Zagrożenia w obszarze cyberprzestrzeni - ataki, detekcja zagrożeń i strategie obrony

dr inż. Maciej Miłostan, Instytut Informatyki Politechniki Poznańskiej / Dział Bezpieczeństwa ICT PCSS
Gerard Frankowski, Dział Bezpieczeństwa ICT PCSS

Codziennie jesteśmy bombardowani informacjami o cyberatakach

Atak hakerów na urząd pracy w Kutnie. Z konta zniknęło 180 tys. złotych

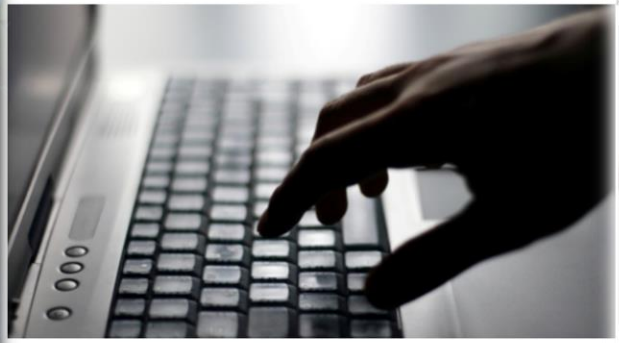
masz Dębowski 2 marca 2015 AKTUALIZACJA: 2 marca 2015 14:25

Marek Zakrzewski/archiwum Polskapresse

o audycie, przeprowadzonym w Powiatowym Urzędzie Pracy w Kutnie, ujawnio koło 180 tysięcy złotych.

Wielki cyberatak! Strony policji i banku zhakowane

PAP 21.11.2013 08:04



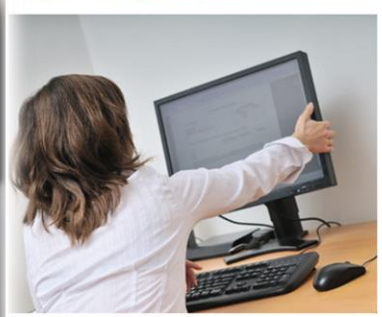
Zdjęcie ilustracyjne Foto: sxc.hu

Strony internetowe australijskiej policji federalnej i banku centralnego stały się celem ataku hakerów z Indonezji - poinformowały media w Australii w czasie napiętych stosunków dyplomatycznych między Canberrą a Dżakartą.

Miasto ofiarą cyberataku, stracili prawie milion złotych

0.01.15

Prawdopodobnie złośliwe oprogramowanie sprawiło, że urzędnicy z Jaworzna przelali 940 tys. zł na podstawiony przez cyberprzestępców numer konta. Policja i Prokuratura prowadzą w tej sprawie dochodzenie.



fot. Thinkstock

Do przestępstwa internetowego doszło 13 stycznia, w trakcie realizacji jednego z przelewów bankowych. Finalnie 940 tys. złotych z kasy Urzędu Miasta w Jaworznie zostało przelanych na podmienione przez cyberprzestępców konto. Sebastian Kuś, rzecznik prasowy Urzędu Miasta w Jaworznie, poinformował jedynie, że sprawą zajmuje się już Policja i Prokuratura i z uwagi na dobro prowadzonego dochodzenia nie jest możliwe udzielenie bardziej szczegółowych wyjaśnień.

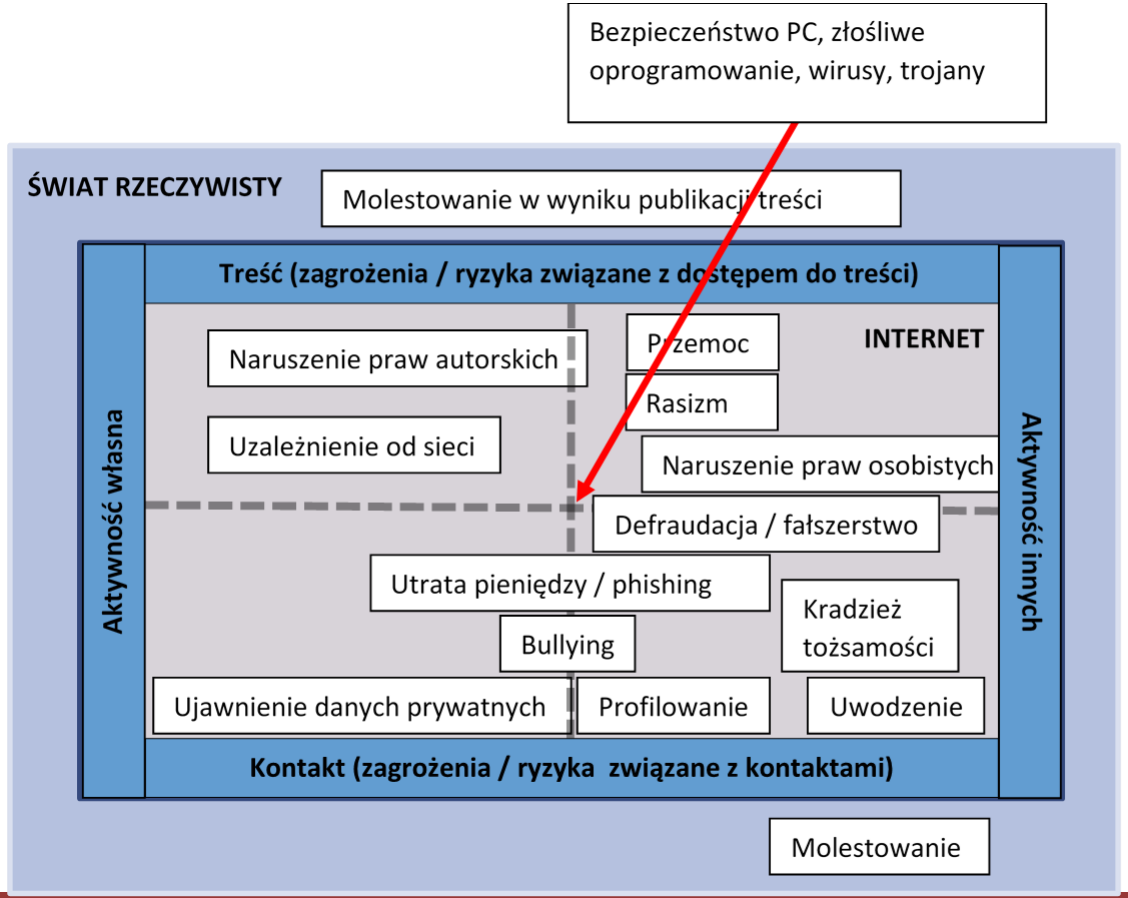
Zdaniem policyjnych ekspertów samorządowy komputer mógł zostać zainfekowany koniem trojańskim, który w momencie wykonywania przelewu podmienia numer konta odbiorcy. Ta sprawa pokazuje jak ważne jest posiadanie uaktualnionego oprogramowania oraz znajomość podstawowych zasad bezpiecznego korzystania z internetu, dodają eksperci.

Źródła: www.samorzad.lex.pl, www.polskieradio.pl, www.dzienniklodzki.pl

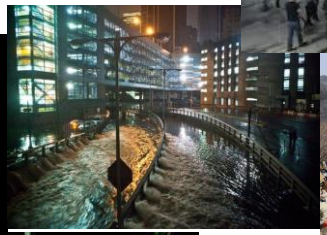
Ataki i zagrożenia

Ochrona osób / infrastruktury

- Zagrożenia online (dotyczące osób)
  - 3 Cs (content, contact, conduct)
- Ataki na infrastrukturę
  - DOS, DDoS, DRDoS
  - Włamania do systemów (np. CMS-ów)
  - Iniekcje kodu / osadzanie złośliwego kodu



High-tech Tots: Childhood in a Digital World, Ilene R. Berson,Michael J. Berso

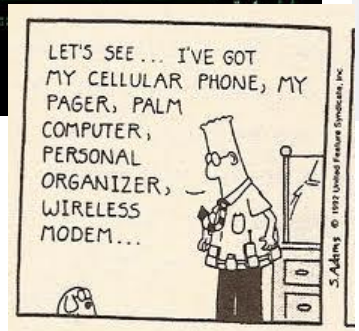



I AM FREE

hacker
inside
SYSTEM FAILURE

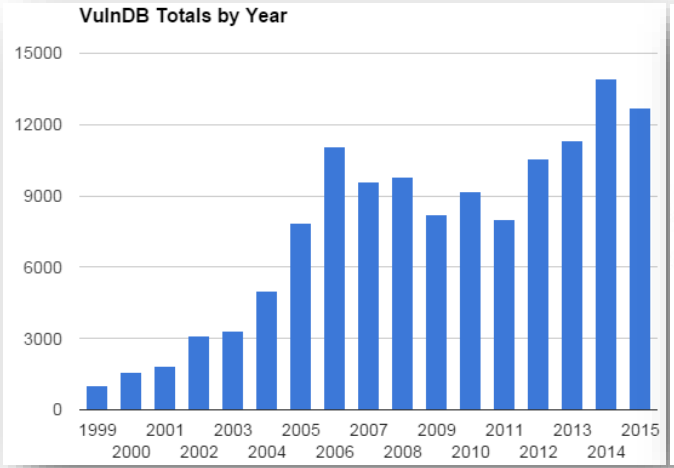

WARNING
TRANSCONTINENTAL
CABLE CROSSING
DO NOT DIG ANYWHERE IN THIS AREA
FOR LOCATION, CALL TOLL FREE
1-800-432-4770
AT&T 1-305-587-0910

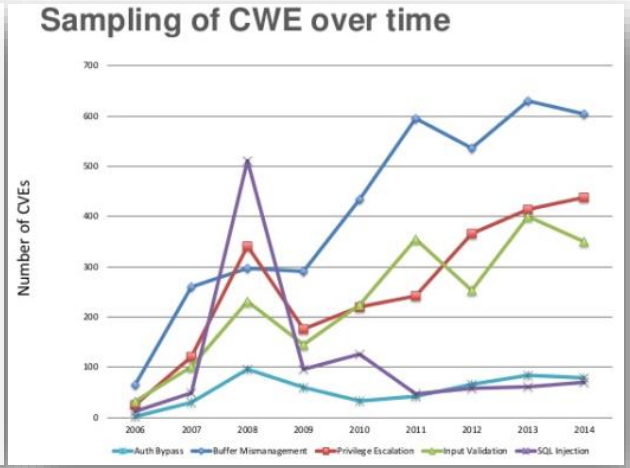

Our Disaster Recovery Plan
Goes Something Like This...
HELP!
HELP!
DILBERT
By Scott Adams


LET'S SEE... I'VE GOT
MY CELLULAR PHONE, MY
PAGER, PALM
COMPUTER,
PERSONAL
ORGANIZER,
WIRELESS
MODEM...
S. Adams © 1992 United Feature Syndicate, Inc.


UNDERSEA
CABLE
CUT BY
ANCHOR

Cyberataków jest coraz więcej, a ich natura zmienia się





Źródła: www.riskbasedsecurity.com, www.slideshare.net/EndgameInc/2015-cody-slidesharefinal

W 2015 r. niemal co trzeci (29%) komputer w środowisku biznesowym był celem co najmniej jednego ataku WWW.

Kaspersky Security Bulletin 2015

92% z 115000 analizowanych urządzeń Cisco podłączonych do Internetu posiadało luki bezpieczeństwa

Cisco Annual Security Report 2016

Celem jest coraz szersze grono przeciętnie coraz mniej świadomych użytkowników

- Urzędy i instytucje muszą działać online
- Kto korzysta z rozwiązań IT?
  - Administrator
  - Programista
  - Kierownictwo, asystenci
  - Kadrowy
  - Obsługa Petenta
  - Petent
  - … ?

W 48 z 50 przypadków osoby, które znalazły podrzuconego smartfona, uruchamiały zainstalowane tam aplikacje

Paweł Wojciechowski, Symantec

Problemy bezpieczeństwa mogą wystąpić na wielu warstwach

- Aplikacje – błędy bezpieczeństwa i konfiguracja
  - Używane oprogramowanie
  - Serwery (WWW, bazy danych)
  - System operacyjny
- Brak albo niewłaściwie dobrane systemy bezpieczeństwa
- Konfiguracja sieci oraz urządzeń
- Procedury i polityki
- Działania użytkownika
  - Także ataki socjotechniczne!

Na 200 przebadanych urzędników odpowiedzialnych za sprawy IT w gminach aż co trzecia osoba deklarowała, że systemy informatyczne ich urzędów nie są wyposażone w firewall

PBS, Gazeta Polska Codziennie

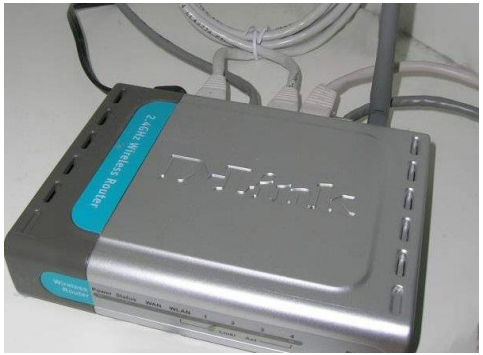
58% niebezpiecznych maili kierowanych jest do działów: sprzedaży, kontaktów z mediami, HR, PR

Maciej Iwanicki, Symantec

PRZYKŁADOWE ŹRÓDŁA ZAGROŻEŃ

Niepozorne urządzenie i duże zagrożenie

Misfortune Cookie



- 12 milionów routerów domowych podatne na ataki
- RomPager < 4.34 (AllegroSoft)
- Używany w 200 modelach włącznie z Linksys, D-Link, Edimax, Huawei, TP-Link, ZTE, and ZyXEL
- CVE-2014-9222 (CVSS score 9.7)
- http://mis.fortunecook.ie

LizardSquad

- Grupa hakerów odpowiedzialna za szereg ataków przeprowadzonych w grudniu, w trakcie świąt Bożego Narodzenia ‘14, na serwisy Sony, Xbox Live oraz sieć Tor,
- Wykorzystuje w swoim botnecie bardzo dużą liczbę przejętych **routerów domowych**.
- LizardSquad oferuje na czarnym rynku, w przystępnych cenach, usługi i narzędzia umożliwiające przeprowadzanie ataków DDoS.

Z czym kojarzy się Państwu zegar?

Synchronizacja czasu = NTP

Czy NTP może być groźne?

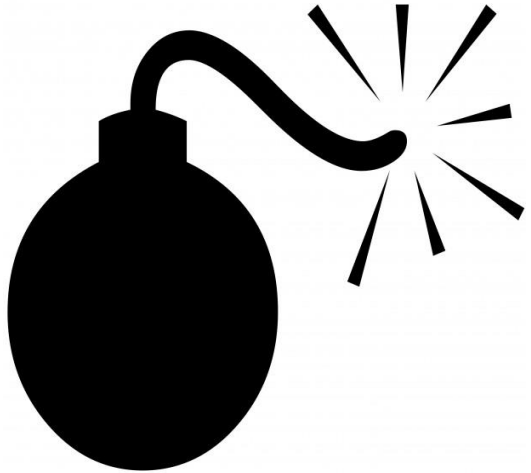
Problemy z NTP

- NTPDC monlist

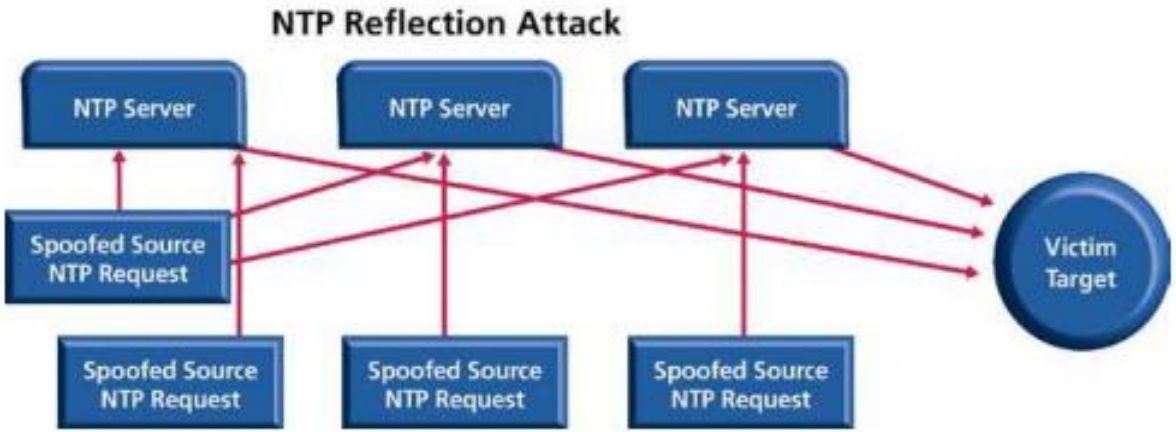
CVE-2013-5211 / VU#348126

- ACLe bazujące na IPv6 ::1 można obejść

Sec 2672 / CVE-2014-9298 / VU#852879



Atak DRDoS z użyciem NTP



Prolexic

Amplifikacja

- Stopień amplifikacji w przypadku NTP wynosi, w zależności od konfiguracji:

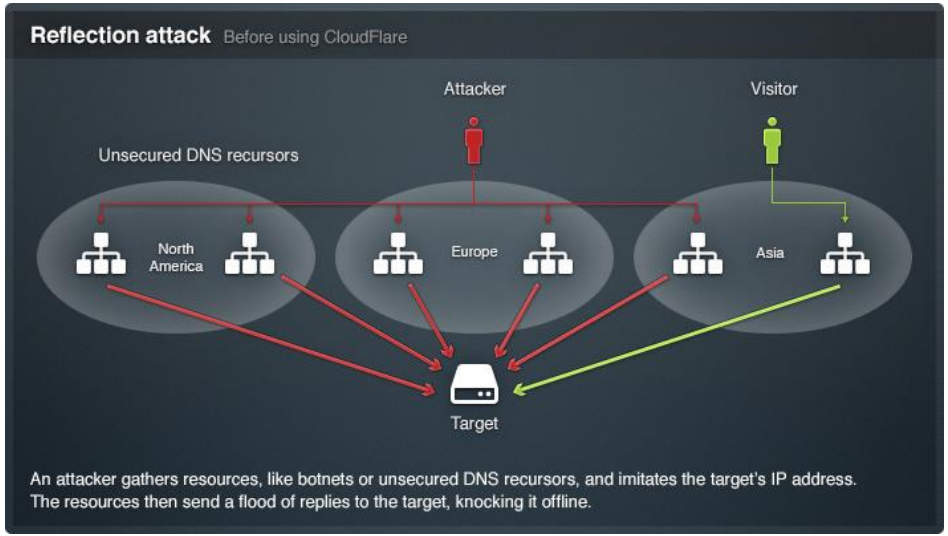
  20:1, 200:1 lub więcej.
- Co to jest stopień amplifikacji?
  - 1 bajt zapytania równa się 20 bajtów odpowiedzi
- Czy inne usługi też można do tego wykorzystać?
  - Tak.

Serwery nazw (DNS)

- Używamy ich codziennie
- Czy są groźne?
- Mogą być…

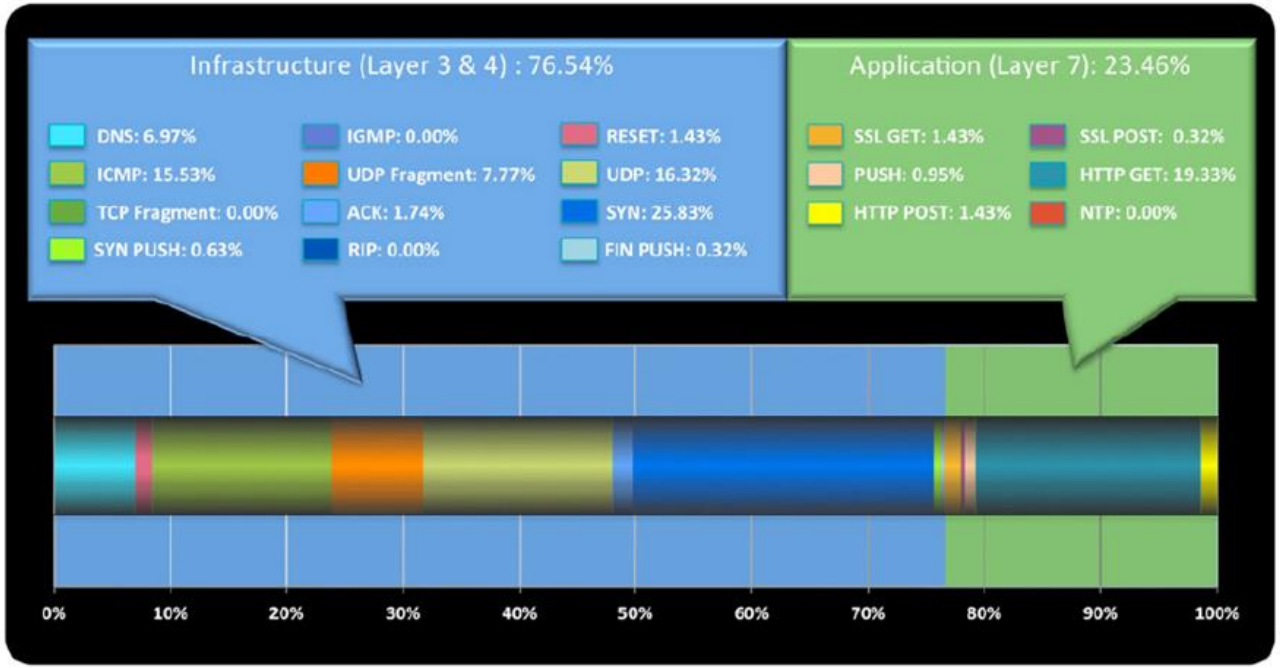
Ataki D(r)DoS z użyciem DNS

- Distributed (reflected) Denial of Services (współczynnik amplifikacji 70:1)



Źródło : http://cloudflare.com

Rodzaje ataków (Q1 2013) - Prolexic



Źródło : http://www.prolexic.com

Atak na Spamhaus

- Marzec 2013
- Największy odnotowany w historii
  - 300 Gbps w szczytowym momencie
- Trzy fazy:
  - Spamhaus
  - Cloudflare
  - Usługodawcy Cloudflare

Źródło : http://www.enisa.europa.eu

Kluczowi gracze – historia w tle

SPAMHAUS

CLOUDFLARE

Metody ataku na SpamHaus

- Niezbyt wyrafinowane, ale skuteczne
  - Amplifikacja przy użyciu otwartych „resolwerów” DNS (OpenDNS resolvers) – co ciekawe, niektóre domowe routery uruchamiają tego typu usługi domyślnie
  - Spoofing (fałszowanie) adresów źródłowych
- Ataki na protokół BGP
  - Ogłaszanie fałszywych prefix-ów w węzłach międzyoperatorskich (IX), m.in. w NL-IX

```
router# show ip bgp 204.16.254.40
   BGP routing table entry for 204.16.254.40/32
   Paths: (1 available, best #1, table Default-IP-Routing-
Table) Advertised to non peer-group peers: xxx.xxx.xxx.xxx
34109 51787 1198 193.239.116.204 from 193.239.116.204
(84.22.127.134) Origin IGP, metric 10, localpref 140,
valid, external, best Last update: Tue Jan 5 11:57:27 1971
```

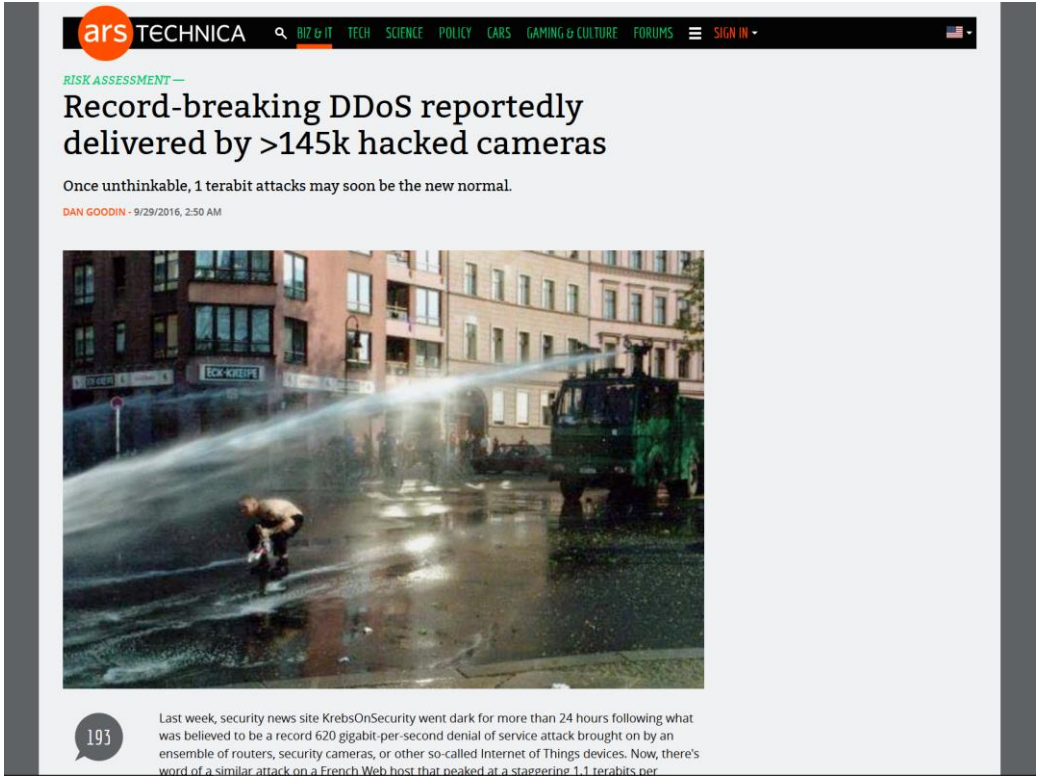
Spamhaus

Cyber Bunker

DDoS z użyciem kamer

Wrzesień 2016

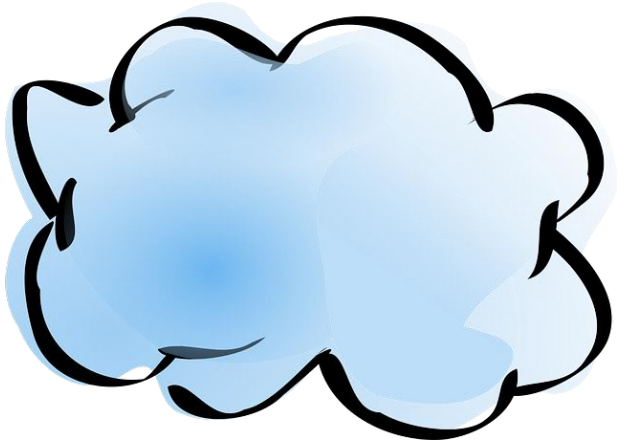
- Szereg ataków od 620Gbps do 1.1Tbps



DDoSy w Polsce?

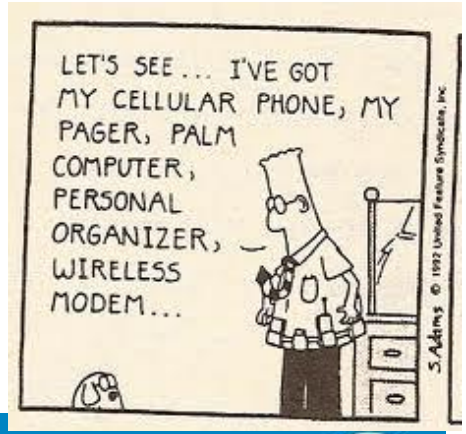
- Najbardziej nagłośnione przypadki:
  - Allegro
  - Inea
  - ?

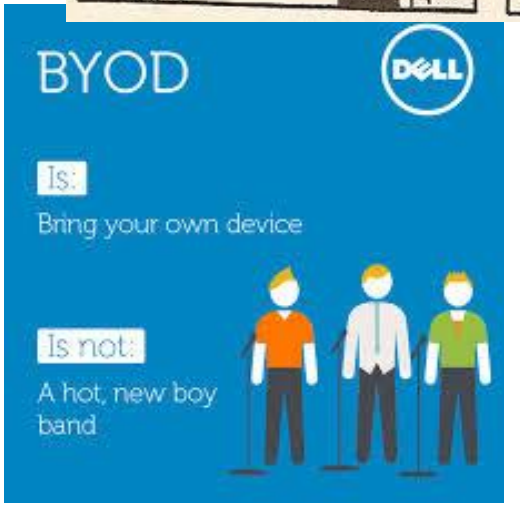
Chmury, urządzenie przenośne



BYOD, chmury itp.

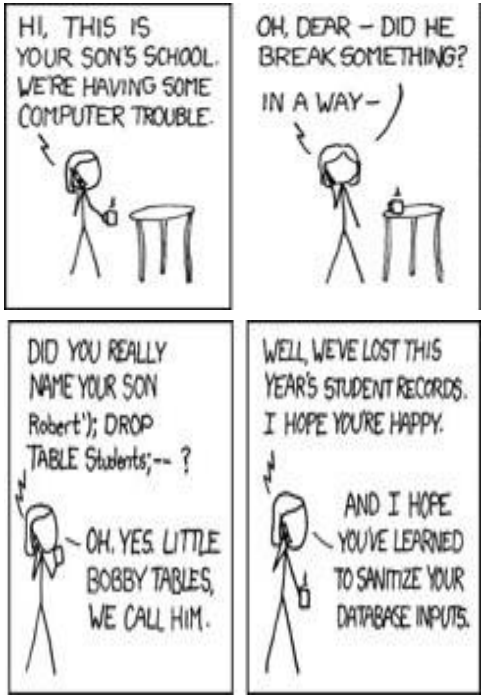
- Nowe trendy, nowe problemy, nowa odsłona starych zagrożeń
- Prywatne urządzenia w sieci firmowej – za, a nawet przeciw
- Przechowywanie danych firmowych w chmurach (przy użyciu służbowych i prywatnych urządzeń)





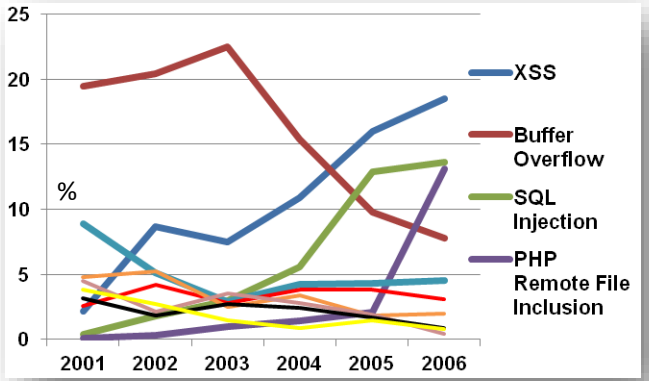
Ataki na aplikacje / usługi udostępniane w sieci

- Odmowa usługi (ang. DoS/DDoS)
- Cross Site Scripting (ang. XSS)
- Przepełnienie bufora (ang. Buffer Overflow)
- Wstrzyknięcie kodu SQL (ang. SQL Injection)
- Dołączenie zdalnych (z innego serwera) plików (ang. Remote File Inclusion)

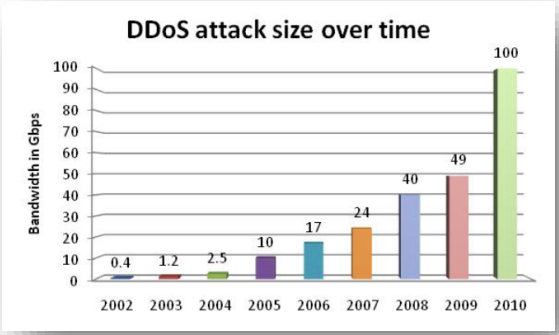


(R)Ewolucja zagrożeń w sektorze IT

- Nowe technologie – nowe zagrożenia
- Bezpieczeństwo też jest procesem, a nie stanem!



Źródło: cve.mitre.org



Źródło: www.internet-security-days.com

Czynnik ludzki

- Cel ataku: coraz szersze grono użytkowników o różnych stopniach technicznego zaawansowania
- Dziś każda większa firma musi działać *online*
  - Wymieniać informacje
  - Istnieć w Internecie
- Kto korzysta z rozwiązań IT?
  - Administrator?
  - Programista?
  - Kadrowy?
  - Obsługa Klienta?
  - Przedstawiciel handlowy?
  - Asystent?
  - … ?

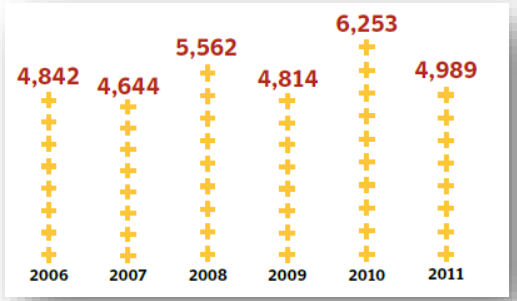
Google

W 48 z 50 przypadków osoby, które znalazły podrzuconego smartfona, uruchamiały zainstalowane tam aplikacje

Paweł Wojciechowski, Symantec – maj 2012

Wiele miejsc, gdzie może wystąpić problem

- Oprogramowanie – podatności i konfiguracja
  - Używane aplikacje klienckie
  - Serwery (WWW, bazy danych)
  - System operacyjny
  - Brak albo niewłaściwe systemy bezpieczeństwa
- Konfiguracja sieci, urządzeń
- Procedury i polityki
- Działania użytkownika
  - Także inżynieria społeczna!

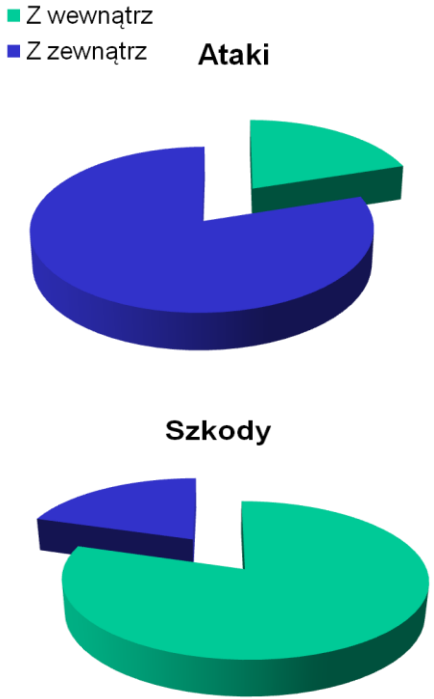


Co roku odkrywa się kilka tysięcy podatności bezpieczeństwa oprogramowania (w 2011 roku zgłoszono ich 4989)

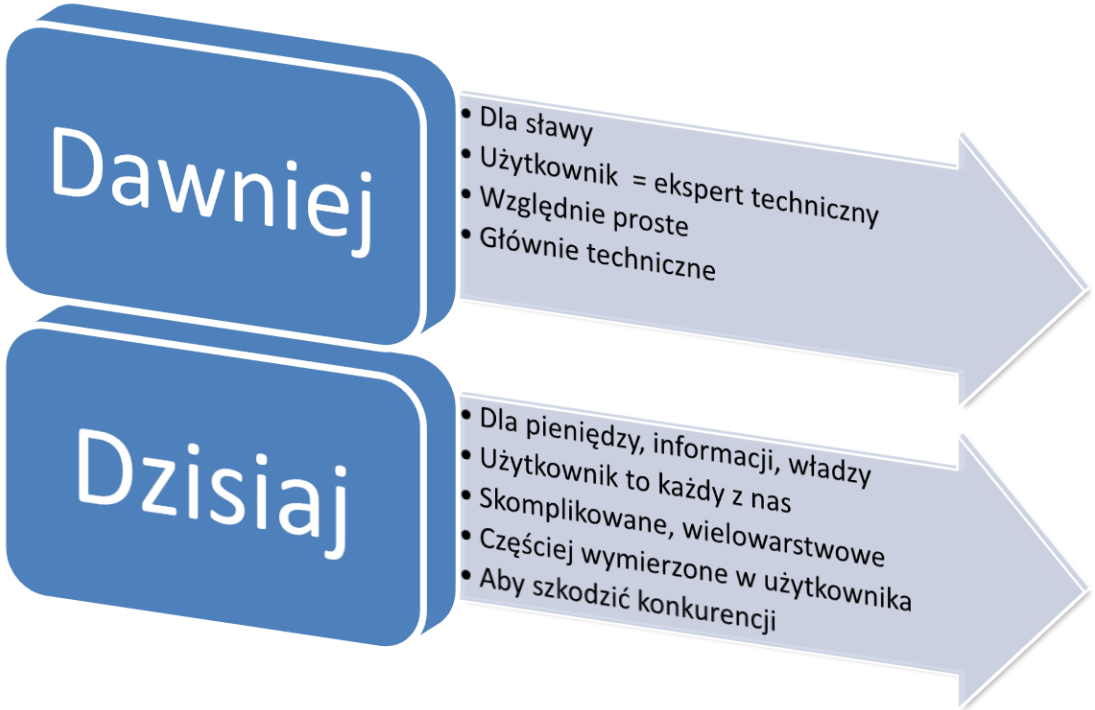
Symantec Internet Threat Report – kwiecień 2012

Ataki z zewnątrz i od wewnątrz

- Sieć często jest odpowiednio chroniona od strony Internetu
- Sieć wewnętrzną chroni się nie tak dobrze, bo traktowana jest jako środowisko zaufane



Ewolucja zagrożeń IT



Ataki Advanced Persistent Threats

- Ataki APT są wykonywane przy pomocy **zaawansowanych**, **ukierunkowanych scenariuszy** w celu **uzyskania i utrzymania** dostępu (dla **stałej korzyści**)
  - Np. kradzież tajemnic firmy
  - Ofiarą padły m.in. Google i Adobe
- Ataki APT wykorzystują:
  - Wyjątkowo wyrafinowane złośliwe oprogramowanie
  - Nieznane podatności, tzw. *0-day*
  - Inżynierię społeczną

If anyone attempts to sell your organization on a hardware or software solution for APT, they either don't understand APT, don't really understand how computers work, or are lying – or possibly all three

Gavin Reid, Cisco CSIRT – marzec 2011

Przykład

- Specjalnie spreparowany e-mail z załącznikiem doc/pdf/jpg etc.
- Z zaproszeniem na bankiet w Ratuszu albo pod Sejmem / zapytaniem ofertowym / zdjęciem kochanki(-a)
- W pliku osadzony dla przykładu obiekt flash (w ciągu ubiegłych lat wykrywano dużo podatności)
- Po otwarciu skrypt Flash uruchamiany jest np. przez MS Word za pomocą Internet Explorera
- FlashPlayer wykonuje złośliwy kod z poziomu przeglądarki
- Kod łączy się z Internetem i pobiera kolejną porcję malware-u.
- Modyfikowane są atrybuty złośliwych plików, aby utrudnić identyfikację
- Komputer został zainfekowany i może być inwigilowany

Czasem nie trzeba nawet podatności

Czynnik ludzki

Temat: Re : Politechnika Poznańska-Potwierdzić swoją tożsamość Webmail
Od: Politechnika Poznańska <maria.lupa@im.pcz.pl>
Data: 12 Lutego 2013, 6:20 am, Wt
Do: undisclosed-recipients:;
Priorytet: Normalny
Opcje: Pokaż cały nagłówek | Podgląd wesji do wydruku | Pobierz jako plik | View Message Details

Potwierdzić swoją tożsamość Webmail

Skrzynka pocztowa przekroczyła jeden lub więcej wielkości limitów ustalonych przez administratora. Możesz nie być w stanie wysyłać i odbierać nowe wiadomości, dopóki rozmiar skrzynki pocztowej jest zmniejszona.

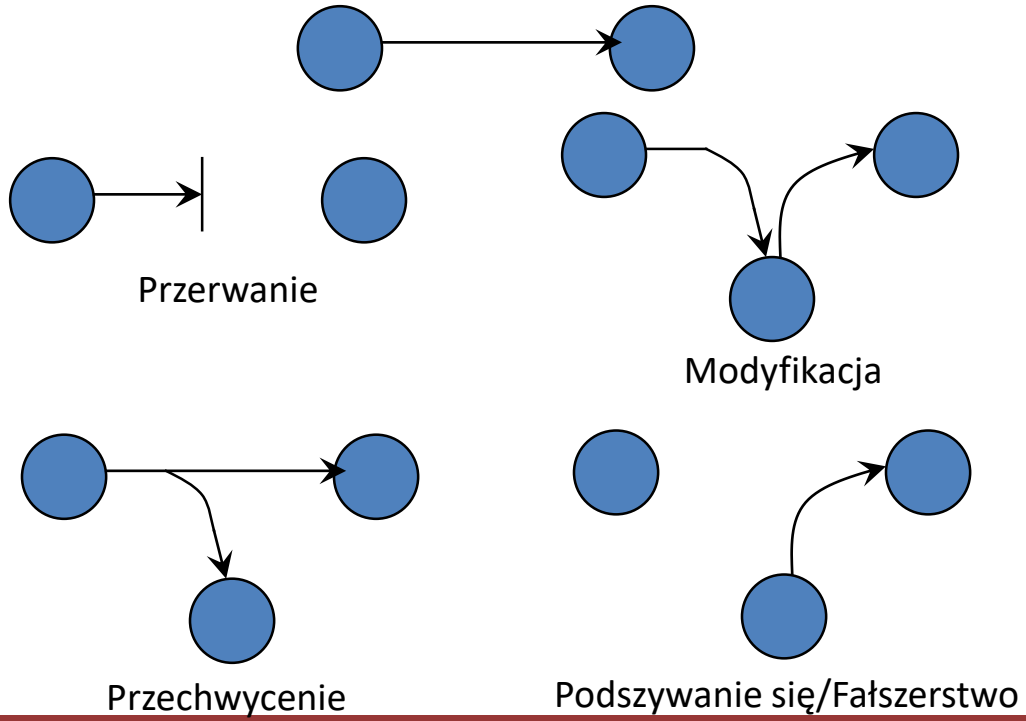
Aby udostępnić więcej miejsca, proszę kliknąć tutaj poniżej w celu skorygowania danych konta.

Kliknij tutaj

Dziękujemy i przepraszamy za niedogodności.

Administratora systemu.

Ataki na bezpieczeństwo danych (w tranzycie)



Dziurawe biblioteki kryptograficzne

- OpenSSL – heartbleed

http://heartbleed.com/

- Twoja pamięć w naszych rękach ☺
- Aktualne bug-i:

https://www.openssl.org/news/vulnerabilities.html

- **CVE-2015-0291:**

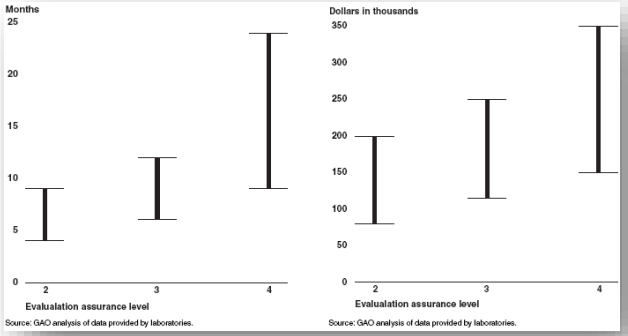
[High severity] 19th March 2015

Jak się chronić?

Czy jest to w ogóle możliwe?

Realia i ekonomia bezpieczeństwa

- Nie są dostępne systemy w 100% bezpieczne



Koszt czasowy oraz finansowy certyfikacji systemu do poziomu EAL4: do 2 lat i 350 000 USD (formalna poprawność to poziom EAL7!)

US Government Accountability Office - 2006

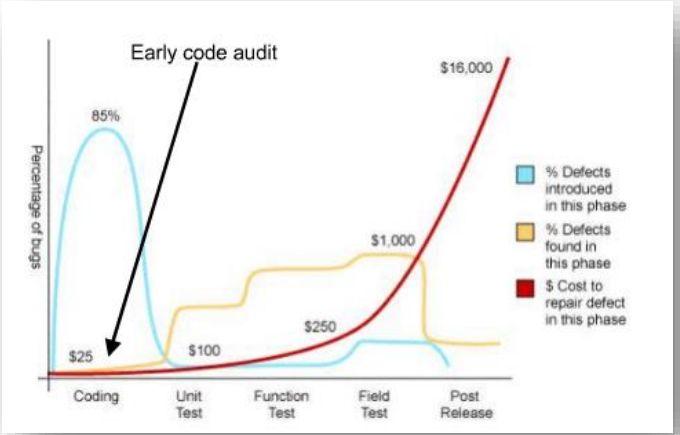
- Ale koszt ataku musi być tylko **wyższy niż oczekiwany zysk**
  - Nie jest potrzebne całkowite bezpieczeństwo!
  - Trzeba mnożyć trudności napastnikowi
  - Koszt zabezpieczeń musi być dostosowany do wartości aktywów

Kompleksowa ochrona

- Bezpieczeństwo nie może być cechą dodaną po zakończeniu projektu (to za drogo kosztuje)

Przykład: błędy oprogramowania. Naprawianie ich po wydaniu aplikacji może być kilkaset razy droższe niż na etapie pisania kodu!

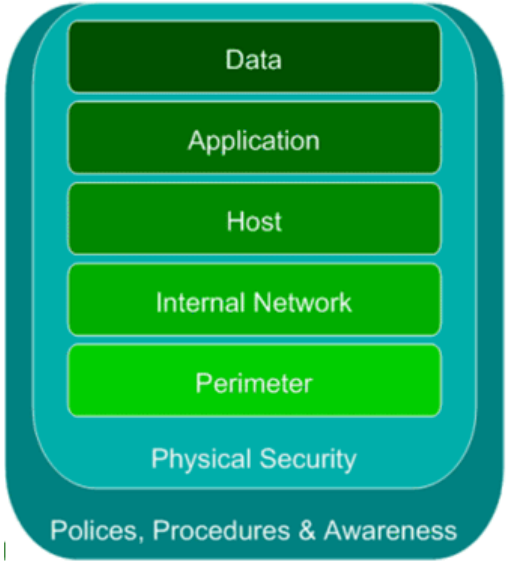
Marco M. Morana - 2006



Źródło: *Building Security Into The Software Life Cycle,* Marco M. Morana, 2006

Strategia Defense-in-Depth

- Ochrona dogłębna – na wielu różnych warstwach
  - Napastnik znajdzie błąd np. w aplikacji WWW, ale nie wykorzysta go, gdy:
    1. Serwer WWW jest dobrze skonfigurowany. Nie można wykonać w zaatakowanym systemie dowolnego kodu.
    2. System IDS wykryje niepożądane działania i powiadomi administratora.
  - Strategia podwyższa koszt udanego ataku, czyniąc go potencjalnie nieopłacalnym dla napastnika



Omówienie wybranych warstw zabezpieczeń

Ochrona serwera

- Konfiguracja systemu operacyjnego
  - Poprawna instalacja
  - Wybór ról serwera
  - Konfiguracja systemu firewall
  - Szablony zabezpieczeń
  - Konfiguracja sieci
  - Aktualizacje
  - Ochrona antywirusowa
  - Użytkownicy
  - Konfiguracja inspekcji, dzienników zdarzeń
- Konfiguracja usług
  - Minimalizacja uprawnień użytkownika (NTFS, rejestr)
  - Ustawienie *quoty*
  - Logowanie działania usługi
  - Przydziały zasobów pamięciowych i procesora
  - Zasady specyficzne dla usługi
- Narzędzia producenta (dla serwerów Windows)
  - Microsoft Security Compliance Manager
  - Microsoft Web Configuration Analyzer
  - Microsoft Baseline Security Analyzer

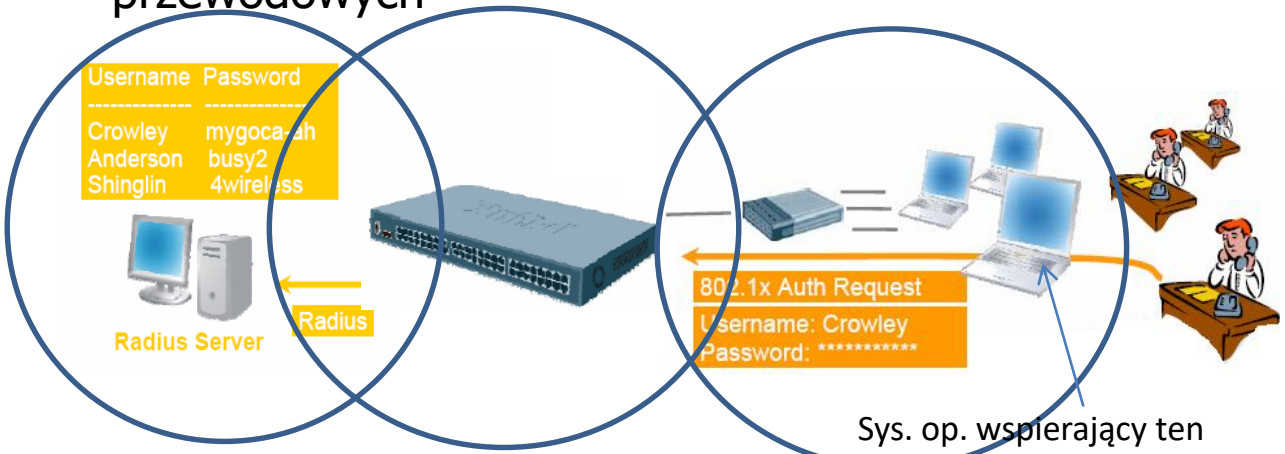
Omówienie wybranych warstw zabezpieczeń – ochrona sieci

Ochrona sieci

- Ograniczony dostęp do sieci komputerowej
  - Uwierzytelnianie użytkowników/urządzeń przy podłączaniu do sieci (IEEE 802.1x)
- Filtrowanie i profilowanie ruchu
- Wdrożenie proaktywnych i reaktywnych mechanizmów ochrony przed atakami (np. przed DDoS)
  - Proaktywne – usuwanie podatności, ale także podnoszenie świadomości użytkowników i pracowników
  - Reaktywne – detekcja anomalii i szybka reakcja, (IDS, fail2ban, OSSEC itp.)

IEEE 802.1X

- Protokół uwierzytelniania w sieciach LAN:
  - bezprzewodowych
  - przewodowych

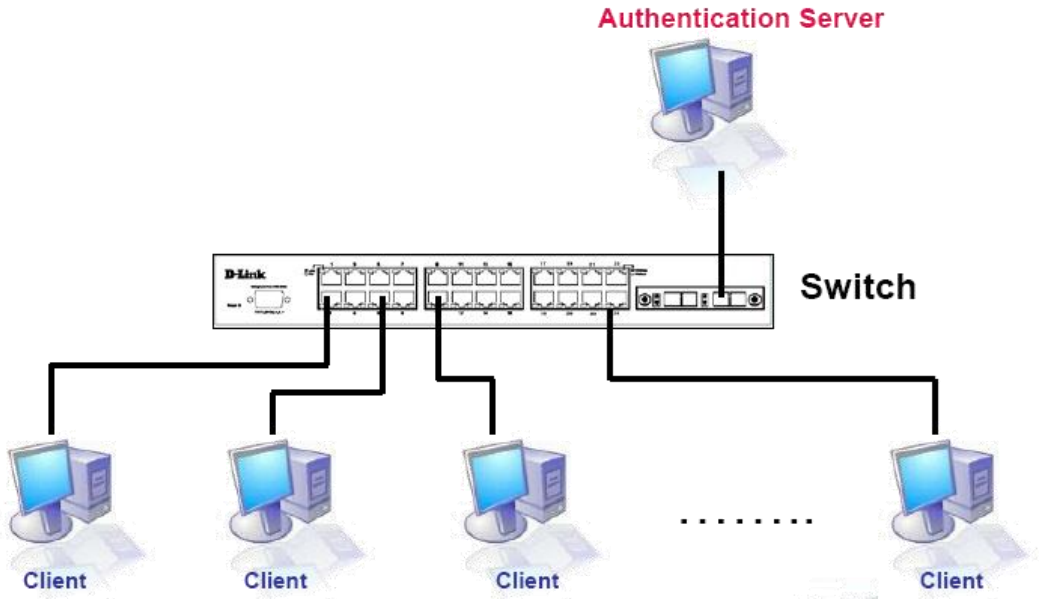


Sys. op. wspierający ten standard

ftp://ftp.dlink.it/FAQs/802.1x.pdf

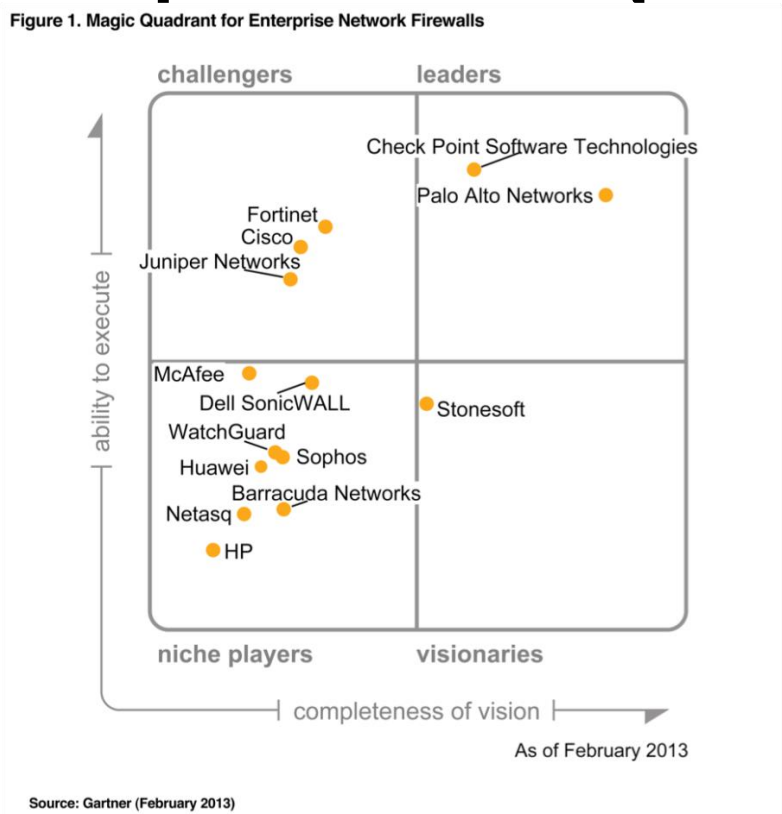
IEEE 802.1x (1)

- Standard ten definiuje kontrolę dostępu opartą na modelu klient-serwer wraz z protokołami uwierzytelniania uniemożliwiającymi dostęp do sieci nieautoryzowanym urządzeniom za pośrednictwem publicznie dostępnych portów. Serwer uwierzytelniania przeprowadza uwierzytelnianie każdego klient, który podłącza się do sieci, zanim zaoferuje mu jakąkolwiek usługę.



Zapora nowej generacji i kompleksowe zarządzanie bezpieczeństwem

- Next Generation Firewall
  - Filtracja w warstwie aplikacji
  - Coś więcej niż tylko blokowanie per port/ip/protokół
- UTM (ang. unified threat management)
  - „Kompleksowe zarządzanie”



Strategie obrony przed DDoS

- Po atakach na SpamHaus ENISA wydała w swoim dokumencie rekomendacje:
  - Agencja ENISA (UE): „Internet Service Providers fail to apply filters against big cyber attacks”
- Wskazano trzy obszary, w których należy wdrożyć najlepsze bieżące praktyki (BCP, best current practice) :
  - implementacja BCP 38 – ograniczenie fałszowania adresów źródłowych
  - implementacja BCP 140 – zabezpieczenie DNS
  - zabezpieczenie się przed atakami BGP

BCP 38

- Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
  - Rekomendacja opublikowana w maju 2000 (13 lat temu!)
  - Celem jest zapobieganie fałszowaniu źródłowych adresów IP
  - Filtrowanie ruchu źródłowego (Ingreess Filtering)
    - uRPF (Unicast Reverse Path Forwarding) RFC3704 działa w 3 trybach, pakiet jest przekazywany, gdy pojawia się na interfejsie będącym:
      - Strict mode (najlepszą ścieżką do nadawcy)
      - Feasible mode (jedną ze ścieżek do nadawcy)
      - Loose mode (istnieje ścieżka do nadawcy)
  - Wdrożenie zalecenia pozwala na łatwe zlokalizowanie źródła ataku

Źródła:
http://tools.ietf.org/html/bcp38
http://tools.ietf.org/html/rfc3704

BCP 140 (1)

- Preventing Use of Recursive Nameservers in Reflector Attacks
  - Rekomendacja opublikowana w październiku 2008
  - Zbiór dobrych praktyk dotyczących konfiguracji rekursywnych serwerów DNS
  - Wprowadzenie rozszerzeń EDNS0 (RFC2671) wymaganych przez DNSSEC zwiększyło potencjał serwerów DNS do wykorzystania ich jako amplifikatorów ataków sieciowych (query/packet size = 80)

BCP 140 (2)

Rekomendacje:

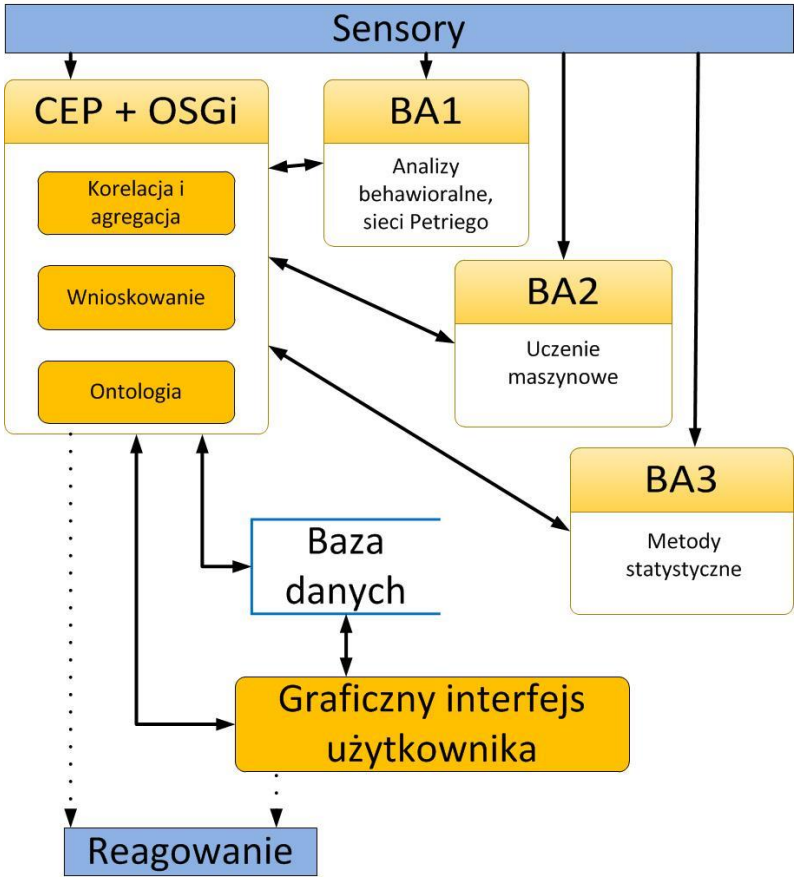
- *By default, nameservers **SHOULD NOT** offer **recursive service** to **external** networks*
- Ograniczenie dostępu do rekursywnych serwerów DNS wyłącznie do własnych sieci i interfejsów
- Ewentualne wdrożenie mechanizmu podpisywania zapytań TSIG w celu autoryzacji klientów
- Użytkownicy mobilni powinni korzystać z lokalnych buforujących resolverów uruchomionych na urządzeniach mobilnych, bądź korzystać serwerów DNS za pośrednictwem VPN

Źródła:

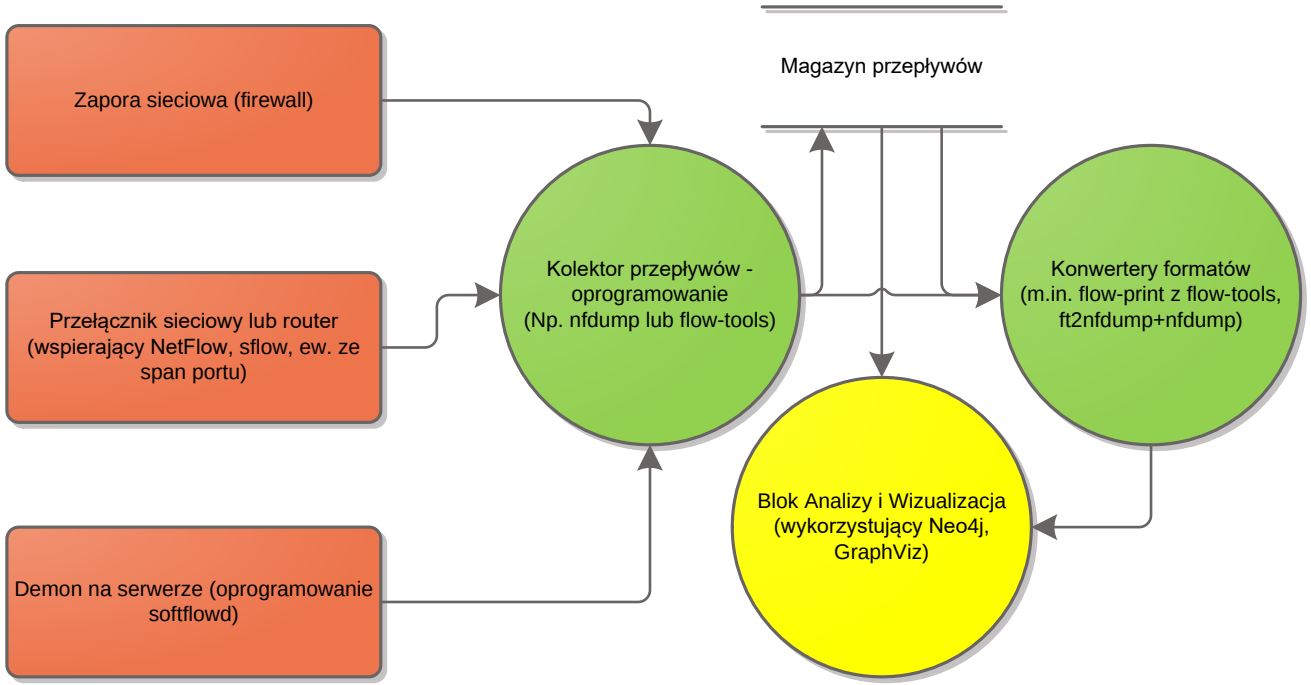
- http://tools.ietf.org/html/bcp140
- http://tools.ietf.org/html/rfc2671

Monitorowanie sieci

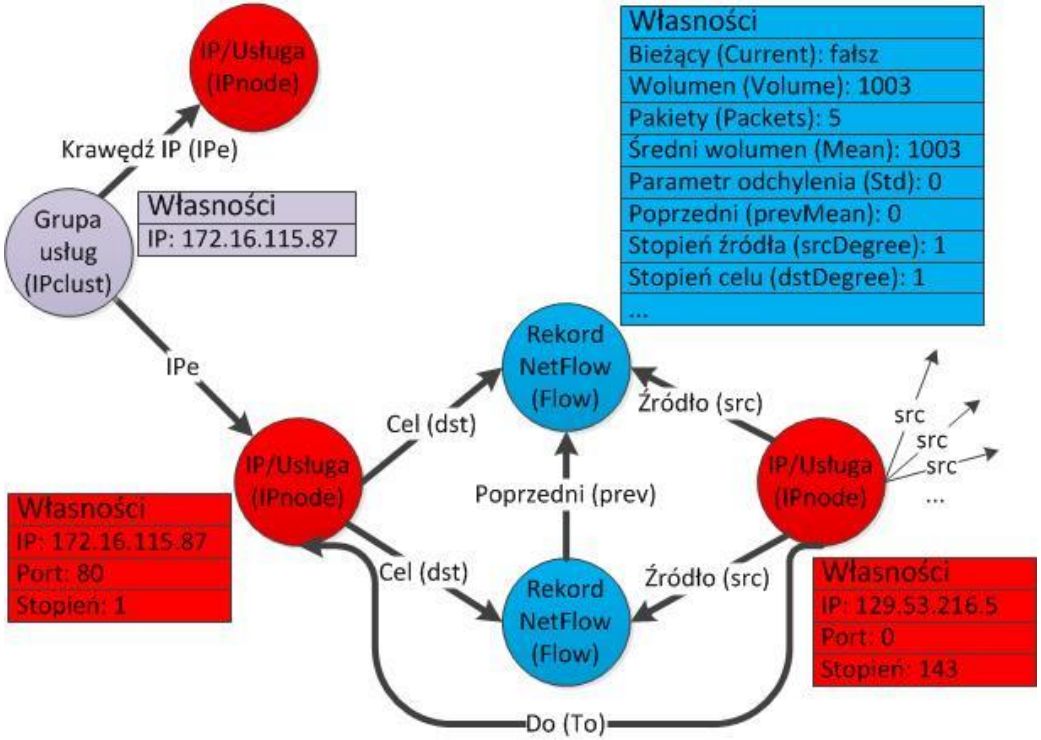
- Z wykorzystaniem sond zainstalowanych w wielu warstwach
- W wielu miejscach infrastruktury
- Z wykorzystaniem różnych metod detekcji
- Przetwarzanie i identyfikacja zdarzeń złożonych



Analiza rekordów przepływów (NetFlows)



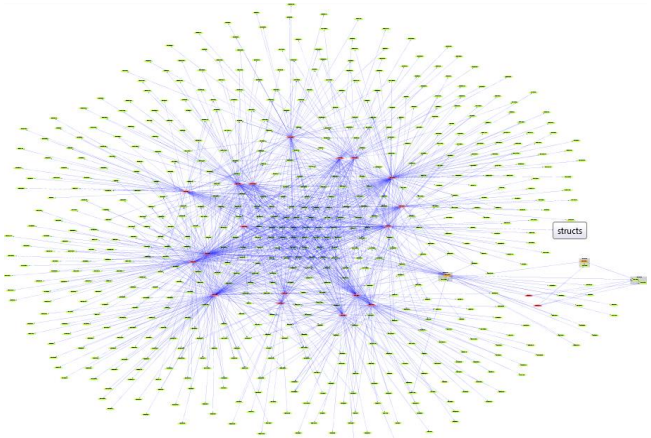
Grafy przepływów

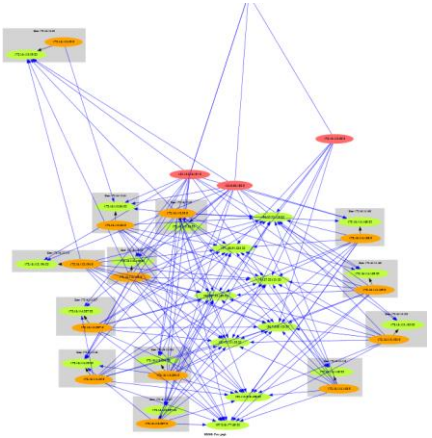


Examples of simplified NetFlow graphs

DARPA sets

HTTP+SSH vs. SMTP





Odpytywanie grafowej bazy danych

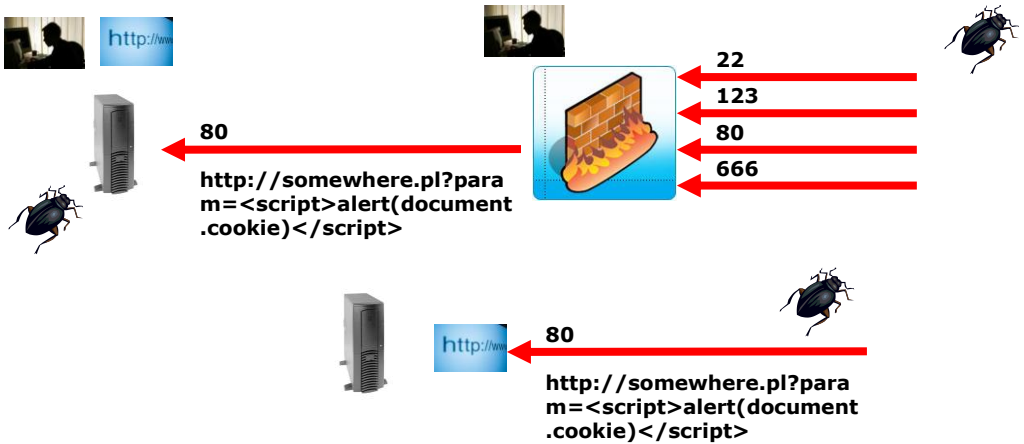
- Identyfikacja usług nasłuchujących na wysokich portach i ich klientów
- Cypher query:

```
MATCH (ip:IPclust)-->(s:IPnode)-->
   (f:Flow {current:true})<--(d:IPnode)
WHERE  d.port >1024
RETURN DISTINCT ip.ip,d.ip;
```

s.ip	d.ip
172.16.114.168	194.27.251.21
172.16.114.168	197.182.91.233
172.16.114.168	195.115.218.108
172.16.114.50	194.27.251.21
172.16.114.50	197.218.177.69
172.16.114.50	195.115.218.108
172.16.114.50	196.37.75.158
172.16.114.50	195.73.151.50
172.16.114.50	197.182.91.233
172.16.114.50	199.174.194.16

Ochrona aplikacji

- Dlaczego potrzebujemy ochrony na poziomie aplikacji?
  - Trudności w odseparowaniu ruchu złośliwego



Ochrona aplikacji (2)

- Kluczowe obszary
  - Kompletność projektu pod kątem zabezpieczeń
  - Filtrowanie danych wejściowych
  - Jakość tworzonego kodu
  - Konfigurowalność i łatwość użytkowania
- Zabezpieczenia
  - Ocena koncepcji/projektu
  - Statyczna lub dynamiczna analiza kodu
    - Testy automatyczne oraz manualne
  - Testy penetracyjne

ZAPEWNIANIE BEZPIECZEŃSTWA JAKO PROCES CIĄGŁY

Bezpieczeństwo jako proces

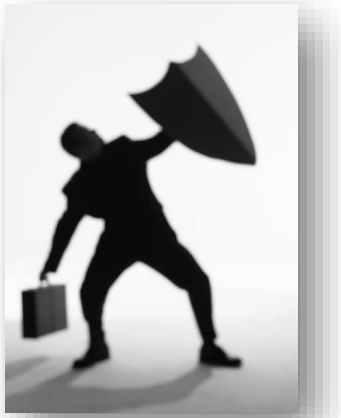
- Ocena bezpieczeństwa jest ważna tylko dla określonego stanu
- A zmienia się przecież:
  - Stan wiedzy w zakresie bezpieczeństwa IT
  - Analizowane środowisko (dodatkowe aplikacje, nowe serwery, więcej kont użytkowników, inny administrator…)

Niezbędne elementy strategii obrony

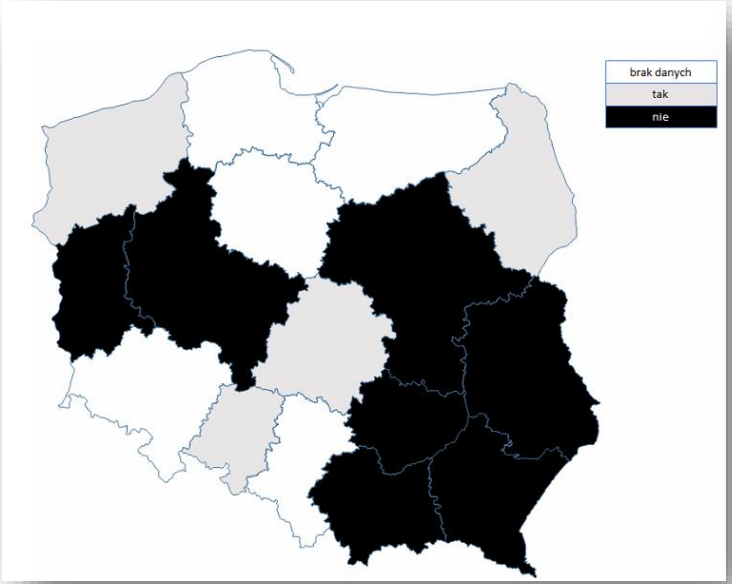
- Sprzęt/oprogramowanie:
  - Firewalle klasyczne i firewalle następnej generacji (aplikacyjne),
  - Filtry antywirusowe i antyspamowe
  - Automatyczne analizatory logów
- Ewaluacja zewnętrzna
  - Pentesty,
  - Audyty zabezpieczeń,
  - Audyty aplikacji (typu black box i white box)
- Szkolenia
  - Podnoszenie świadomości użytkowników
  - Krzewienie dobrych praktyk programistycznych

Najlepsza strategia ochrony?

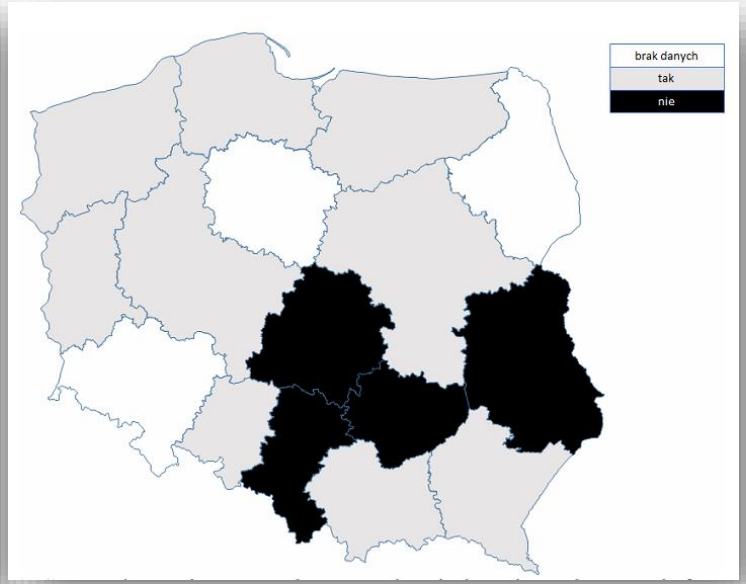
- Docenienie wagi problemu
  - Własny dział (zespół) ds. bezpieczeństwa
- Bezpieczeństwo wbudowane w cykl życia infrastruktury lub systemu
  - Od projektu, przez implementację, wdrożenie aż do utrzymania
- Ochrona na wielu warstwach
- Budowanie świadomości użytkowników
- Badania poziomu bezpieczeństwa
  - Cykliczne
  - Wewnętrzne i zewnętrzne (niezależne)
- Rozważenie outsourcingu bezpieczeństwa IT



Stan zabezpieczeń w sektorze administracji polepsza się, ale wymaga dalszej poprawy



Stan wdrożenia systemów zarządzania bezpieczeństwem informacji (SZBI) w urzędach wojewódzkich.



Stan wdrożenia SZBI w urzędach marszałkowskich. Źródło*: Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*.

Zatem w jaki sposób się chronić?

Środki zaradcze

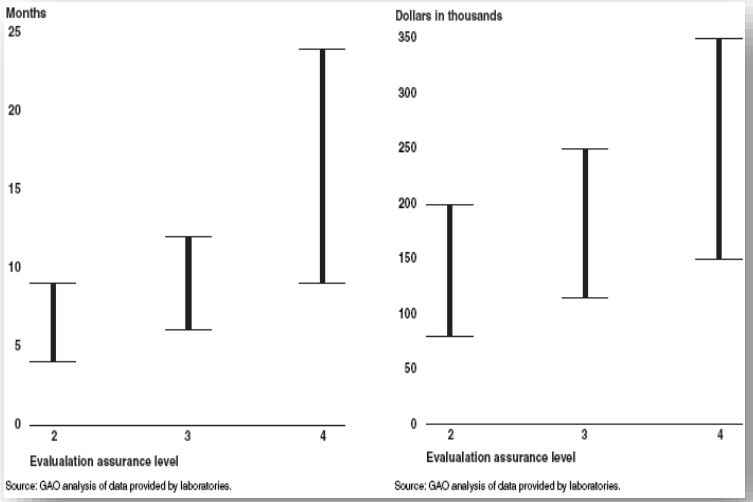
Elementy bazowe

- Wdrożenie systemów zabezpieczeń (zapory sieciowe, filtry sieci web, systemy IDS/IPS, filtry na poziomie DNS, filtry w warstwie aplikacji)
- Podnoszenie świadomości użytkowników sieci (pracowników, uczniów, społeczeństwa) – praca u podstaw
- Automatyczne / regularne aktualizacje krytycznych luk w systemach (nie tylko operacyjnych)
- Ustalone procedury i polityki (przynajmniej w zakresie ochrony informacji)
- Regularna ewaluacja skuteczności podjętych działań
- Właściwe zarządzanie projektami informatycznymi

Czy potrzebujemy całkowitego bezpieczeństwa?

Rzut oka na ekonomię zabezpieczeń

- Koszt ataku musi być tylko wyższy niż oczekiwany zysk
- Nie jest potrzebne całkowite bezpieczeństwo!
  - Nie jest ono zresztą realnie osiągalne
- Trzeba mnożyć trudności napastnikowi
- Koszt zabezpieczeń musi być dostosowany do wartości aktywów
- Problem z inwestycją w bezpieczeństwo: nie widać zysku
  - Za to straty po udanym ataku – już tak



Koszt czasowy i finansowy certyfikacji systemu do poziomu EAL4: 2 lata, 350 000 USD (formalna poprawność to poziom EAL7!)
US Government Accountability Office

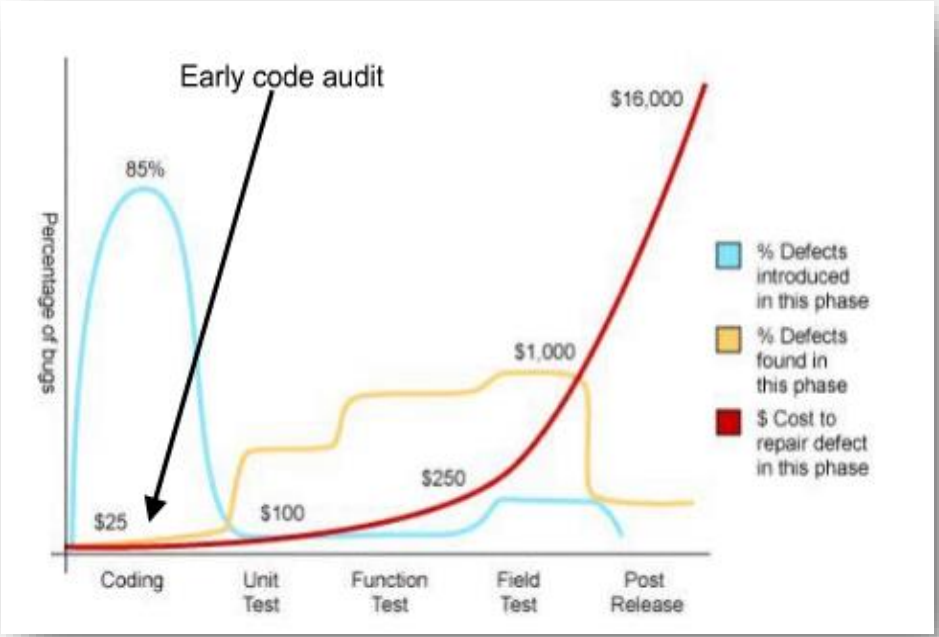
Najtaniej dbać o bezpieczeństwo od początku

Ekonomia raz jeszcze

- Bezpieczeństwo nie może być cechą dodaną po zakończeniu projektu
  - To za wiele kosztuje

Przykład: błędy oprogramowania. Naprawianie ich po wydaniu aplikacji może być kilkaset razy droższe niż na etapie pisania kodu!

Marco M. Morana



Źródło: *Building Security Into The Software Life Cycle,* Marco M. Morana

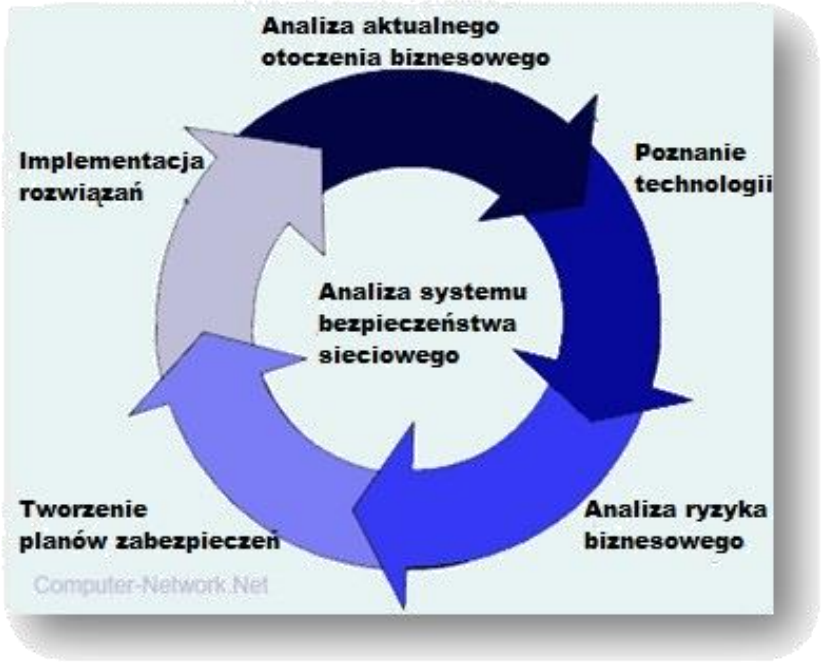
Zasada ochrony dogłębnej jest odpowiedzią na brak idealnego systemu zabezpieczeń

- Ochrona dogłębna (ang. *security-in-depth*) – na wielu różnych warstwach, np.:
  - Istnieje błąd w zakupionej aplikacji Web – można wpisać do aplikacji złośliwe dane
  - Serwer WWW jest jednak dobrze skonfigurowany. Nie pozwoli na wykonanie w zaatakowanym systemie dowolnego polecenia
  - System detekcji intruzów (IDS) wykryje niepożądane działania i powiadomi Administratora
- Strategia podwyższa koszt udanego ataku, czyniąc go potencjalnie nieopłacalnym

Zabezpieczyliśmy infrastrukturę

Czy to wszystko?

- Ocena bezpieczeństwa jest ważna tylko dla określonego stanu
- A zmienia się przecież:
  - Stan wiedzy w zakresie bezpieczeństwa IT
  - Analizowane środowisko (dodatkowe aplikacje, nowe serwery, więcej kont użytkowników, inny administrator…)
- Bezpieczeństwo jest procesem, a nie stanem (B. Schneier)



Potrzeba zapewnienia bezpieczeństwa wynika również z uwarunkowań prawnych

możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpi

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z gó umożliwiający szybkie podjęcie działań korygujących;

14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej

3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpiecz został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, za oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

1) PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;

2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;

3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techni ciągłością działania.

UODO

KRI

UOIN

2) z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37–39 ustawy oraz przepisach wydanych na podstawie art. 39a ustawy;

3) z zasadami przekazywania danych osobowych, o których mowa w art. 47–48 ustawy;

4) z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art. 27 ust. 1 ustawy.

5. Plan sprawdzeń jest przygotowywany przez administratora bezpieczeństwa informacji na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany administratorowi danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

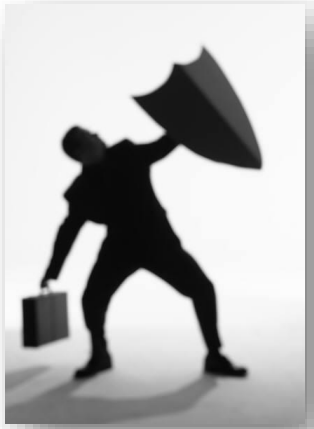
6. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na pięć lat.

7. Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez administratora bezpieczeństwa informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

8. Administrator bezpieczeństwa informacji zawiadamia administratora danych o rozpoczęciu sprawdzenia doraźne-

Podsumowanie najważniejszych wskazówek

- Docenienie wagi problemu
- Bezpieczeństwo wbudowane w cykl życia systemu
  - Od projektu, przez implementację, wdrożenie aż do utrzymania
- Ochrona na wielu warstwach
- Budowanie świadomości wszystkich użytkowników
- Badania poziomu bezpieczeństwa
  - Cykliczne
  - Wewnętrzne i zewnętrzne (niezależne)
- Rozważenie outsourcingu bezpieczeństwa IT



Pytania

- Dziękuję za uwagę!
  - maciej.milostan@man.poznan.pl