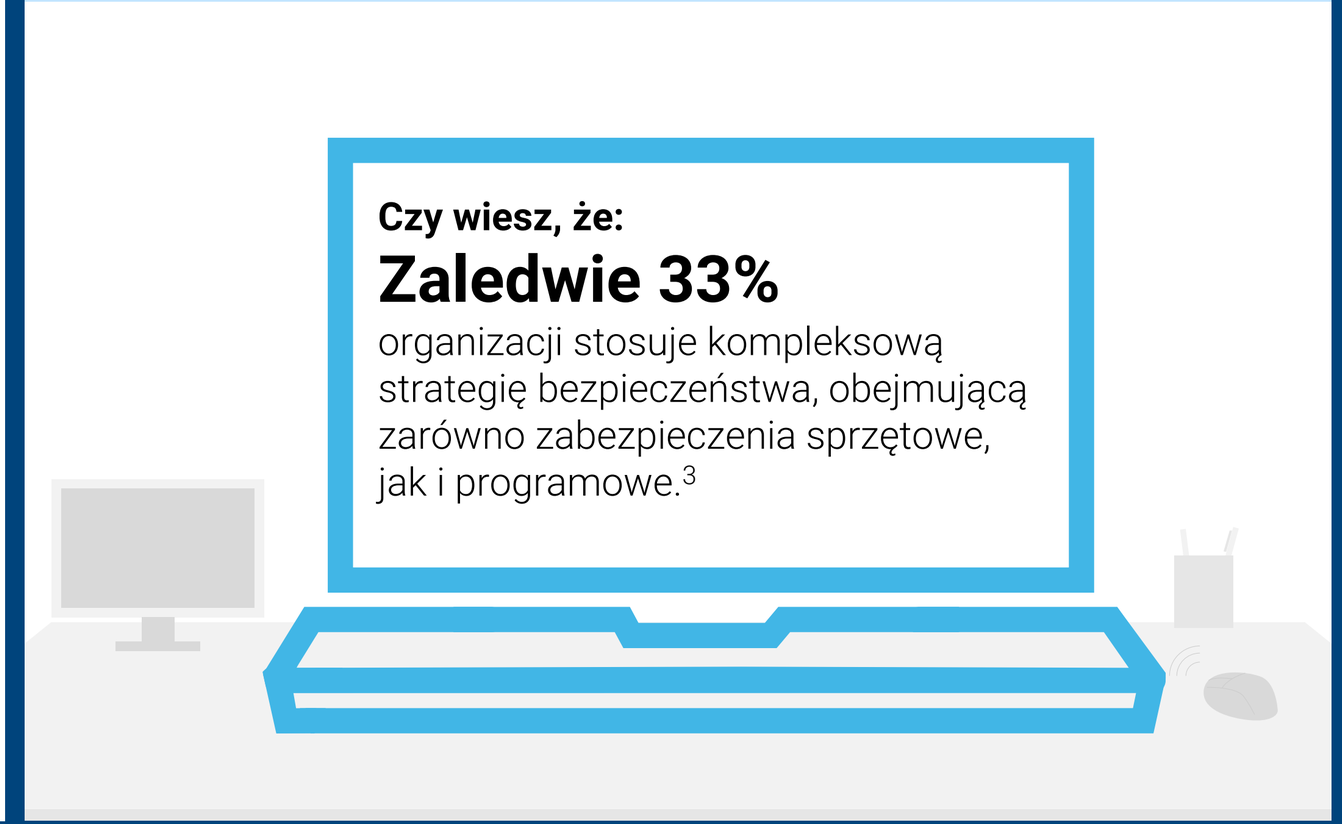
Nie bądź łatwym celem! Zastosuj rozwiązania blokujące ataki.

WYKRYWANIE I REAGOWANIE

Nie lekceważ zagrożenia i zachowaj czujność.

PRZYWRACANIE DZIAŁANIA I ŚRODKI ZARADCZE

Ogranicz skutki ataku i przywróć funkcjonowanie firmy.



Zaufana przestrzeń robocza

Nowoczesne zabezpieczenie punktów końcowych opiera się na trzech elementach:

1. **Zabezpieczenie programowe:** Obecnie użytkownicy, urządzenia i dane częściej niż kiedykolwiek znajdują się z dala od sieci firmowych. Zabezpieczenie programowe chroni nie tylko urządzenia, ale także środowiska sieciowe i chmurowe, z których często pochodzi złośliwa aktywność.

2. **Zabezpieczenie sprzętowe:** Urządzenia powinny mieć wbudowane funkcje zabezpieczające. Dotyczy to zabezpieczeń sprzętowych i oprogramowania wewnętrznego, które chronią urządzenia w trakcie użytkowania. Aby chronić przestrzeń roboczą, należy zapewnić wbudowaną funkcjonalność, która umożliwi wgląd i kontrolę nad urządzeniem.

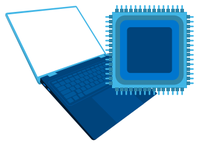
3. **Zabezpieczenie łańcucha dostaw:** Urządzenia muszą być wytwarzane w bezpieczny sposób. To oznacza współpracę z dostawcami, którzy: a) rozumieją krajobraz zagrożeń i b) potrafią wykorzystać tę wiedzę w miarę rozwoju sytuacji. Bezpieczne projektowanie, opracowywanie i testowanie komputerów minimalizuje ryzyko związane z lukami w zabezpieczeniach produktów, a mechanizmy kontroli łańcucha dostaw ograniczają ryzyko ingerencji w produkty.

Poznaj wielowarstwowe mechanizmy zabezpieczające

(Poniżej przedstawiono przykładowe środki bezpieczeństwa)

Zabezpieczenie programowe

- Oprogramowanie antywirusowe nowej generacji (NGAV)
- Endpoint Detection and Response (EDR)
- Rozszerzone wykrywanie zagrożeń i reagowanie na nie (XDR)
- Ochrona danych w chmurze
- Ochrona sieci
- Automatyczna naprawa



Zabezpieczenia sprzętowe i wewnętrzne

- Weryfikacja podczas uruchamiania
- Weryfikacja czasu wykonania
- Uwierzytelnianie użytkowników
- Powiadomienia i alerty bezpieczeństwa / telemetria

Zabezpieczenie łańcucha dostaw

- Bezpieczne praktyki rozwoju
- Bezpieczne praktyki łańcucha dostaw
- Weryfikacja podzespołów
- Opakowanie zabezpieczające przed manipulacją

Nasze podejście: Dell Trusted Workspace

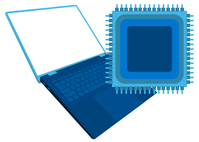
Dell to zaufany partner w zakresie zabezpieczeń i IT dla organizacji na całym świecie. W odróżnieniu od rozwiązań punktowych Dell skupia się na efektach ogólnych w zakresie bezpieczeństwa, tworząc pakiet rozwiązań, które przerywają łańcuchy ataków i zwiększają odporność systemów na zagrożenia. **Dell Trusted Workspace obejmuje:**

- Unikalne **zabezpieczenie sprzętowe i oprogramowania wewnętrznego**, które sprawia, że Dell jest najbezpieczniejszym komputerem komercyjnym na świecie.[4]. *(Zabezpieczenie wbudowane i osadzone)*
- Ekosystem **najlepszych w branży partnerów w zakresie oprogramowania** zapewnia zaawansowaną ochronę przed zagrożeniami dla urządzeń, sieci i chmury. *(Zabezpieczenie wbudowane)*

[4]Na podstawie wyników wewnętrznej analizy przeprowadzonej przez Dell, październik 2024. Stwierdzenie dotyczy komputerów z procesorami Intel. Nie wszystkie funkcje są dostępne na wszystkich komputerach osobistych. W przypadku niektórych funkcji wymagany jest dodatkowy zakup. Zatwierdzenie przez Principled Technologies. A comparison of security features, kwiecień 2024 r.

Wbudowane zabezpieczenie programowe z ekosystemu partnerskiego

- **Dell SafeGuard and Response: CrowdStrike** i **Secureworks** zapewniają wykrywanie zagrożeń, reagowanie na nie i podejmowanie środków zaradczych.
- **Dell SafeData: Netskope** zapewnia widoczność, monitorowanie i zapobieganie utracie danych w przypadku aplikacji opartych na chmurze. **Absolute** umożliwia autonaprawę aplikacji i sieci.



Wbudowane zabezpieczenie sprzętowe i oprogramowania wewnętrznego w najbezpieczniejszych na świecie komputerach komercyjnych[4]

Przykładowe funkcje chroniące urządzenie podczas użytkowania:

- **Dell SafeBIOS** — weryfikacja systemu BIOS poza hostem*, wskaźniki ataku* i CVE Detection* pomagają wychwytywać złośliwą aktywność, zanim zagrozi ona komputerowi.
- **Dell SafeID:** ochrona danych uwierzytelniających użytkownika w specjalnym chipie zabezpieczającym
- **Weryfikacja oprogramowania wewnętrznego poza hostem** chroni integralność oprogramowania wewnętrznego o wysokich uprawnieniach*.
- **Aplikacja Dell Trusted Device umożliwia integrację telemetrii urządzeń z czołowym w branży oprogramowaniem w celu poprawy bezpieczeństwa całej floty*.**

Osadzone zabezpieczenie łańcucha dostaw zapewnia ochronę komputerów od pierwszego uruchomienia

- **Dodatki Dell SafeSupply Chain** , takie jak Dell Secured Component Verification* (SCV), zapewniają dodatkową gwarancję integralności produktu.

** Unikalne rozwiązanie Dell*

Kompleksowe rozwiązanie z Dell

Dysponując zarówno sprzętowymi, jak i programowymi środkami zaradczymi, zmniejszysz obszar ataku dzięki zabezpieczeniom, które pomagają zapobiegać typowym zagrożeniom.

Mechanizmy wykrywania i reagowania radzą sobie z atakami ukrytymi, które mogą ominąć zabezpieczenia.

W przypadku ataku na łańcuch dostaw, o którym mowa na stronie 4, dzięki współpracy z Dell, środki zaradcze takie jak **bezpieczne praktyki łańcucha dostaw**, mogą powstrzymać atak na wczesnym etapie. Jeśli atak ominie zabezpieczenia, istnieją dodatkowe środki zaradcze, takie jak **SCV**.

W przypadku ataku socjotechnicznego, nawet jeśli atakującemu uda się nakłonić użytkownika do przekazania prawidłowych danych uwierzytelniających, **sprzętowa weryfikacja użytkownika, taka jak SafeID**, może powstrzymać atakującego i uniemożliwić mu dalszy dostęp. Oprogramowanie zabezpieczające, takie jak **Bezpieczna brama internetowa nowej generacji,** może zapewnić kolejną warstwę ochrony monitorującej.

Przeciwdziałanie atakom na łańcuch dostaw sprzętu, którego źródłem jest ingerencja w podzespoły.

Atakujący przechwytują przesyłkę z komputerem i dokonują podmiany dysków twardych.

- **Bezpieczne praktyki łańcucha dostaw**
- Opakowanie zabezpieczające przed manipulacją
- Zamki w drzwiach

Dział IT wprowadza zainfekowane urządzenia do użytku w firmie.

- Secured Component Verification (SCV)
- Weryfikacja czasu wykonania

Atakujący instaluje złośliwe oprogramowanie, aby uzyskać dane uwierzytelniające podczas logowania użytkowników.

- Cloud Access Security Broker
- Bezpieczna brama internetowa nowej generacji

Przeciwdziałanie atakowi socjotechnicznemu, którego źródłem jest wiadomość e-mail typu phishing.

Użytkownik końcowy nie jest świadomy zagrożenia i podaje dane uwierzytelniające na sfałszowanej stronie internetowej.

- NGAV
- EDR
- XDR

Atakujący używa prawidłowych danych uwierzytelniających, aby uzyskać zdalny dostęp do sieci.

- Uwierzytelnianie wieloskładnikowe z funkcją SafeID
- Dostęp do sieci w modelu „zero trust”

Atakujący wykrada informacje za pośrednictwem usługi sieciowej, szyfruje skradzione dane i żąda okupu za ich odzyskanie.

- Bezpieczna brama sieciowa nowej generacji + analiza zachowań użytkownika

Najważniejsze wnioski

Naruszenia bezpieczeństwa są nieuniknione. Skuteczna ochrona punktów końcowych zawsze uwzględnia najgorszy scenariusz i koncentruje się na przerwaniu łańcuchów ataków wszędzie tam, gdzie one występują, od urządzenia, przez sieć, aż po chmurę.

Żadne rozwiązanie nie blokuje ataków w 100%. Optymalna ochrona jest możliwa dzięki połączeniu sprzętowych i programowych środków zaradczych.

Twoje bezpieczeństwo zależy wyłącznie od Twoich dostawców. Upewnij się, że Twoi dostawcy stosują odpowiednie środki bezpieczeństwa.

Notebooki i urządzenia „2 w 1” z serii Latitude

Więcej informacji:

Skontaktuj się z nami: Global.Security.Sales@Dell.com

Odwiedź nas: Dell.com/Endpoint-Security

Obserwuj nas: LinkedIn @DellTechnologies | X @DellTech

Dalsze działania

Bezpieczeństwo to trudny temat dla organizacji każdej wielkości. **Zaangażuj doświadczonego partnera w zakresie zabezpieczeń i technologii, aby zmodernizować zabezpieczenia punktów końcowych.**

Dell Trusted Workspace pomaga zabezpieczyć punkty końcowe w nowoczesnym środowisku IT gotowym do modelu „zero trust”. Zmniejsz podatność na ataki dzięki kompleksowej ofercie firmy Dell dotyczącej zabezpieczeń sprzętowych i programowych. Nasze wysoce skoordynowane, oparte na obronie podejście równoważy zagrożenia, łącząc wbudowane zabezpieczenia z ciągłą czujnością. Użytkownicy końcowi mogą działać produktywnie, a dział IT czuć się pewnie dzięki rozwiązaniom zabezpieczającym stworzonym z myślą o współczesnym środowisku chmurowym.