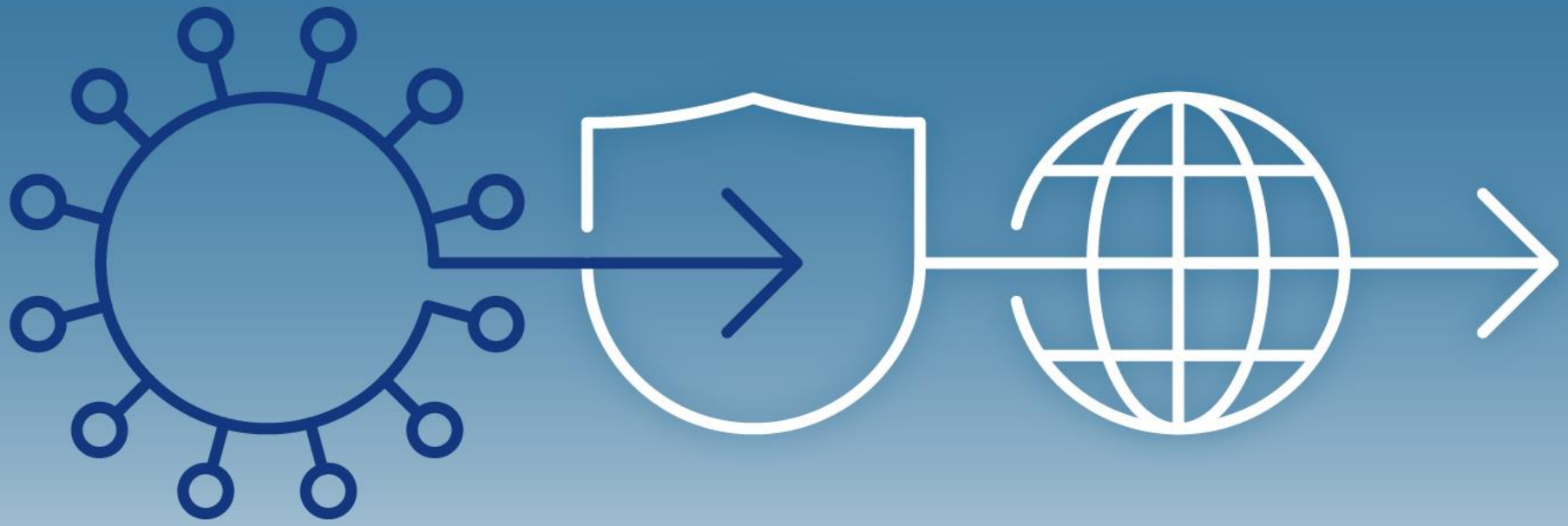
Konferencja Naukowa Bezpieczeństwo w Internecie – Cyberpandemia

22-23 października 2020 r.



Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo

UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

POLSKIE TOWARZYSTWO INFORMATYCZNE

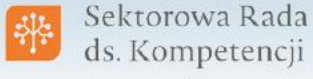
Naukowe Centrum Prawno-informatyczne

Zarządzanie bezpieczeństwem informacji a cyberbezpieczeństwo w podmiotach publicznych

Autor: dr hab. Małgorzata Ganczar

Katedra Publicznego Prawa Gospodarczego

Katolicki Uniwersytet Lubelski Jana Pawła II



Bezpieczeństwo – stan, w którym dane dobra są zabezpieczone, tzn. nie istnieje obawa ich utraty.

W praktyce stan ten jest niemożliwy do osiągnięcia, ponieważ nigdy nie będziemy mieć stuprocentowej pewności, że zasoby, takie jak wiedza czy informacja, nie są narażone na ataki lub próby przejęcia.

Zapewnienie bezpieczeństwa informacji jest procesem ograniczenia ryzyka lub prawdopodobieństwa wystąpienia szkody.

Zagrożenie zawsze będzie istnieć. Wprowadzając jednak parę „prostych” zasad w podmiocie, możemy zmniejszyć ryzyko ujawnienia/utraty cennych informacji.

Zarządzanie bezpieczeństwem informacji w aktach prawnych:

❖ ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych – rozdział 8 bezpieczeństwo teleinformatyczne, art. 49 ust. 1 „Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo.

❖Pojęcia:

ryzyko - kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

szacowanie ryzyka - całościowy proces analizy i oceny ryzyka;

zarządzanie ryzykiem - skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka;

Zarządzanie bezpieczeństwem informacji w aktach prawnych:

❖Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych, dalej rozporządzenie 2016/679)

❖wprowadza skuteczne procedury i mechanizmy koncentrujące się na tych operacjach przetwarzania, które mogą powodować ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.

❖Należy podkreślić, że analizy ryzyka dokonujemy z perspektywy osoby, której dane dotyczą, a nie administratora.

Zarządzanie bezpieczeństwem informacji w aktach prawnych:

❖ Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

❖ §20 rozporządzenia KRI zobowiązuje podmiot realizujący zadania publiczne do opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji, który zapewnia poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

❖W § 20 ust. 2 wskazano warunki jakie powinno zapewnić kierownictwo podmiotu publicznego w zakresie realizacji systemu zarządzania bezpieczeństwem informacji.

Za spełnienie wymagań rozporządzenia KRI uznaje się opracowanie systemu zarządzania bezpieczeństwem informacji na podstawie Polskiej Normy PN-ISO/IEC 27001, przy jednoczesnym ustanawianiu zabezpieczeń, zarządzaniu ryzykiem oraz audytowaniu systemu na podstawie:

- ❖ PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń,
- ❖ PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem,
- ❖ PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

❖SZBI opiera się na zabezpieczeniach proceduralno-prawnych, fizycznych i informatycznych, świadomości pracowników oraz posiadanych aktywach: informacje, sprzęt, zasoby ludzkie, infrastruktura, itd.

❖Norma PN-ISO/IEC 27001 określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji z uwzględnieniem uwarunkowań, w których działa Podmiot. Wymagania mają charakter ogólny i są przeznaczone do stosowania w podmiocie każdego rodzaju, wielkości czy charakteru.

Ryzyko związane z bezpieczeństwem informacji to ryzyko, które wynika z utraty poufności, integralności lub dostępności informacji i odzwierciedla niekorzystny wpływ na działania podmiotu, jego zasoby organizacyjne.

Szacowanie ryzyka wymaga starannej analizy informacji o zagrożeniach i słabych punktach oraz określenia, w jakim stopniu okoliczności lub zdarzenia mogą mieć niekorzystny wpływ na organizację (straty/skutki) oraz prawdopodobieństwo wystąpienia takich okoliczności lub zdarzeń. Ryzyko to możliwość, prawdopodobieństwo, że coś się nie uda, przedsięwzięcie, którego wynik jest nieznany, niepewny, problematyczny.

Ryzyko to wpływ niepewności na cele. Ryzyko jest często określane w odniesieniu do potencjalnych zdarzeń i następstw. Ryzyko jest scenariuszem opisującym zdarzenie i jego konsekwencje, oszacowanym pod względem powagi i prawdopodobieństwa ryzyka.

1) Pierwszym krokiem do wdrożenia systemu zarządzania bezpieczeństwem informacji jest zidentyfikowanie: informacji, zagrożeń występujących w organizacji i aktywów, które są bezpośrednio lub pośrednio związane z obiegiem informacji.
2) Kolejnym etapem szacowania ryzyka jest wartościowanie informacji i przypisanie im właścicieli.
3) Kolejnym etapem jest identyfikacja i analiza zagrożeń.
4) Ostatecznym efektem jest ocena ryzyka, na podstawie której można określić odpowiednie plany zarządzania ryzykiem w celu zminimalizowania istniejącego ryzyka do akceptowalnego poziomu. W ramach analizy ryzyka należy ocenić jakie informacje ma w swoich zasobach podmiot, jakim ryzykiem obarczone jest przetwarzanie informacji w tych zbiorach, by następnie wdrożyć mechanizmy zapobiegające wystąpieniu tych ryzyk.

Efektem przeprowadzonej analizy ryzyka jest stworzenie odpowiedniej polityki bezpieczeństwa informacji, która stanowi zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania (§ 2 pkt 15 rozporządzenia KRI).

Polityka bezpieczeństwa, zawiera w szczególności określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych informacji. Konieczne jest następnie wdrożenie ujętych w niej zasad i procedur poprzez ich zakomunikowanie pracownikom i wreszcie monitorowanie ich stosowania w praktyce.

Polityka bezpieczeństwa może określać w szczególności: obowiązki pracowników/użytkowników, bezpieczeństwo zasobów ludzkich, szacowanie ryzyka dla informacji chronionych, struktury zbiorów informacji, strefy przetwarzania informacji, kontrolę dostępu, zarządzanie systemami i sieciami, rozwój i utrzymywanie systemów informatycznych, zarządzanie incydentami, i in.

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych

„bezpieczeństwo sieci i systemów informatycznych” oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne; (Dyrektywa 2016/1148)

SOC – zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie;

SOC, na podstawie przeprowadzonego szacowania ryzyka, wprowadza zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów, w celu:
1) monitorowania i wykrywania incydentów;
2) reagowania na incydenty;
3) zapobiegania incydentom;
4) zarządzania jakością zabezpieczeń systemów, informacji i powierzonych aktywów;
5) aktualizowania ryzyk w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reakcję na incydent.

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych

Art. 66a. 1. Kolegium może sporządzić, na wniosek członka Kolegium, ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa.

W sporządzania oceny przeprowadza się w szczególności:
1) analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania;
2) prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniającą: (…)
3) liczbę i rodzaje oraz sposób i czas eliminowania wykrytych podatności i incydentów;
4) stopień, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;
5) treść wydanych wcześniej rekomendacji, dotyczących sprzętu lub oprogramowania danego dostawcy.

Wnioski

❖ Analiza ryzykiem jest **składową procesu podejmowania decyzji, ułatwiającą** kierującym podejmowanie świadomych i właściwych wyborów, ustalenia priorytetów działań oraz rozpoznawania alternatywnych kierunków działań w przypadku zaistniałych zagrożeń, zdarzeń i sytuacji kryzysowych

❖ **Analizując ryzyka musimy brać także pod uwagę czynniki ludzkie,** rozpoznając tym samym możliwości, percepcję i intencje osób zarówno wewnątrz, jak i na zewnątrz podmiotu, które mogą ułatwić bądź utrudnić osiągnięcie celów organizacji.

❖ **Analiza ryzyka powinna być dynamiczna, powtarzalna oraz reagować na zmiany, ponieważ wewnętrzne i zewnętrzne ryzyka zmieniają się, pojawiają** się nowe ryzyka, a niektóre zanikają.

❖ System zarządzania bezpieczeństwem informacji wymaga kompleksowego podejścia do zagadnienia, w związku z czym nie można przeprowadzić wdrożenia cząstkowo, wyłącznie w pewnych aspektach, a także w węższym zakresie, np. obejmującym wyłącznie kluczowe działy w podmiocie (np. księgowość, dział kadr, rejestry /ewidencje czy IT).

❖ Systemy teleinformatyczne wspierające funkcjonowanie administracji państwa funkcjonują w ramach złożonego ekosystemu prawno-organizacyjno-technicznego, który musi być zarządzany jednolicie, w sposób spójny i racjonalny, przy zachowaniu autonomii decyzyjnej urzędów j.s.t. i organów państwa na szczeblu centralnym w zakresie ich właściwości. Pozwoli to na zwiększenie zaufania obywateli do usług cyfrowych świadczonych przez administrację publiczną.

❖Idea podejścia opartego na ryzyku polega na tym, że ryzykiem najlepiej zarządza ten kto je zna. Ważne aby skład zespołu ds. szacowania ryzyka bezpieczeństwa informacji obejmował przedstawicieli wszystkich obszarów podmiotu (m.in. pełnomocnik ds. systemu zarządzani jakością, dyrektorzy, kierownicy działów, pracownik kadr, kierownik biura zarządu, administrator sieci, itp.). Praca w tak zbudowanym zespole umożliwiła objęcie wszystkich procesów realizowanych w organizacji związanych z tematem bezpieczeństwa informacji.

Dziękuję za uwagę!

mganczar@kul.pl