Wykaz zagrożeń dla zasobów IT w Akademii Łomżyńskiej

1. Zagrożenia związane z oprogramowaniem

    a. Złośliwe oprogramowanie: wirusy, robaki, konie trojańskie, oprogramowanie szpiegujące (spyware) i inne szkodliwe oprogramowanie.
    b. Błędy w oprogramowaniu: stare wersje oprogramowania, luki w oprogramowaniu, które mogą być wykorzystywane przez cyberprzestępców do ataków.

2. Zagrożenia związane z celowym przestępczym działaniem.

    a. Atak typu DoS: działania mające na celu blokowanie użytkownikom dostępu do systemów lub danych poprzez zalewanie zapytaniami i generowaniem nadmiernego obciążenia.
    b. Atak typu „spoofing" lub „phishing": działania polegające na podszywaniu się pod inną osobę, firmę lub instytucję w celu wyłudzenia poufnych informacji, takich jak dane logowania, dane finansowe lub zainstalowania złośliwego oprogramowania
    c. Atak sieciowy: działania mające na celu uzyskanie nieautoryzowanego dostępu do systemu lub zablokowanie dostępu do danych np. testowanie haseł, wyszukiwanie podatności.

3. Zagrożenia związane z danymi

    a. Nieautoryzowany dostęp do systemów lub danych: dostęp do danych osób nie posiadających stosownych upoważnień.
    b. Ujawnienie/wyciek danych: sytuacja, w której dane znalazły się w posiadaniu osób nieuprawnionych.
    c. Uszkodzenie danych: sytuacja, w której dane zostały usunięte, nieczytelne uszkodzone lub sfałszowane

4. Zagrożenia fizyczne

    a. Kradzież,
    b. Powódź, pożar lub katastrofa budowlana,
    c. Awarie sprzętowe: awaria urządzenia lub podzespołu.
    d. Zagrożenie środowiskowe: zbyt wysoka lub niska temperatura, zbyt wysoka lub niska wilgotność powietrza mogące wpłynąć na poprawność funkcjonowania urządzeń.
    e. Awarie zasilania: brak zasilania, niestabilne parametry zasilania zbyt niskie lub wysokie napięcie itp.