XXIII Międzynarodowy Kongres Otwartego Systemu Ochrony Zdrowia

Jak opracować skuteczną strategię ochrony danych osobowych w podmiotach leczniczych – analiza ryzyka i praktyczne wskazówki w zakresie doboru zabezpieczeń.

Katowice 2018/04/24

Centrum Systemów Informacyjnych
Ochrony Zdrowia

RODO - ewolucja czy rewolucja ?

UODO

Art. 7.

Ilekroć w ustawie jest mowa o:

zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

Art. 36.

1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

RODO

Artykuł 24 **Obowiązki administratora**

1.Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2.Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów rozporządzenia. Aby móc wykazać przestrzeganie rozporządzenia, administrator powinien przeprowadzić ocenę skutków dla ochrony danych - analizę ryzyka przetwarzania danych pod kątem zidentyfikowanych podatności i przyczyn związanych z powstawaniem incydentów bezpieczeństwa w zakresie przetwarzania danych osobowych szczególnej kategorii.

Zarządzanie ochroną danych osobowych oparte na ryzyku ma na celu:

a) zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

b) definiowanie i wdrażanie odpowiednich środków technicznych i organizacyjnych, zapewniający adekwatny stopień bezpieczeństwa odpowiadający ryzyku;

c) ocenę czy stopień bezpieczeństwa jest odpowiedni, uwzględniając ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Zgodnie z dobrymi praktykami oraz opinią Grupy Roboczej ds. Ochrony danych 29 14/EN WP 218, zaleca się by zarządzanie ryzykiem w ochronie danych osobowych zapewniało:

a) zidentyfikowanie operacji przetwarzania danych osobowych o wysokim ryzyku naruszenia praw lub wolności osób fizycznych;

b) oszacowanie ryzyka z punktu widzenia operacji przetwarzania tzn. czy są niezbędne oraz proporcjonalne w stosunku do celów przetwarzania;

c) oszacowanie ryzyka z punktu widzenia ich skutków urzeczywistnienia ryzyka naruszenia praw lub wolności osób fizycznych oraz prawdopodobieństwa ich wystąpienia;

d) postępowanie z ryzykiem w celu zredukowania ryzyka;

e) informowanie o ryzyku interesariuszy i konsultacje eksperckie;

monitorowanie i przegląd ryzyka oraz procesu zarządzania ryzykiem.

Aby poprawić przestrzeganie RODO, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy zobowiązać administratora do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka.

Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem.

Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, **którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia,** przed przetwarzaniem należy skonsultować się z organem nadzorczym.

W przypadkach, w których nie jest jasne, czy wymagane jest przeprowadzenie oceny skutków dla ochrony danych, zaleca się jednak przeprowadzenie tej oceny, ponieważ stanowi ona narzędzie ułatwiające administratorowi przestrzeganie przepisów o ochronie danych.

Niespełnienia warunków nakładających obowiązek przeprowadzenia oceny skutków dla ochrony danych nie zmniejsza jednak ogólnego obowiązku wdrożenia przez administratorów środków umożliwiających odpowiednie zarządzanie ryzykiem naruszenia prawa i wolności osób, których dane dotyczą

Oceny skutków dla ochrony danych może być przeprowadzona przez inny podmiot wybrany przez Administratora danych, jednak ostateczną odpowiedzialność za wykonanie tego zadania odpowiada Administrator danych.

Jeżeli proces przetwarzania jest całkowicie lub częściowo realizowany przez podmiot przetwarzający dane, podmiot przetwarzający na mocy umowy powierzenia pomaga administratorowi danych w przeprowadzeniu oceny skutków dla ochrony danych i dostarcza wszelkich niezbędnych informacji.

Grupy danych chronionych:

- Dane osobowe pracowników medycznych
- Dane osobowe usługodawców
- Dane osobowe usługobiorców (bez danych medycznych)
- Jednostkowe dane medyczne
- Dane uwierzytelniające użytkowników
- Dane uwierzytelniające administratorów biznesowych
- Dane uwierzytelniające administratorów technicznych
- Materiał kryptograficzny
- Dane uwierzytelniające i autoryzacyjne: silniki bazodanowe, systemy operacyjne (maszyn fizycznych i wirtualnych), serwery aplikacji

Procesy operacyjne - obsługa pacjentów

- profilaktyki zdrowotnej
- medycyny pracy, w tym oceny zdolności pracownika do pracy
- diagnozy medycznej i leczenia
- zapewnienia opieki zdrowotnej oraz zarządzania systemami i usługami opieki zdrowotnej – opieka szpitalna
- zapewnienia opieki zdrowotnej oraz zarządzania systemami i usługami opieki zdrowotnej – opieka ambulatoryjna
- zapewnienia zabezpieczenia społecznego oraz zarządzania systemami i usługami zabezpieczenia społecznego
- Przetwarzanie danych w celach marketingowych
- Przetwarzanie danych w celach prowadzenia badań klinicznych
- Przetwarzanie w celach profilowania i automatycznego podejmowania decyzji

Procesy wspomagające

- kadry – przetwarzanie w celach rekrutacyjnych, zatrudnienia pracownika
- księgowość – przetwarzanie w celach zarządzania finansowego jednostką
- ochrona fizyczna - Przetwarzanie w celach zapewnienie bezpieczeństwa osób, danych i mienia w obszarze objętym ochroną fizyczną
- IT - Przetwarzanie w celach zapewnienie ciągłości działania oraz bezpieczeństwa danych
- Monitoring wizyjny - Przetwarzanie w celach zapewnienie bezpieczeństwa osób, danych i mienia w obszarze objętym monitoringiem

Zagrożenia i podatności

Zagrożenia i podatności uzależnione są kontekstu organizacyjnego podmiotu i między innymi mogą dotyczyć:

- Organizacja
- Personel
- Lokalizacja
- Sprzęt i nośniki
- Oprogramowanie i sieć

Zagrożenia i podatności

- Uwierzytelnienie użytkowników w systemach teleinformatycznych
- Nieuprawniony dostęp przez użytkowników
- Nieuprawniony dostęp przez osoby z zewnątrz organizacji
- Nieuprawnione wykorzystanie aplikacji przetwarzającej dane osobowe
- Możliwość uszkodzenia lub wprowadzenia do systemu destrukcyjnego oprogramowania obejmującego np. wirusy, lub inne "złośliwe oprogramowanie
- Nadużywanie zasobów
- Infiltracja komunikacji elektronicznej
- Przechwycenie komunikacji
- Brak niezaprzeczalności
- Błąd połączenia
- Osadzanie kodu złośliwego
- Przekierowanie połączenia
- Awaria techniczna systemu lub infrastruktury sieciowej
- Awaria środowiska wsparcia
- Awaria systemu lub oprogramowania sieciowego
- Awaria oprogramowania aplikacji
- Błędne operacje
- Odzyskiwanie po awarii (w tym tworzenia kopii zapasowych i przywracania systemów)
- Błąd konserwacji
- Błąd użytkownika
- Kradzież przez użytkowników w tym kradzież sprzętu lub danych
- Samowolne uszkodzenia przez użytkowników
- Terroryzm.

Katalog skutków

Lp.	Katalog skutków naruszenia praw i wolności osób fizycznych
1	Dyskryminacja
2	Kradzież tożsamości lub oszustwo dotyczące tożsamości
3	Strata finansowa
4	Naruszenie dobrego imienia
5	Naruszenie poufności danych osobowych chronionych tajemnicą zawodową
6	Nieuprawnione odwrócenie pseudonimizacji
7	Wszelka inna znacząca szkoda gospodarcza lub społeczna

Skutki

Kategoria skutków	Skala poziomu skutków			
	1 - pomijalne	2 – niskie	3 – średnie	4 – wysokie
Ocena skutków naruszenia praw i wolności osób fizycznych	Szum medialny, np. z powodu ujawnienia danych niepodlegających ochronie prawnej.	Nałożenie kar ustawowych w dolnej granicy kary. Koszty nielicznych procesów sądowych (obsługa prawna, informacyjna, odszkodowania).	Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych, jednakże nie są one wysokie. Wysokie ustawowe kary pieniężne. Koszty kilkudziesięciu procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Kontrole i kary UODO.	Skutki mogą prowadzić do wysokiego uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych Zagrożenie ustawową karą pozbawienia wolności. Koszty kilkuset procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Kontrole organów ścigania.

Prawdopodobieństwo materializacji zagrożenia

Ocena prawdopodobieństwa wystąpienia zagrożenia		
Wartość (P)	**Nazwa**	**Opis**
5	Niemal pewne	Istnieją racjonalne przesłanki by ocenić, że zagrożenie zmaterializuje się w najbliższym czasie (prawie na 90%).
4	Wysoce prawdopodobne	Istnieją racjonalne przesłanki by ocenić, że zagrożenie raczej się zmaterializuje, istnieje więcej niż połowa szans na wystąpienie. Materializowało się w przeciągu ostatniego roku.
3	Bardzo prawdopodobne	Wystąpienie zagrożenia jest realne, lecz nie przekracza 50% prawdopodobieństwa. Materializowało się sporadycznie w przeszłości (w ciągu ostatnich 2 lat)
2	Średnio prawdopodobne	Zagrożenie może wystąpić sporadycznie. Materializowało się sporadycznie w przeszłości (w ciągu ostatnich 3 lat).
1	Mało prawdopodobne	Zagrożenie raczej nie wystąpi lub możliwość jego wystąpienia jest znikoma (bliska zeru). Zagrożenie nie materializowało się w przeszłości.

RYZYKO

$$R = S * P$$

gdzie:

R - Ocena powagi ryzyka naruszenia praw i wolności osób fizycznych

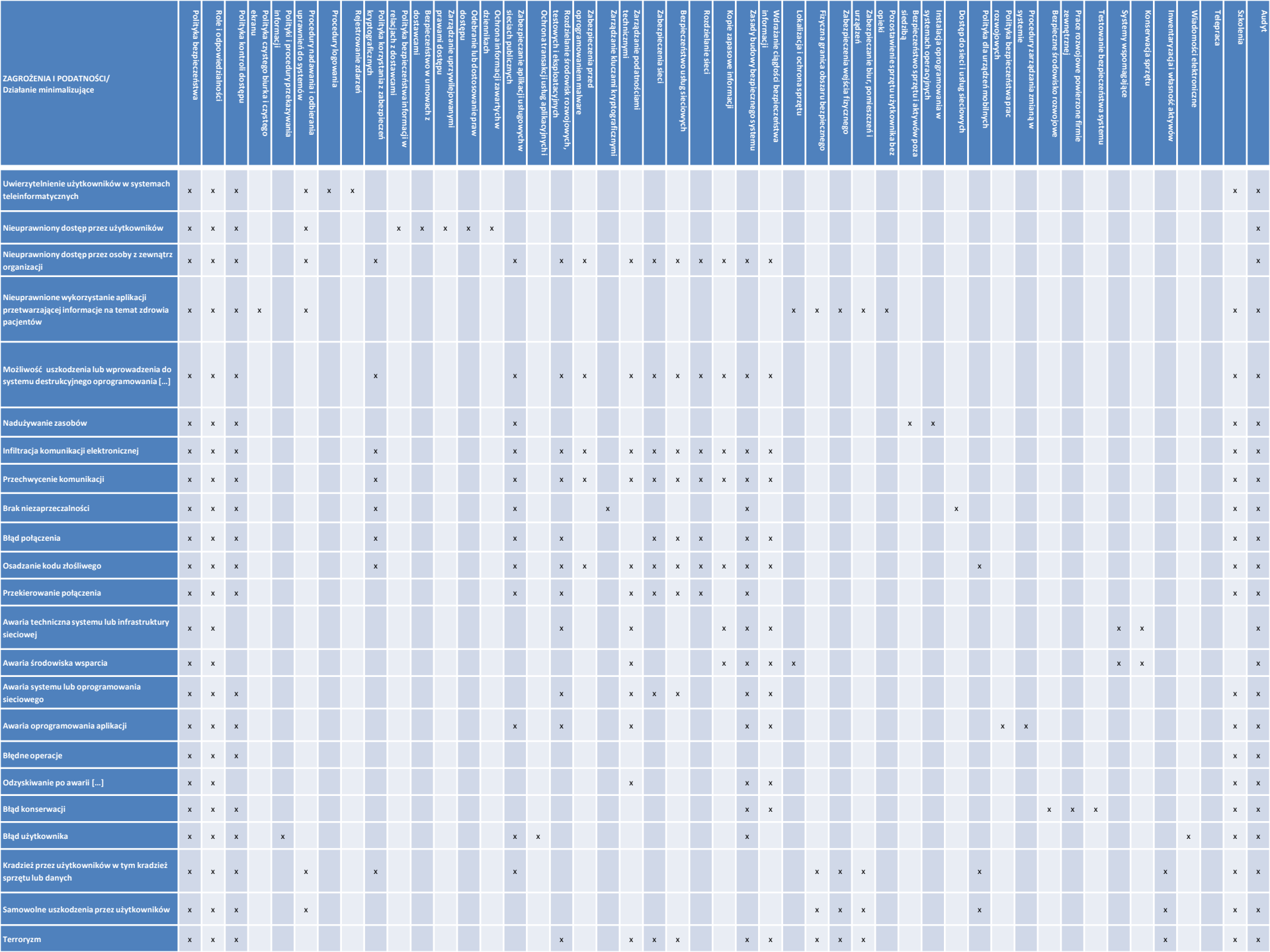
S- Ocena skutków naruszenia praw i wolności osób fizycznych

P- Ocena prawdopodobieństwa urzeczywistnienia się zagrożenia

RYZYKO i WAGA

Ocena skutków		Ocena prawdopodobieństwa				
		1	**2**	**3**	**4**	**5**
	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20

Wielkość ryzyka	Sposób postępowania
1-6	Wskazane skutki w kontekście urzeczywistnienia się analizowanego zagrożenia nie występują. Ryzyka akceptowane, niewymagające dalszego postępowania.
8-20	Ryzyka nieakceptowane, wymagające zastosowania postępowania z ryzykiem. Ryzyka, które powinny być kompensowane wszystkimi możliwymi zabezpieczeniami, adekwatnie do potencjalnych kosztów rekompensaty. Powinny być możliwie stale monitorowane w całym okresie przetwarzania danych.


ZAGROŻENIA I PODATNOŚCI/ Działanie minimalizujące
Polityka bezpieczeństwa
Role i odpowiedzialności
Polityka kontroli dostępu
Polityka czystego biurka i czystego ekranu
Polityki i procedury przekazywania informacji
Procedury nadawania i odbierania uprawnień do systemów
Procedury logowania
Rejestrowanie zdarzeń
Polityka korzystania z zabezpieczeń kryptograficznych
Polityka bezpieczeństwa informacji w relacjach z dostawcami
Bezpieczeństwo w umowach z dostawcami
Zarządzanie uprzywilejowanymi prawami dostępu
Odebranie lub dostosowanie praw dostępu
Ochrona informacji zawartych w dziennikach
Zabezpieczanie aplikacji usługowych w sieciach publicznych
Ochrona transakcji usług aplikacyjnych i
Zabezpieczenia przed oprogramowaniem malware
Rozdzielanie środowisk rozwojowych, testowych i eksploatacyjnych
Zabezpieczenia przed oprogramowaniem malware
Zarządzanie kluczami kryptograficznymi
Zarządzanie podatnościami technicznymi
Zabezpieczenia sieci
Bezpieczeństwo usług sieciowych
Rozdzielanie sieci
Kopie zapasowe informacji
Zasady budowy bezpiecznego systemu
Wdrażanie ciągłości bezpieczeństwa informacji
Lokalizacja i ochrona sprzętu
Fizyczna granica obszaru bezpiecznego
Zabezpieczenia wejścia fizycznego
Zabezpieczanie biur, pomieszczeń i urządzeń
Pozostawienie sprzętu użytkownika bez opieki
Bezpieczeństwo sprzętu i aktywów poza siedzibą
Instalacja oprogramowania w systemach operacyjnych
Dostęp do sieci i usług sieciowych
Polityka dla urządzeń mobilnych
Polityka bezpieczeństwa prac rozwojowych
Procedury zarządzania zmianą w systemie
Bezpieczne środowisko rozwojowe
Prace rozwojowe powierzone firmie zewnętrznej
Testowanie bezpieczeństwa systemu
Systemy wspomagające
Konserwacja sprzętu
Inwentaryzacja i własność aktywów
Wiadomości elektroniczne
Telepraca
Szkolenia
Audyt
Uwierzytelnienie użytkowników w systemach teleinformatycznych
Nieuprawniony dostęp przez użytkowników
Nieuprawniony dostęp przez osoby z zewnątrz organizacji
Nieuprawnione wykorzystanie aplikacji przetwarzającej informacje na temat zdrowia pacjentów
Możliwość uszkodzenia lub wprowadzenia do systemu destrukcyjnego oprogramowania [...]
Nadużywanie zasobów
Infiltracja komunikacji elektronicznej
Przechwycenie komunikacji
Brak niezaprzeczalności
Błąd połączenia
Osadzanie kodu złośliwego
Przekierowanie połączenia
Awaria techniczna systemu lub infrastruktury sieciowej
Awaria środowiska wsparcia
Awaria systemu lub oprogramowania sieciowego
Awaria oprogramowania aplikacji
Błędne operacje
Odzyskiwanie po awarii [...]
Błąd konserwacji
Błąd użytkownika
Kradzież przez użytkowników w tym kradzież sprzętu lub danych
Samowolne uszkodzenia przez użytkowników
Terroryzm

Dziękuję za uwagę

Jarosław Pudzianowski

Pełnomocnik ds. Zarządzania Bezpieczeństwem Informacji

e-mail: j.pudzianowski@csioz.gov.pl