Analiza ryzyka bezpieczeństwa informacji oraz plan postępowania z ryzykiem

1. Cel dokumentu

Celem niniejszego dokumentu jest identyfikacja, analiza oraz ocena ryzyk związanych z bezpieczeństwem informacji w Instytucie oraz określenie sposobu postępowania z tymi ryzykami. Dokument ten wspiera zgodność z wymaganiami prawnymi, takimi jak RODO, KRI, ISO/IEC 27001 oraz polityką bezpieczeństwa informacji obowiązującą w Instytucie.

2. Zakres stosowania

Analiza obejmuje wszystkie kluczowe zasoby informacyjne Instytutu, systemy informatyczne, procesy przetwarzania danych oraz personel mający dostęp do informacji i systemów. Dokument ma zastosowanie do całego Instytutu.

3. Metodyka analizy ryzyka

Analiza ryzyka została przeprowadzona w oparciu o metodykę szacowania ryzyka zgodną z normą ISO/IEC 27005. Proces obejmuje następujące etapy:

- Identyfikacja zasobów
- Identyfikacja zagrożeń i podatności
- Ocena skutków i prawdopodobieństwa
- Określenie poziomu ryzyka
- Planowanie działań zaradczych
- Akceptacja ryzyka lub podjęcie działań minimalizujących

4. Identyfikacja i ocena ryzyk

Poniżej przedstawiono przykładowe ryzyka zidentyfikowane w Instytucie wraz z oceną skutków i prawdopodobieństwa:

- Zasób: System e-mail
- Zagrożenie: Phishing
- Skutek: Ujawnienie danych osobowych
- Prawdopodobieństwo: Średnie
- Skutki: Wysokie
- Poziom ryzyka: Wysokie
- Działania: Szkolenia, filtr antyphishingowy, MFA

Sporządził: J. Maciejski, dnia 12-12-2024

5. Plan postępowania z ryzykiem

Dla każdego ryzyka określono sposób postępowania:
- Akceptacja ryzyka: np. niskie ryzyko z niewielkimi skutkami.
- Minimalizacja: wdrażanie środków ochronnych (technicznych, organizacyjnych).
- Transfer: np. ubezpieczenie, outsourcing.
- Unikanie: rezygnacja z procesu, który generuje wysokie ryzyko.

6. Kategoria zagrożeń

Wyróżnia się następujące kategorie zagrożeń w interakcji systemu teleinformatycznego i cyberprzestrzeni oraz przykładowych podatności powodujących, że materializacja zagrożenia będzie miała oddziaływanie na zasób informacyjny lub system teleinformatyczny:

Lp.	Podatności
1. Kategoria zagrożenia: Wniknięcie kodu złośliwego z sieci WAN	
1	brak lub złe umiejscowienie w systemie, lub brak aktualizacji oprogramowania typu AV
2	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)
3	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS ijego sond
4	niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach WAN
5	brak monitorowania obciążenia serwerów
6	podatność użytkowników na oddziaływanie metod inżynierii społecznej w celu uzyskania informacji lub wprowadzenia kodu złośliwego
2. Kategoria zagrożenia: Wprowadzenie kodu złośliwego z sieci LAN	
1	brak lub złe umiejscowienie w systemie, lub brak aktualizacji oprogramowania typu AV
2	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)
3	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond
4	niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach LAN
3. Kategoria zagrożenia: Atak typu DDoS lub DoS	
1	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)
2	brak, niewłaściwe umiejscowienie w topologii SIeCI lub zła konfiguracja oprogramowania IPS/IDS i jego sond
3	brak nadzoru nad ruchem w sieci (QoS)
4	brak monitorowania obciążenia serwerów
5	błąd oprogramowania
6	utrata dostępu do usług sieci WAN (w tym Internetu) w wyniku ataku na komponenty sieci WAN
7	Wykorzystywanie do obsługi systemu przestarzałego sprzętu
8	Nie podejmowanie działań w celu wymiany sprzętu na nowocześn iejszy (zapewniający wsparcie techniczne)
4. Kategoria zagrożenia: Nieautoryzowany dostęp do informacji	
1	brak nadzoru nad uprawnieniami użytkowników, uprawnienia nieadekwatne do zadań
2	zbyt wolne wnoszenie zmian uprawnień użytkowników
3	brak kontroli dostępu fizycznego do elementów system
5. Kategoria zagrożenia: Nieumiejętne posługiwanie się systemem przez użytkownika	
1	brak właściwych szkoleń użytkowników w zakresie użycia systemu
2	brak kontroli jakości danych wprowadzanych do systemu

Sporządził: J. Maciejski, dnia 12-12-2024

3	odzyskanie informacji z nośników wycofanych z użycia
4	podatność użytkowników na oddziaływanie metod inżynierii społecznej w celu uzyskania informacji **lub** wprowadzenia kodu złośliwego.
6. Kategoria zagrożenia: Przełamanie zabezpieczeń dostępu wewnątrz systemu	
1	brak nadzoru nad uprawnieniami użytkowników, uprawnienia nieadekwatne do zadań (np. możliwość instalacji programów, w tym służącym przełamaniu zabezpieczeń)
2	zbyt wolne wnoszenie zmian uprawnień użytkowników
3	brak nadzoru nad aktywnością użytkowników w systemie
4	brak **lub** złe umiejscowienie w systemie, **lub** brak aktualizacji oprogramowania typu AV
5	brak, niewłaściwe umiejscowienie w topologii sieci **lub** zła konfiguracja zapór sieciowych (firewall)
6	brak, niewłaściwe umiejscowienie w topologii sieci **lub** zła konfiguracja oprogramowania IPS/IDS i jego sond
7. Kategoria zagrożenia: Podsłuch danych, przechwyt danych	
1	brak nadzoru nad ruchem w sieci (QoS)
2	emisja ujawniająca
3	brak szyfrowania w łączach WAN
4	podsłuch informacji w sieci wewnętrznej (LAN)
5	pozyskanie informacji z nośników wycofanych z użycia
8. Kategoria zagrożenia: Włamanie do systemu teleinformatycznego z sieci zewnętrznej WAN (przełamanie zabezpieczeń)	
1	brak aktualizacji oprogramowania systemowego
2	brak, niewłaściwe umiejscowienie w topologii sieci **lub** zła konfiguracja zapór sieciowych (firewall)
3	brak, niewłaściwe umiejscowienie w topologii sieci **lub** zła konfiguracja oprogramowania IPS/IDS i jego sond
4	brak nadzoru nad ruchem w sieci (QoS)
5	brak monitorowania obciążenia serwerów
6	podatność użytkowników na oddziaływanie metod inżynierii społecznej w celu uzyskania informacji **lub** wprowadzenia kodu złośliwego
9. Kategoria zagrożenia: System podmiotu (urzędu) źródłem zakłóceń w **cyberprzestrzeni**	
1	brak nadzoru nad ruchem w sieci (QoS)
2	brak **lub** złe umiejscowienie w systemie, **lub** brak aktualizacji oprogramowania typu AV
3	brak, niewłaściwe umiejscowienie w topologii sieci **lub** zła konfiguracja zapór sieciowych (firewall)
4	brak, niewłaściwe umiejscowienie w topologii sieci **lub** zła konfiguracja oprogramowania IPS/IDS i jego sond

6. Monitorowanie i przegląd

Analiza ryzyka podlega przeglądowi co najmniej raz w roku lub po wystąpieniu istotnych zmian w środowisku informacyjnym Instytutu. Za przegląd i aktualizację odpowiada wyznaczony Koordynator ds. bezpieczeństwa informacji.

Sporządził: J. Maciejski, dnia 12-12-2024

DYREKTOR
Prof. dr hab. Mariusz K. Piskuła
czł. koresp. PAN