

Aktywa	Przykładowa podatność	Zagrożenie
Personel	Niewystarczająca obsada stanowisk. Utrata kluczowego pracownika.	Nieobecność pracownika – brak ciągłości działania
	Praca obcego personelu bez odpowiedniego nadzoru	Kradzież, kopiowanie lub inny nieuprawniony dostęp do informacji
	Niewystarczające przeszkolenie	Błędy związane z obsługą
	Niewłaściwe wykorzystanie sprzętu lub oprogramowania	Awaria sprzętu, trwała utrata danych.
	Brak zasad korzystania z urządzeń teleinformatycznych, brak procedur, brak kontroli.	Wykorzystanie urządzeń w sposób nieautoryzowany np.: przesyłanie wiadomości z danymi poufnymi przez e-mail z prywatnej strony WWW
	Brak komunikacji pomiędzy pracownikami i wydziałem	Niewłaściwe wykonywanie działań, opóźnienia w realizacji zadań
	Brak świadomości pracowników o wynikającym z tego zagrożeniu, brak szkoleń.	Plotkarstwo. Nieumyślne przekazywanie poufnych informacji.
Otoczenie fizyczne i infrastruktura	Niewłaściwa ochrona fizyczna budynku, pomieszczeń, drzwi i okien	Kradzież
	Niewłaściwa lub niedbała kontrola dostępu do budynku i pomieszczeń	Nieuprawniony dostęp osób trzecich np. celowe uszkodzenie.
	Lokalizacja budynku, niewłaściwy dobór pomieszczeń, brak klimatyzacji	Zawilgocenie
	Brak stałej konserwacji	Awaria systemu alarmowego. Awaria systemu kontroli dostępu.
	Brak procedur regulujących bezpieczeństwo aktywów	Utrata danych, Niezgodność z przepisami prawa, Nieautoryzowany dostęp
Sprzęt	Brak planu wymiany zużywających się części, zła obsługa, sprzęt niskiej jakości	Uszkodzenie urządzenia, wygaśnięcie wsparcia producenta.
	Niewłaściwa obsługa lub błędna instalacja urządzeń, błędnie napisana instrukcja, brak przeszkolenia pracowników. Użytkowanie sieci napięcia niezgodnie z przeznaczeniem.	Uszkodzenie urządzenia podczas obsługi
	Brak lub niewłaściwa kontrola zmian, błędnie napisana instrukcja, brak przeszkolenia pracowników	Błędy pracowników obsługujących klientów
	Brak stosownych procedur	Utrata nośnika z informacją, utrata laptopa
	Niezabezpieczone urządzenie do przechowywania danych	Kradzież danych lub dokumentów
	Brak procedur niszczenia nośników. Brak przestrzegania procedur.	Nieuprawniony dostęp do danych.
	Brak planów okresowej wymiany sprzętu.	Awaria urządzenia.
Teleinformatyka	Wilgotność, zalanie z rur C.O., podwyższenie temperatury, pożar (brak czujników temperatury, zalania i dymu), niezabezpieczone okno	Uszkodzenie lub unieruchomienie serwera
	Brak kopii zapasowych lub kopie zapasowe przechowywane w tym samym pomieszczeniu lub na tym samym serwerze	Oprogramowanie szkodliwe, siły wyższe, częściowe lub całkowite zniszczenie informacji
	Zmiana przeznaczenia lub likwidacja nośników pamięciowych bez trwałego usunięcia z nich poprzednich informacji wrażliwych	Nieautoryzowane przekazanie dostępu do informacji
	Przekazywanie haseł pracownikom, przesyłanie tekstem jawnym	Nieautoryzowany dostęp do informacji

	Brak stosowania polityki czystego pulpitu Komputera	Pobranie plików i informacji z pulpitu
Dokumentacja	Przechowywanie bez właściwej ochrony, Kopiowanie bez kontroli, Brak należytej uwagi ze strony użytkującego	Kradzież
	Pozostawione bez kontroli i nadzoru dokumenty w drukarkach lokalnych i sieciowych, faxach, kserokopiarkach; dokumenty wyrzucane do koszy na śmieci, brak niszczonek, bałagan na biurku,	Dostęp osoby niepowołanej do dokumentacji, zgubienie dokumentów.
	Bałagan na biurku, pozostawianie w biurach dokumentów niezabezpieczonych, przeznaczonych do archiwizacji.	Dostęp do dokumentów archiwalnych lub ich zniszczenie przez osoby nieuprawnione.
	Przestarzała instalacja elektryczna w pomieszczeniach biurowych	Pożar
	Przestarzała instalacji wodna i c.o. w pomieszczeniach	Zalanie archiwum
	Brak wylogowywania przy opuszczaniu stacji roboczej	Nieuprawniony dostęp do danych