KOMPAS IT

DELL Technologies

Bezpieczny PC
– referencyjne mechanizmy ochrony dla laptopów i desktopów

W czasach, gdy praca zdalna i mobilność są na porządku dziennym, a kluczowe operacje organizacji są powiązane z dynamicznym rozwojem technologii informatycznych i pracą na komputerach osobistych – zarówno laptopach, jak i desktopach, bezpieczeństwo tych elementów infrastruktury IT organizacji staje się kluczowym elementem.
Podniesienie poziomu bezpieczeństwa urządzeń końcowych w organizacji i utrzymanie go na wszystkich płaszczyznach użytkowania, to dla organizacji ogromne wyzwanie i kluczowy priorytet, aby zapewnić spokój i stabilność w codziennych operacjach. Dlatego liczy się solidne wsparcie i innowacyjne technologie:

- **Kompleksowe podejście do bezpieczeństwa**
  Dell Technologies oferuje szeroki wachlarz rozwiązań, od ochrony łańcucha dostaw, przez zabezpieczenia sprzętowe, po zaawansowane narzędzia do zarządzania i monitorowania bezpieczeństwa.

- **Ochrona przed najnowszymi zagrożeniami**
  Rekomendacje obejmują najnowsze technologie i praktyki, które skutecznie zabezpieczają przed atakami na firmware, BIOS oraz złośliwe oprogramowanie.

- **Wsparcie ekspertów**
  Dell zapewnia profesjonalne wsparcie oraz usługi zarządzania i monitorowania bezpieczeństwa, co pozwala na odciążenie wewnętrznych zespołów IT i skoncentrowanie się na kluczowych zadaniach biznesowych.

- **Zgodność z międzynarodowymi standardami**
  Rekomendowane rozwiązania są zgodne z certyfikacjami ISO, FIPS i TCG, co gwarantuje najwyższy poziom bezpieczeństwa i zgodności z przepisami.

- **Skalowalność i elastyczność**
  Rozwiązania Dell są elastyczne i skalowalne, co pozwala na ich dostosowanie do indywidualnych potrzeb organizacji, niezależnie od jej wielkości i branży.

- **Ochrona danych i ciągłość działania**
  Regularne tworzenie kopii zapasowych oraz zaawansowane mechanizmy zabezpieczające dane zapewniają ciągłość operacyjną i szybkie przywracanie działania w przypadku awarii.

- **Budowanie zaufania**
  Inwestycja w bezpieczeństwo to nie tylko ochrona przed zagrożeniami, ale także budowanie zaufania wśród klientów i partnerów biznesowych.

Bezpieczny PC – to strategia oparta na pięciu filarach:

1. Zabezpieczenia sprzętowe
2. Zabezpieczenia softwarowe
3. Zaawansowane narzędzia do monitorowania bezpieczeństwa środowiska pracy
4. Narzędzia zwiększające bezpieczeństwo infrastruktury
5. Niezawodna kopia zapasowa danych

ROLA I ZNACZENIE

Nawet najbardziej zaawansowane technologie wdrożone do prowadzenia operacji biznesowych są narażone na bezprecedensowe cyberataki, które mogą doprowadzić do utraty przychodów, spadku wydajności oraz naruszenia wiarygodności i reputacji firm, organizacji rządowych, edukacyjnych i komercyjnych.
Dlatego też organizacje poszukują produktów i rozwiązań IT, które zapewniają najwyższy poziom bezpieczeństwa, jednocześnie eliminując ryzyka i zagrożenia złośliwych modyfikacji na poziomie ich hardware i firmware. Bezpieczeństwo sprzętu IT oraz łańcucha dostaw – na każdym etapie procesu produkcji, dystrybucji i dostarczania produktów – jeszcze nigdy nie były tak istotne. Futurum w publikacji „Four Keys to Navigating the Hardware Security Journey" potwierdza, że 44% organizacji przyznało, iż w ciągu ostatnich 12 miesięcy doświadczyło przynajmniej jednego ataku na oprogramowanie sprzętowe, urządzenia lub BIOS. To potwierdza, jak wysokim priorytetem jest bezpieczeństwo sprzętu IT.

W odpowiedzi na te wyzwania, Dell Technologies koncentruje się na tworzeniu i utrzymywaniu światowej klasy zabezpieczeń zarówno dla swoich produktów, jak i dla łańcucha dostaw. Poniższy dokument przedstawia rekomendacje Dell Technologies dotyczące szerokiego spektrum rozwiązań podnoszących bezpieczeństwo urządzeń końcowych – od zabezpieczenia łańcucha dostaw, przez bezpieczeństwo sprzętu, aż po proces wdrożenia, utrzymania i wycofania produktów z eksploatacji.

Bezpieczeństwo łańcucha dostaw

Dell Technologies stosuje kompleksowe podejście do ochrony swojego łańcucha wartości w łańcuchu dostaw, dbając o bezpieczeństwo na każdym jego etapie, by dostarczać rozwiązania, którym klienci mogą zaufać. Niezależnie od tego, czy jest to komputer stacjonarny, laptop, serwer czy macierz pamięci masowej, wszystkie elementy i funkcje produktu są opracowywane, projektowane, prototypowane, implementowane, wprowadzane do produkcji, wdrażane, konserwowane i zatwierdzane z uwzględnieniem wysokiego bezpieczeństwa łańcucha dostaw jako najwyższego priorytetu.
Bezpieczeństwo łańcucha wartości i łańcucha dostaw oznacza stosowanie m.in. wykrywania zagrożeń i środków zapobiegawczych, chroniących fizyczne aktywa, zasoby, informacje, własność intelektualną oraz pracowników. Nadzór nad bezpiecznym przepływem informacji, fizyczna ochrona urządzeń oraz kontrola personelu zapewnia bezpieczeństwo całego łańcucha dostaw, ograniczając możliwości wprowadzenia złośliwego oprogramowania i podrobionych komponentów. Bezpieczeństwo łańcucha dostaw gwarantuje, że produkty docierające do klientów są wolne od zagrożeń, co jest kluczowe dla zachowania zaufania i ochrony wartości całej organizacji.

Bezpieczeństwo łańcucha dostaw w Dell Technologies obejmuje:

Bezpieczeństwo informacji

W celu ochrony własnej organizacji, jak i wytwarzanych rozwiązań oferowanych swoim klientom, Dell Technologies wykorzystuje szereg technologii oraz procesów, takich jak szyfrowanie, techniki kodujące, prywatne kanały komunikacji, śledzenie ruchu sieciowego, SIEM, EDR, firewalle oraz wiele innych.

Bezpieczeństwo związane z personelem

Kontrolowanie pracowników oraz ograniczanie ich uprawnień dostępu do danych i manipulowania nimi, stanowi gwarancję skuteczności wewnętrznych działań w zakresie bezpieczeństwa. Dell Technologies prowadzi program weryfikacji zatrudnionych pracowników oraz rozbudowany system szkoleń, którego celem jest stałe podnoszenie świadomości zagrożeń i eliminacji ryzyk.

Bezpieczeństwo fizyczne

Pomieszczenia, w których produkty Dell Technologies są projektowane, budowane, dostosowywane lub wysyłane do klientów, spełniają wymagania stowarzyszenia Transported Asset Protection Association (TAPA) w zakresie bezpieczeństwa obiektów. Obejmuje to stosowanie kamer z zamkniętym obwodem w kluczowych obszarach, kontrolę dostępu oraz stały monitoring wejść i wyjść. Dodatkowe środki kontroli są stosowane zarówno w zakładach Dell Technologies oraz u dostawców, a także w przypadku przesyłek lotniczych, kolejowych i morskich, z uwzględnieniem zróżnicowanych zagrożeń w zależności od formy, typu i regionu transportu. Zabezpieczenia obejmują m.in. opakowania zabezpieczone przed manipulacją (uniemożliwiające niezauważalne otwarcie), przeglądy bezpieczeństwa szlaków żeglugowych oraz specjalne blokady spełniające normy dotyczące integralności kontenera. Kontenery są wyposażone w urządzenia śledzące GPS oraz inne czujniki monitorujące ich trasę i stan realizacji dostawy. Dell Technologies otrzymało również **certyfikat partnerstwa celno-handlowego Stanów Zjednoczonych przeciwko terroryzmowi (C-TPAT).** Chociaż głównym celem tego programu jest zapobieganie przemytowi, zabezpieczenia wymagane do uzyskania certyfikatu wzmacniają również ochronę przed manipulowaniem importowanymi produktami.

Integralność sprzętu

Aby zminimalizować możliwość pojawienia się podrobionych komponentów w łańcuchu dostaw, Dell Technologies zamawia je bezpośrednio od producentów, a odbiór dostaw jest połączony z restrykcyjnym procesem weryfikacji. System zarządzania jakością pozwala na bieżącą weryfikację zgodności dostaw ze specyfikacjami, identyfikację niewłaściwego oznakowania oraz różnic w parametrach wydajności lub nieprawidłowych identyfikatorach.
W celu identyfikacji wszystkie kluczowe części są oznaczane etykietą z unikatowym numerem seryjnym lub symbolem, etykietą PPID (Piece-Part Identification) zalecaną przez Dell Technologies lub identyfikatorem elektronicznym, który można sprawdzić na każdym etapie produkcji. Ponadto Dell Technologies uzyskało **certyfikat ISO 9001** w zakresie praktyk kontroli jakości we wszystkich globalnych zakładach produkcyjnych. Przestrzeganie tych procedur i procesów kontroli pomaga zminimalizować ryzyko naruszenia bezpieczeństwa i wbudowania podrobionych komponentów w produkty Dell Technologies.

Integralność oprogramowania

Dell Technologies stosuje procedury zgodne z wytycznymi **Software Assurance Forum for Excellence in Code (SAFECode)** oraz **ISO 27034** w całym procesie projektowania i rozwoju oprogramowania. Proaktywne działania

w zakresie weryfikacji, walidacji i testowania zabezpieczeń w czasie całego cyklu życia produktów pomagają chronić oprogramowanie oraz zmniejszają prawdopodobieństwo wprowadzenia do niego złośliwego oprogramowania lub wykorzystania luk w kodzie.
Skuteczny program bezpieczeństwa cyfrowego poprawia integralność oprogramowania, zapobiegając nieautoryzowanemu dostępowi do kodu źródłowego i minimalizuje możliwość wprowadzenia złośliwego oprogramowania do produktu przed jego wysłaniem do użytkownika.

Projektowanie i rozwój

Cykl projektowania zabezpieczeń opracowany przez Dell Technologies **(Secure Development Lifecycle, SDL)** określa środki kontroli bezpieczeństwa, które zespoły produktowe stosują podczas opracowywania nowych cech i funkcji. Dell Technologies współpracuje z wieloma organizacjami branżowymi, takimi jak **Software Assurance Forum for Excellence in Code (SAFECode), Building Security In Maturity Model (BSIMM) oraz IEEE Center for Secure Design,** aby zapewnić przestrzeganie najlepszych praktyk branżowych. Firmowy pakiet SDL obejmuje zarówno działania analityczne, jak i proaktywne kontrole normatywne w kluczowych obszarach ryzyka.

Testy penetracyjne

Testy penetracyjne (pentesty) stały się synonimem dojrzałych praktyk w zakresie bezpieczeństwa w całej branży. Dell Technologies wykorzystuje zarówno własne zespoły, jak i zewnętrznych specjalistów do przeprowadzania testów penetracyjnych swoich komputerów, serwerów i urządzeń pamięci masowej już na etapie projektowania. Testy te koncentrują się na dostępie fizycznym i są uporządkowane pod względem ważności w oparciu o ocenę ryzyka poszczególnych komponentów zintegrowanych z urządzeniem.

Cyfrowe podpisywanie oprogramowania układowego

Jednym z krytycznych zagrożeń dla łańcucha dostaw jest nieautoryzowana modyfikacja kodu lub danych. Inżynierowie Dell Technologies stosują kryptograficzny podpis cyfrowy do oprogramowania, aplikacji i oprogramowania układowego, aby umożliwić potwierdzenie autentyczności oraz integralności – znany jako proces podpisywania kodu.

MOŻLIWOŚCI I ZASTOSOWANIE

Bezpieczeństwo komputerowe w firmach obejmuje szeroki zakres działań mających na celu ochronę danych i infrastruktury przed zagrożeniami cybernetycznymi. Współczesne organizacje wykorzystują zaawansowane rozwiązania technologiczne, takie jak wbudowane sprzętowe mechanizmy bezpieczeństwa, firewalle, programy antywirusowe, oprogramowanie do wykrywania zagrożeń oraz systemy monitorowania zdarzeń, aby zapewnić bezpieczeństwo swoich komputerów PC. Zastosowania te mają na celu eliminację ryzyka ataków typu malware, phishing czy ransomware oraz ochronę poufności danych firmowych.
Ważnym aspektem jest również stałe aktualizowanie oprogramowania oraz edukacja pracowników w zakresie świadomości cyberbezpieczeństwa, aby minimalizować ryzyko naruszeń spowodowanych przez czynniki ludzkie. Dzięki właściwej implementacji i monitorowaniu zabezpieczeń komputerowych, firmy mogą skutecznie chronić swoje zasoby cyfrowe, zapewnić ciągłość działania i stabilność operacyjną biznesu.

Nieodpowiednio zabezpieczone urządzenia końcowe stanowią najsłabsze ogniwo w łańcuchu bezpieczeństwa. Dlatego niezwykle ważne jest, aby inwestowanie w wysokiej klasy komputery biznesowe prowadziło do zwiększenia bezpieczeństwa urządzeń końcowych w organizacji. Świadome inwestycje w najnowsze technologie i rozwiązania, w połączeniu z podnoszeniem kwalifikacji użytkowników, przekładają się na ogólny wzrost poziomu bezpieczeństwa w firmie.

ARCHITEKTURA – STRUKTURA I DZIAŁANIE

Zabezpieczenia wbudowane, sprzętowe

Zabezpieczenia sprzętowe wbudowane w nowoczesne komputery PC stanowią kluczowy element ochrony danych i zapewnienia bezpieczeństwa użytkownikom. Współczesne technologie sprzętowe integrują zaawansowane funkcje, które mają na celu minimalizowanie ryzyka ataków cybernetycznych oraz zabezpieczenie poufności informacji.

Dell SafeBIOS to zestaw mechanizmów chroniący komputer bez konieczności wykorzystywania systemu operacyjnego. Umożliwia m.in. weryfikację poprawności obrazu BIOS, monitorowanie i analizę ustawień BIOS pod kątem ewentualnych nieuprawnionych zmian konfiguracji, co pozwala na wczesne wykrycie ataku.

Dell SafeID wykorzystuje dodatkowyukładu zabezpieczeń na płycie głównej, który przechowuje dane uwierzytelniające użytkowników końcowych. Chroni informacje, utrzymując je w izolacji i poza zasięgiem atakujących.

Intel Hardware Shield to zestaw technologii wbudowanych w wybrane procesory Intel, które chronią komputer przed atakami typu ransoware czy cryptojacking. Technologia ta odpowiada również za szyfrowanie pamięci RAM przy użyciu wielu kluczy.

Czujnik otwarcia obudowy wykrywa wszelkie próby otwarcia obudowy, informując i przekazując dane o możliwości ingerencji w integralność podzespołów.

TPM (Trusted Platform Module) to dedykowany mikroprocesor znajdujący się na płycie głównej, wykorzystywany do wykonywania funkcji kryptograficznych z użyciem klucza publicznego. Za pomocą modułu TPM można włączyć funkcję szyfrowania dysku twardego BitLocker w systemie Windows. Układ TPM 2.0 jest zgodny z certyfikatem FIPS-140-2 oraz zgodny ze specyfikacją TCG.

Dell Data Wipe to funkcja w systemie BIOS , która daje klientom możliwość wymazania danych z wewnętrznych urządzeń pamięci masowej w komputerach. Pozwala to na wydajne usuwanie danych w celu zmiany ich przeznaczenia lub ponownego wdrożenia.

Dzięki integracji tych zaawansowanych technologii, Dell Technologies zapewnia wysoki poziom bezpieczeństwa sprzętowego, chroniąc zarówno dane, jak i integralność systemów użytkowników.

Zabezpieczenia programowe

Zabezpieczenia oprogramowania (software) w nowoczesnych komputerach PC są kluczowym elementem zapewniania bezpieczeństwa danych i ochrony przed różnorodnymi zagrożeniami cybernetycznymi. Rozwój technologii informatycznych sprawia, że coraz więcej firm i użytkowników korzysta

z zaawansowanych rozwiązań programowych, które pomagają w minimalizowaniu ryzyka ataków oraz utrzymaniu integralności danych.

Dell Support Assist to narzędzie umożliwiające optymalizację komputera poprzez usuwanie niechcianych plików tymczasowych i optymalizację ustawień sieciowych. Rozwiązanie to identyfikuje także krytyczne aktualizacje sterowników dostępne dla komputera i dokonuje ich aktualizacji. W wersji dla komputerów biznesowych **(Support Assist for Business PC)** pozwala dodatkowo na zcentralizowane zarzadzanie flotą komputerów w organizacji z wykorzystaniem portalu Tech Direct. Dzięki wykorzystaniu telemetrii może zapewnić również predykcyjne i proaktywne wykrywanie potencjalnych problemów ze sprzętem.

Dell Tech Direct to chmurowy portal dostępny bezpłatnie dla wszystkich organizacji korzystających z komputerów Dell. Oferuje możliwość dokonywania zgłoszeń serwisowych oraz, w połączeniu z aplikacją **SupportAssist for Business PC**, dostarcza informacje na temat poziomu zabezpieczeń na wszystkich komputerach, uwzględniając: poprawność aktualnie uruchomionego obrazu BIOS, wskaźniki wektorów ataku na BIOS, weryfikacje TPM, posiadanie ustawionego hasła do BIOS, weryfikację firewall, antywirusa, enkrypcji dysku oraz Intel Management Engine.

Dell Command Update to narzędzie, które ułatwia zarządzanie i aktualizację oprogramowania na komputerach firmy Dell. Pozwala ono na szybką i efektywną aktualizację sterowników, firmware'u oraz aplikacji, co zapewnia nie tylko zgodność z najnowszymi standardami, ale także zwiększa bezpieczeństwo i wydajność systemów.

Dell Command Endpoint Configure for Microsoft Intune (DCECMI) umożliwia łatwe i bezpieczne zarządzanie ustawieniami systemu BIOS zdalnie na komputerach w organizacji przy wykorzystaniu integracji z Microsoft Intune. Oprogramowanie to umożliwia generowanie i utrzymywania unikalnych haseł do BIOS w celu zapewnienia najwyższych standardów bezpieczeństwa.

Dell Security Advisories to portal informujący o pojawiających się możliwych podatnościach urządzeń końcowych Dell w kontekście globalnie rozpoznanych zagrożeń CVE zgodnie z bazą wiedzy MITRE. Portal zawiera aktualne rekomendacje Dell mające na celu minimalizowanie ryzyk związanych z wykrytymi lukami w zabezpieczeniach urządzeń.

Zabezpieczenia środowiska pracy

Zabezpieczenie środowiska pracy w nowoczesnych komputerach PC jest kluczowym elementem zapewnienia efektywności i bezpieczeństwa w dowolnym miejscu pracy. Współczesne technologie oraz rosnące zagrożenia cybernetyczne wymagają ścisłej ochrony infrastruktury IT oraz danych organizacji.

Dell Managed Detection and Response (MDR) to w pełni zarządzana, kompleksowa usługa dostępna przez całą dobę, która monitoruje i wykrywa zagrożenia w całym środowisku IT organizacji. Wykwalifikowani eksperci Dell Technologies ds. bezpieczeństwa zapewniają stałą ochronę organizacji przed cyberatakami, jednocześnie zmniejszając obciążenie personelu IT. Dzięki zastosowaniu telemetrii i wiedzy eksperckiej Dell MDR pozwala na rozpoznanie zagrożeń, które nie są wykrywalne przez tradycyjne oprogramowanie antywirusowe. W przypadku wykrycia ataku, zespół ten jest w stanie odpowiednio zareagować poprzez wstrzymanie podejrzanego ruchu sieciowego, poddanie kwarantannie zainfekowanych systemów czy przekazanie zaleceń mających na celu wyeliminowanie zagrożenia. Dell MDR działa w oparciu o sprawdzone rozwiązanie **XDR Taegis Secureworks**, co zapewnia najwyższy poziom bezpieczeństwa i niezawodności usługi.

Rozwiązanie Absolute to oprogramowanie przeznaczone dla biznesowych komputerów przenośnych Dell. Fabrycznie wbudowana w oprogramowanie układowe technologia posiada funkcjonalność samoinstalacji, dzięki czemu działa ona pomimo wymiany dysku czy reinstalacji systemu operacyjnego. Absolute umożliwia zespołom IT na geolokalizację urządzenia, zdalne jego zablokowanie i usunięcie danych.

Zabezpieczenia danych

Backup danych w środowisku PC jest kluczowym elementem zapewnienia bezpieczeństwa i ochrony danych przed utratą lub uszkodzeniem. Współczesne komputery PC przechowują ogromne ilości cennych informacji, dlatego regularne tworzenie kopii zapasowych jest niezbędne dla zapewnienia ciągłości działania oraz szybkiego przywrócenia danych w przypadku awarii lub ataku cybernetycznego.

Dell Backup as a Service (BaaS) to kompleksowe rozwiązanie zapewniające Klientom firmy Dell możliwość skutecznego zarządzania i zabezpieczania swoich danych poprzez tworzenie kopii zapasowych z komputerów Dell. Jest to usługa oparta na chmurze, oferująca przechowywanie minimum trzech kopii danych w minimum trzech niezależnych lokalizacjach Data Center. Daje to pewność, że dane przechowywane i zarządzane w infrastrukturze chmurowej firmy Dell są odpowiednio zabezpieczone oraz łatwo dostępne.

Usługa Dell BaaS oferuje szereg funkcji i możliwości, które obejmują:

- **Automatyczne tworzenie kopii zapasowych**
  System automatycznie tworzy regularne kopie zapasowe danych, co eliminuje konieczność ręcznego planowania i wykonywania tych czynności;
- **Zarządzanie cyklem życia danych**
  Zapewnia śledzenie i zarządzanie cyklem życia danych, umożliwiając klientom zachowanie odpowiednich kopii zapasowych przez określony czas, zgodnie z ich wymaganiami i przepisami prawnymi;
- **Opcje odzyskiwania danych**
  Usługa umożliwia szybkie odzyskiwanie danych w przypadku awarii lub utraty danych. Klienci mogą przywracać pojedyncze pliki, foldery lub całe systemy w zależności od potrzeb;
- **Bezpieczeństwo danych**
  Zapewniając silne szyfrowanie danych w czasie przechowywania i transmisji, Dell BaaS chroni poufność i integralność danych klientów;
- **Monitoring i raportowanie**
  Usługa oferuje narzędzia do monitorowania wydajności kopii zapasowych oraz raportowania, co umożliwia klientom śledzenie stanu i efektywności ich strategii kopii zapasowych;
- **Elastyczność skalowania**
  Dzięki elastycznym opcjom skalowania można dostosować pojemność i wydajność kopii zapasowych do zmieniających się potrzeb biznesowych;
- **Wsparcie i usługi profesjonalne**
  Dostęp do wsparcia technicznego i usług profesjonalnych firmy Dell, pomaga w konfiguracji, wdrożeniu i utrzymaniu rozwiązania Backup as a Service.

Po zakończeniu cyklu życia produktu, ważne jest, aby dane przechowywane na dysku urządzenia zostały odpowiednio usunięte. Dell Technologies oferuje usługi bezpiecznego usuwania danych w ramach wybranych pakietów, które obejmują:

- Usuwanie danych na urządzeniach przy pełnej zgodności ze standardami NIST;

- Fizyczne niszczenie dysków, na których oczyszczanie danych się nie powiodło;
- Możliwość usuwania danych na urządzeniach i niszczenia dysków twardych w lokalizacji klienta, co zapewnia większe bezpieczeństwo;
- Aktywne weryfikowanie, audytowanie i rozliczanie partnerów z najwyższych standardów bezpieczeństwa danych i zgodności środowiskowej;
- Szczegółowy raport o stanie oczyszczania danych i wynikach dotyczących każdego wycofanego systemu.

KLUCZOWE FUNKCJE I KORZYŚCI

Zapewnienie bezpiecznego środowiska PC jest kluczowym elementem ochrony danych, zapewnienia ciągłości działania organizacji oraz zwiększenia wydajności pracy użytkowników. Bezpieczne środowisko PC opiera się na zastosowaniu kompleksowych zabezpieczeń sprzętowych i programowych, takich jak moduły TPM, czytniki linii papilarnych, oprogramowanie antywirusowe, zaawansowane usługi zabezpieczeń, zapory sieciowe oraz regularne tworzenie kopii zapasowych.

Wyzwania organizacji

Rosnąca liczba i złożoność cyberataków
Organizacje muszą zmagać się z coraz bardziej zaawansowanymi atakami na swoje systemy.

Bezpieczeństwo sprzętu i firmware
Ataki na hardware i firmware stanowią poważne zagrożenie, często trudne do wykrycia i neutralizacji.

Zarządzanie bezpieczeństwem danych
Ochrona danych przed utratą, kradzieżą i nieautoryzowanym dostępem jest kluczowym elementem strategii bezpieczeństwa każdej organizacji.

Zgodność z regulacjami
Utrzymanie zgodności z międzynarodowymi standardami i przepisami prawa to wyzwanie wymagające ciągłego monitorowania i aktualizacji procedur.

Odpowiedzi technologiczne i wsparcie Dell:

Zaawansowane zabezpieczenia sprzętowe i programowe
Technologie takie jak Dell SafeBIOS, SafeID i Intel Hardware Shield zapewniają ochronę na poziomie hardware i firmware.

Profesjonalne wsparcie i zarządzanie
Dell Managed Detection and Response (MDR) oraz inne usługi zarządzane oferują stały monitoring i szybką reakcję na zagrożenia.

Kompleksowe rozwiązania do backupu danych
Dell Backup as a Service (BaaS) zapewnia skuteczne zarządzanie kopiami zapasowymi i szybkie odzyskiwanie danych.

Szkolenia i świadomość zagrożeń
Dell prowadzi programy szkoleniowe w zakresie dostępnych rozwiązań oraz podnoszące świadomość zagrożeń wśród pracowników, co jest kluczowe dla minimalizacji ryzyka związanego z czynnikami ludzkimi.

Certyfikacje i standardy
Rozwiązania Dell są zgodne z międzynarodowymi standardami, co zapewnia najwyższy poziom bezpieczeństwa i zgodności z regulacjami.

Korzyści wynikające **wdrożenia zaawansowanych zabezpieczeń komputerów osobistych** i posiadania bezpiecznego środowiska PC obejmują ochronę danych przed utratą i kradzieżą, minimalizację ryzyka cyberataków oraz zapewnienie zgodności z przepisami prawnymi dotyczącymi ochrony danych osobowych. Dodatkowo, odpowiednie zabezpieczenia przyczyniają się do zwiększenia wydajności pracy poprzez eliminację przestojów związanych z incydentami naruszenia bezpieczeństwa.

Redukcja ryzyka cyberataków
Zastosowanie nowoczesnych technologii zabezpieczeń zmniejsza ryzyko udanych ataków cybernetycznych.

Ochrona poufnych danych
Skuteczne mechanizmy ochrony danych zapewniają integralność i poufność informacji biznesowych.

Ciągłość operacyjna
Zapewnienie stabilności systemów IT poprzez regularne monitorowanie i aktualizacje zabezpieczeń minimalizuje ryzyko przestojów.

Podniesienie świadomości pracowników
Regularne szkolenia i edukacja w zakresie cyberbezpieczeństwa pomagają pracownikom rozpoznawać i unikać potencjalnych zagrożeń.

Zgodność z regulacjami
Wdrożenie zaawansowanych zabezpieczeń pomaga firmom spełniać wymagania prawne i regulacyjne dotyczące ochrony danych i bezpieczeństwa cyfrowego organizacji.

Bezpieczne środowisko PC nie tylko chroni dane i infrastrukturę IT, ale także buduje zaufanie użytkowników do systemów informatycznych, zapewniając komfort i pewność podczas codziennej pracy. Inwestycja w bezpieczeństwo środowiska PC jest niezbędna dla każdej organizacji, która pragnie osiągnąć sukces i utrzymać konkurencyjność na rynku.
Dzięki kompleksowym strategiom bezpieczeństwa komputerowego, firmy mogą nie tylko zabezpieczać swoje zasoby cyfrowe, ale także budować zaufanie wśród klientów i partnerów biznesowych, co jest kluczowe dla rozwoju i długoterminowego sukcesu.

CERTYFIKACJE

- ISO 27001
- TPM 2.0 FIPS + Common Criteria + certyfikat TCG (Nuvoton)
- C-TPAT

ZOBACZ TAKŻE

> Bezpieczne środowisko serwerowe – optymalizacja konfiguracji urządzeń i usług

Zgodność z NIS2 – cyberbezpieczeństwo w zgodzie z dyrektywą europejską

Zgodność z DORA – efektywne strategie bezpieczeństwa cyfrowego

Kompas IT – innowacyjne rozwiązania dla efektywności i cyfrowej odporności IT

Poznaj rozwiązania Dell Technologies

Porozmawiajmy o bezpieczeństwie PC oraz referencyjnych mechanizmach ochrony dla laptopów i desktopów

Kazimierz Szczepanik
Technical Sales Representative CSG
kazimierz.szczepanik@dell.com

Sebastian Antkiewicz
CSG Senior Manager Poland & Czech Republic
sebastian.antkiewicz@dell.com

DELL Technologies