

Projekt końcowy cz. 2: wdrożenie, testy i dokumentacja

Czas: 2 × 45 min

praca w parach (te same pary co w zadaniu 33)

Cel: Dokończenie wdrożenia stanowiska z zadania 33: kopia zapasowa, zabezpieczenia, testy akceptacyjne, dokumentacja dla użytkownika i przekazanie rozwiązania klientowi.

Po zajęciach potrafisz:

- konfiguruje i sprawdza kopię zapasową z odtworzeniem pliku
- zabezpiecza stanowisko zgodnie z wymaganiami klienta
- przeprowadza testy akceptacyjne na podstawie listy wymagań
- pisze zwięzłą instrukcję dla użytkownika i protokół odbioru
- prezentuje rozwiązanie w 5 minut i odpowiada na pytania

Sprzęt i materiały

- komputer stacjonarny z systemem zainstalowanym w zadaniu 33 na drugim dysku
- nośnik lub udział na kopię zapasową (pendrive, drugi wolumin albo udział na serwerze szkolnym — ścieżkę podaje nauczyciel)
- rzutnik lub ekran do prezentacji

Oprogramowanie

- **Narzędzia kopii zapasowej** — Windows: Historia plików / Kopia zapasowa systemu Windows; Linux: np. `rsync` lub Déjà Dup — zgodnie z zadaniem 14
- **Zabezpieczenia Windows i BitLocker** — BitLocker tylko w Windows 11 Pro/Education/Enterprise
learn.microsoft.com/windows/security/operating-system-security/data-protection/bitlocker
- **Edytor tekstu i program do prezentacji** — LibreOffice lub pakiet szkolny
libreoffice.org/download/download-libreoffice

Przygotowanie przed zajęciami

- Przejrzyj tabelę wymagań z zadania 33 — wypisz wymagania oznaczone „zad. 34”.
- Przygotuj szkic prezentacji (4–6 slajdów): klient i wymagania, rozwiązanie, koszt, testy, wnioski.

Bezpieczeństwo

- Pracuj nadal tylko na drugim dysku — sprawdź po uruchomieniu, że to system z zadania 33.
- Klucz odzyskiwania BitLocker zapisz w pliku na nośniku wskazanym przez nauczyciela (lub wydrukuj) — nie zapisuj go na szyfrowanym dysku ani w sprawozdaniu publicznym.
- Kopia zapasowa na udziale szkolnym nie może zawierać danych osobowych — używaj fikcyjnych plików klienta.
- W instrukcji dla użytkownika nie podawaj haseł; opisz tylko, jak je zmienić.

Przebieg zadania

1 Kopia zapasowa

1. Skonfiguruj kopię danych użytkownika zgodnie z wymaganiami (co, gdzie, jak często). Zapisz konfigurację w dzienniku projektu.
2. Wykonaj pierwszą kopię, usuń jeden plik testowy i odtwórz go z kopii. Zrób zrzut odtworzenia.
3. Opisz, jak rozwiązanie realizuje (lub nie) zasadę 3-2-1 i co klient powinien dokupić lub robić samodzielnie.

2 Zabezpieczenia

Tylko te, które wynikają z wymagań i rodzaju stanowiska.

1. Sprawdź aktualizacje, ochronę antywirusową i zaporę (Windows: Zabezpieczenia Windows; Linux: `sudo apt update && sudo apt upgrade`, `sudo ufw status`).
2. Sprawdź, że użytkownik pracuje na koncie standardowym, a konto administratora ma silne hasło.
3. Wdróż pozostałe zabezpieczenia z wymagań (np. BitLocker, blokada nośników USB, ograniczenia zasadami grupy, logowanie SSH kluczem).

3 Testy akceptacyjne i dokumentacja

1. Przygotuj listę kontrolną testów: dla każdego wymagania W1, W2... opis testu i oczekiwany wynik.
2. Wykonaj testy na koncie użytkownika (nie administratora) i zapisz wynik: spełnione / niespełnione / uwagi.
3. Każdy niespełniony test popraw i powtórz; zapisz w dzienniku, co zmieniłeś.
4. Napisz instrukcję dla użytkownika (1–2 strony): logowanie, gdzie zapisywać pliki, jak działa kopia, co zrobić w razie problemu, kontakt do serwisu. Pisz prostym językiem.
5. Wypełnij protokół odbioru i przekaz go klientowi (nauczycielowi) do podpisu.

4 Prezentacja

5 minut na parę, potem 1–2 pytania z sali.

1. Przećwicz prezentację w parze z zegarem — zmieść się w 5 minutach.
2. Przedstaw: zlecenie i wymagania, wybrane rozwiązanie, koszt, wyniki testów, problemy i ich rozwiązania.
3. Pokaż na żywo jedną funkcję stanowiska (np. odtworzenie pliku z kopii).
4. Odpowiedz na pytania i zanotuj uwagi klasy oraz nauczyciela.

W sprawozdaniu umieść

- ☐ konfiguracja kopii zapasowej i zrzut odtworzenia pliku
- ☐ lista wdrożonych zabezpieczeń
- ☐ lista kontrolna testów akceptacyjnych z wynikami
- ☐ instrukcja dla użytkownika (1–2 strony) jako załącznik
- ☐ podpisany protokół odbioru i plik prezentacji
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego testy akceptacyjne wykonuje się na koncie użytkownika, a nie administratora?
2. Kopia zapasowa „działa”, ale nikt nie próbował odtworzyć danych. Jakie jest ryzyko?
3. Co powinien zawierać protokół odbioru i do czego przyda się firmie serwisowej w przypadku reklamacji?

4. Które z wdrożonych zabezpieczeń najbardziej utrudni codzienną pracę klienta i jak to wyjaśnisz klientowi?

Kryteria oceny

Kryterium	Punkty
Kopia zapasowa z udanym odtworzeniem	3
Zabezpieczenia zgodne z wymaganiami	3
Lista kontrolna i rzetelne testy akceptacyjne	4
Instrukcja dla użytkownika i protokół odbioru	4
Prezentacja i odpowiedzi na pytania z sali	3
Odpowiedzi na pytania kontrolne	3
Razem	20

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