Seminarium „Dzieje Internetu w Polsce” 14.05.2013 r.

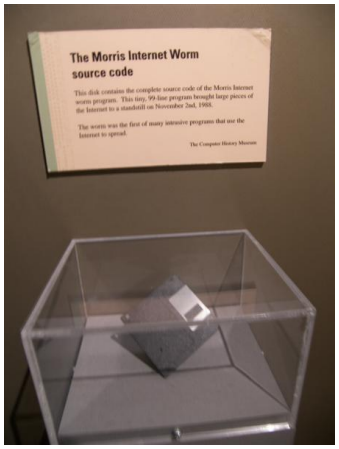
(Nie)bezpieczeństwo w sieci

Krzysztof Silicki

Początki problemu na świecie

- Internet Worm (Morris) – 1988 r.

2 listopada 1988 został uruchomiony robak Morris Worm, które potrafi automatycznie infekować inne systemy wykorzystując internet[1]. Zainfekował ponad 6 tys. komputerów, co stanowiło około 10% całego ówczesnego Internetu. Straty oszacowano na 10 do 100 mln dolarów[2]. Sprawca przyznał się do winy i został skazany na 3 lata obserwacji sądowej, 400 godzin prac społecznych i grzywnę w wysokości 10 tys. dolarów amerykańskich.



Dyskietka z robakiem Morrisa jako eksponat w Muzeum technologii w Bostonie.

- Powstanie CERT CC

WIKIPEDIA
The Free Encyclopedia

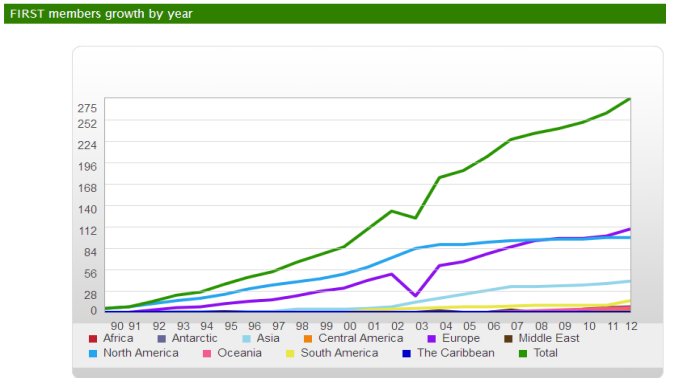
Main page

CERT Coordination Center

From Wikipedia, the free encyclopedia

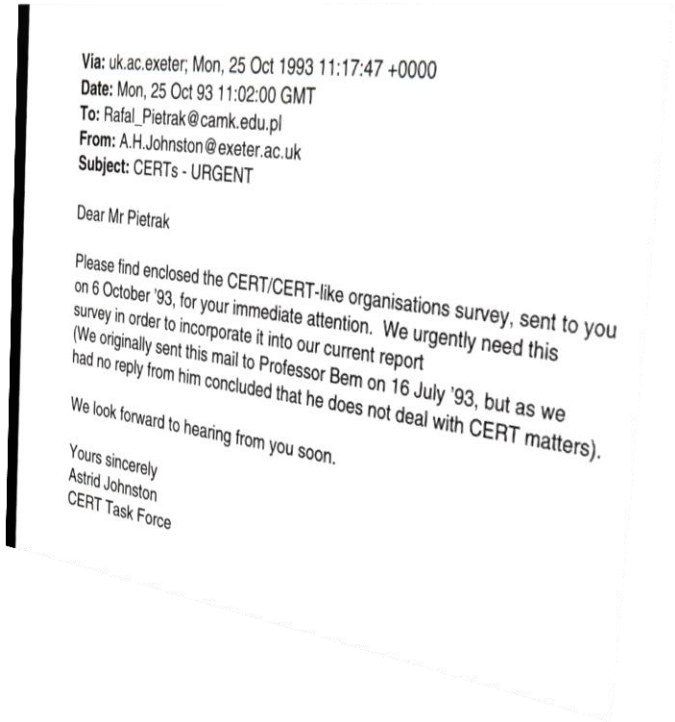
The **CERT Coordination Center** (CERT/CC) is the coordination center of the computer emergency response team (CERT) for Internet security incidents. The first center of its kind, it was created in Pittsburgh in November 1988 at DARPA's direction in response to the Morris worm incident. The CERT/CC is now part of the CERT Program, which has more than

- Powstanie FIRST – 1990 r.
  - (forum współpracy CERTów)



Skąd nasze zainteresowanie?

- Zainteresowanie ze strony Europy
  - Koniec 1993 roku – ankieta grupy roboczej powołanej przez RARE
- Konferencja INET 95
  - całodzienny warsztat CERT CC
  - kontakt z niemieckim DFN-CERT: (Klaus Peter Kossakowski)
- Konferencja o bezpieczeństwie w Londynie
- Wizyta w Hamburgu w DFN-CERT
- ale także…



Via: uk.ac.exeter; Mon, 25 Oct 1993 11:17:47 +0000
Date: Mon, 25 Oct 93 11:02:00 GMT
To: Rafal_Pietrak@camk.edu.pl
From: A.H.Johnston@exeter.ac.uk
Subject: CERTs - URGENT

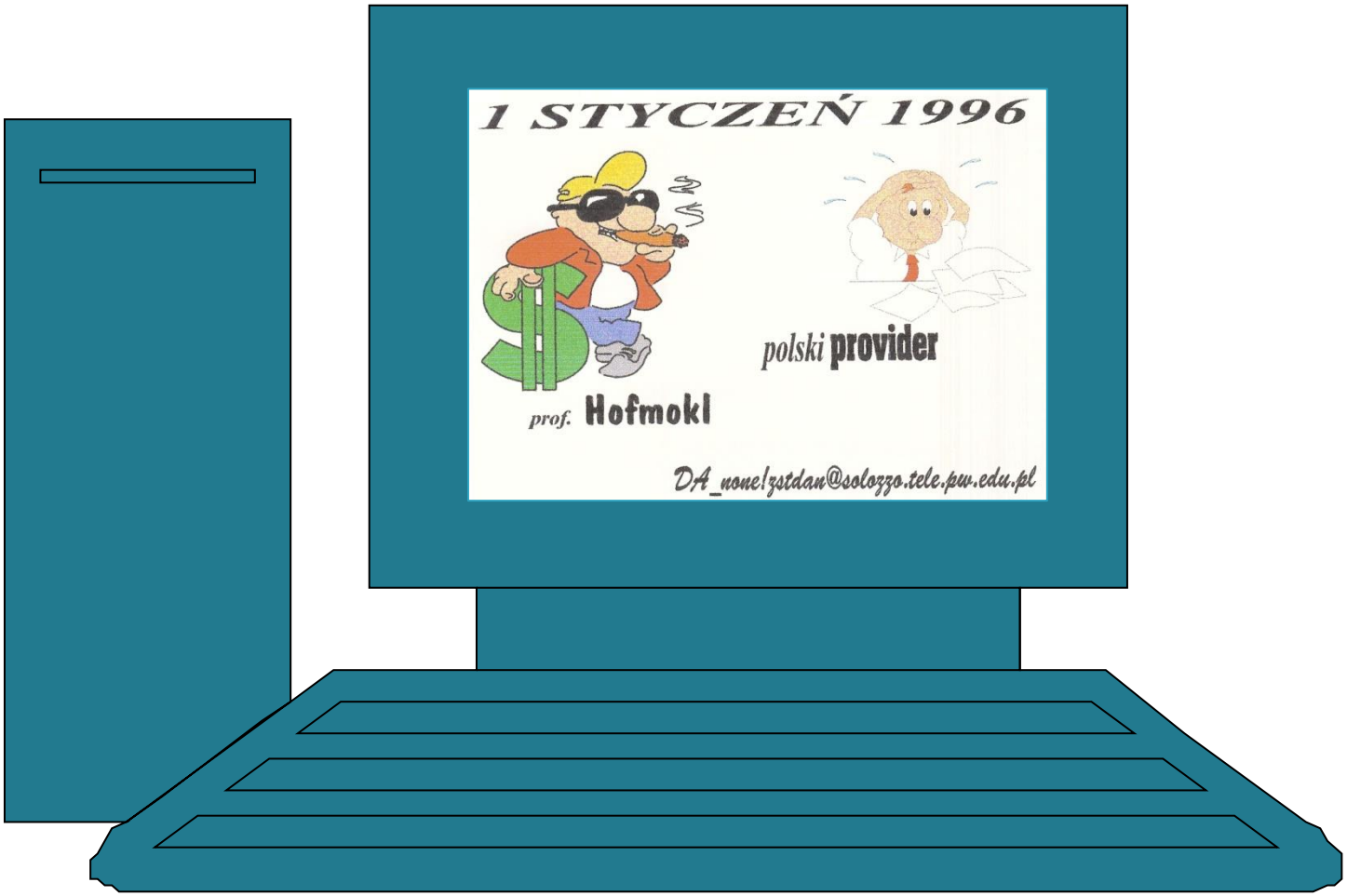
Dear Mr Pietrak

Please find enclosed the CERT/CERT-like organisations survey, sent to you on 6 October '93, for your immediate attention. We urgently need this survey in order to incorporate it into our current report
(We originally sent this mail to Professor Bem on 16 July '93, but as we had no reply from him concluded that he does not deal with CERT matters).

We look forward to hearing from you soon.

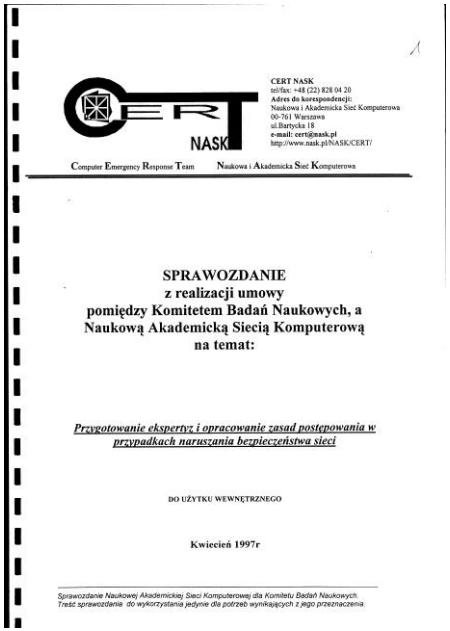
Yours sincerely
Astrid Johnston
CERT Task Force

„Pionierski defacement”



Początki CERT

- CERT w NASK – CERT NASK zaczął działalność w marcu 1996 roku
  - Powołanie decyzją dyrektora NASK – prof. Hofmokla
- W tym czasie działało już kilka CERTów w Europie
- Naszym wprowadzającym zespołem, był niemiecki DFN-CERT
- Zielone światło ze strony dyrekcji NASK
- Wsparcie ze strony KBN



CERT NASK
tel/fax: +48 (22) 828 04 20
Adres do korespondencji:
Naukowa i Akademicka Sieć Komputerowa
00-761 Warszawa
ul.Bartycka 18
e-mail: cert@nask.pl
http://www.nask.pl/NASK/CERT/

Computer Emergency Response Team Naukowa i Akademicka Sieć Komputerowa

SPRAWOZDANIE
z realizacji umowy
pomiędzy Komitetem Badań Naukowych, a
Naukową Akademicką Siecią Komputerową
na temat:

Przygotowanie ekspertyz i opracowanie zasad postępowania w przypadkach naruszania bezpieczeństwa sieci

DO UŻYTKU WEWNĘTRZNEGO

Kwiecień 1997r

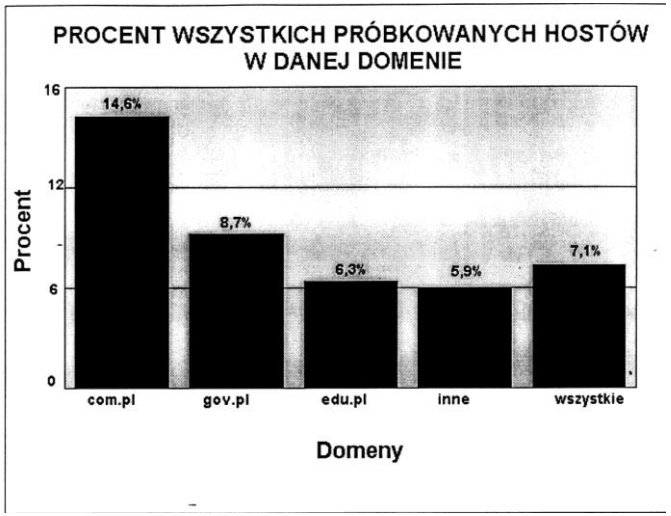
Sprawozdanie Naukowej Akademickiej Sieci Komputerowej dla Komitetu Badań Naukowych.
Treść sprawozdania do wykorzystania jedynie dla potrzeb wynikających z jego przeznaczenia.

Pierwszy poważny incydent

- Otrzymaliśmy zgłoszenie z DFN-CERT
  - Skanowanie kilkunastu tysięcy adresów w .pl
  - Kilkadziesiąt jeśli nie ponad setka instytucji
  - Kontakty telefonicznie i mailowo
  - W wielu przypadkach okazało się, że skanowanie było początkiem udanych ataków na systemy lokalne
  - Incydent trudny logistycznie do obsłużenia ale:
  - Stał się „wielkim otwarciem” dla CERT NASK – wiele instytucji i firm dowiedziało się w krótkim czasie o istnieniu CERTu

Pierwsze statystyki

- W pierwszym roku 65% zgłoszeń pochodziło z Polski a 35% z zagranicy
- 7% zarejestrowanych adresów w polskiej przestrzeni internetowej było próbkowane w poszukiwaniu łatwych celów ataku
  - tzn. tyle przypadków było wykrytych i zgłoszonych do CERT NASK
  - tę liczbę spokojnie można pomnożyć przez nieznane N



Ewolucja rodzajów zagrożeń i typów ataków

- Wykorzystywanie słabych haseł – 1988
- Wykorzystanie słabości (luk) w systemach operacyjnych – 1989
- Instalowanie programów przechwytujących (sniffery) – 1993
- Aktywne poszukiwanie nieznanych podatności – 1993
- Ataki na anonymous ftp, pocztę elektroniczną, NFS, NIS – 1994
- IP spoofing – 1995
- Fragmentacja pakietów,, DoS, buffer overflow, stack overflow , słabości www– 1996
- To co raz wymyślone – nie odchodzi do historii, dalej straszy

Szybki rozwój CERT NASK

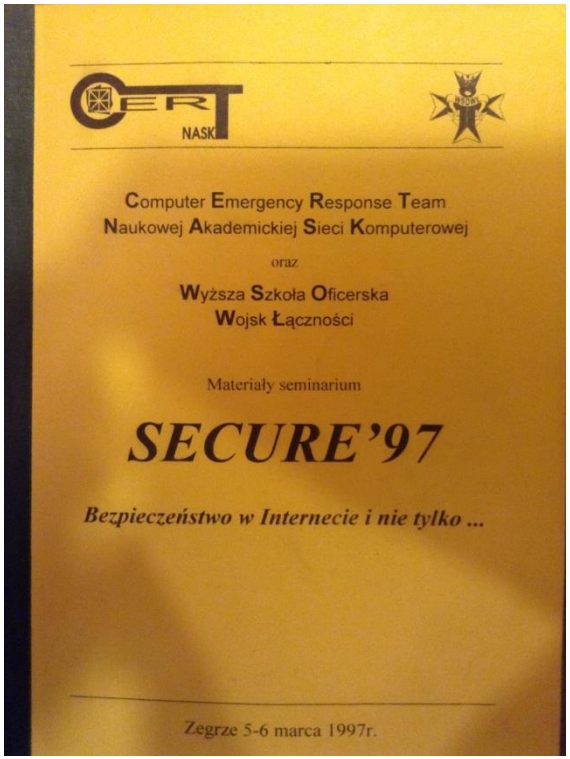
- Luty 97 – wstąpienie do FIRST
  - wtedy było ok. 60 członków
  (zespołów CERT działających w ramach FIRST)

- Marzec 97 – zorganizowanie pierwszej w Polsce konferencji poświęconej bezpieczeństwu komputerowemu: SECURE

Konferencja SECURE

- Najstarsza w Polsce konferencja poświęcona bezpieczeństwu
- Pierwsza edycja SECURE 97
  - odbyła się 5-6 marca 1997 r.

  w Zegrzu w nieistniejącej już WSOWŁ



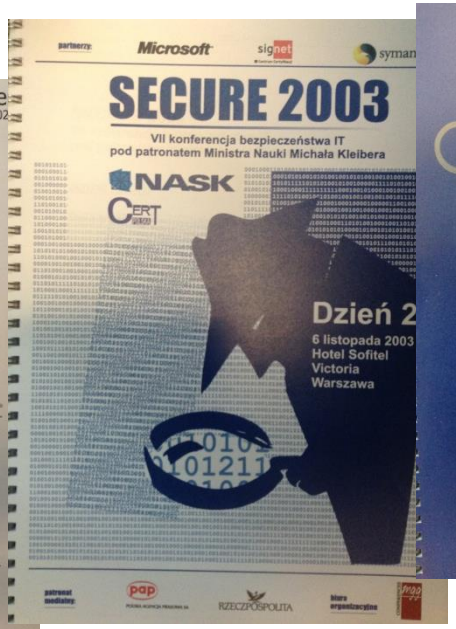
SECURE 97

- Tematyka:
  - Rola zespołów reagujących
  - Rodzaje zagrożeń i ataków
  - Przegląd programów podwyższających bezpieczeństwo
    - Testowanie: COPS, ISS, Tiger
    - Kontrola integralności: Tripwire
    - Programy antywirusowe
    - Uwierzytelnianie: Kerberos, Radius
    - Firewalle: IPFW, SOCKS
    - Filtrowanie pakietów: TCP_Wrapper
    - Monitorowanie sieci: Argus, netman
    - Szyfrowanie poczty: PGP, PEM

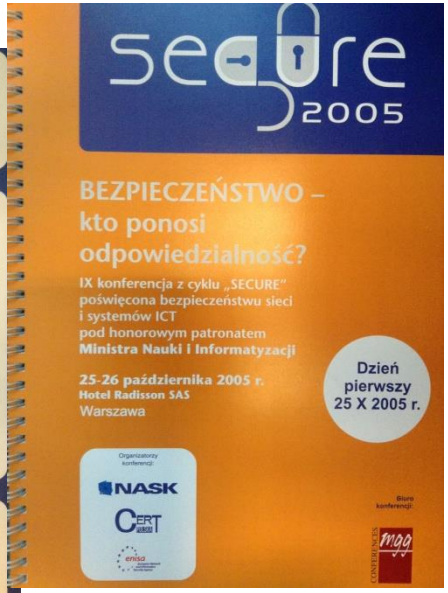
SECURE 97 – tematyka (2)

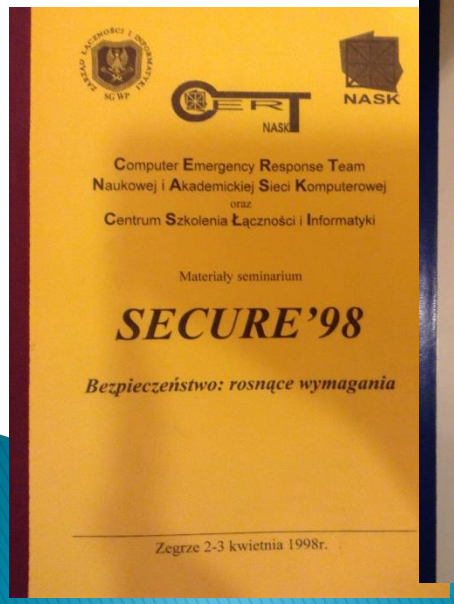
- Przestępczość komputerowa w Polsce
- Bezpieczeństwo routerów (Cisco)
- Hasła jednokrotnego użytku (OTP)
- Bezpieczeństwo TCP/IP
- Słabości systemów UNIX
- Kompatybilnośc elektromagnetyczna
- Porady praktyczne


II dzie
7.11.2002
IT.FORUM
SECURE 2002
Organizatorzy konferencji
Partnerzy konferencji
Warszawa 2002, Hotel Holiday Inn

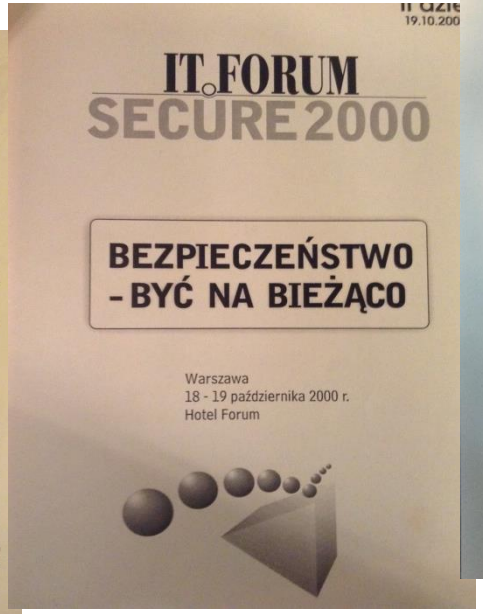

partnerzy:
Microsoft
SECURE 2003
VII konferencja bezpieczeństwa IT
pod patronatem Ministra Nauki Michała Kleibera
NASK
Dzień 2
6 listopada 2003
Hotel Sofitel
Victoria
Warszawa


secure 2004
Organizatorzy:
Partnerzy:
Patronat medialny:
VIII Konferencja bezpieczeństwa IT
20 - 21 października 2004
Hotel Sheraton
Warszawa
DZIEŃ PIERWSZY
20 października 2004


secure 2005
BEZPIECZEŃSTWO –
kto ponosi
odpowiedzialność?
IX konferencja z cyklu „SECURE"
poświęcona bezpieczeństwu sieci
i systemów ICT
pod honorowym patronatem
Ministra Nauki i Informatyzacji
25-26 października 2005 r.
Hotel Radisson SAS
Warszawa
Dzień
pierwszy
25 X 2005 r.
NASK

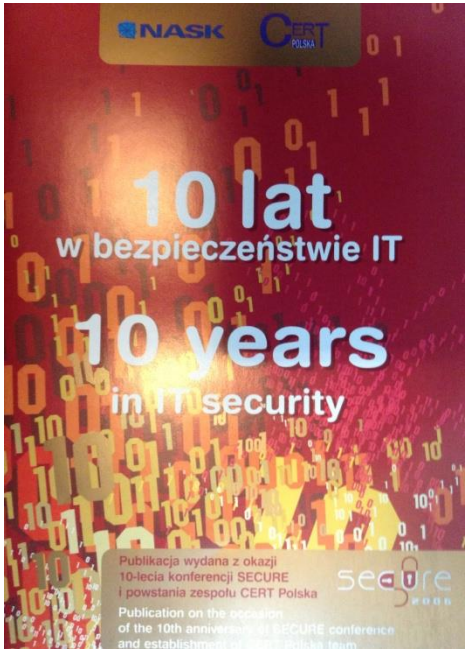

Computer Emergency Response Team
Naukowej i Akademickiej Sieci Komputerowej
oraz
Centrum Szkolenia Łączności i Informatyki
Materiały seminarium
SECURE'98
Bezpieczeństwo: rosnące wymagania
Zegrze 2-3 kwietnia 1998r.


NASK
SECURE '99
III KONFERENCJA CERT NASK
Aktywna ochrona
systemów
teleinformatycznych
26-27 października 1999 r.
MATERIAŁY KONFERENCYJNE


IT.FORUM
SECURE 2000
BEZPIECZEŃSTWO
- BYĆ NA BIEŻĄCO
Warszawa
18 - 19 października 2000 r.
Hotel Forum


II dzień
8.11.2001 r.
IT.FORUM
SECURE 2001
BEZPIECZEŃSTWO - NOWE WYZWANIA
Organizatorzy konferencji
Partnerzy konferencji
Patron medialny

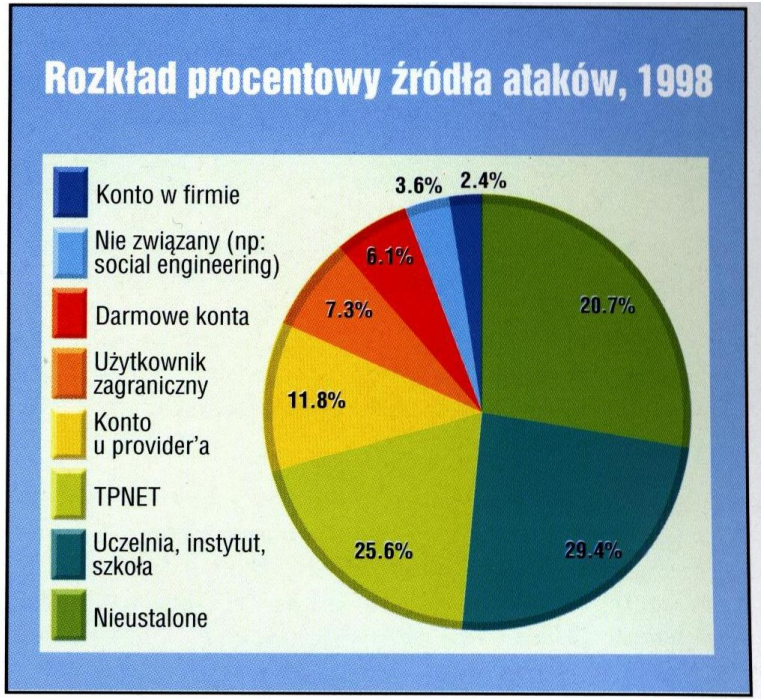
Po dziesięciu latach…

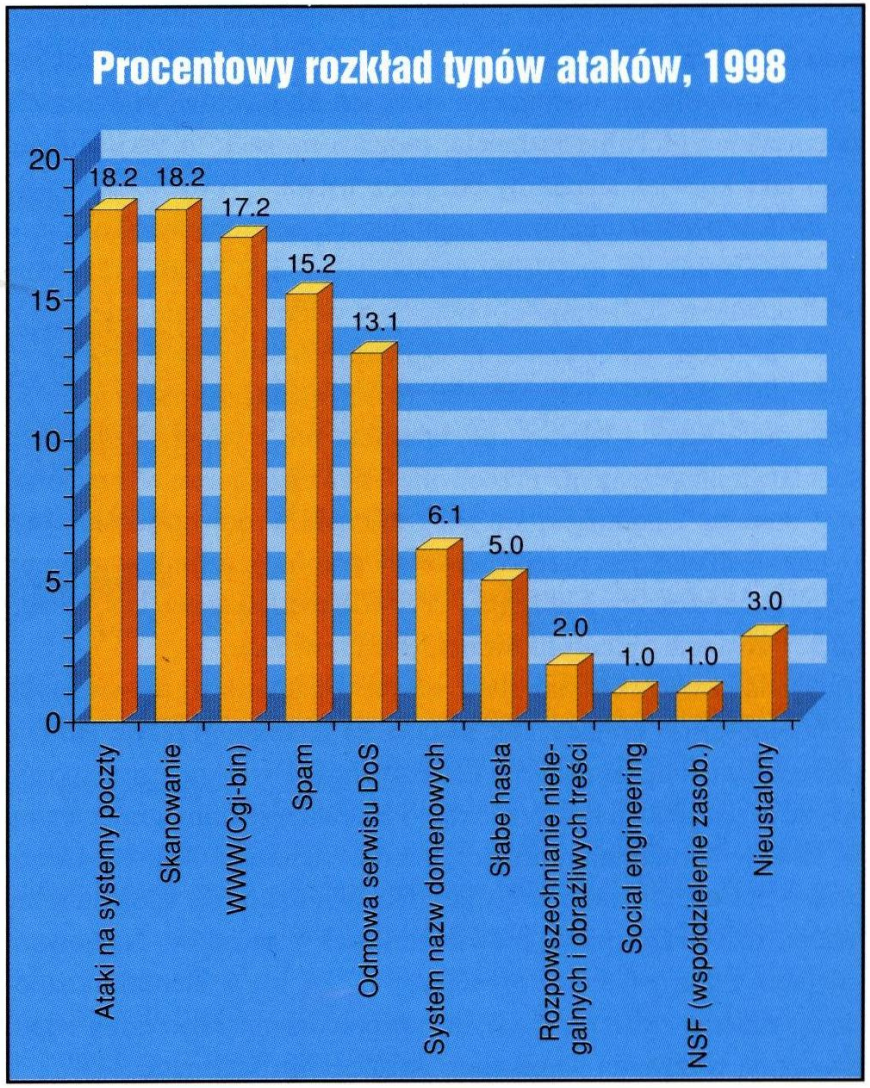


Inne wydarzenia

- ENIGMA – powstaje konferencja poświęcona zagadnieniom bezpieczeństwa i kryptografii (maj 1997)
  - grupa dr. Ryszarda Kossowskiego z PW
- Powstanie pierwszego w kraju systemu PKI
  - w NASK na potrzeby akademickie
  - szyfrowanie poczty elektronicznej
  - klucze na dyskietkach
- W 98 r. CERT NASK notuje wzrastająca liczbę incydentów związanych z darmowym dostępem do sieci TPNET
  - sporo zgłoszeń od zagranicznych CERTów to efekt działania „uzytkowników”poprzez dial-up TP
  - od marca 1997 r. działał już w TP zespół bezpieczeństwa - Abuse Team

Statystyki CERT – rok 1998



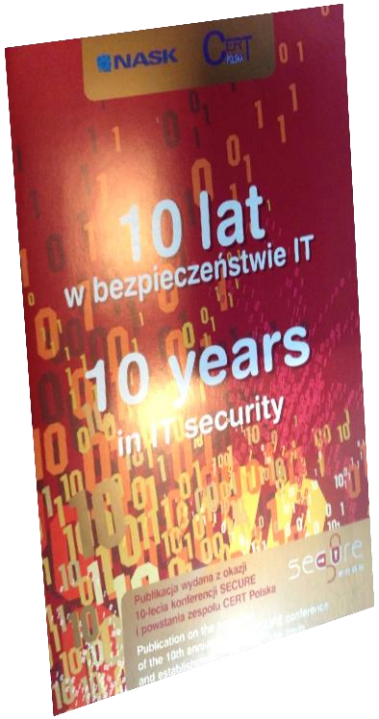


CERT

Wydarzenia (2)

- Rok 2000 – przemiana CERT NASK w CERT Polska
- Rok 2001 – akredytacja CERT Polska w TERENA TF CSIRT
- Rok 2004 – powstanie Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA)
- Rok 2005 – powstanie NIFC Hotline Polska (Dyżurnet.pl) – w ramach Safer Internet Action Plan Komisji Europejskiej
  - Polskie centrum Safer Internet: NASK wraz z Fundacją Dzieci Niczyje
- Rok 2005 – powstanie Abuse Forum
  - nieformalne forum współpracy zespołów bezpieczeństwa operatorów, providerów, banków
- Rok 2005 – powstanie systemu wczesnego ostrzegania ARAKIS
- Rok 2006 – podsumowanie pierwszego dziesięciolecia…

Pierwsze dziesięć lat...



1. Zmiana wizerunku hakera:
   1995r. : entuzjasta systemu komputerowego ⇒ chuligan ⇒ przestępca 2005 r.

2. Upowszechnienie Internetu (szerokopasmowego)
   np. Slammer w Korei Pd, ataki DDoS

3. Ustalił się kanon zabezpieczeń: FW, AV, IDS, łatanie luk
   … jednak pomino powszechności tych zabezpieczeń brak znaczącej poprawy ogólnego poziomu bezpieczeństwa

4. Wzrost znaczenia socjotechniki
   np. phishing

5. Większa uwaga zwracana na tworzenie bezpiecznego oprogramowania
   np.. Inicjatywa Trustworthy Computing f-my Microsoft z 2002 roku

WIKIPEDIA
Wolna encyklopedia

ILOVEYOU [edytuj]

ILOVEYOU, znany także jako **VBS/Loveletter** oraz **Love Bug** jest wirusem komputerowym napisanym w języku VBScript.

ILOVEYOU

Lietuvių
Bahasa Melayu
Nederlands

Wirus rozpoczął swój żywot 4 maja 2000, i rozprzestrzenił się na cały świat w ciągu jednego dnia zarażając 10 procent wszystkich komputerów mających dostęp do Internetu[1] i powodując straty w wysokości 5.5 miliardów dolarów[2]

WIKIPEDIA
Wolna encyklopedia

Strona główna
Kategorie artykułów
Najlepsze artykuły
Zgłoś błąd
Częste pytania (FAQ)

Code Red (wirus) [edytuj]

Ten artykuł dotyczy wirusa komputerowego. Zobacz też: Code Red – zespół muzyczny.

Code Red jest specyficznym rodzajem wirusa komputerowego – robakiem wykorzystującym błąd w oprogramowaniu serwera Microsoft Internet Information Server (IIS).

Istnieją dwie wersje tego robaka Code Red I i Code Red II.

Code Red I pojawił się 13 lipca 2001 r. i został po raz pierwszy zlokalizowany i nazwany przez programistów z eEye Digital Security. Robak wykorzystywał błąd w module indeksowania, będącym częścią pakietu IIS i wykonywał następujące działania:

WIKIPEDIA
Wolna encyklopedia

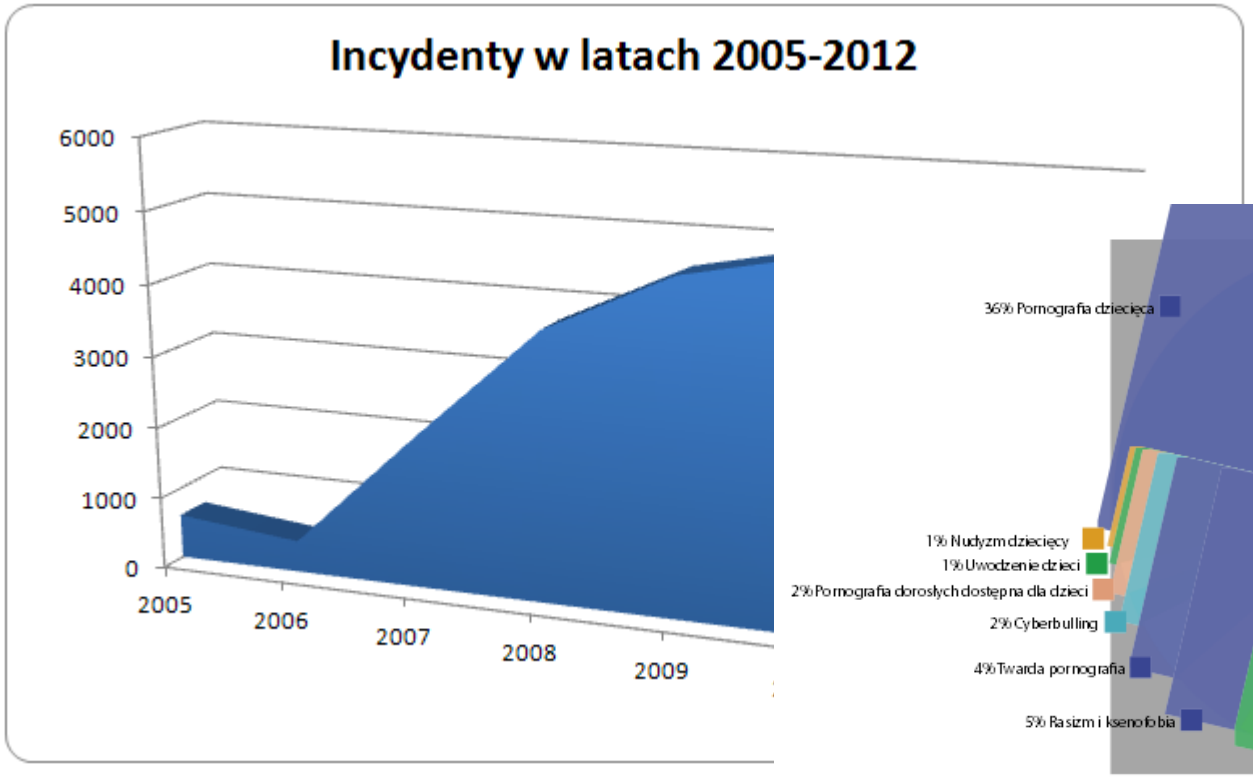
Strona główna
Kategorie artykułów

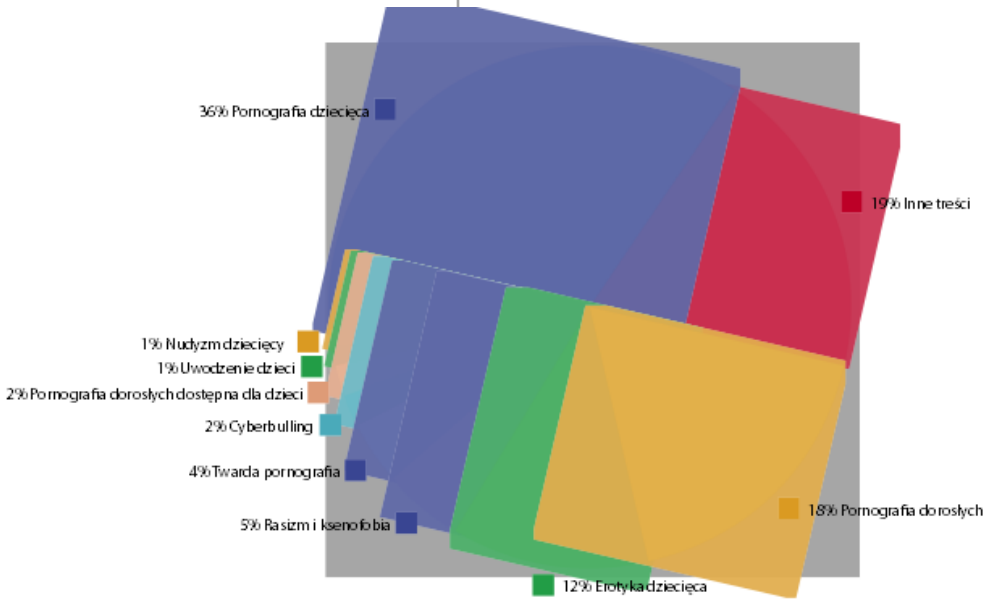
SQL Slammer [edytuj]

SQL Slammer to robak, który 25 stycznia 2003 zainfekował serwery Microsoft SQL na całym świecie.

Cechą szczególną SQL Slammera była niespotykana dotychczas szybkość rozprzestrzeniania się. Tempo podwajania liczby zainfekowanych komputerów wynosiło ok. 8 i pół sekundy, w porównaniu z 37 minutami w przypadku Code Red.

Statystyki Dyżurnet





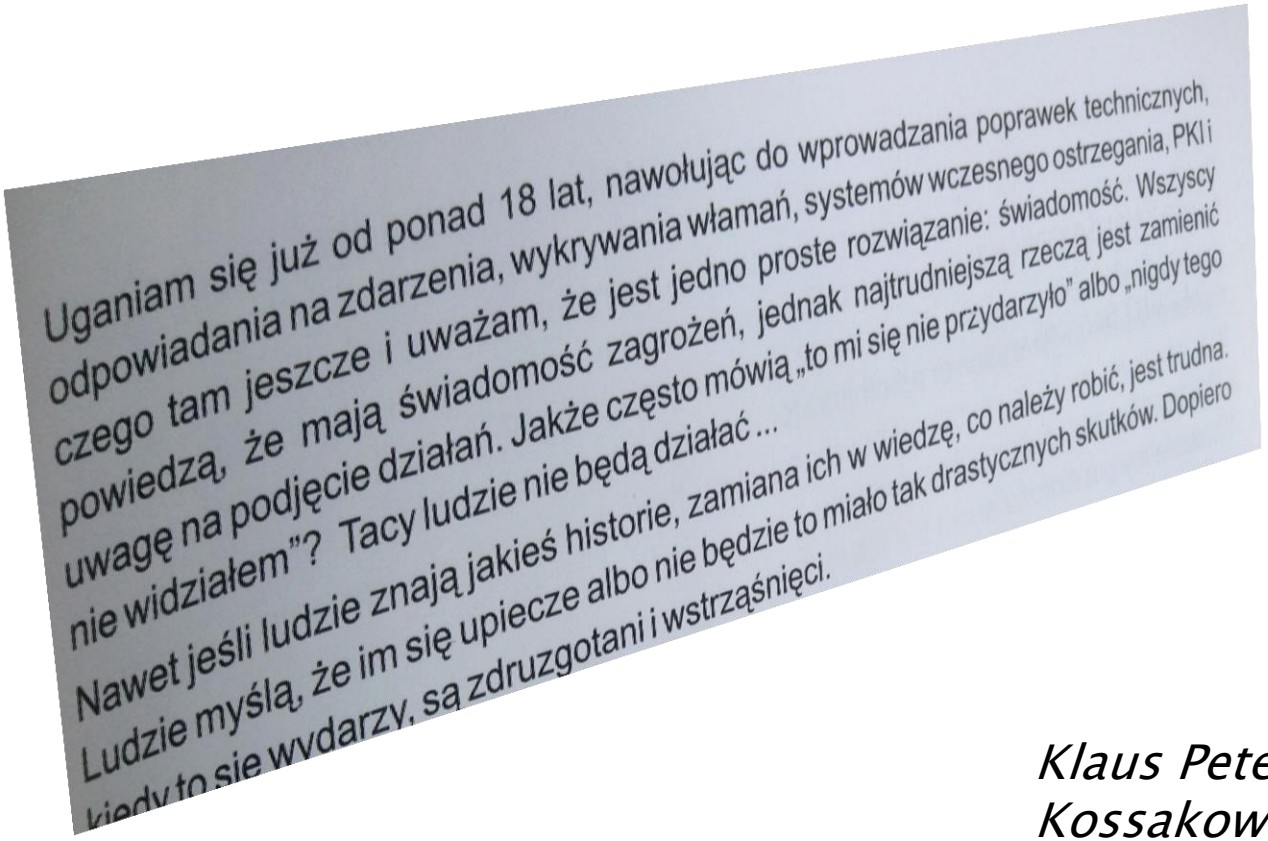
Wykres 4. Klasyfikacja zgłoszonych treści dokonana przez pracowników zespołu w latach 2005 - 2009

dyżurnet.pl

Pierwsze dziesięć lat... (3)

- Nowe technologie, nowe zagrożenia
  - komunikatory P2P
  - VoIP
- Nowe cele ataków
  - SCADA
  - Systemy bankowości elektronicznej
- Niepożądane i nielegalne treści
- Budowanie systemu prawnego

Od poznania do działania…



Uganiam się już od ponad 18 lat, nawołując do wprowadzania poprawek technicznych, odpowiadania na zdarzenia, wykrywania włamań, systemów wczesnego ostrzegania, PKI i czego tam jeszcze i uważam, że jest jedno proste rozwiązanie: świadomość. Wszyscy powiedzą, że mają świadomość zagrożeń, jednak najtrudniejszą rzeczą jest zamienić uwagę na podjęcie działań. Jakże często mówią „to mi się nie przydarzyło" albo „nigdy tego nie widziałem"? Tacy ludzie nie będą działać ...

Nawet jeśli ludzie znają jakieś historie, zamiana ich w wiedzę, co należy robić, jest trudna. Ludzie myślą, że im się upiecze albo nie będzie to miało tak drastycznych skutków. Dopiero kiedy to się wydarzy, są zdruzgotani i wstrząśnięci.

Klaus Peter Kossakowski, DFN-CERT
„Inwestowac w ludzi" – broszura CERT Polska „ 10 lat w bezpieczeństwie IT"

CERTy – jeden z kluczowych elementów bezpieczeństwa

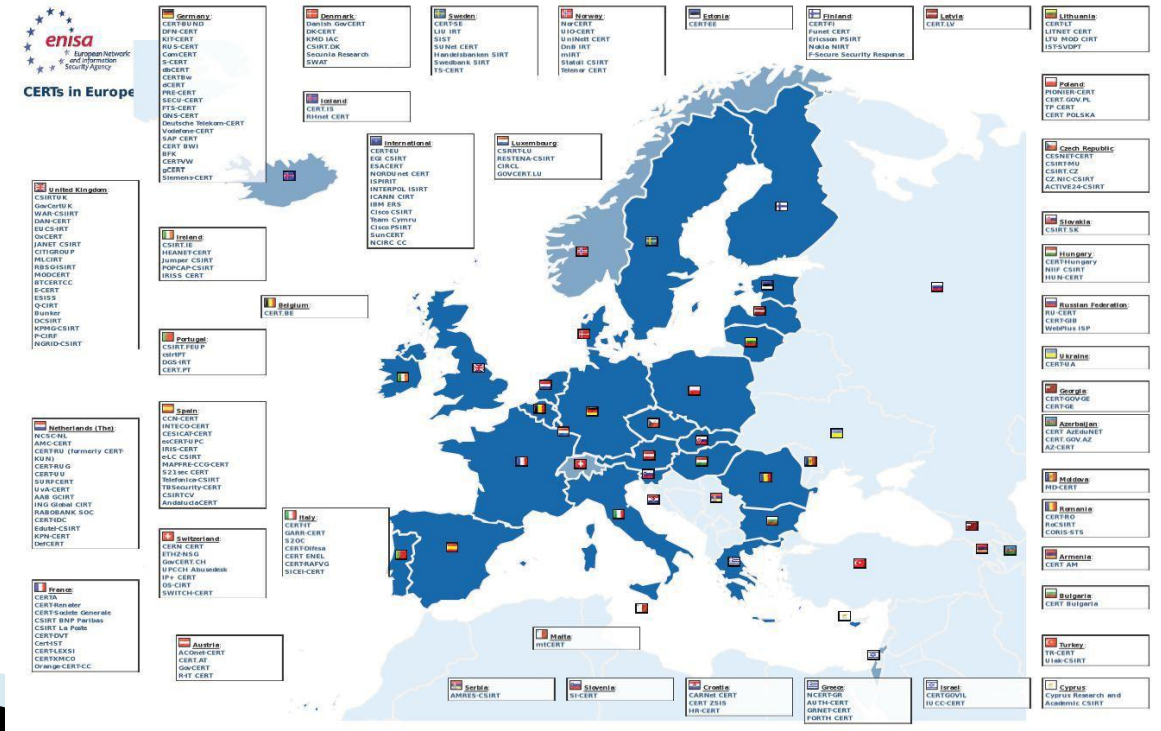
- Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) stawia na CERTy jako jeden z filarów bezpieczeństwa
- Komisja Europejska w swej strategii cyberbezpieczeństwa wskazuje na potrzebe powstawania CERTów w każdym z sektorów gospodarki
  - sektor przemysłu (infrastruktura krytyczna),
  - sektor finansowy,
  - administracja publiczna

Stały rozwój społeczności CERTowej

Poland

This section includes the details of the CERTs for this country:

Nr.	CERT name	Date of establishment	TI Status	FIRST Membership	Constituency	Additional information
133.	CERT POLSKA	1Q 1996	Accredited	Member	De Facto National	See: www.cert.pl
134.	CERT.GOV.PL	2008	Listed	Not member	Governmental CERT	See: www.cert.gov.pl
135.	PIONIER-CERT		Listed	Not member	Research and Education	Formerly POL34-CERT. See: http://cert.pionier.gov.pl
136.	TP CERT		Listed	Member	ISP Customer Base	See: http://www.orange.pl/cert.ph



Źródło: ENISA, Inventory of CERT activities in Europe, 2012

- Dziękuję za uwagę

Krzysztof.Silicki@nask.pl