Bezpieczeństwo Informacji

Kamil Kowalczuk, CEH, LA27001

Agenda

- ✓ Czym jest informacja?
- ✓ Podstawowe cechy bezpieczeństwa informacji – obszary ochrony
- ✓ Obszary ochrony
- ✓ Dane osobowe – podstawy
- ✓ Architektura bezpieczeństwa
- ✓ Normy i dobre praktyki
- ✓ Analiza skutków ataku

Co chronimy, a co powinniśmy?

Co chronimy w organizacji?

Informacje!!!

- Cechy informacji: (kompletna, zrozumiała, istotna, terminowa, wiarygodna).
- Rodzaje informacji: (dokument papierowy, dokument elektroniczny, kody źródłowe, rysunki techniczne).

Czy informacja ma określoną wartość w danym czasie i dla danego podmiotu?

Wartość informacji

- Informacja o wylosowanych numerach w LOTTO na godzinę przed losowaniem = wartość wygranej.

- Informacja o wygrywających numerach w LOTTO dzień po losowaniu = wartość „ZERO”.

Ryzyko – Zasoby informacyjne

- ryzyko utraty **poufności** (zdarzenie mogące doprowadzić do ujawnienia informacji przetwarzanej przez system informatyczny nieautoryzowanemu użytkownikowi)
- ryzyko utraty **dostępności** (zdarzenie mogące doprowadzić do braku dostępu w określonym czasie do systemu informatycznego, programu lub informacji)
- ryzyko utraty **integralności** (zdarzenie mogące doprowadzić do nieautoryzowanej modyfikacji lub zniszczenia danych przetwarzanych przez system teleinformatyczny)

Obszary bezpieczeństwa informacji

- Organizacyjne
- Fizyczne
- Prawne
- Techniczne (teleinformatyczne)

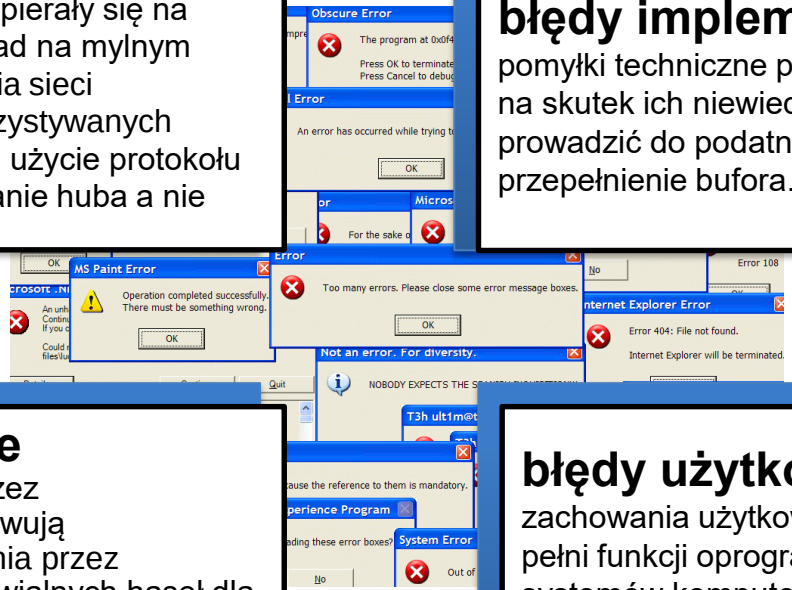
Geneza błędów zabezpieczeń IT

błędy projektowe

założenia dla oprogramowania opierały się na błędnych przesłankach, na przykład na mylnym rozumieniu zasad funkcjonowania sieci komputerowych i budowy wykorzystywanych protokołów komunikacyjnych np. użycie protokołu „http” a nie „https” lub zastosowanie huba a nie switcha.

błędy implementacyjne

pomyłki techniczne popełniane przez programistów na skutek ich niewiedzy lub nieuwagi np. może prowadzić do podatności na ataki typu przepełnienie bufora.



błędy konfiguracyjne

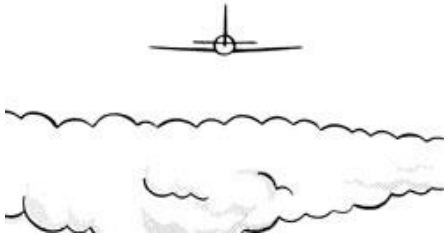
obejmuje pomyłki popełniane przez administratorów, którzy przygotowują oprogramowanie do wykorzystania przez użytkowników np. ustawienie trywialnych haseł dla uprzywilejowanych kont, albo udostępnienie zbędnej funkcjonalności bez adekwatnej kontroli dostępu.

błędy użytkownika

zachowania użytkowników, którzy nie rozumieją w pełni funkcji oprogramowania i zasad działania systemów komputerowych np. uruchamianie załączników od niepewnych nadawców przysłanych w poczcie elektronicznej.

„fałszywy horyzont”

podejmowanie decyzji w oparciu o nieprawdziwe dane



wrażenie pilotującego

faktyczny tor lotu

źródło: http://www.jalbrecht.ca

„fałszywy horyzont”

- Decyzje winny być podejmowane w oparciu o pełne, realne dane

- Podejście holistyczne, w którym każde ryzyko jest mierzone tą samą miarą i rozpatrywane pod różnymi aspektami skutków jego materializacji

Architektura Bezpieczeństwa

Ochrona IT

- „Trzeba wdrożyć DLP…”
- „Kupmy nowe szyfrowane pendrive, te sprzętowe…”
- „Zmieńmy Firewalle, te co mamy są kiepskie…”
- „Trzeba przejść z wersji 2013 na 2014 ma takie fajne kolory…”
- „Trzeba robić dwie niezależne kopie bezpieczeństwa… kupmy dodatkową macierz”

Po co? – bo tak jest łatwiej… i na tym się znamy…

Ochrona bez analizy

Architektura Bezpieczeństwa

Standardy

Większość standardów w zakresie projektowania Architektury Bezpieczeństwa IT oraz metod jego kontroli są aktualnie zgodne, to biznes i kontekst w którym funkcjonuje przedsiębiorstwo jest istotą dobrej architektury bezpieczeństwa.

SABSA®

COBIT
GOVERNANCE, CONTROL and ASSURANCE for INFORMATION and RELATED TECHNOLOGY

Information Security Management System
ISO
27001
Certified

OSA

OWASP
The Open Web Application Security Project

Architektura Bezpieczeństwa

SABSA

[Sherwood Applied Business Security Architecture]

- Co chronimy?
- Po co chronimy – dlaczego?
- Jak chcemy chronić?
- Kto ma to robić?
- Gdzie umiejscawiamy ochronę?
- Kiedy chronimy i kontrolujemy?

Metodyka pomaga tworzyć architekturę bezpieczeństwa nie utrudniając kluczowych procesów biznesowych.

OSA

[Open Security Architecture]

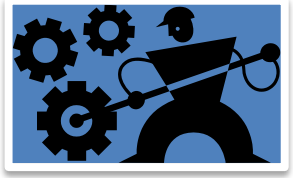
- Wzorce do zastosowania.
- Tworzone przez społeczność.
- Ty możesz stworzyć wzorzec i się nim podzielić.
- W oparciu o wiele standardów [ISO 27001, PCI DSS, COBIT, ITL]
- Techniczne podejście, ale nie tylko.

Metodyka określa gotowe modele do implementacji architektury bezpieczeństwa dla konkretnych przykładów.

Architektura Bezpieczeństwa – dla kogo?

Biznes i jego cele

Ludzie



Technologia

Bezpieczeństwo

Tworzenie Architektury Systemów Bezpieczeństwa

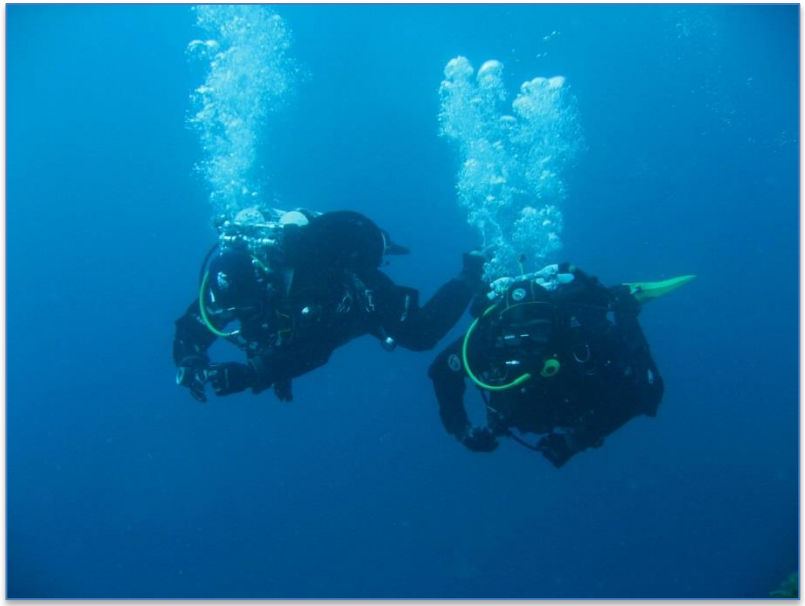
Ludzie

+

Bezpieczeństwo

+

Technologia



Dziękuję za uwagę

Kamil.kowalczuk@spnt.pl

Jak dokonać analizy skutków ataku i oszacować straty

- dodatkowo

-=[hacked]=- Telekomunikacja Polska S.A. -=[wybrykniete :-)]=-

POWERED
by
Prośiaczek

TELEKOMPLIKACJA POLSKA S.A.

Cześć, to my,
Puchatek Miś, Tygrys, Prosiaczek oraz Krzyś :-),
Kł apouchy i Króliczek, Sowa - Bardzo Mądra Gł owa.
Chcemy cał ą tepsę zdł awić i serwerów ich pozbawić.

speszial
pozdrowienia
dla
Agatki :**

Etapy procesu

- Minimalizacja skutków i strat – zanim przejdziemy do analizy
- Określenie zasobów, które uległy kompromitacji
- Analiza strat po fakcie wystąpienia zdarzenia
- Określenie grupy zasobów powiązanych z zasobem skompromitowanym:
  - przepływ danych
  - środowisko zasobu
  - warstwa sprzętowa

Minimalizacja skutków i strat – zanim przejdziemy do analizy (wyciągamy wnioski ze zdarzenia).

Na podstawie przeprowadzonej Analizy BIA zostaną określone skutki ataku cybernetycznego w obszarze:

- finansowym,
- wizerunkowym,
- zdrowie.

Analiza wpływu na działalność (Business Impact Analysis) to proces analizy funkcji biznesowych pozwalający określić, jaki wpływ na działalność organizacji miałoby ich ewentualne poważne zakłócenie lub przerwanie. Podstawą analizy BIA są procesy wykonywane przez organizację.

Analiza skutków ataku – Określenie zasobów, które uległy kompromitacji

- Informacje – co było celem?
- System – po przez jakie podatności się dostał atakujący?
- Proces – jakie procesy biznesowe zakłócił?
- Relacje – jakie inne systemy są zaangażowane w proces biznesowy?

Analiza skutków ataku – Analiza strat po fakcie wystąpienia zdarzenia

- Co się stało? – podmieniono stronę
- Przyczyna ataku? – popularność marki
- Jakie konsekwencje? – wizerunkowe, możliwy odpływ klientów

Konsekwencje wizerunkowe, są trudno mierzalne, ponieważ mogą mieć reperkusje długofalowe dla organizacji – trudna wycena

Analiza skutków ataku – określenie grupy zasobów powiązanych z zasobem skompromitowanym

- przepływ danych – jakie inne systemy przetwarzające informacje, były połączone i mogła w nich nastąpić kompromitacja.

- środowisko zasobu – jakie elementy systemów wspomagających mogły zostać zaatakowane:
  IIS, AD, Radius itp.

- warstwa sprzętowa – jakie elementy infrastruktury mogły zostać zaatakowane i wskazanie ich elementów:
  switche, firewalle itp. oraz czy występują podobne w innych systemach.

<u>Typujemy elementy do audytu – z uwzględnieniem krytycznych procesów biznesowych z analizy BIA</u>

Analiza skutków ataku – wycena

- **Ustawodawca,**
- **Administracja państwowa,**
- **Regulatorzy,**
- **Instytucje nadzorcze**

- **Klienci,**
- **Partnerzy biznesowi**

Wymogi prawne

Wymogi umowne

SLA, KPI

Cele biznesowe Stabilność finansowa

Odpowie-dzialność społeczna

- **Akcjonariusze**
- **Kredytodawcy**
- **Pracownicy**

- **Społeczeństwo**
- **Środowisko**