# Rekomendacje Dell Technologies w zakresie konfiguracji urządzeń, oprogramowania i usług w sposób maksymalizujący skuteczność mechanizmów zabezpieczających dla urządzeń końcowych (komputery i laptopy)

## Uwagi wstępne

Dane stały się najważniejszym zasobem dla wielu organizacji. Ochrona danych i infrastruktury IT, która je obsługuje, to jedne z najważniejszych celów CIO, CISO oraz kierowników IT. Coraz większe wyzwania związane z ochroną infrastruktury IT są po-chodną złożoności i ilości złośliwego oprogramowania.

Każdy cyberatak niesie za sobą ryzyko utraty danych, przestoju w pracy i nadszarpnięcia wizerunku firmy. Dlatego od lat globalne wydatki na ochronę przed atakami nieustannie rosną. Jednak choć świadomość zewnętrznych i wewnętrznych zagrożeń stale wzrasta, nadal najwięcej uwagi poświęca się tylko zabezpieczeniu systemów operacyjnych i aplikacji. Tymczasem dla bezpieczeństwa infrastruktury nie mniej ważne jest też zabezpieczenie sprzętu i oprogramowania układowego.

Ponieważ powszechne zagrożenia są coraz częściej udaremniane, cyberprzestępcy szukają bardziej zaawansowanych sposobów uzyskiwania krytycznych informacji. W związku z tym przedmiotem zainteresowania stały się ukierunkowane ataki na oprogramowanie wewnętrzne komputerów. W takich przypadkach ochrona systemu BIOS komputera, najniższego poziomu systemu komputerowego, ma kluczowe znaczenie dla bezpieczeństwa organizacji. Jeśli osoba atakująca uzyska dostęp do systemu BIOS, może naruszyć wszystkie funkcje zabezpieczeń końcowego urządzenia, a także całą sieć organizacji. Ten rodzaj ataku jest wysoce zaawansowany, a po wykonaniu - bardzo szkodliwy.

Wraz z rosnącą częstotliwością ataków specyficznych dla systemu BIOS i nowymi wariantami złośliwego oprogramowania, które mają możliwość podmiany BIOS, organizacje potrzebują bardziej wyrafinowanego sposobu nie tylko ochrony swoich systemów, ale także pewności, że ich systemy nie zostały naruszone.

Idealnie powinny być to wbudowane w firmware funkcjonalności związane z zapewnieniem bezpieczeństwa. Przykładem takiego rozwiązania jest Dell SafeBIOS Events & Indicators of Attack (IoA). SafeBIOS Events & IoA wykorzystuje wykrywanie zagrożeń na poziomie BIOS-u, aby wykrywać zaawansowane zagrożenia dla punktów końcowych.

Ta technologia weryfikuje BIOS po rozruchu w komputerach komercyjnych dając IT pewność, że BIOS pracowników nie został zmieniony. W przypadku uszkodzenia lub manipulacji BIOS-em są dostępne elastyczne opcje tworzenia obrazów, dzięki czemu można przeanalizować naruszony BIOS, aby zrozumieć naturę ataku.

## Rodzaje ataków

- Ataki zewnętrzne

  Zagrożenia rosną w zastraszającym tempie i są coraz bardziej wyrafinowane. W rzeczywistości zagrożenie może czaić się w środowisku przez średnio 108 dni przed jego wykryciem. W między czasie dochodzi do wycieku danych, naruszenia bezpieczeństwa.

- Zachowanie użytkownika (ataki wewnętrzne)

  Wyzwanie to komplikuje fakt, że użytkownicy końcowi pracują i współpracują w większej liczbie miejsc z większą liczbą urządzeń, udostępniając coraz to większą liczbę informacji. Czasami robią to bezkrytycznie. 72% z nich będzie udostępniać dane na zewnątrz, a połowa z nich będzie korzystać z osobistych aplikacji chmurowych do udostępniania danych służbowych (co już ma miejsce). Przy tej okazji 41% z nich obchodzi bezpieczeństwo nie zdając sobie sprawy, jakie to może nieść konsekwencje.

- Ograniczone zasoby ds. bezpieczeństwa

  Nie ma wystarczającej liczby specjalistów ds. bezpieczeństwa, aby w pełni pokryć zapotrzebowanie rynku. Branża security ma 0% stopę bezrobocia. Oznacza to, że firmy mają trudności z zatrudnieniem i zatrzymaniem kluczowych pracowników opowiadających za bezpieczeństwo w przedsiębiorstwie. Wiele instytucji boryka się z faktem, że nie ma nawet dedykowanego działu bezpieczeństwa. Ta rola jest niestety często dzielona z działem IT.

Połączone wektory zagrożeń zwiększają ryzyko dla punktu końcowego. Słabe konfiguracje, luki w oprogramowaniu układowym czy ataki na niskim poziomie (poniżej systemu operacyjnego) to tylko część zagrożeń, która może mieć wpływ na dalsze działanie i funkcjonowanie firmy.

## Ochrona

Funkcja „ochrony” jest kluczowym elementem wytycznych dotyczących Cyberbezpieczeństwa organizacji NIST (Amerykańskiego Narodowy Instytut Standaryzacji i Technologii) i zasad ochrony przed cyberatakami. Te wytyczne składają się z kilku kategorii, w tym kontroli dostępu, bezpieczeństwa danych, utrzymania i przeciwdziałania. Kluczową filozofią leżącą u podstaw tych wytycznych i zgodności z nimi jest to, że zasoby infrastruktury muszą zapewniać pewną ochronę przed nieautoryzowanym dostępem do zasobów i danych

w ramach kompleksowo bezpiecznego środowiska instalacyjnego i obliczeniowego. Obejmuje to ochronę przed nieautoryzowanymi modyfikacjami kluczowych komponentów, takich jak BIOS i oprogramowanie układowe.

Odporna na cyberataki architektura zarówno serwerowa jak i systemów PC zapewnia wysoki poziom ochrony, który obejmuje następujące możliwości:

- Zweryfikowane kryptograficzne bezpieczne uruchamianie
- Zabezpieczenie dostępu dla Użytkownika
- Podpisane kryptograficznie aktualizacje oprogramowania układowego
- Szyfrowane przechowywanie danych
- Bezpieczeństwo fizyczne
- Integralność i bezpieczeństwo łańcucha dostaw

Strategia Dell, związana z bezpieczeństwem urządzeń końcowych określana nazwą Dell Trusted Security, obejmuje dwa obszary:

| | |
|---|---|
| **Trusted Devices:** Zestaw narzędzi, których zada-niem jest ochrona platformy sprzętowej, takich jak: Dell Off-host BIOS Verification, BIOS Resilience, BIOS Recovery, Intel BIOS Guard | **Trusted Data:** Zestaw narzędzi i usług, których za-daniem jest ochrona kluczowych danych (Carbon Black, Dell Encryption, SecureWorks) |

| Obszar zastosowania | Grupa produktów | Produkt / nazwa funkcjonalności |
|---|---|---|
| Trusted Device | SafeBIOS | Dell Off-host BIOS Verification<br>BIOS Resilience<br>BIOS Recovery<br>BIOS Controls, including Intel BIOS<br>Guard |
| | SafeID | Dell ControlVault<br>FIPS 140-2 TPM<br>FIPS 201 smart card and fingerprint readers |
| Trusted Data | SafeGuard and Response | Prevent:<br>- Dell ControlVault<br>Detect:<br>- Carbon Black EDR<br>- Secureworks Managed Endpoint Protection Respond |

| Obszar zastosowania | Grupa produktów | Produkt / nazwa funkcjonalności |
|---|---|---|
| | SafeData | - Secureworks Incident ---------- Management Retainer<br>Dell Encryption<br>Dell Endpoint Security Services |
| | Inne | Absolute<br>Carbonite |

Wybrane elementy i funkcjonalności zostały opisane poniżej.

## Dell SafeBIOS Events & Indicators of Attack

Funkcja „ochrony" jest kluczowym elementem wytycznych dotyczących Cyberbezpieczeństwa organizacji NIST (Amerykański Narodowy Instytut Standaryzacji i Technologii) i zasad ochrony przed cyberatakami. Te wytyczne składają się z kilku kategorii, w tym kontroli dostępu, bezpieczeństwa danych, utrzymania i przeciwdziałania. Kluczową filozofią leżącą u podstaw tych wytycznych i zgodności z nimi jest to, że zasoby infrastruktury muszą zapewniać pewną ochronę przed nieautoryzowanym dostępem do zasobów i danych w ramach kompleksowo bezpiecznego środowiska instalacyjnego i obliczeniowego. Obejmuje to ochronę przed nieautoryzowanymi modyfikacjami kluczowych komponentów, takich jak BIOS i oprogramowanie układowe.

Dell SafeBIOS chroni komputer na poziomie poniżej systemu operacyjnego. SafeBIOS i IoA zapewniają monitorowanie i analizę ustawień BIOS pod kątem ewentualnych nieuprawnionych zmian konfiguracji, pozwalając w ten sposób na wczesne wykrycie ataku i skuteczne usunięcie jego skutków.

Zidentyfikowano około 60 atrybutów, które wpływają na stan bezpieczeństwa urządzenia, takie jak:

- Ataki rozruchowe
- Aktualizacje systemu BIOS
- Zmiany TPM
- Uwierzytelnianie
- Zdalne ataki
- Manipulowanie dziennikiem zdarzeń

Wybrane funkcjonalności to np. SafeBIOS Verification i SafeBIOS Image Capture. Pierwsza sprawdza podczas uruchamiania, czy BIOS w punkcie końcowym jest zgodny ze znanym dobrym wzorcem BIOS, który jest bezpiecznie przechowywany w chmurze. Dodatkowo, jeśli zostanie wykryta niezgodność, nieuprawniona modyfikacja SafeBIOS

Image Capture wykona migawkę uszkodzonego obrazu BIOS, aby umożliwić jego dalszą analizę.

SafeID służy do ochrony przed atakami złośliwego oprogramowania. Używa dodatkowego układu zabezpieczeń na płycie głównej, który przechowuje dane uwierzytelniające użytkowników końcowych. To sprzętowe rozwiązanie do przechowywania lepiej chroni informacje, utrzymując je w izolacji i poza zasięgiem atakujących.

## Wsparcie dla UEFI Secure Boot

Rozwiązanie UEFI Secure Boot sprawdza podpisy kryptograficzne sterowników UEFI i innego kodu załadowanego przed uruchomieniem systemu operacyjnego. Producenci systemów komputerowych, dostawcy kart rozszerzeń i dostawcy systemów operacyjnych współpracują w zakresie tej specyfikacji, aby promować ich bezkolizyjną współpracę.

Po włączeniu UEFI Secure Boot funkcjonalność ta zapobiega ładowaniu niepodpisanych (tzn. niezaufanych) sterowników urządzeń UEFI, wyświetla komunikat o błędzie i nie pozwala na uruchomienie systemu operacyjnego.

## Dynamiczne włączanie i wyłączanie portów USB

Aby zwiększyć bezpieczeństwo, można całkowicie wyłączyć porty USB. Można również wyłączyć tylko wybrane porty USB.

## Elementy sprzętowe związane z bezpieczeństwem:

### Układ TPM 2.0 z ceryfikatem FIPS-140-2 / zgodny ze specyfikacją TCG

Układ TPM może być wykorzystywany do wykonywania funkcji kryptograficznych z użyciem klucza publicznego, obliczania funkcji skrótu (hash), generowania, zarządzania i bezpiecznego przechowywania kluczy oraz do ich poświadczania. Obsługi-wana jest również funkcja Intel TXT (Trusted Execution Technology). Za pomocą modułu TPM można włączyć funkcję szy-frowania dysku twardego BitLocker w systemie Windows. Moduł może być również wykorzystywany do zdalnej atestacji i do wykonywania pomiarów w czasie uruchamiania sprzętu, hiperwizora, systemu BIOS i systemu operacyjnego oraz porównywania ich w sposób bezpieczny pod względem kryptograficznym z danymi bazowymi przechowywanymi w module TPM. Jest to rozwiązanie częściej stosowane w serwerach niż w PC. TPM jest oferowany jako rozwiązanie modułu plug-in na płycie głównej. Posiada certyfikat NIST FIPS 140-2, co jest ważne dla umów zgodnych z amerykańską DoD i innych powiązanych rządowych.

W celu podniesienia poziomu bezpieczeństwa w zakresie uwierzytelniania użytkownika Dell oferuje wybór różnych opcji zabezpieczeń w wybranych modelach laptopów Dell Latitude i Mobile Precision. Opcje obejmują sprzęt do uwierzytelniania wie-loskładnikowego, m.in. bezdotykowy czytnik kart inteligentnych (Smart ard reader), dotykowy czytnik kart inteligentnych FIPS • 201 i czytnik linii papilarnych.

### Czytnik linii papilarnych (w przycisku zasilania) oraz Control Vault 3.0 Advanced Authentication z certyfikatem FIPS140-2 Level 3

Czytnik linii papilarnych wbudowany w przycisk zasilania pozwala na użycie palca do uwierzytelnienia użytkownika w systemie.

Wspiera rozwiązanie Windows Hello, ale też może być używany w połączeniu z Dell Control Vault.

Dell ControlVault to sprzętowe rozwiązanie bezpieczeństwa, które zapewnia bezpieczny sposób przechowywania i przetwarzania danych uwierzytelniających użytkownika.

Zarówno ControlVault jak i TPM przechowują klucze, ale ControlVault:

- Może przechowywać i wykonywać kod za pomocą bezpiecznego dedykowanego procesora
- Wykorzystuje uwierzytelnianie osobiste (FP, SC, zbliżeniowe) w celu uzyskania dostępu do danych uwierzytelniających
- Przechowuje wszystkie typy danych uwierzytelniających, aby umożliwić pojedynczy punkt migracji

Obsługuje algorytmy szyfrujące takie jak Suite B, native ECC

### Czytnik Contacted Smart Card

Zintegrowany czytnik kart inteligentnych, w zależności od modelu laptopa, obsługuje wiele bezstykowych kart inteligentnych 13,56 MHz, w tym dane uwierzytelniające HID iCLASS®, a także inne karty zbliżeniowe zgodne z ISO i standardem przemysłowym. (Należy pamiętać, że karty zbliżeniowe 125 kHz NIE są obsługiwane).

Dell zaleca wykorzystanie zintegrowanego czytnika kart inteligentnych do wieloskładnikowego uwierzytelniania przy użyciu oprogramowania DigitalPersona® firmy Crossmatch (część HID Global).

### Kamera IR (kompatybilna z Windows Hello)w połączeniu z ExpressSign-in (Proximity Sensor)

Rozwiązanie ExpressSign-in steruje czujnikiem zbliżeniowym na PC z wykorzystaniem Intel® Context Sensing Technology. Idea działania polega na automatycznym budzeniu systemu i zalogowaniu się za pomocą kamery na podczerwień i Windows Hello. Blokuje się również automatycznie komputer, gdy użytkownik oddali się, zwiększając w ten sposób bezpieczeństwo i oszczędzając baterię.

### Dell SafeScreen

SafeScreen to rozwiązanie, które steruje poborem energii i współczynnikiem kontrastu tak, aby uniemożliwić osobom postronnym oglądanie zawartości ekranu.

### VMware Carbon Black

VMware Carbon Black Cloud to oprogramowanie jako usługa (SaaS), które zapewnia funkcję antywirusa nowej generacji (NGAV), wykrywanie i reagowanie na stan urządzeń

końcowych (EDR), zaawansowane wykrywanie zagrożeń i zarządzanie podatnością w ramach jednej konsoli za pomocą jednego czujnika.

### Secureworks Threat Detection and Response

Wykrywanie i reagowanie na zagrożenia poprzez opartą na chmurze aplikacja do analizy bezpieczeństwa, która zmienia sposób, w jaki zespół ds. bezpieczeństwa wykrywa, analizuje i reaguje na zagrożenia w punktach końcowych, sieci i chmurze.

### Dell Encryption Enterprise

Dell Encryption Enterprise zapewnia oparte na oprogramowaniu szyfrowanie skoncentrowane na danych, które chroni wszystkie typy danych w wielu punktach końcowych i systemach operacyjnych. Zarządzanie standardowymi urządzeniami OPAL (dyski samoszyfrujące – SED) jest zintegrowane z tą samą platformą ochrony danych, co szyfrowanie plikowe, Microsoft BitLocker i szyfrowanie nośników wymiennych.

### Absolute® Endpoint Visibility and Control

Absolute to firma zajmująca się bezpieczeństwem urządzeń końcowych, oferując w tym celu rozwiązanie: wbu-dowane sprzęt oprogramowanie - technologię Persistence, która umożliwia zarówno automatyczne przywracanie systemu/aplikacji do stanu sprzed uszkodzenia, jeśli zostały usunięte lub naruszone, jak i kontrolę zarządzania. Technologia ta, będąca kluczowym elementem platformy do kontroli punktów końcowych firmy, zapewnia organizacjom bezpieczeństwa IT połączenie z ich punktami końcowymi w celu uzyskania wglądu i kontroli w celu ochrony użytkowników, danych i urządzeń w sieci firmowej lub poza nią.

## Integralność i bezpieczeństwo łańcucha dostaw

- Utrzymanie integralności sprzętowej: upewnienie się, że przed wysyłką produktu do klientów nie modyfikuje się produktu ani nie wprowadza niebezpiecznych komponentów

- Utrzymanie integralności oprogramowania: zapewnienie, że żadne złośliwe oprogramowanie nie zostanie wbudowane do oprogramowania układowego lub sterowników urządzeń przed wysłaniem produktu do klientów, a także zapobieganie lukom w zabezpieczeniach związanych z kodowaniem oprogramowania

Dell Technologies definiuje bezpieczeństwo łańcucha dostaw jako praktykę stosowania środków kontroli w celu zapobiegania i wykrywania potencjalnych zagrożeń, które chronią aktywa fizyczne, komponenty, informacje, własność intelektualną i ludzi. Te środki bezpieczeństwa pomagają również zapewnić bezpieczeństwo i integralność łańcucha dostaw, zmniejszając możliwości celowego lub nieintencjonalnego wprowadzania złośliwego oprogramowania i niebezpiecznych komponentów do łańcucha dostaw.

## Odzyskiwanie BIOS i Systemu Operacyjnego

Urządzenia końcowe Dell oferują dwa rodzaje powrotu do pożądanego stanu: odzyskiwanie systemu BIOS i odzyskiwanie sys-temu operacyjnego. Pierwotne obrazy używane do odzyskiwania systemu mogą pochodzić z partycji odzyskiwania, klucza USB lub mogą zostać pobrane z chmury za pomocą technologii BIOSConnect. Wszystkie te opcje są częścią szerszego rozwiązania o nawie SupportAssist OS Recovery.

W skrajnych przypadkach, jeśli BIOS jest uszkodzony (z powodu złośliwego ataku, utraty zasilania podczas procesu aktualizacji lub innego nieprzewidzianego zdarzenia), ważne jest, aby zapewnić sposób na przywrócenie BIOS-u do jego pierwotnego stanu (funkcja BIOS Recovery). Automatyczne przywracanie systemu może być inicjowane automatycznie przez BIOS lub ręcznie przez użytkownika.

Zaleca się aktualizowanie oprogramowania układowego/BIOS, aby zapewnić najnowszą funkcjonalność i aktualizacje  zabezpieczeń. Jednak w przypadku wystąpienia problemów po aktualizacji może być konieczne wycofanie aktualizacji lub zainstalowanie wcześniejszej wersji. Jeśli przywrócona zostanie poprzednia wersja, zostanie ona również zweryfikowana pod kątem jej podpisu.

Jest obsługiwane przywracanie oprogramowania układowego z istniejącej wersji produkcyjnej „N” do poprzedniej wersji „N-1”.