

Szyfrowanie dysku BitLocker

Czas: 2 × 45 min

praca indywidualna lub w parach

Cel: Zaszycrowanie BitLockerem dysku danych i partycji systemowej Windows 11, bezpieczne zarządzanie kluczem odzyskiwania oraz zmierzenie wpływu szyfrowania na wydajność dysku i czas uruchamiania.

Po zajęciach potrafisz:

- sprawdza stan TPM i szyfrowania (`tpm.msc` , `manage-bde -status`)
- konfiguruje zasady grupy BitLockera dla komputera z TPM i bez TPM
- szyfruje dysk danych i partycję systemową oraz bezpiecznie zapisuje klucz odzyskiwania
- mierzy wydajność dysku i czas uruchamiania przed szyfrowaniem i po nim
- odszyfrowuje dyski i wyjaśnia, kiedy BitLocker żąda klucza odzyskiwania

Sprzęt i materiały

- komputer stacjonarny z Windows 11 Pro na drugim dysku (z zadania 13)
- pendrive z Ventoy — tylko do zapisania pliku z kluczem odzyskiwania
- stoper (telefon)

Oprogramowanie

- **BitLocker**, `manage-bde` , **Edytor zasad grupy** `gpedit.msc` (**wbudowane w Windows 11 Pro**) — dokumentacja BitLockera
learn.microsoft.com/pl-pl/windows/security/operating-system-security/data-protection/bitlocker
- **CrystalDiskMark** — wersja portable (zip), pomiar przed i po szyfrowaniu
crystalmark.info/en/software/crystaldiskmark

Przygotowanie przed zajęciami

- Sprawdź w zadaniu 6, czy twój komputer ma włączony TPM (fTPM/PTT).
- Upewnij się, że na drugim dysku jest Windows 11 w edycji Pro (`winver`) — w edycji Home BitLocker nie jest dostępny.

Bezpieczeństwo

- Szyfruj wyłącznie Windows 11 na drugim dysku i dysk VHDX. Nigdy nie włączaj BitLockera w szkolnym systemie ani na pendrivie z Ventoy.
- Klucz odzyskiwania zapisz do pliku na pendrivie przed rozpoczęciem szyfrowania i oddaj go nauczycielowi. Bez klucza utrata hasła oznacza bezpowrotną utratę danych.
- Hasła, PIN-u ani klucza odzyskiwania nie wpisuj do sprawozdania, nie fotografuj i nie wysyłaj nikomu. W sprawozdaniu podaj tylko identyfikator klucza (pierwsze 8 znaków).
- Nie wyłączaj komputera w trakcie szyfrowania i odszyfrowywania — proces można przerwać tylko wstrzymaniem w panelu BitLocker.
- Zmiana kolejności rozruchu, aktualizacja UEFI lub reset CMOS przy włączonym BitLockerze mogą wywołać żądanie klucza odzyskiwania — nie zmieniaj ustawień UEFI do czasu odszyfrowania.

Przebieg zadania

1 Stan wyjściowy i pomiary przed

1. Wykonaj `manage-bde -status` i `tpm.msc`. Zapisz, czy dysk C: jest już zaszyfrowany (Windows 11 czasem włącza „Szyfrowanie urządzenia” automatycznie) i czy TPM jest gotowy. Jeśli C: jest już zaszyfrowany, zgłoś to nauczycielowi.
2. Uruchom CrystalDiskMark dla dysku C: (3 przebiegi, 1 GiB). Zrób zrzut wyników.
3. Zmierz stoperem czas uruchamiania: od naciśnięcia przycisku zasilania do pojawienia się pulpitu. Wykonaj 2 pomiary.
4. W Zarządzaniu dyskami utwórz dysk VHDX 2 GB na partycji danych drugiego dysku (Akcja → Utwórz wirtualny dysk twardy), zainicjuj go, sformatuj NTFS i nadaj literę `V:`. Skopiuj na niego kilka plików testowych.

2 Szyfrowanie dysku danych

1. Otwórz Panel sterowania → System i zabezpieczenia → Szyfrowanie dysków funkcją BitLocker. Przy dysku `V:` kliknij „Włącz funkcję BitLocker”.
2. Wybierz odblokowanie hasłem. Klucz odzyskiwania zapisz do pliku na pendrivie (opcja „Zapisz w pliku”).
3. Wybierz „Szyfruj tylko używane miejsce na dysku” i nowy tryb szyfrowania. Po zakończeniu sprawdź `manage-bde -status V:`.
4. Odłącz dysk VHDX (Zarządzanie dyskami → prawy przycisk na dysku → Odłącz wirtualny dysk twardy), podłącz go ponownie dwuklikiem na pliku `.vhdx` i odblokuj hasłem. Zrób zrzut okna z prośbą o hasło.

3 Zasady grupy i szyfrowanie partycji systemowej

1. Uruchom `gpedit.msc` → Konfiguracja komputera → Szablony administracyjne → Składniki systemu Windows → Szyfrowanie dysków funkcją BitLocker → Dyski z systemem operacyjnym → „Wymagaj dodatkowego uwierzytelniania przy uruchamianiu”.
2. Ustaw „Włączone”. Bez TPM: zaznacz „Zezwalaj na używanie funkcji BitLocker bez zgodnego modułu TPM”. Z TPM: w polu konfiguracji numeru PIN uruchomienia modułu TPM wybierz opcję zezwalającą na PIN. Zatwierdź i wykonaj `gpupdate /force`.
3. W panelu BitLocker włącz szyfrowanie dysku C:. Wybierz hasło (bez TPM) albo numer PIN (z TPM). Klucz odzyskiwania zapisz w pliku na pendrivie.
4. Wybierz „Szyfruj tylko używane miejsce na dysku”, nowy tryb szyfrowania, zaznacz „Uruchom sprawdzanie systemu funkcji BitLocker” i uruchom ponownie komputer. Zrób zdjęcie ekranu z prośbą o hasło lub PIN.
5. Obserwuj postęp poleceniem `manage-bde -status C:` (pole „Procent zaszyfrowania”). Zapisz identyfikator klucza odzyskiwania z `manage-bde -protectors -get C:` — tylko pierwsze 8 znaków identyfikatora, nie klucz.

4 Pomiary po i odszyfrowanie

1. Po zakończeniu szyfrowania powtórz CrystalDiskMark dla C: i 2 pomiary czasu uruchamiania (czas wpisywania hasła lub PIN-u zanotuj osobno).
2. Oddaj nauczycielowi pliki z kluczami odzyskiwania (nauczyciel potwierdza odbiór podpisem w sprawozdaniu).
3. Odszyfruj oba dyski: `manage-bde -off C:` i `manage-bde -off V:` (lub „Wyłącz funkcję BitLocker” w panelu). Sprawdź postęp `manage-bde -status`.
4. Po odszyfrowaniu przywróć w `gpedit.msc` ustawienie „Nie skonfigurowano”, odłącz i usuń plik VHDX, usuń plik z kluczem z pendrive'a.

W sprawozdaniu umieść

- ☐ stan wyjściowy: TPM, wynik `manage-bde -status` (bez kluczy)
- ☐ zrzuty ekranu kolejnych etapów (zasady grupy, kreator BitLockera, ekran hasła lub PIN-u przy starcie)
- ☐ tabela CrystalDiskMark przed i po oraz czasy uruchamiania
- ☐ identyfikator klucza (8 znaków) i potwierdzenie nauczyciela, że klucze zostały oddane — bez haseł i kluczy
- ☐ potwierdzenie odszyfrowania (zrzut `manage-bde -status`)
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Do czego służy moduł TPM w BitLockerze i co zmienia dodanie PIN-u?
2. W jakich sytuacjach BitLocker zażąda klucza odzyskiwania?
3. Dlaczego klucza odzyskiwania nie wolno przechowywać na zaszyfrowanym dysku ani wpisywać do sprawozdania?
4. Czym różni się szyfrowanie „tylko używanego miejsca” od szyfrowania całego dysku? Kiedy wybrać drugą opcję?
5. Czy BitLocker chroni dane przed złośliwym oprogramowaniem działającym w uruchomionym systemie? Uzasadnij.

Kryteria oceny

Kryterium	Punkty
Pomiary przed i po szyfrowaniu z porównaniem	4
Szyfrowanie dysku danych VHDX i test odblokowania	3
Zasady grupy i szyfrowanie partycji systemowej z uwierzytelnianiem przy starcie	5
Prawidłowe postępowanie z kluczem odzyskiwania i odszyfrowanie	4
Odpowiedzi na pytania kontrolne	4
Razem	20

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