KURS

Cyberbezpieczne środowisko w szkole

ATOM 3

Bezpieczeństwo w Windows 11

PROWADZĄCY

Artur Rudnicki
Microsoft Innovative Educator Expert

Zabezpieczenia w Windows 11 Pro

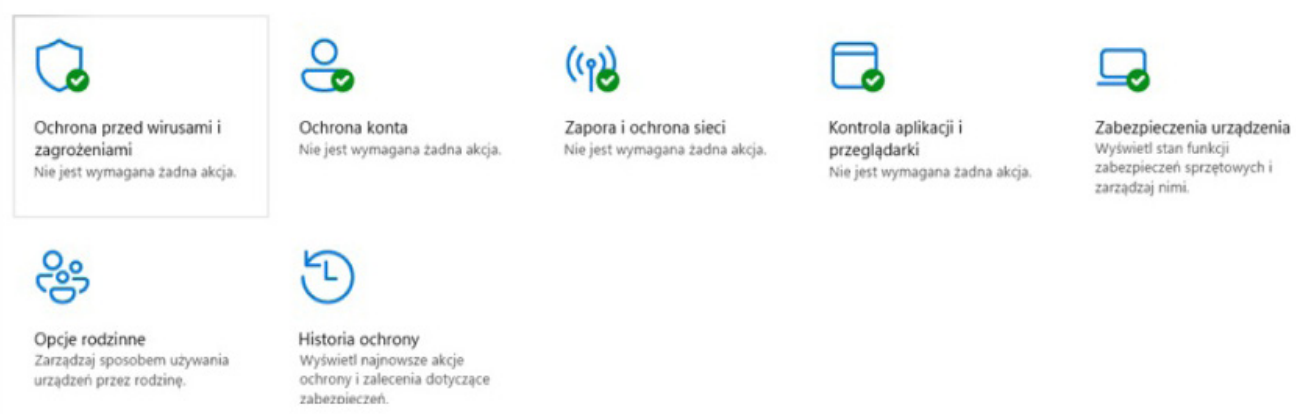
Windows 11 Pro ma na stałe wiele zabezpieczeń, o których nawet użytkownik nie wie, ale które zabezpieczają go przed atakami, wyłudzenia, itp. Oto niektóre z nich, które są w systemie:

1. **BitLocker:** To narzędzie do szyfrowania całych dysków, które chroni dane przed nieautoryzowanym dostępem. BitLocker używa algorytmów szyfrowania, aby zabezpieczyć dane na dyskach twardych i przenośnych, takich jak pendrive'y.
2. **Windows Hello:** Umożliwia bezpieczne logowanie do urządzeń za pomocą biometrii, takiej jak rozpoznawanie twarzy, odcisk palca, lub kodu PIN. To znacznie zwiększa bezpieczeństwo w porównaniu do tradycyjnych haseł.
3. **Windows Defender:** Wbudowany program antywirusowy i antymalware, który chroni system przed wirusami, złośliwym oprogramowaniem i innymi zagrożeniami online. Regularnie aktualizuje swoje definicje zagrożeń, aby zapewnić najnowszą ochronę.
4. **Hyper-V:** Technologia wirtualizacji, która pozwala na uruchamianie wielu systemów operacyjnych na jednym komputerze. Jest to przydatne do testowania oprogramowania w izolowanych środowiskach.
5. **Windows Sandbox:** Bezpieczne środowisko do uruchamiania nieznanych aplikacji i plików bez ryzyka dla głównego systemu. Po zamknięciu Sandbox wszystkie dane są usuwane, co zapewnia, że system pozostaje czysty.
6. **Microsoft Defender Application Guard:** Chroni przeglądarkę i aplikacje przed złośliwym oprogramowaniem, uruchamiając je w izolowanym kontenerze. Nawet jeśli aplikacja zostanie zainfekowana, nie wpłynie to na resztę systemu.
7. **Secured-core PCs:** Urządzenia te mają dodatkowe warstwy zabezpieczeń sprzętowych, które chronią przed zaawansowanymi atakami. Są one bardziej odporne na ataki typu firmware i inne zagrożenia na poziomie sprzętu.

8. **Microsoft Pluton Security Processor:** Nowy procesor bezpieczeństwa, który integruje się bezpośrednio z CPU, aby chronić wrażliwe dane, takie jak klucze szyfrowania, przed atakami fizycznymi i zdalnymi.
9. **Virtualization-Based Security (VBS):** Używa technologii wirtualizacji do ochrony krytycznych części systemu operacyjnego przed złośliwym oprogramowaniem. VBS tworzy izolowane środowisko, które utrudnia atakom dostęp do systemu.
10. **Hypervisor-Protected Code Integrity (HVCI):** Chroni przed atakami na jądro systemu operacyjnego, zapewniając, że tylko zaufany kod może być wykonywany.
11. **Windows Information Protection (WIP):** Pomaga chronić dane firmowe przed przypadkowym wyciekiem, umożliwiając kontrolę nad tym, które aplikacje mogą uzyskiwać dostęp do danych firmowych.
12. **Credential Guard:** Chroni poświadczenia użytkowników przed kradzieżą przez złośliwe oprogramowanie, izolując je w bezpiecznym środowisku.
13. **Advanced Threat Protection (ATP):** Zaawansowane narzędzie do wykrywania i reagowania na zagrożenia, które monitoruje system w czasie rzeczywistym i analizuje podejrzane działania.
14. **Passkeys:** Umożliwia bezhasłowe logowanie, co zwiększa bezpieczeństwo i zmniejsza ryzyko ataków phishingowych. Passkeys są bardziej bezpieczne niż tradycyjne hasła, ponieważ nie są podatne na kradzież.

Domyślnie włączone zabezpieczenia w Windows 11 Pro to:

- Windows Defender: Ochrona przed wirusami i złośliwym oprogramowaniem jest włączona domyślnie.



- Secure Boot: Zapewnia, że komputer uruchamia się tylko z zaufanego oprogramowania.
- Windows Hello: Możliwość logowania za pomocą biometrii lub kodu PIN jest dostępna, ale wymaga konfiguracji.
- Firewall and Network Protection: Monitoruje i kontroluje ruch sieciowy.
- Credential Guard: Chroni poświadczenia użytkowników przed kradzieżą.

Zabezpieczenia, które można włączyć ręcznie:

BitLocker

- Otwórz Ustawienia.
- Przejdź do Aktualizacja i zabezpieczenia.
- Wybierz Szyfrowanie urządzenia.
- Kliknij Włącz BitLocker i postępuj zgodnie z instrukcjami na ekranie.

Hyper-V

- Otwórz Panel sterowania.
- Przejdź do Programy.
- Kliknij Włącz lub wyłącz funkcje systemu Windows.
- Zaznacz opcję Hyper-V i kliknij OK.
- Uruchom ponownie komputer, aby zastosować zmiany.

Windows Sandbox

- Otwórz Panel sterowania.
- Przejdź do Programy.
- Kliknij Włącz lub wyłącz funkcje systemu Windows.
- Zaznacz opcję Windows Sandbox i kliknij OK.
- Uruchom ponownie komputer, aby zastosować zmiany.

Microsoft Defender Application Guard

- Otwórz Panel sterowania.
- Przejdź do Programy.
- Kliknij Włącz lub wyłącz funkcje systemu Windows.
- Zaznacz opcję Microsoft Defender Application Guard i kliknij OK.
- Uruchom ponownie komputer, aby zastosować zmiany.

Virtualization-Based Security (VBS) i Hypervisor-Protected Code Integrity (HVCI)

- Otwórz Ustawienia.
- Przejdź do Aktualizacja i zabezpieczenia.
- Wybierz Windows Security.
- Kliknij Device security.
- Wybierz Core isolation details.
- Włącz Memory integrity.

Windows Information Protection (WIP)

- Wymaga użycia narzędzi zarządzania IT, takich jak Microsoft Intune.
- Skonfiguruj zasady ochrony danych w Intune i przypisz je do odpowiednich urządzeń.

Advanced Threat Protection (ATP)

- Wymaga subskrypcji Microsoft Defender for Endpoint.
- Skonfiguruj ATP za pomocą portalu Microsoft 365 Defender.

Passkeys

- Otwórz Ustawienia.
- Przejdź do Konta.
- Wybierz Opcje logowania.
- Wybierz Klucz bezpieczeństwa i postępuj zgodnie z instrukcjami na ekranie.

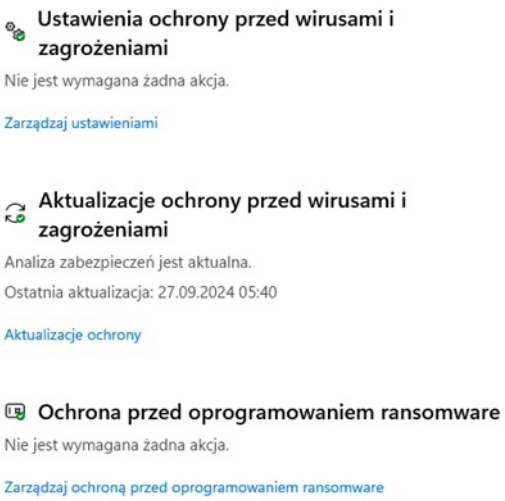
Jak włączyć zabezpieczenia przed niektórymi cyberatakami (np. przed ransomware)

Aby włączyć ochronę przed ransomware w Windows 11 Pro i Education, można skorzystać z funkcji Controlled Folder Access wbudowanej w Microsoft Defender.

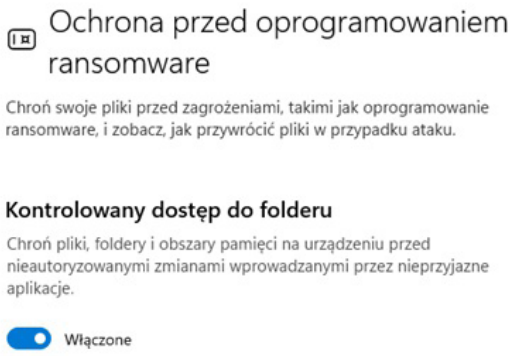
Oto kroki, jak to zrobić:

1. **Otwórz Windows Security:**
   - Kliknij ikonę lupy na pasku zadań i wpisz "Windows Security", a następnie wybierz aplikację z wyników wyszukiwania.

2. **Przejdź do sekcji Virus & threat protection:**
   - W oknie Windows Security kliknij na Virus & threat protection.



3. **Zarządzaj ochroną przed ransomware:**
   - Przewiń w dół do sekcji Ransomware protection i kliknij Manage ransomware protection.
4. **Włącz Controlled Folder Access:**
   - Przełącz przełącznik Controlled folder access na On.



5. **Dodaj chronione foldery:**
   - Kliknij Protected folders, aby dodać dodatkowe foldery, które chcesz chronić przed ransomware. Domyślnie chronione są foldery Dokumenty, Obrazy, Filmy i Pulpit.
6. **Zezwalaj aplikacjom na dostęp do chronionych folderów:**
   - Kliknij Allow an app through Controlled folder access, aby dodać aplikacje, którym ufasz i które mogą mieć dostęp do chronionych folderów. Możesz wybrać aplikacje z listy ostatnio zablokowanych lub przeglądać wszystkie aplikacje.