Bezpieczeństwo systemów operacyjnych

Głównym celem zajęć powinno być zapoznanie studenta w jaki sposób można zwiększyć bezpieczeństwo systemów operacyjnych Windows, Linux oraz Mac OS, czyli w jaki sposób można „utwardzać" (ang. hardening) systemy operacyjne.

W tym celu student powinien zostać zaznajomiony z:

- atakami cybernetycznymi wykorzystującymi słabości systemów operacyjnych,
- polityką Zero Trust, która ma pomagać w walce z tymi atakami,
- źródłami, w których można znaleźć informacje o podatnościach,
- mechanizmami dostępnymi w systemach operacyjnych pozwalającymi na zwiększenie bezpieczeństwa użytkownika i jego danych, takimi jak:
    - bezpieczny rozruch,
    - możliwość ustawiania haseł wymaganych podczas rozruchu systemu oraz aktualizacji BIOS-u,
    - autentykacja i uwierzytelnianie użytkowników (wymuszanie silnych haseł, MFA),
    - zabezpieczenie konta administratora,
    - nadawanie ograniczonego zestawu uprawnień do zasobów użytkownikom,
    - wykonywanie aktualizacji systemowych i oprogramowania,
    - wyłączenie zbędnych usług oraz protokołów,
    - zablokowanie nieużywanych portów,
    - odinstalowanie zbędnych programów,
    - zmiana domyślnych poświadczeń,
    - zapewnienie ochrony danych w spoczynku i w transmisji (szyfrowanie danych w spoczynku i transmisji, użycie programów antywirusowych, firewalli),
    - stosowanie zasady grupy (GPO) wymuszające stosowanie odpowiednich reguł bezpieczeństwa systemu operacyjnego na wszystkich urządzeniach w firmie.

Student powinien poznać narzędzia:

- wspierające testowanie bezpieczeństwa konfiguracji systemu operacyjnego oraz usług w nim działających (np. Lynis dla systemu Linux oraz Mac OS, OpenSCAP dla systemu Windows),
- pozwalające wykrywać zagrożenia i je blokować (znać różnicę pomiędzy pojęciami IPS, IDS oraz SIEM).

Sugerowana literatura:

1. Mark Dunkerley, Matt Tumbarello, Mastering Windows Harderning. Second edition. Pact Publishing, 2022

2. Donald A. Tevault, Mastering Linux Security and Hardening, Pact Publishing, 2018