SZACOWANIE RYZYKA
dla bezpieczeństwa informacji

Podatności mogące prowadzić do wystąpienia ryzyk dla bezpieczeństwa informacji w Urzędzie Gminy i Miasta w Gryfowie Śląskim (1 – niskie, 2 – średnie, 3 – wysokie):

1. Wprowadzenie kodu złośliwego – sieć LAN

Lp.	Ryzyko	Podatność
1.	1	Złe umiejscowienie w systemie lub brak aktualizacji bądź brak oprogramowania typu AV.
2.	1	Brak lub niewłaściwe umiejscowienie w topologii sieci bądź zła konfiguracja zapór sieciowych.
3.	1	Brak lub niewłaściwe umiejscowienie w topologii sieci bądź zła konfiguracja oprogramowania typu IPS/IDS.
4.	1	Niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach LAN.

2. Wniknięcie kodu złośliwego – sieć WAN

Lp.	Ryzyko	Podatność
1.	1	Złe umiejscowienie w systemie lub brak aktualizacji bądź brak oprogramowania typu AV.
2.	1	Brak lub niewłaściwe umiejscowienie w topologii sieci bądź zła konfiguracja zapór sieciowych.
3.	1	Brak lub niewłaściwe umiejscowienie w topologii sieci bądź zła konfiguracja oprogramowania typu IPS/IDS.
4.	1	Niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach WAN.
5.	1	Nie monitorowanie bieżącego obciążenia serwerów.
6.	1	Podatność użytkowników systemu na oddziaływanie metod inżynierii społecznej, mającej na celu uzyskania informacji lub wprowadzenia złośliwego kodu.

3. Nieautoryzowany dostęp do informacji

Lp.	Ryzyko-	Podatność
1.	1	Brak nadzoru nad uprawnieniami użytkowników.
2.	1	Nadane uprawnienia nieadekwatne do wykonywanych zadań.
3.	1	Brak wnoszenia zmian uprawnień użytkowników.
4.	1	Brak kontroli fizycznego dostępu do elementów systemu.

4. Zagrożenie atakiem DDoS lub DoS

Lp.	Ryzyko	Podatność
1.	1	Brak nadzoru nad ruchem w sieci.
2.	1	Występowanie błędu oprogramowania.
3.	1	Wykorzystywanie przestarzałego sprzętu do obsługi systemu.
4.	1	Brak działań w celu wymiany sprzętu na nowocześniejszy.
5.	1	Brak monitorowania obciążenia serwerów.
6.	1	Brak lub niewłaściwe umiejscowienie w topologii sieci bądź zła konfiguracja oprogramowania.
7.	1	Brak lub niewłaściwe umiejscowienie w topologii sieci bądź zła konfiguracja zapór sieciowych.

5. Podsłuch/przechwyt danych

Lp.	Ryzyko	Podatność
1.	1	Brak nadzoru nad ruchem w sieci.
2.	1	Brak szyfrowania w łączach WAN.
3.	1	Podsłuch informacji w sieci wewnętrznej LAN.
4.	1	Pozyskiwanie informacji z nośników danych wycofanych z użycia.

6. Służbowe telefony komórkowe

Lp.	Ryzyko	Podatność
1.	2	Zagubienie telefonu komórkowego.
2.	2	Kradzież telefonu komórkowego.
3.	2	Zniszczenie telefonu komórkowego.
4.	1	Pozyskanie poufnych informacji wyświetlanych na ekranie.
5.	1	Pobranie aplikacji zawierającej złośliwy kod.
6.	2	Korzystanie z niezabezpieczonej sieci WIFI.

7. Rozmowy telefoniczne

Lp.	Ryzyko	Podatność
1.	1	Przekazanie informacji poufnej w trakcie rozmowy telefonicznej.
2.	1	Dokonanie określonej przez rozmówcę czynności wywołującej szkodę.

8. Kontakt drogą e-mail

Lp.	Ryzyko	Podatność
1.	1	Dokonanie w treści podejrzanej wiadomości, określonej przez adresata czynności.

Zabezpieczenia możliwe dla zastosowania w celu minimalizacji ryzyk dla bezpieczeństwa informacji w Urzędzie Gminy i Miasta w Gryfowie Śląskim:

1. Wprowadzenie kodu złośliwego – sieć LAN

Lp.	Działanie zabezpieczające	
1.	Blokowanie portów USB na stacjach roboczych.	-
2.	Nadzór nad niewykorzystywanymi zakończeniami sieci LAN.	+
3.	Autoryzacja dostępu do serwera.	+
4.	Zastosowanie oprogramowania klasy AV na stacjach roboczych.	+
5.	Blokowanie możliwości instalowania oprogramowania przez użytkownika.	+
6.	Weryfikacja zainstalowanego oprogramowania na stacjach roboczych.	+

2. Wniknięcie kodu złośliwego – sieć WAN

Lp.	Działanie zabezpieczające	
1.	Translacja adresów sieciowych.	-
2.	Oprogramowanie klasy AV na styku sieci WAN z LAN.	+
3.	Systemy klasy IDS/IPS.	+
4.	Zastosowanie serwerów PROXY.	-
5.	Wykrywanie oraz blokowanie spamu.	+
6.	Budowanie topologii sieci z uwzględnieniem obszarów bezpiecznych.	+

3. Nieautoryzowany dostęp do informacji

Lp.	Działanie zabezpieczające	
1.	Procedury nadawania i odbierania uprawnień w systemie.	+
2.	Procedury przeglądania uprawnień w systemach.	+
3.	Rozpraszanie uprawnień.	+

4. Zagrożenie atakiem DDoS lub DoS

Lp.	Działanie zabezpieczające	
1.	Stosowanie techniki rozpraszania danych.	+
2.	Przejście na statyczne wersje serwisu po wykryciu ataku typu DDoS/DoS.	+
3.	Blokowanie ruchu sieciowego z określonych adresów IP.	+
4.	Monitorowanie ruchu w sieci.	+

5. Podsłuch/przechwyt danych

Lp.	Działanie zabezpieczające	
1.	Stosowanie urządzeń o obniżonej emisji ujawniającej.	-
2.	Prowadzenie okablowania sieciowego w zamkniętych kanałach.	+
3.	Nadzór nad niewykorzystywanymi zakończeniami sieci LAN.	+
4.	Stosowanie strefowania.	-

6. Służbowe telefony komórkowe

Lp.	Działanie zabezpieczające	
1.	Stosowanie blokady telefonu przy pomocy hasła.	+
2.	Stosowanie blokady telefonu przy pomocy hasła oraz	-
3.	Tworzenie kopii zapasowych.	+
4.	Czasowa blokada wyświetlacza.	+
5.	Pobieranie zweryfikowanych aplikacji z zaufanych źródeł.	+
6.	Korzystanie z zweryfikowanych, zaufanych sieci WIFI.	+

7. Rozmowy telefoniczne

Lp.	Działanie zabezpieczające	
1.	Przeprowadzanie testów socjotechnicznych oraz szkoleń pracowników.	+

8. Kontakt drogą e-mail

Lp.	Działanie zabezpieczające	
1.	Przeprowadzanie testów socjotechnicznych oraz szkoleń pracowników.	+