

Bezpieczeństwo systemu: Defender, zapora, konta

Czas: 2 × 45 min

praca w parach (test reguły portu wymaga drugiego komputera)

Cel: Sprawdzenie i skonfigurowanie podstawowych zabezpieczeń Windows 11: programu Microsoft Defender, zapory, kont i kontroli konta użytkownika, z bezpiecznym testem wykrywania zagrożeń plikiem EICAR.

Po zajęciach potrafisz:

- sprawdza stan ochrony Microsoft Defender i uruchamia skanowanie szybkie, pełne i offline
- konfiguruje ochronę przed naruszeniami i kontrolowany dostęp do folderów
- tworzy regułę zapory blokującą program i port oraz sprawdza jej działanie
- ocenia konta użytkowników, poziom UAC, stan BitLockera i aktualizacji
- bezpiecznie testuje wykrywanie zagrożeń plikiem EICAR

Sprzęt i materiały

- komputer stacjonarny z Windows 11 na drugim dysku (z zadania 13)
- laptop lub komputer sąsiedniej pary do testu zapory

Oprogramowanie

- **Zabezpieczenia Windows / Microsoft Defender (wbudowane)** — opis skanowania Microsoft Defender Offline learn.microsoft.com/pl-pl/defender-endpoint/microsoft-defender-offline
- **Plik testowy EICAR** — nieszkodliwy plik testowy, który programy antywirusowe wykrywają jak wirusa eicar.org/download-anti-malware-testfile
- **Zapora Windows Defender z zabezpieczeniami zaawansowanymi (wf.msc)** — wbudowana

Przygotowanie przed zajęciami

- Przeczytaj na stronie EICAR, czym jest plik testowy i dlaczego jest nieszkodliwy.

Bezpieczeństwo

- Ćwiczenie wykonuj tylko w Windows 11 na drugim dysku. Nie wyłączaj ochrony w szkolnym systemie.
- Do testu antywirusa używaj wyłącznie pliku EICAR. Nigdy nie pobieraj prawdziwego złośliwego oprogramowania „do testów”.
- Nie wyłączaj ochrony w czasie rzeczywistym ani nie dodawaj wykluczeń, aby „przepuścić” plik testowy.
- Skanowanie offline uruchamia ponownie komputer (ok. 15 minut) — zapisz wcześniej wszystkie pliki. Gdy dysk systemowy jest zaszyfrowany BitLockerem, najpierw wstrzymaj ochronę, inaczej system zapyta o klucz odzyskiwania.
- Na koniec usuń utworzone reguły zapory i konta testowe, aby nie zostawić komputera z nietypową konfiguracją.

Przebieg zadania

1 Stan zabezpieczeń

1. Otwórz Zabezpieczenia Windows i zrób zrzut strony „Zabezpieczenia w skrócie”. Zapisz w tabeli stan każdej sekcji (zielony, żółty, czerwony).
2. W Terminalu (administrator) wykonaj `Get-MpComputerStatus | Select-Object AMServiceEnabled, RealTimeProtectionEnabled, IsTamperProtected, AntivirusSignatureLastUpdated` i zapisz wyniki.
3. Zaktualizuj definicje: Ochrona przed wirusami i zagrożeniami → Aktualizacje ochrony → Sprawdź aktualizacje. Uruchom skanowanie szybkie i zanotuj jego czas.
4. Uruchom skanowanie pełne w tle (Opcje skanowania → Pełne skanowanie) — wróć do niego na koniec zajęć.

2 Ochrona przed naruszeniami i ransomware

1. Ochrona przed wirusami i zagrożeniami → Zarządzaj ustawieniami: sprawdź, że „Ochrona przed naruszeniami” jest włączona. Wyjaśnij w sprawozdaniu, przed czym chroni.
2. Ochrona przed oprogramowaniem wymuszającym okup → włącz „Kontrolowany dostęp do folderów”. Sprawdź listę chronionych folderów.
3. Spróbuj zapisać plik w folderze Dokumenty z programu portable spoza systemu (np. zapis raportu z HWINFO lub plik rozpakowany przez 7-Zip). Zapisz, czy zapis został zablokowany i jaki komunikat się pojawił (Historia ochrony).
4. Dodaj ten program do „Zezwalaj aplikacji przez kontrolowany dostęp do folderów” i powtórz zapis. Potem wyłącz kontrolowany dostęp do folderów, jeśli nauczyciel tak zdecyduje.

3 Test EICAR

1. Przy włączonej ochronie pobierz ze strony EICAR plik `eicar.com.txt`. Zapisz, na którym etapie Defender go zatrzymał (przeglądarka, zapis na dysk) i zrób zrzut powiadomienia.
2. Pobierz `eicar.com.zip` i sprawdź, czy Defender wykrywa plik w archiwum.
3. W Historii ochrony odszukaj wykrycia, odczytaj nazwę zagrożenia i podjętą akcję. Usuń wykryte elementy (Akcje → Usuń). Nie przywracaj ich z kwarantanny.

4 Zapora — reguły i test

1. Sprawdź działanie programu: `curl -I https://www.microsoft.com` (powinien zwrócić nagłówki HTTP).
2. W `wf.msc` → Reguły ruchu wychodzącego → Nowa reguła → Program → `%SystemRoot%\System32\curl.exe` → Blokuje połączenie → wszystkie profile → nazwa „Blokada curl – nazwisko”. Powtórz polecenie `curl` i zapisz wynik.
3. Partner sprawdza z drugiego komputera `Test-NetConnection NAZWA-KOMPUTERA -Port 445`. Utwórz regułę ruchu przychodzącego: Port → TCP 445 → Blokuje połączenie. Partner powtarza test — porównajcie wyniki.
4. Wyłącz lub usuń obie reguły i potwierdź, że `curl` znów działa.

5 Konto, UAC, BitLocker, aktualizacje i skanowanie offline

1. Wykonaj `net user` i `net localgroup Administratorzy`. Oceń, czy na komputerze nie ma zbędnych kont administratorów i czy konto Gość jest wyłączone.
2. Sprawdź poziom UAC (`UserAccountControlSettings`), stan BitLockera (`manage-bde -status`) i datę ostatniej aktualizacji (Ustawienia → Windows Update → Historia aktualizacji).
3. Odczytaj wynik pełnego skanowania. Uruchom skanowanie offline (Opcje skanowania → Skanowanie w trybie offline programu Microsoft Defender) (lub `Start-MpWDSscan`) i zanotuj, ile trwało. Wynik sprawdź w Historii ochrony. Jeśli skanowanie nie startuje, sprawdź `reagentc /info` — wymaga włączonego środowiska WinRE.

W sprawozdaniu umieść

- ☐ tabela stanu zabezpieczeń i wynik `Get-MpComputerStatus`
- ☐ opis testu kontrolowanego dostępu do folderów z komunikatem
- ☐ rzuty wykrycia EICAR i wpisu w Historii ochrony
- ☐ opis reguł zapory i wyników testów przed i po ich włączeniu
- ☐ ocena kont, UAC, BitLockera i aktualizacji z zaleceniami
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Czym różni się skanowanie pełne od skanowania offline? Kiedy stosuje się skanowanie offline?
2. Przed czym chroni kontrolowany dostęp do folderów i dlaczego czasem blokuje zwykłe programy?
3. Dlaczego codzienna praca na koncie standardowym zamiast administratora zwiększa bezpieczeństwo?
4. Dlaczego plik EICAR nadaje się do testów, a prawdziwe złośliwe oprogramowanie nie?
5. Czym różni się reguła zapory dla programu od reguły dla portu?

Kryteria oceny

Kryterium	Punkty
Stan zabezpieczeń, aktualizacja i skanowania	4
Ochrona przed naruszeniami i kontrolowany dostęp do folderów	3
Test EICAR z analizą Historii ochrony	3
Reguły zapory i ich test	4
Ocena kont, UAC, BitLockera i aktualizacji	3
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).