

(Nie)bezpieczeństwo w sieci

Krzysztof Silicki



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 Bern 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
Abrid 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

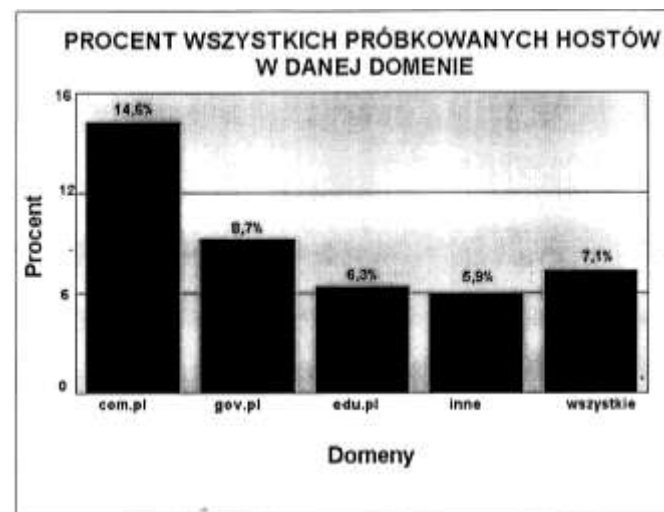


Pierwszy poważny incydent

- ▶ 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 przechwytyjących (sniffery) – 1993
- ▶ Aktywne poszukiwanie nieznanymi 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

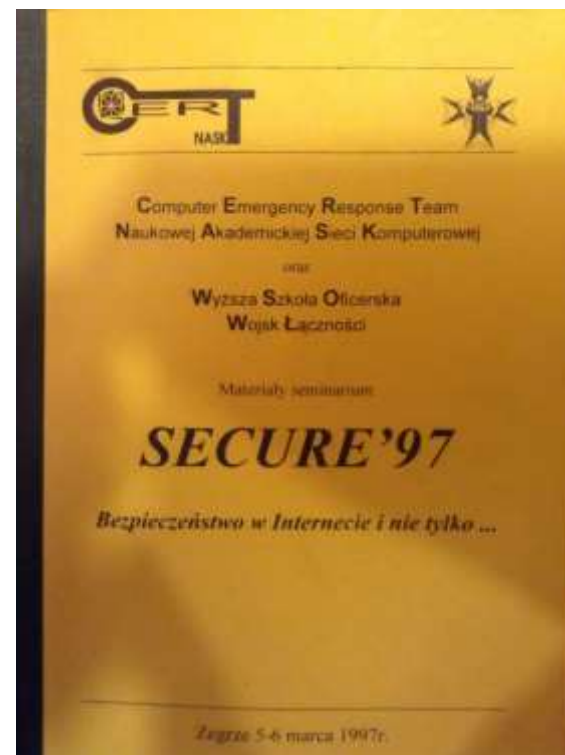
Szybki rozwój CERT NASK



- ▶ 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

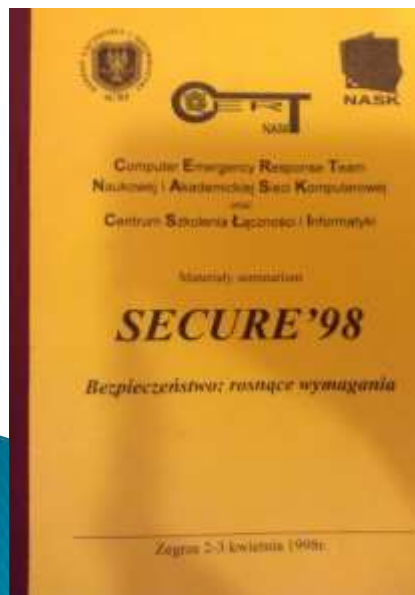


SECURE 97

- 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)

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



Po dziesięciu latach...



ORGANIZATORZY:

NASK

CERT
POLSKA

enisa

secure
2006

**Bezpieczeństwo
- czas na przełom**

X jubileuszowa konferencja SECURE
17 - 18 października 2006 r.
Hotel Radisson SAS, Warszawa

**Pierwszy dzień
konferencji
17 X 2006 r.**

**PATRONAT
HONOROWY:**
Michał Seweryński
Minister Nauki i Szkolnictwa Wzrostu
Grzegorz Biliński
Podsekretarz Stanu w Ministerstwie
Spraw Wewnętrznych i Administracji

**BIURO
ORGANIZACYJNE:**
mga

CONFERENCE



NASK **CERT**

10 lat
w bezpieczeństwie IT

10 years
in IT security

Publikacja wydana z okazji
10-lecia Konferencji SECURE
i jubileusza 10-lecia CERT Polska

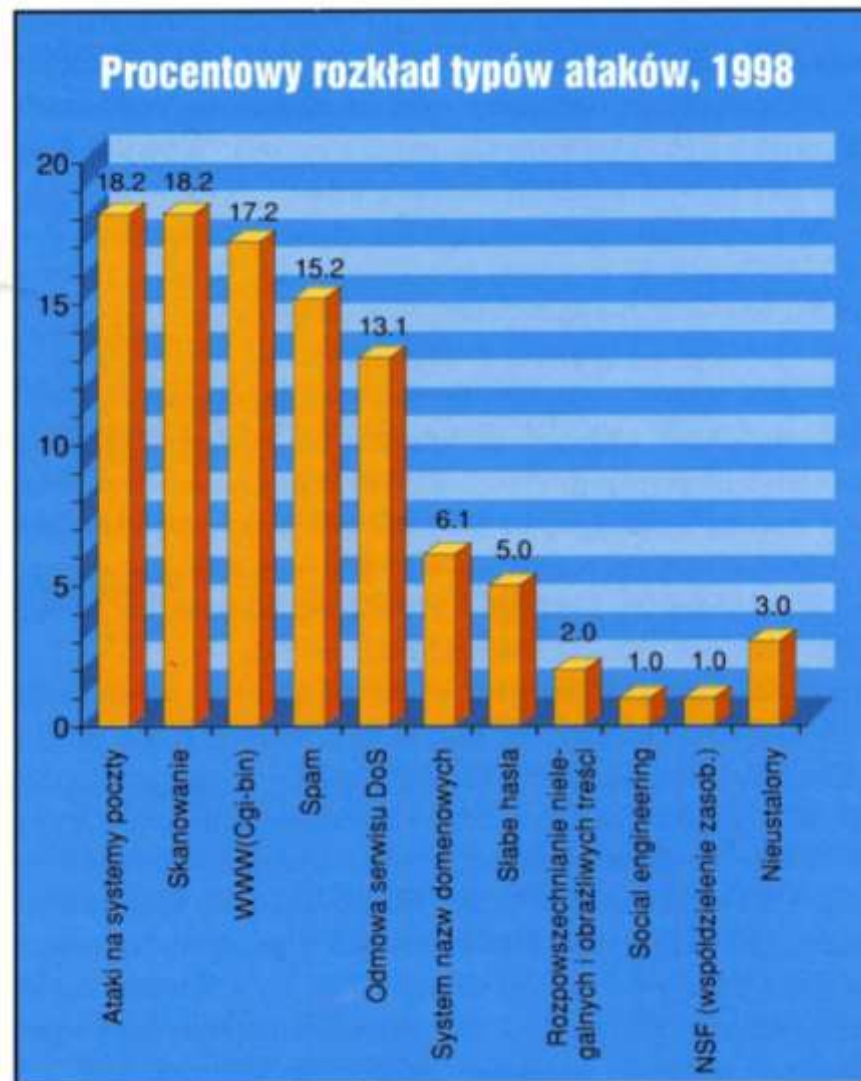
Publication on the occasion
of the 10th anniversary of the conference
and jubilee of CERT Polska

secure
2016

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 wzrastającą liczbę incydentów związanych z darmowym dostępem do sieci TPNET
 - sporo zgłoszeń od zagranicznych CERTów to efekt działania „użytkowników” poprzez dial-up TP
 - od marca 1997 r. działał już w TP zespół bezpieczeństwa – Abuse Team

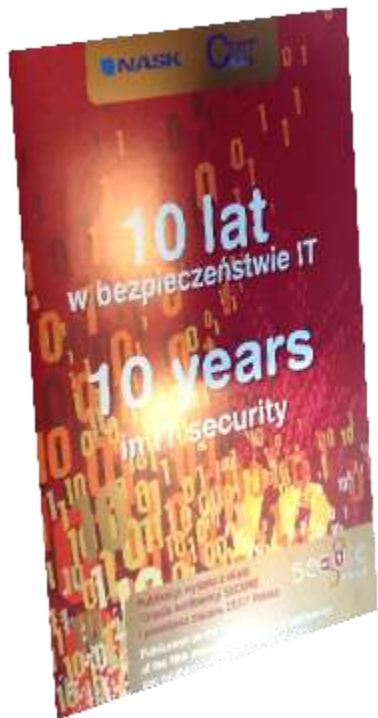
Statystyki CERT – rok 1998



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 pomimo 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


ILOVEYOU [edytuj]

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

ILOVEYOU

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]

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:

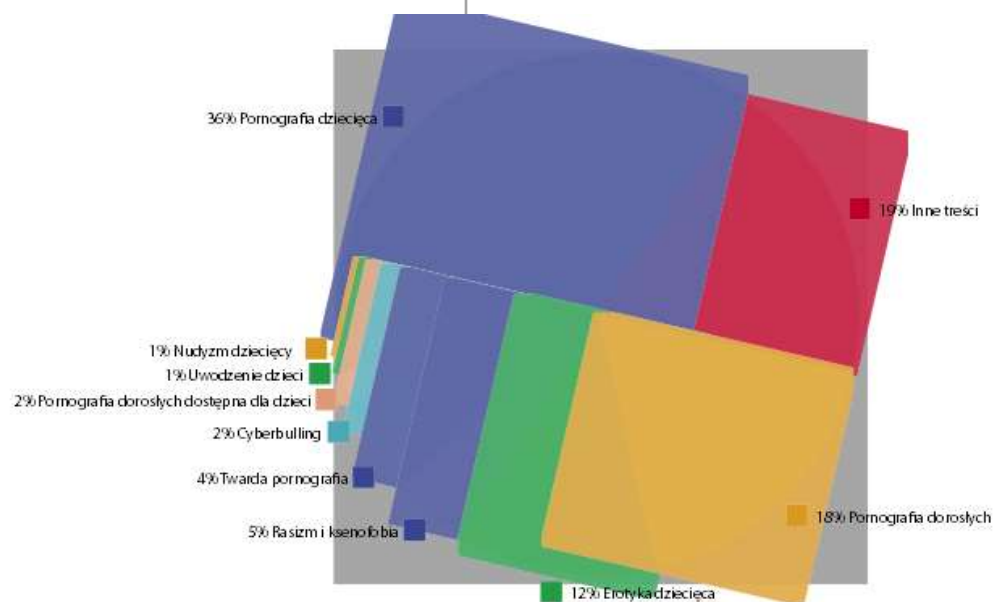
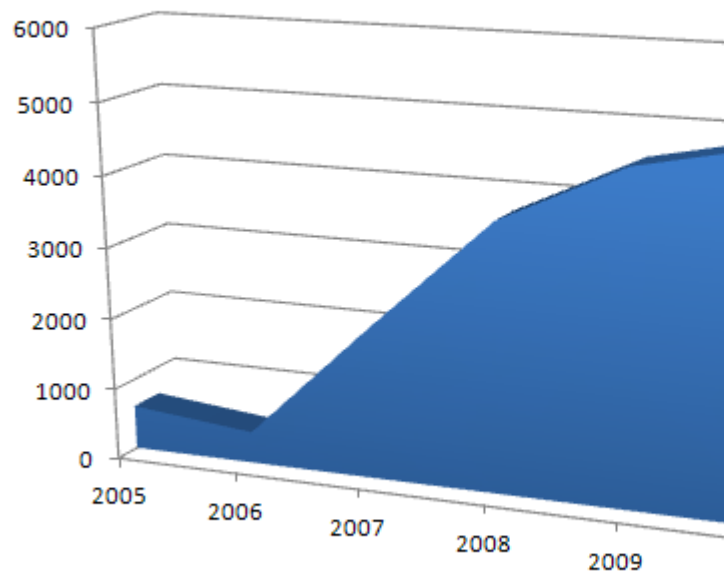
SQL Slammer [edytuj]

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

Incydenty w latach 2005-2012



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

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

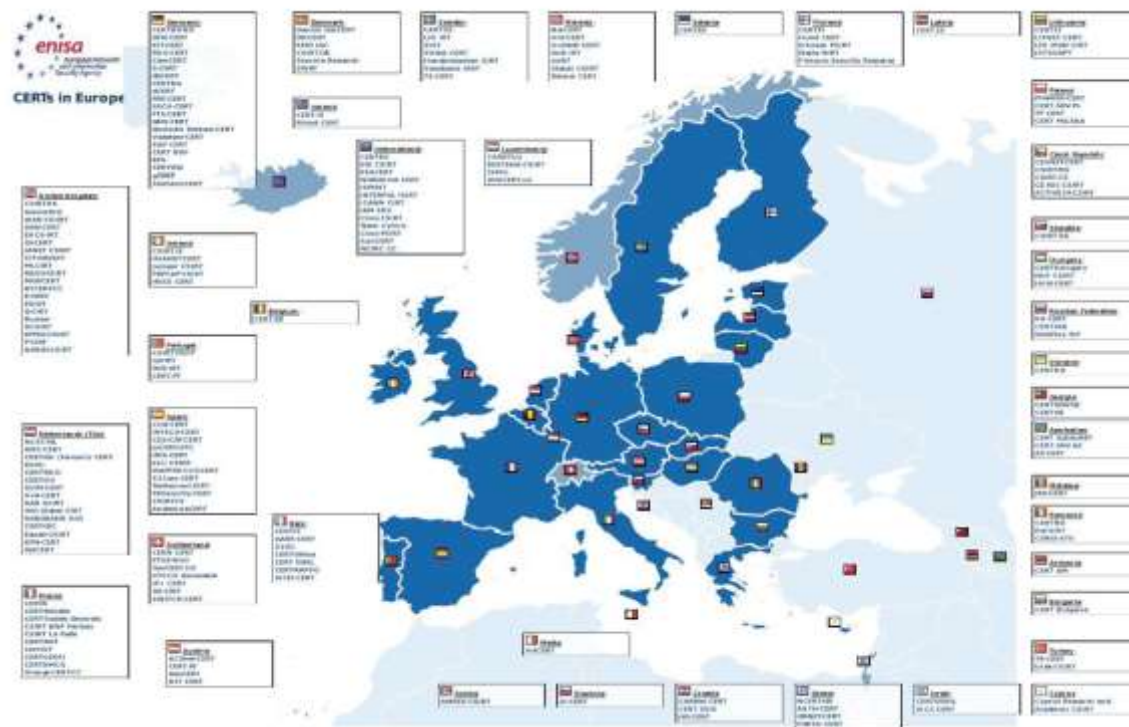
- ▶ Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) stawia na CERTy jako jeden z filarów bezpieczeństwa
- ▶ Komisja Europejska w swej strategii cyberbezpieczeństwa wskazuje na potrzebe powstawania CERTów w każdym z sektorów gospodarki
 - sektor przemysłu (infrastruktura krytyczna),
 - sektor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



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

▶ Dziękuję za uwagę

Krzysztof.Silicki@nask.pl