SPOTKANIE INFORMACYJNE

Zapewnij bezpieczeństwo informacji stosując międzynarodowe standardy wynikające z norm ISO 27001

16 czerwca 2016
Warszawa Centrum Szkoleniowo-Konferencyjne JUPITER

Prelekcja: Bezpieczeństwo Informacji w ujęciu systemowym

Prelegent: Tadeusz Zawistowski

Bezpieczeństwo informacji to nie tylko:

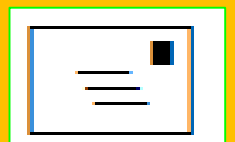
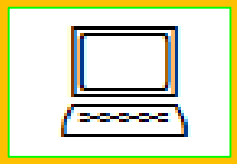
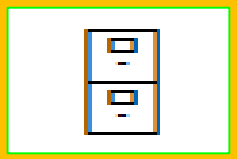
- ✓ Internet, Antywirusy, Firewall i Bezpieczna sieć
- ✓ Hasła
- ✓ **Poufność**

Bezpieczeństwo informacji to także:

- ✓ Ludzie ich wiedza, podejście i słabości
- ✓ Sposób wykonywania codziennych zadań
  - ✓ Wydruki zabierane z drukarek
  - ✓ Dostarczenie listu odpowiedniej osobie
  - ✓ Zamknięte drzwi i porządek na biurku
- ✓ **Dostępność do informacji**
- ✓ **Integralność informacji, w tym jej kompletność**
- ✓ (...)

Mnie bezpieczeństwo informacji nie dotyczy, nie mam żadnych tajemnic!

- ✓ Czy na pewno nie masz żadnych obowiązków wynikających z prawa?
- ✓ Czy nie masz obowiązków wynikających z umów?
- ✓ Czy nigdy nie utraciłeś danych?
- ✓ Czy nigdy nie zagubiłeś dokumentu, pliku?
- ✓ Czy Twoi współpracownicy wywiązują się z obowiązków np. w zakresie przekazywaniu informacji?
- ✓ Czy Twoje informacje nie są interesujące dla konkurencji (np. jaka cena będzie w Twojej ofercie, baza klientów)?
- ✓ Czy wiadomo skąd firmy, które ciągle nękaj Cię ofertami mają Twój telefon?
- ✓ Czy nie korzystasz z bankowości elektronicznej?
- ✓ Czy nie dokonujesz zakupów przez internet?
- ✓ (…)

Tworząc (gromadząc)	Przekazując	Przetwarzając	Archiwizując (przechowując)	Niszcząc (usuwając)
				
Gdy zapisujesz informacje:	Gdy przekazujesz informacje:	Gdy przetwarzasz informacje:	Gdy przechowujesz informacje:	Gdy niszczysz informacje:
• które powinny / muszą być zapisane • kompletne • niesprzeczne • czytelnie • we właściwych miejscach • we właściwej formie • we właściwym czasie	• właściwym adresatom • w terminie • odpowiednim kanałem • w tajemnicy przed niepożądanymi odbiorcami	• tak by nikt nieuprawniony ich nie podejrzał • tak by ci którzy powinni mieli do nich dostęp • bez utraty informacji • w odpowiedni sposób	• te które trzeba • te które można • odpowiednio długo • w odpowiednich miejscach • w odpowiedniej formie • w odpowiedni sposób • z możliwością szybkiego odtworzenia	• które trzeba • które można • skutecznie • w odpowiednim czasie

Informacja nie jest bezpieczna wtedy, gdy:

- ✓ **osoby niepowołane mają do niej dostęp** (np. wtedy, gdy pozostawisz niewylogowany komputer i odchodzisz z miejsca pracy) NIEZACHOWANIE **POUFNOŚCI**

- ✓ **ten kto ma prawo dostępu do niej z tego prawa nie może skorzystać** (np. zauważamy to wtedy, gdy chcemy skorzystać z internetu a nie jest on dostępny) NIEZACHOWANIE **DOSTĘPNOŚCI**

- ✓ **niezachowana jest jej spójność, kompletność czy dokładność** (np. dane w PM Projekt dotyczące projektu nie są aktualne) NIEZACHOWANIE **INTEGRALNOŚCI**

Źli ludzie

- Złodzieje (kradną pieniądze albo sprzedaj ukradzione/ wyłudzone informacje)
- Szantażyści (kompromitujące informacje, zaszyfrowanie danych)
- Przestępcy (wykorzystanie naszego komputera do celów przestępczych)

Sami sobie

- Zapomnienie hasła, wysłanie emaila do nieodpowiedniej osoby, potrzeba chwalenia się

Nasza lub innych lekkomyślność lub brak świadomości

- Udostępnienie hasła, praca na hasłach producentów, nie wykonywanie kopii bezpieczeństwa, rozmowy w miejscach publicznych

Pech

- Kradzież komputera, awaria łącza, pożar, zalanie, przypadkowe skasowanie

Niesolidni partnerzy

- Klienci lub dostawcy nie zabezpieczający danych
- Dostawcy nie realizujący usługi (np. telefon, internet)
- Urzędnicy niedbający o bezpieczeństwo

Błędnie działające albo źle zaprojektowane urządzenia i programy

Patrz na bezpieczeństwo w sposób całościowy i systemowy

Zapewnij bezpieczeństwo informacji stosując międzynarodowe standardy wynikające z norm ISO 27001
Warszawa, 16 czerwca 2016

Środowisko ataków

- Atrakcyjność aktywa
- Agresor
- Ekspozycja

Dlaczego?

- Dla pieniędzy
- Dla sławy
- Z głupoty
- Z zazdrości
- Dla zemsty
- Z niedowartościowania
- (…)

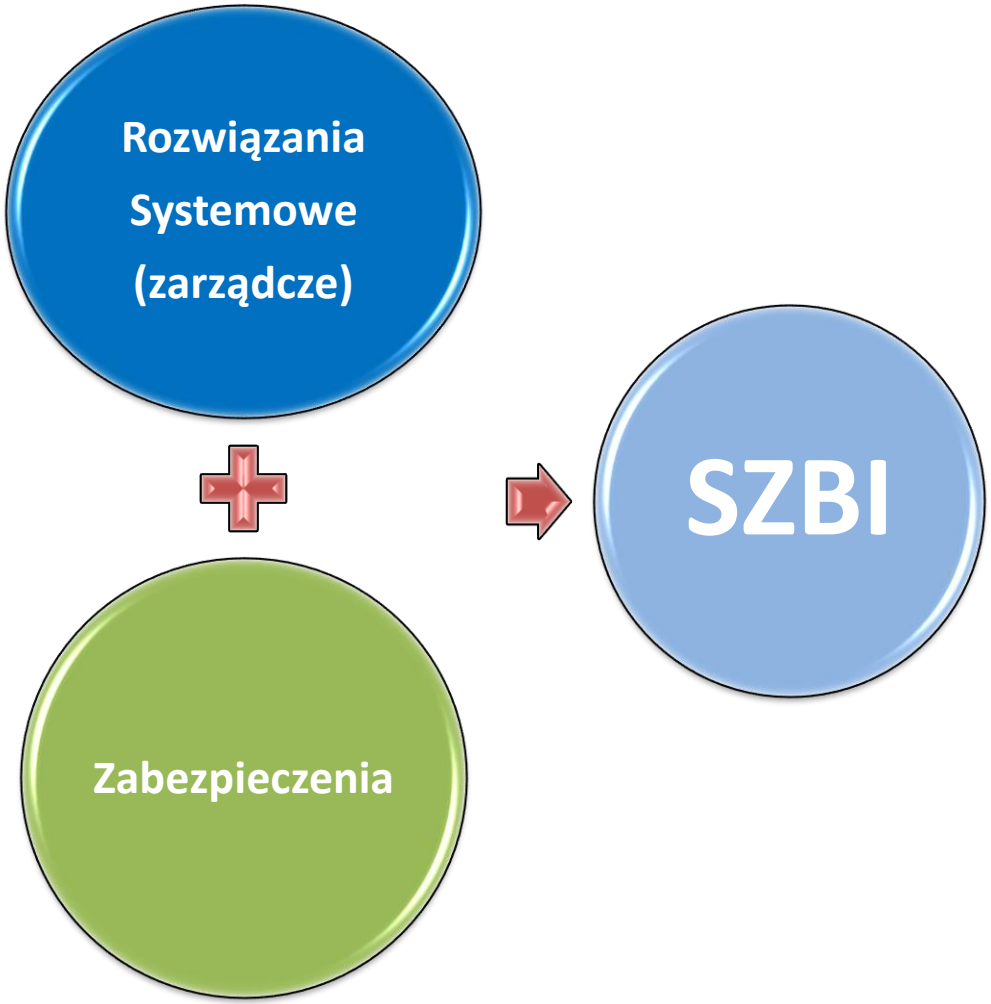
ZABEZPIECZENIA ?

Podatności/ luki

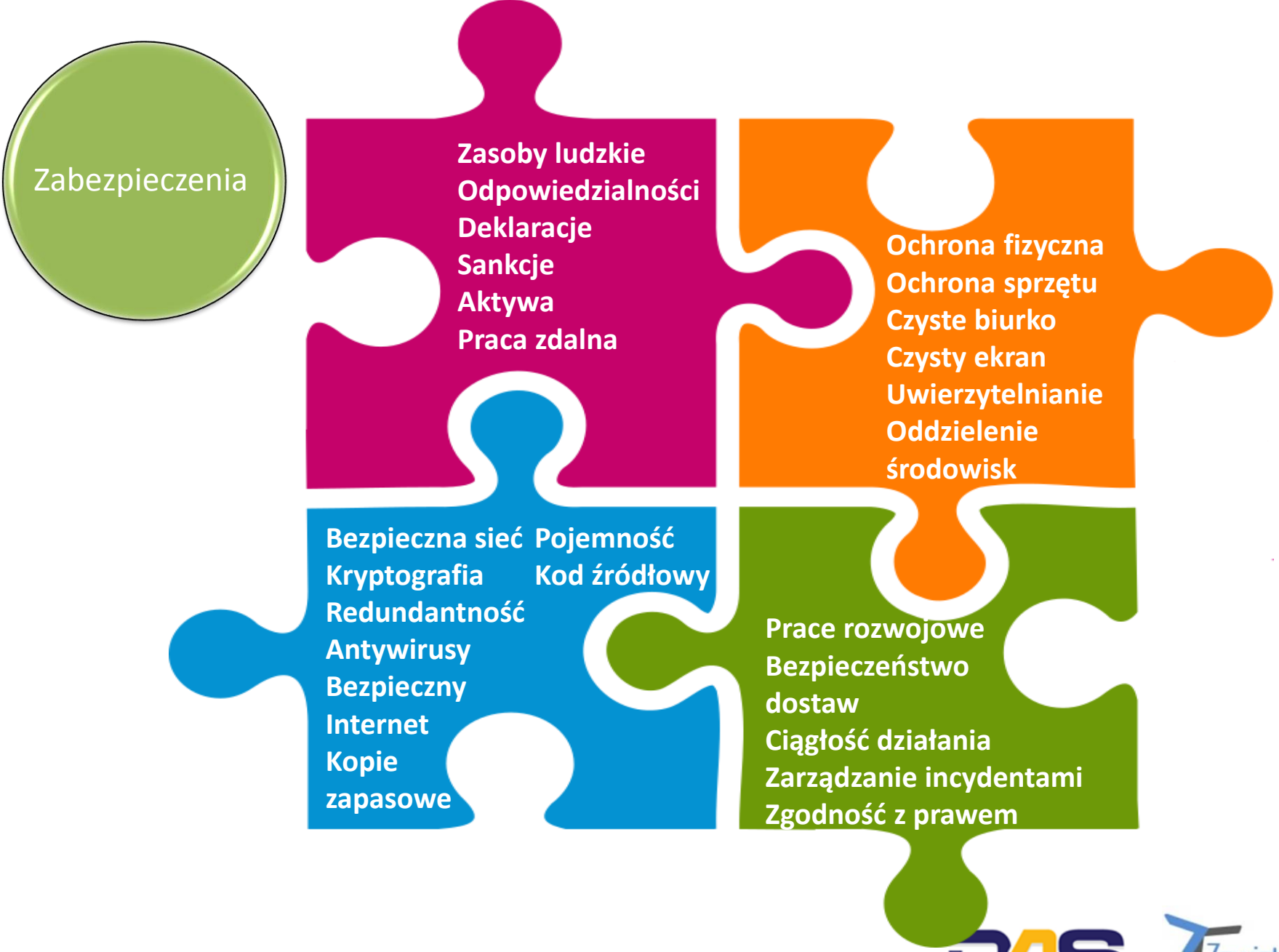
- Wykorzystanie naszych słabości (ładnie poprosić, zrobić wrażenie, lenistwo, łatwowierność)
- Wykorzystanie naszej niewiedzy
- Wykorzystanie podatności technicznych (braku zabezpieczeń, luk w zabezpieczeniach, błędów w zabezpieczeniach)

Szkoda czasu na wymyślanie wymyślonego

Bezpieczeństwo informacji to ich całościowa i systemowa ochrona




Rozwiązania
Systemowe
(zarządcze)
Przywództwo
Polityka
Cele
Ryzyko
Dokumentacja
Świadomość
Komunikacja
Wiedza
Monitorowanie
Audyty
Przeglądy
Korekcja
Doskonalenia


Zabezpieczenia
Zasoby ludzkie
Odpowiedzialności
Deklaracje
Sankcje
Aktywa
Praca zdalna
Ochrona fizyczna
Ochrona sprzętu
Czyste biurko
Czysty ekran
Uwierzytelnianie
Oddzielenie środowisk
Bezpieczna sieć
Kryptografia
Redundantność
Antywirusy
Bezpieczny Internet
Kopie zapasowe
Pojemność
Kod źródłowy
Prace rozwojowe
Bezpieczeństwo dostaw
Ciągłość działania
Zarządzanie incydentami
Zgodność z prawem