System Zarządzania Bezpieczeństwem Informacji - *czy stać nas na to ryzyko?*

SZBI - System Zarządzania Bezpieczeństwem Informacji

Na SZBI składają się: polityka, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych.

SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji w organizacji w celu osiągnięcia celów biznesowych.

Podejście **bazuje na szacowaniu ryzyka i poziomach akceptacji ryzyka** dla organizacji zaprojektowanych tak, aby skutecznie postępować z ryzykiem i nim zarządzać. Analiza wymagań ochrony **aktywów informacyjnych** i stosowanie właściwych zabezpieczeń w celu zapewnienia ochrony tych aktywów informacyjnych, tak jak jest to wymagane, przyczynia się do udanego wdrożenia SZBI.

Fundamentalne zasady przyczyniające się do udanego wdrożenia SZBI:

a) **świadomość potrzeby** bezpieczeństwa informacji;

b) przypisanie **odpowiedzialności** za bezpieczeństwo informacji;

c) nieodłączne **zaangażowanie kierownictwa** i zainteresowanie uczestników;

d) podnoszenie społecznych wartości;

e) **szacowanie ryzyka** determinujące właściwe zabezpieczenia w celu osiągnięcia akceptowalnych poziomów ryzyka;

f) bezpieczeństwo włączone jako istotny **element systemów i sieci** informacyjnych;

g) **aktywne** zapobieganie i **wykrywanie incydentów** związanych z bezpieczeństwem informacji;

h) zapewnienie **wszechstronnego** podejścia do zarządzania bezpieczeństwem informacji;

i) **ciągłe,** ponowne szacowanie bezpieczeństwa informacji i wprowadzanie modyfikacji, jeśli jest to właściwe.

PN-ISO/IEC 27000:2014-11

(…) **Z 16 urzędów**, do których wysłano wiadomości z prośbą o wzięcie udziału w badaniu, otrzymano **11 pozytywnych odpowiedzi**.

Cztery urzędy wojewódzkie pomimo podejmowanych prób ponownego kontaktu **nie przesłały** żadnej odpowiedzi.

Spośród 11 badanych urzędów wojewódzkich **tylko w czterech wdrożono** systemy zarządzania bezpieczeństwem informacji.

W pozostałych **pięciu** taki system **nie funkcjonuje** i w przeszłości nie były podejmowane próby jego wdrożenia.

Dziewięć posiada politykę bezpieczeństwa informacji zawierającą politykę ochrony danych osobowych.

Dwa posiadają **tylko politykę ochrony danych osobowych**.

CYBERBEZPIECZEŃSTWO ADMINISTRACJI PUBLICZNEJ W POLSCE
Wybrane zagadnienia EUROPEAN ASSOCIATION for SECURITY
KRAKÓW - Dominika LISIAK-FELICKA, Maciej SZMIT 2016 rok
Badanie przeprowadzono w połowie 2015 roku

Bezpieczeństwo jest rzeczą nieuchwytną, nie dająca się, zmierzyć, zważyć, dokładnie określić, mogącą jednak oddziaływać i mieć znaczenie, wpływ.

Bezpieczeństwo jest jedną z najważniejszych potrzeb człowieka, jest wartością pierwotną i podstawą i jest to wewnętrzne przekonanie, że należące do niego zasoby pozostaną nienaruszone.

W związku z tym, zaliczając bezpieczeństwo do dóbr podstawowych, powinno ono stanowić przedmiot szczególnej uwagi w zarządzaniu jednostkami administracji publicznej niezależnie od form zorganizowania, szczebla hierarchicznego i stopnia rozwoju technologicznego.

Bezpieczeństwo jest związane ze spełnianiem pewnych jego własności, zwanych atrybutami bezpieczeństwa. Są to:

Integralność, Poufność, Dostępność, Autentyczność, Rozliczalność,

Niezawodność.

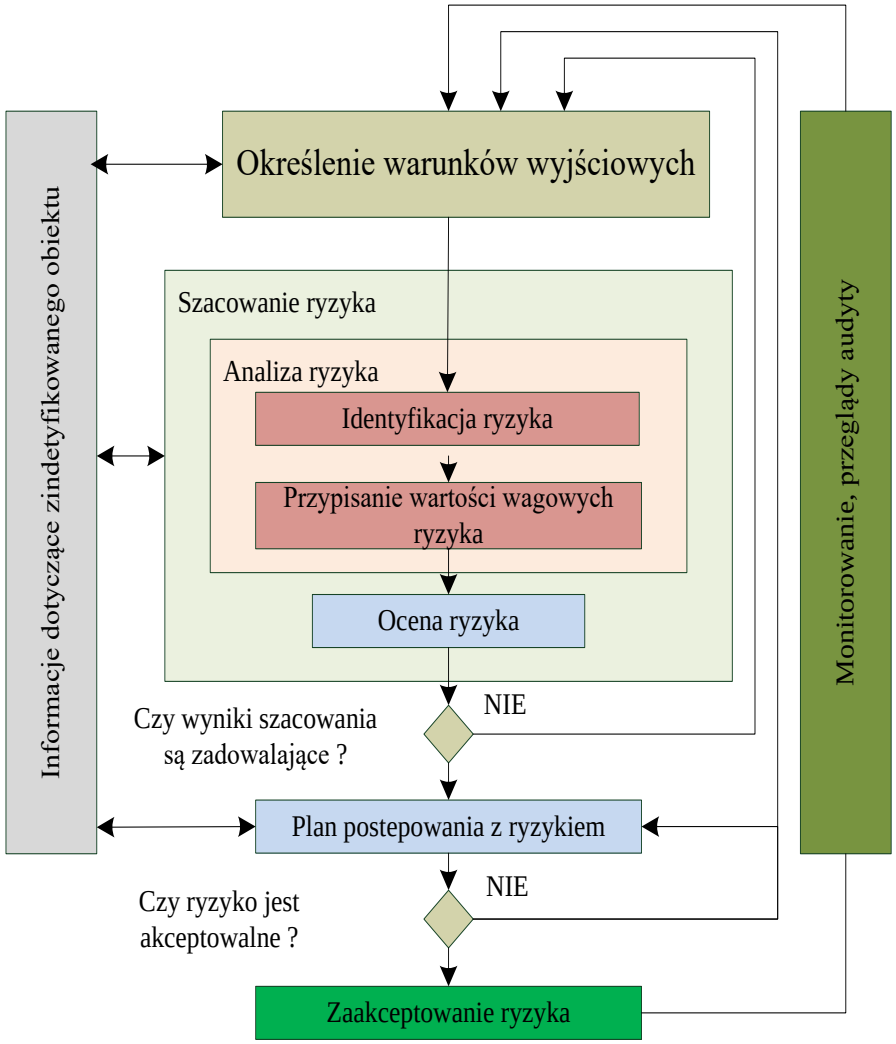
Spełnianie przez organizację tych własności nazywane jest aspektem bezpieczeństwa.

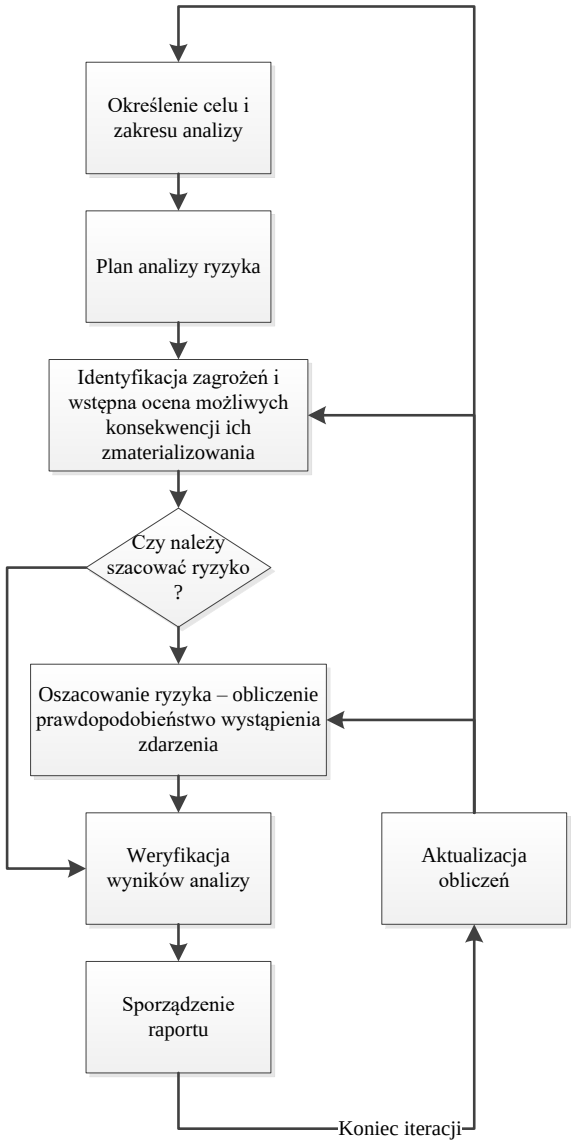
Bezpieczeństwo teleinformatyczne

jest warunkiem koniecznym, ale nie wystarczającym dla bezpieczeństwa informacji i usług. Integralność odnosi się zarówno do informacji, usług, sprzętu i oprogramowania.

Dla informacji najważniejsze są: integralność, autentyczność, poufność i dostępność.

Dla usług: dostępność, integralność i rozliczalność.


Informacje dotyczące zindetyfikowanego obiektu
Określenie warunków wyjściowych
Szacowanie ryzyka
Analiza ryzyka
Identyfikacja ryzyka
Przypisanie wartości wagowych ryzyka
Ocena ryzyka
Czy wyniki szacowania są zadowalające ?
NIE
Plan postepowania z ryzykiem
Czy ryzyko jest akceptowalne ?
NIE
Zaakceptowanie ryzyka
Monitorowanie, przeglądy audyty


Określenie celu i zakresu analizy
Plan analizy ryzyka
Identyfikacja zagrożeń i wstępna ocena możliwych konsekwencji ich zmaterializowania
Czy należy szacować ryzyko ?
Oszacowanie ryzyka – obliczenie prawdopodobieństwo wystąpienia zdarzenia
Weryfikacja wyników analizy
Aktualizacja obliczeń
Sporządzenie raportu
Koniec iteracji

Analiza ryzyka – mocny mechanizm, marne efekty przy błędnych założeniach

Zarządzanie ryzykiem związanym z funkcjonowaniem cyberprzestrzeni jest kluczowym elementem procesu ochrony cyberprzestrzeni, determinującym i uzasadniającym działania podejmowane w celu jego obniżenia do akceptowalnego poziomu.

Polityka Ochrony Cyberprzestrzeni RP

Etapy procesu zarządzania ryzykiem:

1. opracowanie tzw. metodyki zarządzania ryzykiem oraz określenie odpowiedzialności w zakresie zarządzania ryzykiem, ze szczególnym uwzględnieniem roli kierownictwa w etapie określenia kryteriów akceptacji ryzyka;
2. identyfikacja ryzyk, która polega na określeniu przyczyn i sposobu materializacji niepożądanych incydentów;
3. wykonanie estymacji ryzyka;
4. dokonanie oceny ryzyka;
5. uwzględniając kryteria oceny ryzyka, dla wyznaczonych ryzyk, należy określić odpowiednie postępowanie;
6. po opracowaniu planów postępowania z ryzykiem, należy dokonać ponownej akceptacji tzw. ryzyk szczątkowych, czyli ryzyk z uwzględnieniem zastosowanych mechanizmów ochrony;
7. informowanie uczestników procesu o aktualnym jego statusie;
8. monitorowanie i przegląd ryzyk.

Innymi słowy, celem analizy ryzyka jest podniesienie, czy wręcz zbudowanie naszej świadomości dotyczącej stanu bezpieczeństwa zarządzanego przez nas systemu IT, a w kolejnym kroku podjęcie pewnych działań zaradczych. Prowadzimy ją, przez cały czas mając na uwadze główny cel organizacji (czyli najczęściej maksymalizację profitów / minimalizację strat).

Potrzeba pomiaru wartości informacji wynika z następujących jej własności:

- informacja jest jednym z czynników wytwórczych [D T Dziuba, 2007, s. 19-23],
- informacja jest nabywana za określony mierzalny koszt, który może być znaczny,
- dostępne są substytuty do każdej specyficznej cząstki informacji i mogą być przeliczone jako mniej lub bardziej kosztowne,
- koszt wykorzystania informacji może być znaczący,
- jak każdy czynnik wytwórczy informację należałoby wykorzystać optymalnie [M Oleander-Skowronek, K. B Wydro, 2007, s. 1]

Powyżej przytoczone cechy informacji powodują, że najbardziej adekwatną oceną wartości informacji będzie ocena subiektywna tzn. zależy od osoby, która ją użytkuje [M Oleander-Skowronek, K. B Wydro, 2007, s. 75].

Pomiar wartości informacji jest trudny ze względu na:

- informacja ma użytkowość pośrednią [M Oleander-Skowronek, K. B Wydro, 2007, s. 72];
- informacja ma naturę zmienną, co wynika z jej wieloaspektowości, różnorodności i złożoności. Może być wykorzystywana i interpretowana na wiele sposobów przez różnych użytkowników [D T Dziuba, 2007, s. 19-23];
- informacja może redukować niepewność jak i ją generować;
- informację trzeba aktualizować;
- wartość informacji zależy od efektu skali, wartość ta jest rosnąca funkcja bogactwa;
- wartość informacji maleje w czasie;
- im częściej stosuje się pewnego rodzaju informacje tym bardziej zyskują na wartości;
- informacja jest bezwartościowa gdy nie istnieje możliwość jej przekazu;
- informacje można przekazać dzięki wykorzystaniu technologii IT;
- jest źródłem niewyczerpalnym;
- można ją przetwarzać w celu uzyskania nowych informacji.

Jakie możliwości prawne ?

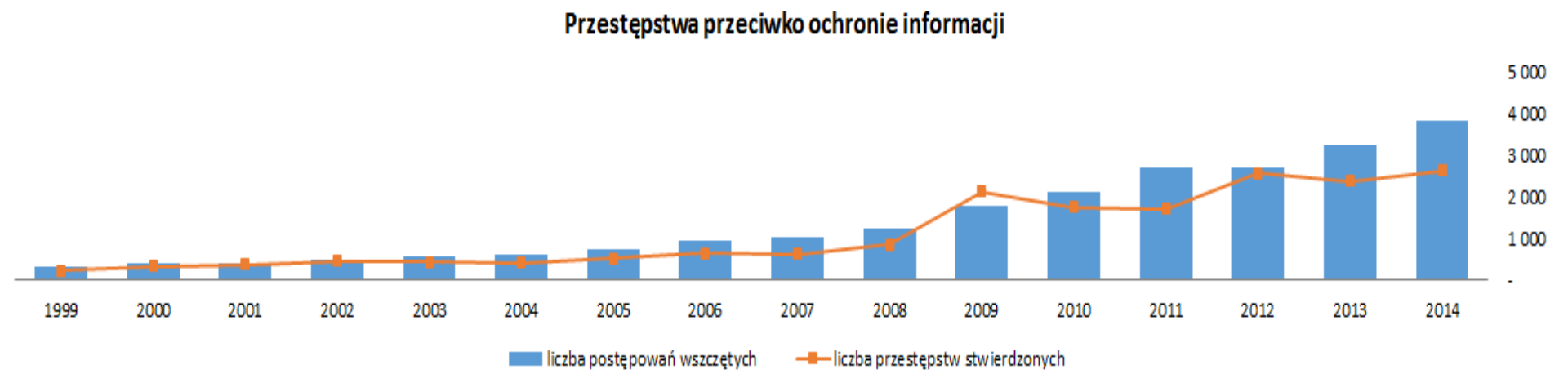
Regulacje, które wysuwają się przed szereg to:

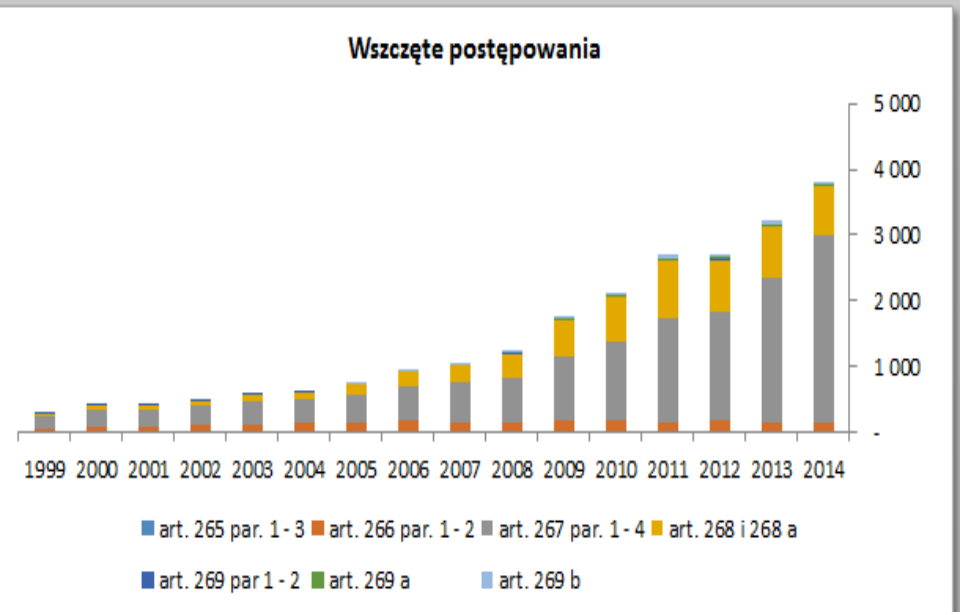
1. Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego;
2. Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji;
3. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych;
4. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych;
5. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
6. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
7. 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;
5. *Oczekiwana ustawa o cyberbezpieczeństwie.*

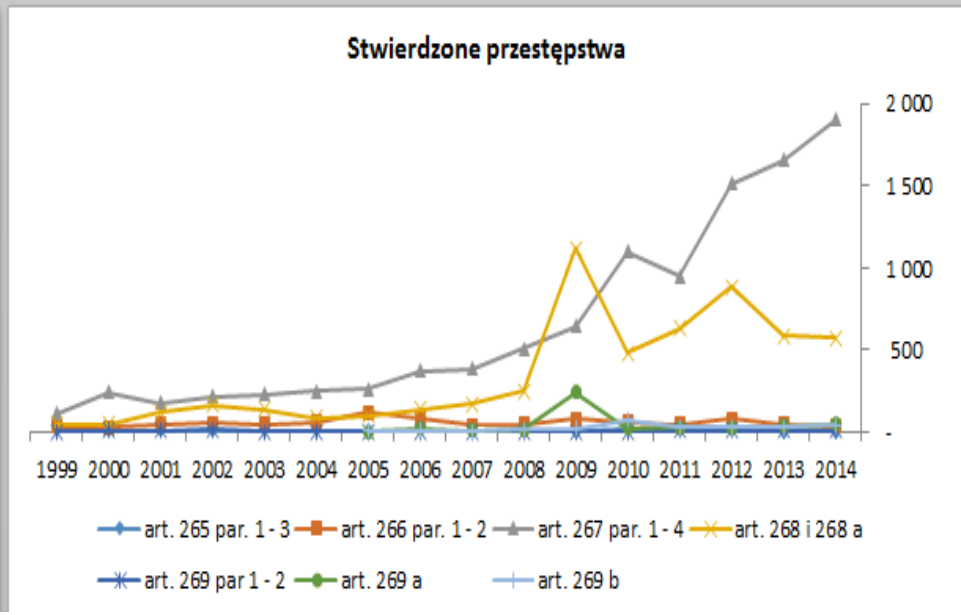
§ 20 ust. 1. (KRI) „Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność”.

§ 20 ust. 2 – określa działania, jakie powinny zostać podjęte a następnie egzekwowane, w celu realizacji zarządzania bezpieczeństwem informacji

§ 20 ust. 3 „Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 (…)”







*Źródło - http://blog.e-odo.pl – na podstawie http://statystyka.policja.pl do końca 2014 r.

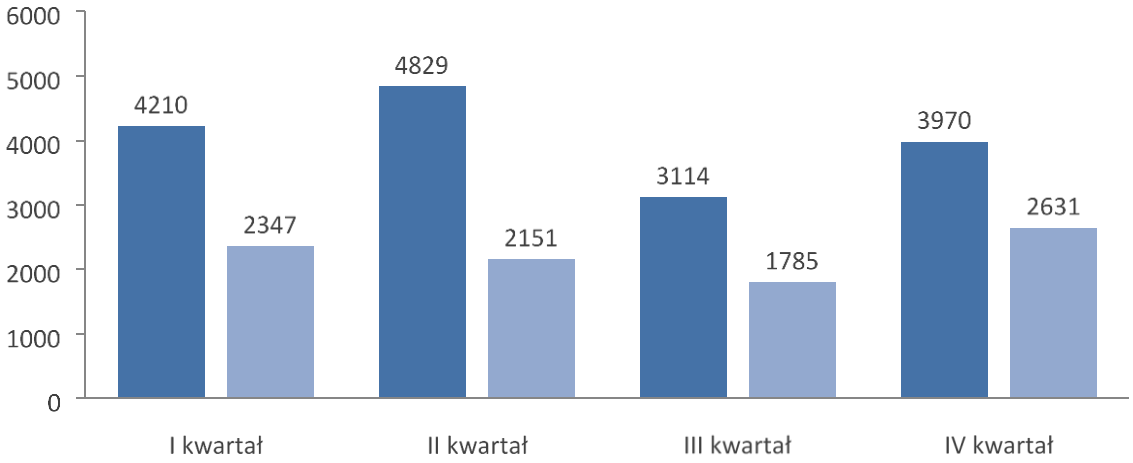
- Najczęściej dochodzi do naruszenia **tajemnicy korespondencji** (w samym 2014 roku stwierdzono 1901 przestępstw tego typu). Problematyka tajemnicy korespondencji uregulowana została w art. 267 Kodeksu Karnego. Zachowanie korespondencji w tajemnicy polega na ochronie poufności informacji, prawie do dysponowania informacją z wyłączeniem innych osób, a także bezpieczeństwie ich przekazywania.
- Drugim najczęściej występującym przestępstwem z naruszenia bezpieczeństwa informacji (w 2014 roku było to 572 stwierdzone przestępstwa) jest przestępstwo określone w art. 268 Kodeksu Karnego, które polega na naruszeniu prawa do zachowania integralności informacji oraz prawa do ich dostępu.
- Najniższą wykrywalność zauważono w przypadku przestępstw polegających na niszczeniu danych informatycznych (sabotaż komputerowy zwany także dywersją informatyczną). Dla zobrazowania skali problemu w 2014 roku wszczęto raptem 10 postępowań w tym tylko 6 stwierdzono.

http://statystyka.policja.pl do końca 2014 r.

- Ujawnienie tajemnicy państwowej (art. 265)
- Ujawnienie tajemnicy służbowej i zawodowej (art. 266)
- Naruszenie tajemnicy korespondencji (art. 267)
- Udaremnienie lub utrudnienie korzystania z informacji (art. 268 i 268a)
- Niszczenie danych informatycznych (art. 269)
- Sabotaż komputerowy (art. 269a)
- Wytwarzanie programu komputerowego do popełnienia przestępstwa (art. 269b)

Ustawa o ochronie danych osobowych nie definiuje wprost, czym jest **incydent w ochronie danych osobowych**. Szczegółowe wyjaśnienie tego pojęcia można odnaleźć w normie PN-ISO/ IEC 27001. Zgodnie z jej treścią przez **incydent związany z bezpieczeństwem informacji** należy rozumieć pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

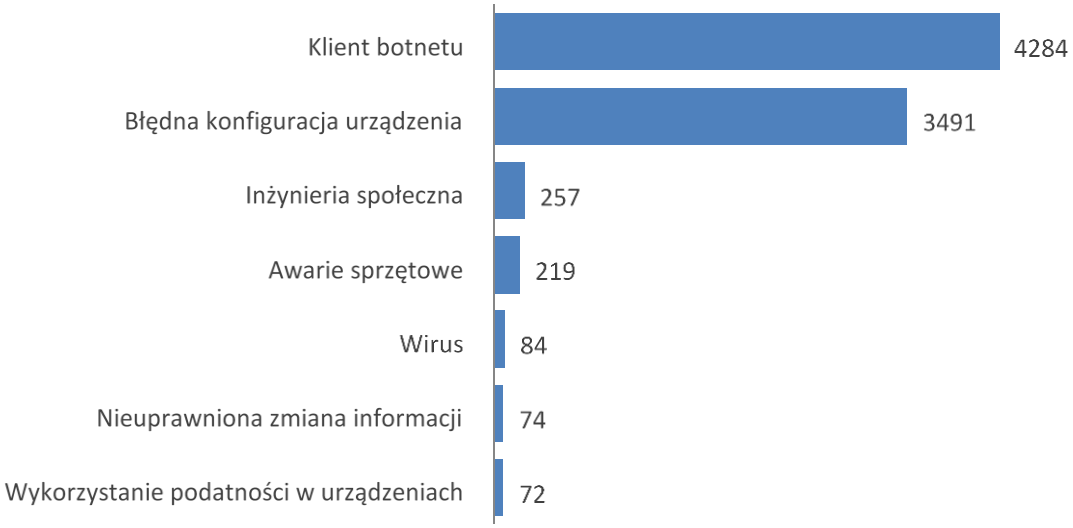
W 2015 roku łącznie zarejestrowanych zostało 16 123 zgłoszeń, z których aż 8 914 zostało zakwalifikowanych jako faktyczne incydenty. Najwięcej zgłoszeń odnotowano w II kwartale, natomiast najmniej w III kwartale.



Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2015 roku*

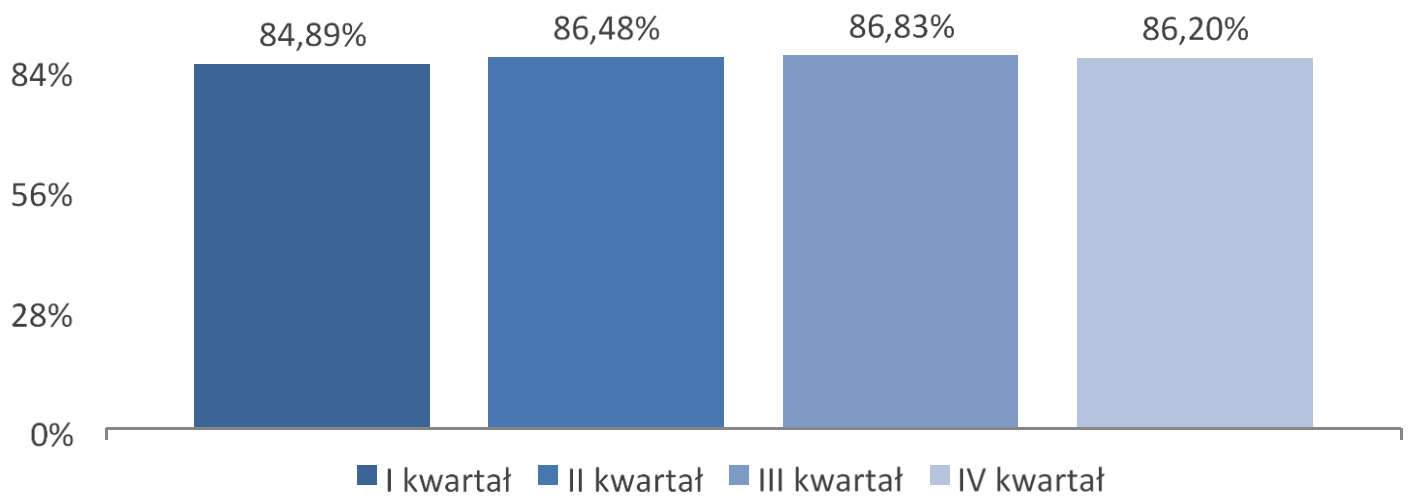
*Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 r. - CERT

Wybrane kategorie incydentów zarejestrowanych w 2015 roku.

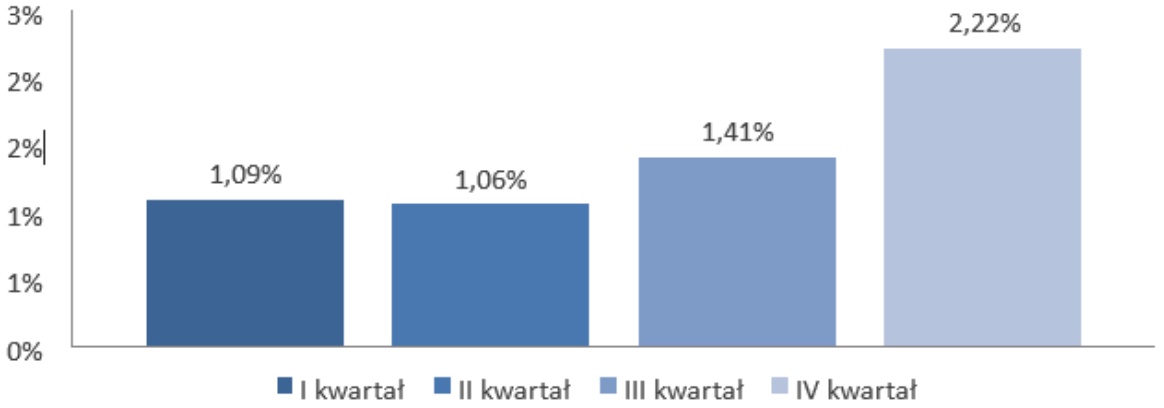


Statystyka wybranych incydentów w 2015 roku z podziałem na kategorie

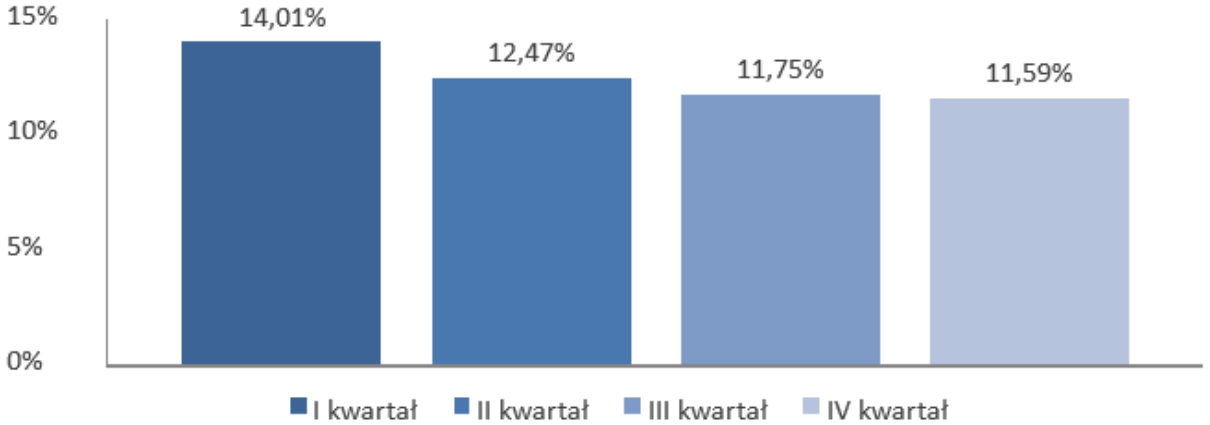
*Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 r. - CERT



*Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 r. - CERT



Źródła incydentów – ustalenia własne



Źródła incydentów – zgłoszenia podmiotów zewnętrznych

*Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 r. - CERT

Incydenty?… U nas nie ma…

Problemy, na które należy zwrócić szczególną uwagę to:

- braki kadrowe i kompetencyjne do obsługi incydentów.

W administracji samorządowej, rządowej administracji terenowej (zespolonej i niezespolonej) brakuje specjalistów przygotowanych do interdyscyplinarnego łączenia spraw z zakresu prawa, IT, bezpieczeństwa informacji, audytu;

- zbieranie logów i ich analizowanie w sposób nieusystematyzowany;
- SIEM – marzeniem większości działów IT;
- brak automatyzacji procesów analitycznych;

Incydenty… U nas nie ma…

Jak w takim razie mówić o zarządzaniu incydentami, skoro administrator nawet nie chce wiedzieć, co się dzieje w jego systemie?

Zarządzanie incydentami jest dalekie od właściwego rozumienia zapisów normy ISO 27001. Innym słowem zarządzanie incydentami w sektorze publicznym to marzenie, marzenie pasjonatów IT security, którzy dostali kilka mechanizmów typu Ustawy, KRI, Rządowy Program Ochrony Cyberprzestrzeni i jeśli trafią w swojej instytucji na „sprzyjający klimat” to zrobią coś pożytecznego i użytecznego dla bezpieczeństwa informacji.

Zarządzanie bezpieczeństwem nie może zależeć od przypadków i chęci – musi stać się regułą na poziomie całej organizacji, administracji, kraju.

I co dalej…

- Wsparcie kierownictwa dla realizacji procesów obejmujących bezpieczeństwo informacji,
- analiza ryzyka, identyfikacja zasobów – kluczem do bezpieczeństwa – ale jedynie gdy jest procesem ciągłym,
- ustalenie odpowiedzialności za poszczególne mechanizmy, etapy przetwarzania informacji,
- utrzymanie aktualności procedur bezpieczeństwa dla zasobów,
- spójne wymagania i przepisy prawa w zakresie konieczności zapewnienia bezpieczeństwa informacji,
- kompetencje kadry IT oraz świadomość pracowników o wartości informacji.
- działania spontaniczne, „ad hock”, bez głębszej analizy skazane są na niską efektywność w stosunku do nakładów,
- tylko działania prowadzone systemowo w oparciu o najlepsze praktyki dają szansę optymalnej ochrony informacyjnych aktywów danej organizacji,

Dziękuję za uwagę

Dariusz Binkowski

Dyrektor Biura Informatyki
i Rozwoju Systemów Informatycznych
Mazowiecki Urząd Wojewódzki