Bezpieczny dostęp do Internetu w polskich szkołach – nowe otwarcie

Gerard Frankowski, Tomasz Nowocień, Marek Pawłowski – Dział Bezpieczeństwa ICT PCSS

Konferencja „Cyfrowe bezpieczeństwo w szkole XXI wieku”

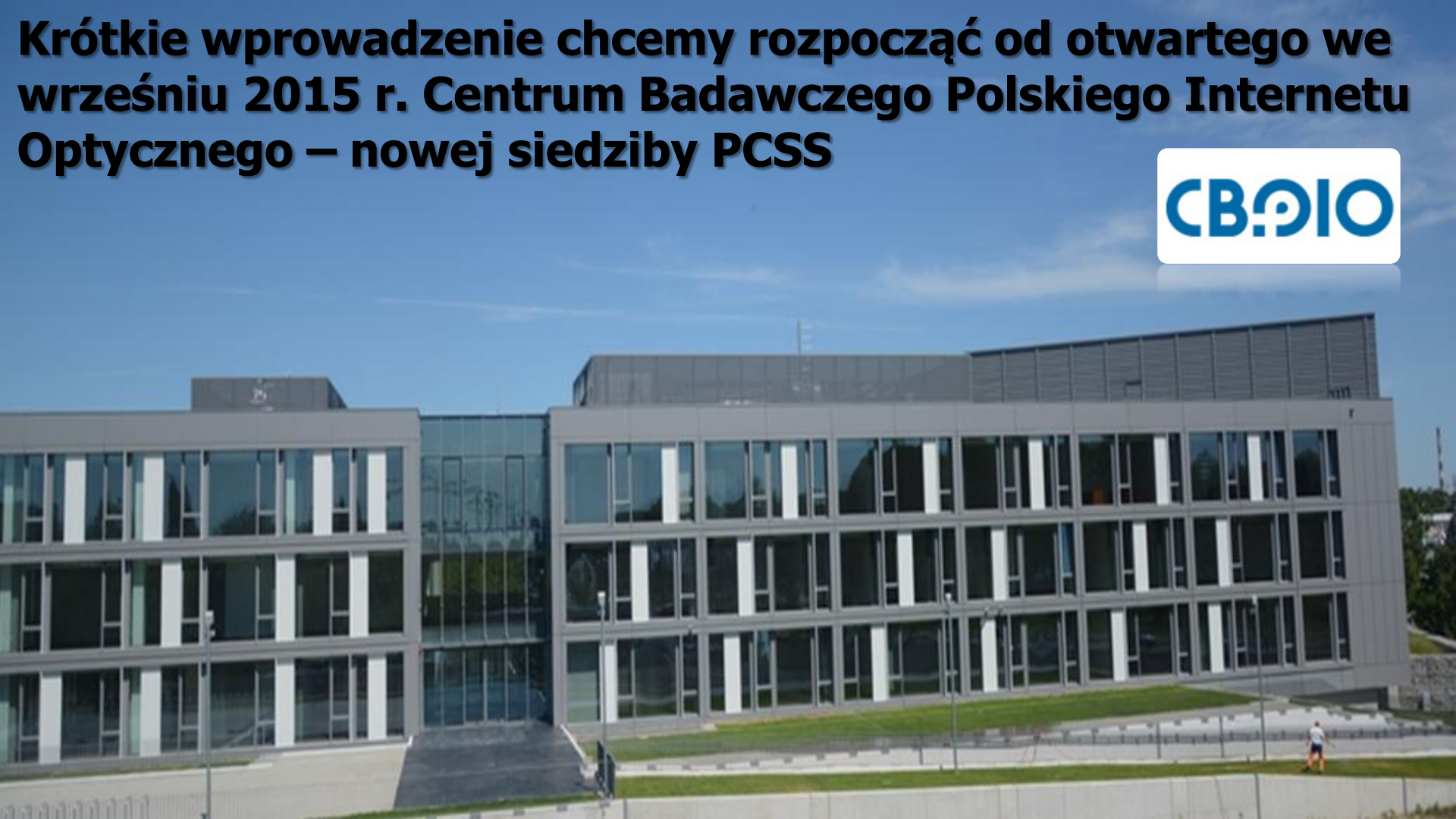
Warszawa, 29.04.2016

cyfrowo bezpieczni.pl

Agenda

- PCSS i PIONIER a cyberbezpieczeństwo w szkołach
- Najważniejsze fakty dotyczące bezpieczeństwa IT
- Specyfika zagrożeń cyberbezpieczeństwa w sektorze edukacji
- Jak zwalczać zaawansowane zagrożenia?
- Model bezpiecznego dostępu do Internetu dla szkół – główne założenia
- Pytania, dyskusja

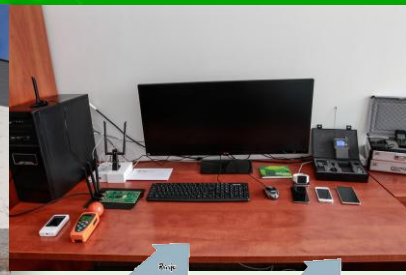
Krótkie wprowadzenie chcemy rozpocząć od otwartego we wrześniu 2015 r. Centrum Badawczego Polskiego Internetu Optycznego – nowej siedziby PCSS

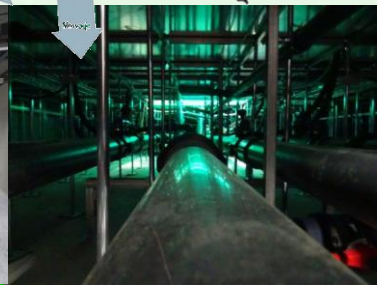


PCSS

Rok założenia – 1993

- Operator sieci PIONIER oraz POZMAN
- Uczestnik europejskich i krajowych projektów naukowo-badawczych
- Realizacja prac B+R z nauką, administracją oraz biznesem
- Główne obszary zainteresowań
  - Sieci nowej generacji (NGN)
  - Nowe architektury przetwarzania danych
  - Zaawansowane aplikacje
  - Usługi Internetu Rzeczy
  - Bezpieczeństwo sieci i systemów





Konsorcjum PIONIER

21 jednostek MAN, 5 centrów KDM, wiele wspólnych projektów dla środowiska nauki

KMD krajowy magazyn danych

CLUSTERIX

PL GRID

KMD2 Krajowy Magazyn Danych

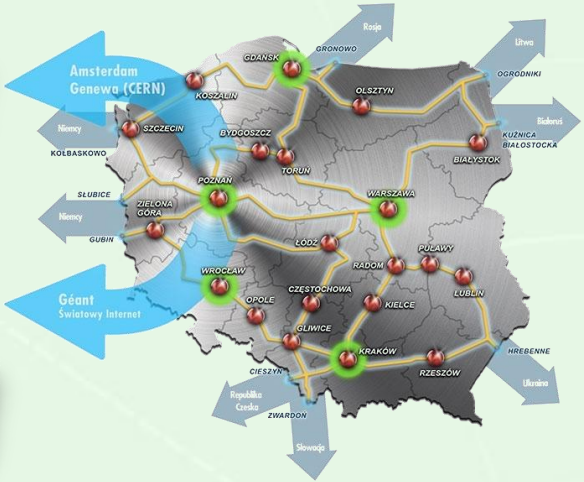
PL GRID+

PL GRID NG

PLATON POLSKI INTERNET OPTYCZNY

POWIEW Program Obliczeń Wielkich Wyzwań Nauki i Techniki

POLSKI INTERNET OPTYCZNY MAN-HA



PCSS · CYFRONET · PUlMAN · NASK · BYMAN · CzestMAN · ci task · KOS MAN · POLITECHNIKA ŁÓDZKA Centrum Komputerowe ŁODMAN · CKZ · CK

KIEMAN · WCSS · LUBMAN · TORMAN · UNIWERSYTET OPOLSKI · RAMAN · UTP · OLMAN · icm · zielMAN · Akademickie Centrum Informatyki

Działalność PCSS dla szkół

- ePodręczniki do kształcenia ogólnego
  - Partner technologiczny
- System rekrutacji NABÓR
- Laboratorium Szkoły Przyszłości
- Współpraca w zakresie SIO
- Wirtualne lekcje
- Szkolenia dla kadry pedagogicznej, rodziców, uczniów

epodreczniki.pl

SIO SYSTEM INFORMACJI OŚWIATOWEJ

NABÓR 2016

laboratorium szkoły przyszłości

DZIEŃ BEZPIECZNEGO INTERNETU

Podstawowe obszary działania PCSS w zakresie bezpieczeństwa IT

- Nadzór nad infrastrukturą („Praca operacyjna”)
- Zadania bezpieczeństwa w projektach naukowo-badawczych
- Realizacja misji szkoleniowej
- Współpraca z jednostkami zewnętrznymi
- Badania własne w dziedzinie bezpieczeństwa IT

ZSŁ

Zespół Szkół Łączności w Poznaniu
im. Mikołaja Kopernika

4 GIMNAZJUM

GIMNAZJUM NR 4 | TECHNIKUM | REKRUTACJA | KURSY ZAWODOWE | KONTAKT

platonTV

PLATFORMA NAUKOWEJ INTERAKTYWNEJ TELEWIZJI W SIECI PIONIER

lekcja

Najnowsze Informacje Katalog

PARTNERZY PRZEDSIĘWZIĘCIA: ZSŁ Genius loci PCSS REALIZACJA TRANSMISJI: platonTV

PRZEŁĄCZ ODTWARZACZ NA SILVERLIGHT

Chrzest Polski w badaniach archeologicznych grodu poznańskiego

PCSS IChB PAN - Poznańskie Centrum Superkomputerowo-Sieciowe

- Strona główna
- Serwis wewnętrzny
- Dzienniczek ucznia
- Wirtualna Klasa
- Strefa ucznia
- Fundusz Stypendialny
- Plan lekcji
- Galeria fototechnika
- Bufet Łącznik
- Konsultacje dla rodziców i uczniów
- O szkole

Lekcja z sercem

« powrót

17.12.201 WANIA

Dnia 28.11.2012 Pani wicedyrektor **Magdalena Jurczyk-Maciuszonek** wzięła udział eksperymencie edukacyjnym przeprowadzonym w Poznańskim Centru Superkomputerowo-Sieciowym. Głównym celem przedsięwzięcia było zweryfikowan przydatności nowoczesnych technologii w zastosowaniach edukacyjnych. Eksperyme polegał na przeprowadzeniu zdalnej lekcji z wykorzystaniem wideokonferen wzbogaconej o generowaną w czasie rzeczywistym grafikę 3D. Tematem lekcji by budowa serca ludzkiego. Dla uatrakcyjnienia anglojęzycznego wykładu, pa wicedyrektor wykorzystała trójwymiarowy, sterowany za pomocą gestów wirtualny model. Słuchaczami wykładu byli uczniow

ZSŁ

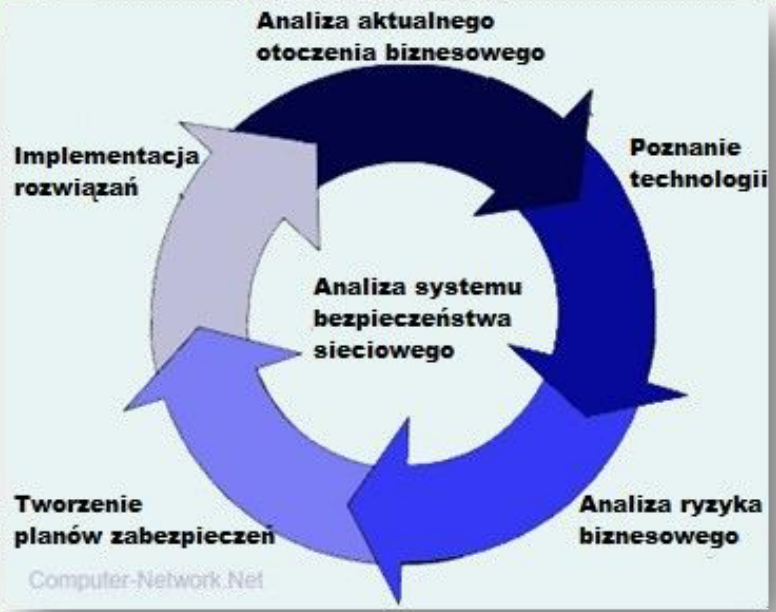
Szanowny Pan
mgr inż. Gerard Frankowsk
PCSS w Poznaniu

Dyrekcja Zespołu Szkół Łączności w Poznaniu
składa serdeczne podziękowania za twórczy udział w konferencji
Portale społecznościowe jako nowa jakość życia w świecie wirtualnym"

W kolejnej części prezentacji zamierzamy opowiedzieć o kilku istotnych aspektach bezpieczeństwa IT

Cyberbezpieczeństwo – dwa kluczowe fakty

- Bezpieczeństwo jest **procesem**, a nie stanem
- Należy dbać o bezpieczeństwo **od początku** cyklu życia systemu

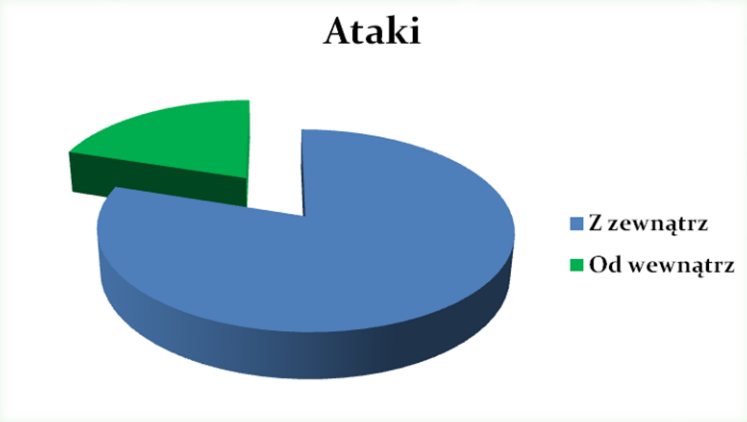


Ataki cybernetyczne mogą mieć różną postać

Atak	Przygotowanie	Zysk napastnika	Ochrona	Przykłady
Wandalizm	Łatwe	Żaden lub prawie żaden	Dość łatwa	DDoS, podmiana strony
Ataki masowe	Łatwe	Istotny (wynika z liczby ofiar, których indywidualne straty nie są duże)	Łatwa	Phishing, skany, wysyłanie *ransomware*
Ataki ukierunkowane	Trudne, długotrwałe	Duży lub bardzo duży	Praktycznie niemożliwa	Google Aurora, Stuxnet

Możemy zostać zaatakowani z zewnątrz, ale i od wewnątrz

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




Czy środowisko sieci szkolnej charakteryzuje się szczególnymi cechami w aspekcie zagrożeń IT?

19-LETNI UCZEŃ WŁAMAŁ SIĘ NA SZKOLNY SERWER

Publikacja: 23 kwietnia 2015, 18:15

Lubię to! 105

LEGNICA POWIAT REGION

ca.pl » Fakty » Legnica

Uczeń Zespołu Szkół Ekonomicznych w Starogardzie Gdańskim bezkarnie penetrował system informatyczny swojej wcześniejszym informacjom podawanych przez niektóre ma włamał się do dziennika elektronicznego. Nie mógł więc zmieniać ocen. Dyrektor placówki kazał wzmocnić zabezpieczenia i zawiadomił policję o możliwości popełnienia przestępstwa.

Pt. 24.10.2012, 15:30

Polec 66 wykop Tweet

Uczeń wpisał sobie 52 oceny do elektronicznego dziennika

15-letni gimnazjalista z Kalisza Pomorskiego przyznał się do wpisania s ocen do elektronicznego dziennika. Uczeń tłumaczył swoje postępowan dostania się do lepszej szkoły po ukończeniu gimnazjum. Nie wiadomo, 15-latek uzyskał dostęp do kodów potrzebnych do zalogowania się na platformie internetowej, za pomocą której nauczyciele wpisują stopnie.

Poznań: Młody haker zmieniał szkolne oceny

Agnieszka Smogulecka, Katarzyna Sklepik 5 marca 2011 AKTUALIZACJA: 6 marca 2011 12:03

Nastolatek włamał się do systemu informatycznego szkoły. Wykorzystał hasła nauczyciela … pozmieniał oceny kolegów - dowiedział się nieoficjalnie "Głos Wielkopolski". - Chciałe sprawdzić, czy się uda - miał tłumaczyć później. O sprawie plotkuje młodzież, jednak dorośli nabrali wody w usta. O incydencie, choć doszło do niego miesiąc temu, nawet nie powiadomiono Wydziału Oświaty Urzędu Miasta Poznania.

Chłopak miał wykorzystać metodę, którą stosują złodzieje ogołacający cudze konta. Stworzył replikę strony internetowej szkoły, później wkleił odpowiedni skrypt, na końcu - wysłał odnośnik do linku do jeszcze innej strony internetowej. Kolejne zabiegi pozwoliły mu uzyskać dostęp do hasła jednego z nauczycieli. Wy

Nastoletni haker zarządzał profilem magistratu!

2013-12-19 11:30:47

Policja zatrzymała 16-latka, który zaatakował profil Urz Miasta na jednym z portali społecznościowych. Ze względu jego wiek, zajmie się nim sąd dla nieletnich.

Włamywanie się na strony internetowe trenował już w namysłowski łatwością buszował po stronach szkoły. Nigdy niczego na nich nie z wszystkim pokazać, że potrafi to zrobić. To imponowało kolegom, jego pobytu w szkole oddali na Łukasza S... najwięcej głosów w wy uczniowskiego.

Sprawą 14-letniego hakera zajmie się sędzia rodzinny, fot. sxc.hu / Źródło: sxc.hu

14-latek włamywał się na fanpage'e na Facebooku, przejmował nad nimi kontrole i próbował je sprzedać - informuje TVN24.

Policja z Ostrowa ustaliła tożsamość hakera, który włamywał się na konta na Facebooku i próbował je sprzedać. Okazało się, że podejrzany ma 14 lat. Haker włamał się m.in. na konta znanych czasopism, firm i jednego zespołu muzycznego. Ponadto chłopak dopuścił się oszustw internetowych, polegających na oferowaniu do sprzedaży towaru, którego nie posiadał oraz posłużenia się przy zakupie fałszywym dowodem wpłaty - mówi TVN24 aspirant Artur Kurczaba, oficer prasowy KPP w Ostrowie.

Źródła: gdansk.tvp.pl, www.gloswielkopolski.pl, wiadomosci.wp.pl, fakty.lca.pl, www.wprost.pl

Przykładowe problemy bezpieczeństwa IT w szkole

- Częsty brak zaawansowanej infrastruktury oraz dogłębnej wiedzy w zakresie bezpieczeństwa IT
- Duża liczba użytkowników o potencjalnie złośliwych intencjach
- Intensywne używanie i wymiana treści cyfrowych
- Możliwość podłączania do sieci własnych urządzeń (BYOD)
- Korzystanie z współdzielonych komputerów w pracowniach
- Duża ilość cennych danych, w tym danych osobowych i wrażliwych

Główne zagrożenia w szkołach

Wymienione zagrożenia koncentrują się tylko na aspekcie technicznym korzystania z usług IT!

- Działanie złośliwych użytkowników z wnętrza sieci
- Możliwość ataku ze strony sieci Internet (przypadkowego lub intencjonalnego)
- Ataki z sieci szkoły w stronę Internetu
  - Przez umyślnego atakującego
  - Przez komputer zombie
- Dostęp do nieodpowiednich treści przez uczniów szkoły (narkotyki, przemoc, pornografia, hazard, …)
- Naruszanie praw autorskich

Ogólne podejście do zaawansowanej ochrony IT musi być oparte na strategii ochrony w głąb

Zasada ochrony w głąb jest odpowiedzią na brak idealnego systemu zabezpieczeń

- Ochrona w głąb (ang. *security-in-depth*) – na wielu różnych warstwach, np.:
  - Istnieje błąd w aplikacji dziennika elektronicznego – można wpisać 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

Proponujemy ogólny model zapewnienia wysokiego poziomu bezpieczeństwa IT w sieciach placówek edukacyjnych

Elementy modelu bezpiecznego dostępu do Internetu

- Szerokopasmowa sieć dla nauki PIONIER
- Systemy firewall nowej generacji (NGFW)
- Zaawansowane rozwiązania detekcji zagrożeń
- Obsługa incydentów bezpieczeństwa
- Konsulting w zakresie bezpieczeństwa
- Bezpieczne usługi w szkole (następna prezentacja)
- Bonus…

Założeniem modelu jest możliwość maksymalnego uproszczenia obsługi infrastruktury IT na poziomie szkoły.

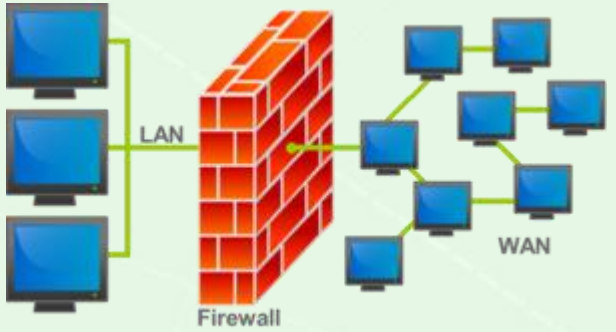
Z udostępnianych usług będą wszakże mogły korzystać wszystkie placówki.

Podłączenie szkół

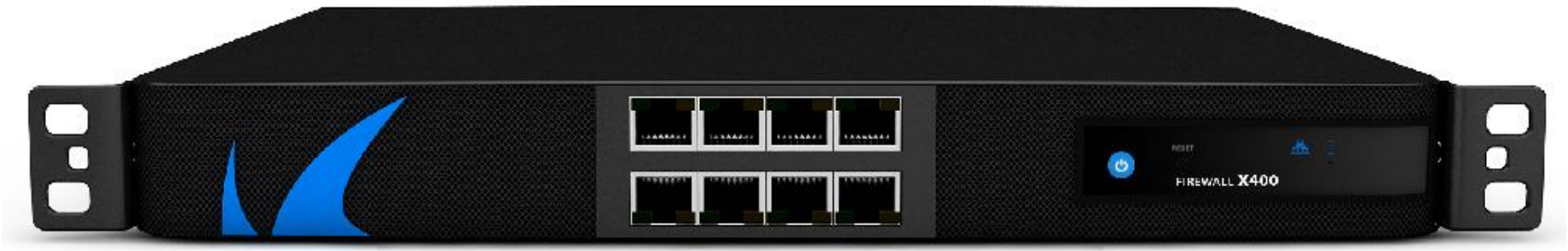
Zapewnienie szkołom bezpiecznego dostępu do Internetu

Szerokopasmowy, efektywny dostęp do zasobów Internetu

Gwarancja ochrony brzegu sieci
jako jeden z filarów bezpieczeństwa



Szerokopasmowa sieć PIONIER jako gwarancja niezawodnego i bezpiecznego dostępu do Internetu



Firewall nowej generacji (NGFW) to kluczowy system bezpieczeństwa

Funkcjonalność NGFW (1)

Wybrane moduły

SSL proxy

Sandbox

Kontrola aplikacji

IPS

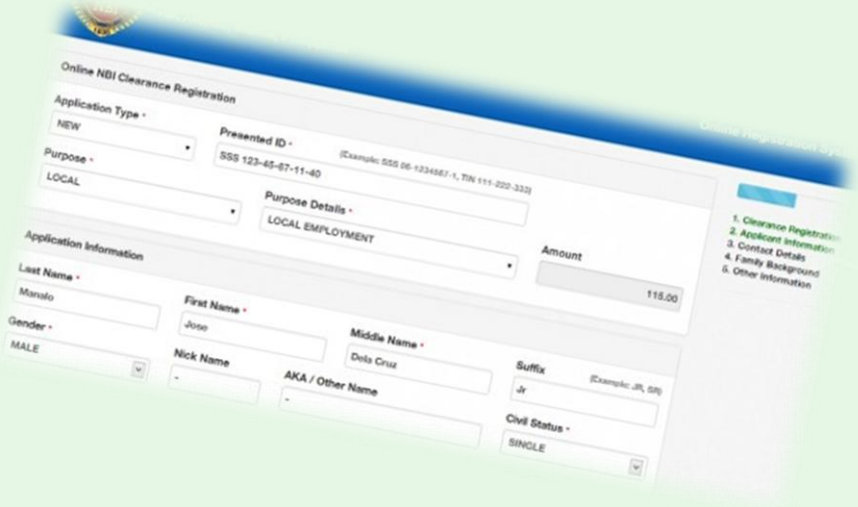
Filtracja URL

Antywirus

AntySPAM

Funkcjonalność NGFW (2)

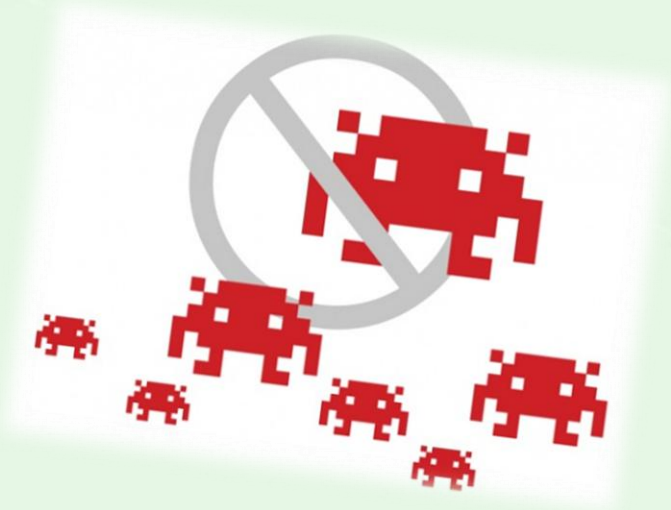
Kontrola aplikacji



Umożliwia filtrowanie dostępu tylko dla określonych aplikacji

Funkcjonalność NGFW (3)

IPS (Intrusion Prevention System)



Chroni urządzenia sieciowe przed atakami z zewnątrz

Funkcjonalność NGFW (4)

Filtracja URL

Umożliwia filtrację niepożądanej treści (pornografia, używki, przemoc, hazard, itp.)

Art. 4a Ustawy o systemie oświaty. Szkoły i placówki zapewniające uczniom dostęp do Internetu są obowiązane podejmować działania zabezpieczające uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju, w szczególności zainstalować i aktualizować oprogramowanie zabezpieczające.

Funkcjonalność NGFW (5)

Antywirus

Dodatkowa ochrona przed szkodliwym oprogramowaniem

UWAGA!

Uzupełnia, lecz nie zastępuje systemu antywirusowego na „końcówce” (stacjach roboczych, urządzeniach użytkownika)

Funkcjonalność NGFW (6)

SSL proxy

Umożliwia analizę ruchu zaszyfrowanego (ssl)

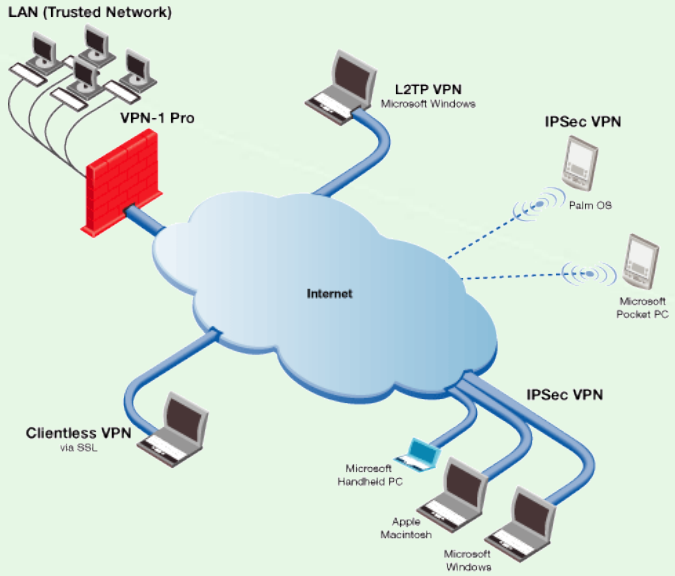
Funkcjonalność NGFW (7)

Sandbox

Chroni przed nowymi zagrożeniami

Funkcjonalność NGFW (8)

Zdalny dostęp



Umożliwia bezpieczny zdalny dostęp do zasobów sieci z Internetu


Krótko przedstawimy pozostałe elementy
modelu bezpiecznego dostępu do Internetu

Zaawansowane systemy rozpoznawania zagrożeń (1)

Analiza anomalii czy analiza sygnatur?

- Na zasadzie analizy sygnatur działa większość programów antywirusowych
- Ale co z nieznanymi zagrożeniami?
- Wspomniane podejścia nie powinny ze sobą konkurować, ale się uzupełniać

Najważniejsze wyróżniki rozwiązań wykrywających anomalie

Możliwość detekcji nieznanych zagrożeń

Możliwość uzyskania błędnych wyników

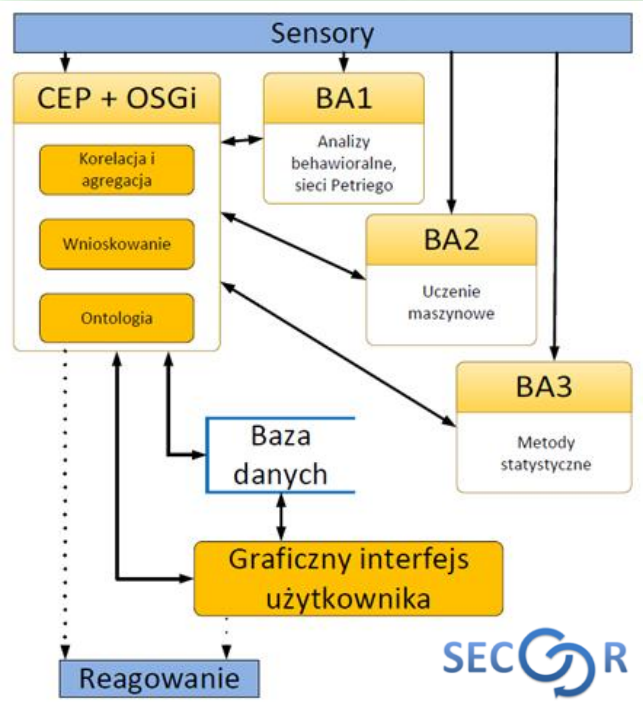
Brak zależności od bazy sygnatur

Konieczność nauczenia systemu

Zaawansowane systemy rozpoznawania zagrożeń (2)

Doświadczenie w budowie systemów detekcji anomalii

- Projekt SECOR (2012-2015)
- Wykorzystanie „sztucznej inteligencji”
  - Algorytmy uczenia maszynowego (ML)
  - Techniki optymalizacji ML
  - Metodologia zaawansowanego przetwarzania zdarzeń (CEP)
- Możliwość wdrożenia systemu detekcji anomalii w różnych punktach sieci
  - System centralny
  - Sonda w sieci szkoły



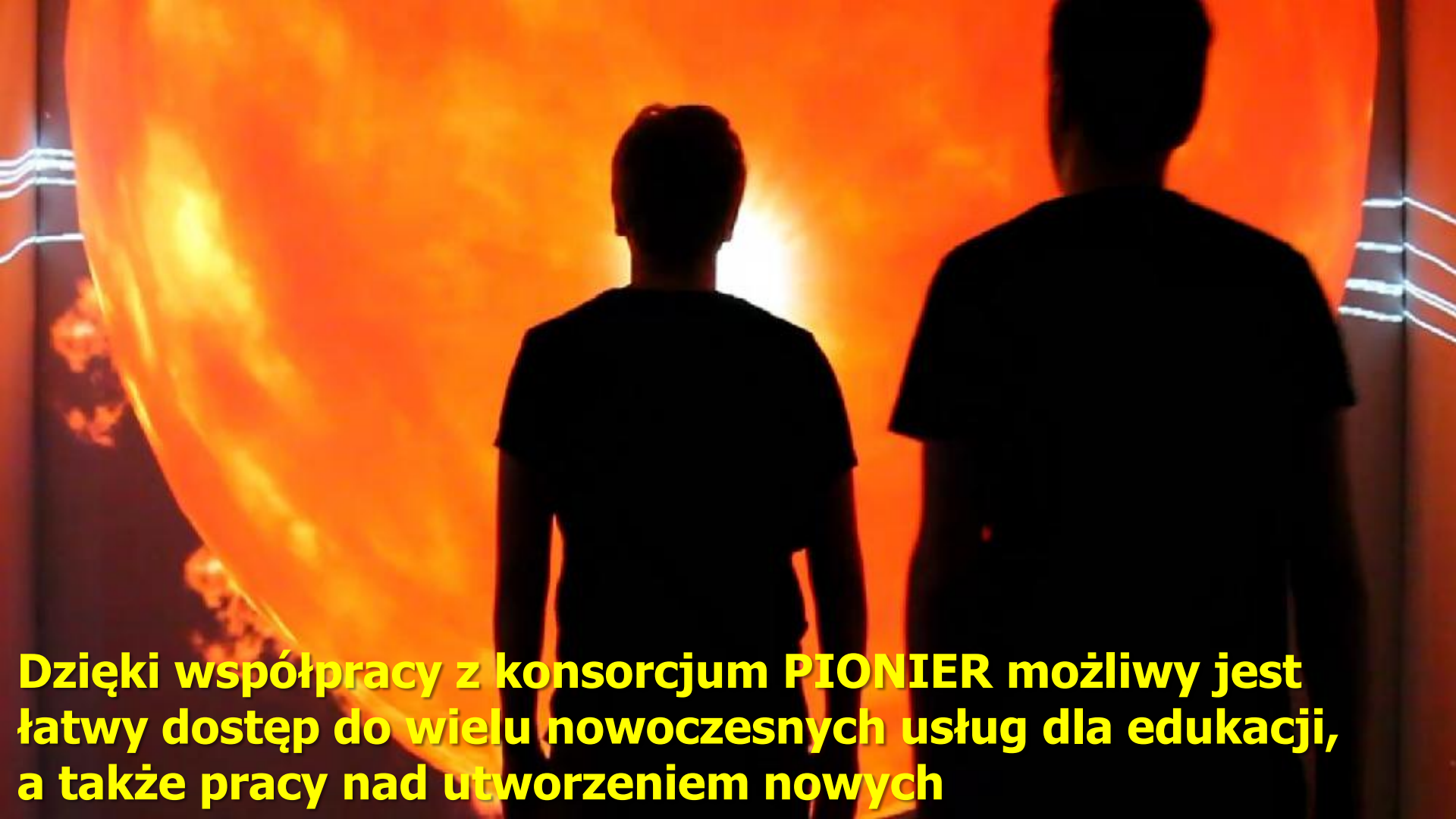
Obsługa incydentów sieciowych

Wykorzystanie doświadczenia oraz bazy zasobowej PIONIER CERT

- CERT = *Computer Emergency Response Team*, zespół obsługi incydentów sieciowych
- Grupa robocza Konsorcjum PIONIER z aktywnym udziałem PCSS
  - Głównym zadaniem grupy PIONIER-CERT jest obsługa wszelkich incydentów w których bezpośrednio lub pośrednio zaangażowane są komputery przyłączone do Krajowej Szerokopasmowej Sieci Naukowej PIONIER
  - Więcej: http://cert.pionier.gov.pl/Misja
- Zapewnienie spójnej metodologii i procedur obsługi incydentów w poszczególnych sieciach dołączonych do PIONIER-a

Konsulting i ciągłe wsparcie

- Polska odczuwa gwałtowny brak specjalistów bezpieczeństwa IT, widoczny szczególnie w sektorach takich jak administracja publiczna czy edukacja
- Konsorcjum PIONIER gotowe jest zapewnić wsparcie:
  - Pomoc przy konfiguracji sieci i systemów
  - Wsparcie w tworzeniu SZBI
  - Niezależne oceny bezpieczeństwa
  - Usługa SOC (Security Operations Center)



Dzięki współpracy z konsorcjum PIONIER możliwy jest łatwy dostęp do wielu nowoczesnych usług dla edukacji, a także pracy nad utworzeniem nowych

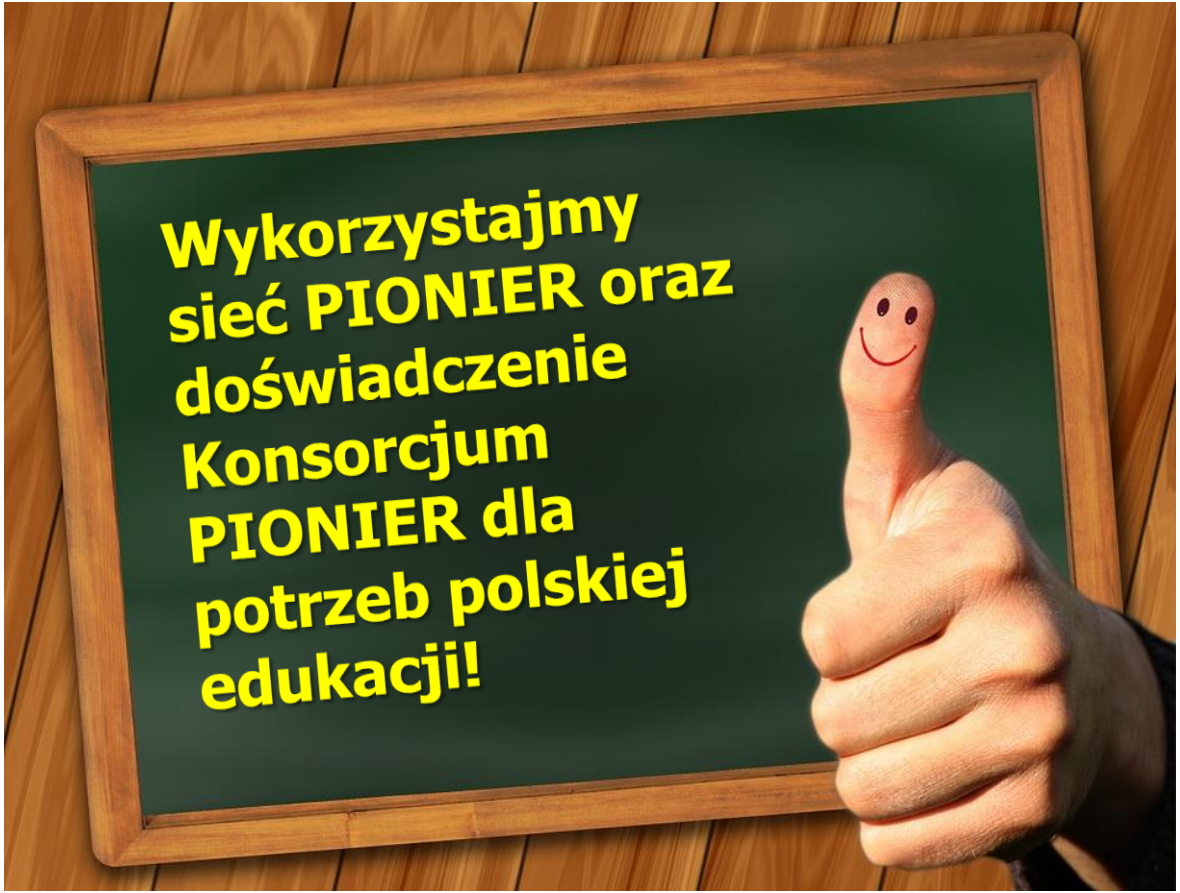
Dostęp do zaawansowanych usług dla edukacji

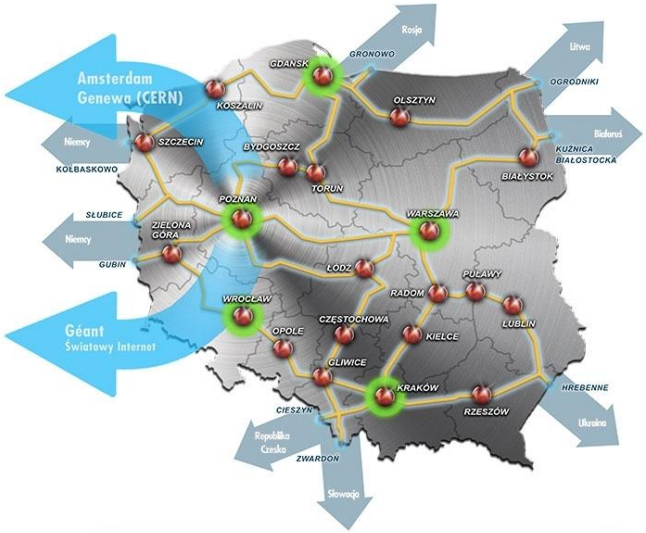
Bonus!

- Usługi o ugruntowanej pozycji, udostępniane przez członków konsorcjum PIONIER
  - Bezpieczne rozwiązania do archiwizacji i składowania danych
  - Usługi wideokonferencji
  - Telewizja naukowa
  - Usługi kampusowe
  - Bezpieczne uwierzytelnianie – *eduroam*

- Usługi edukacyjne nowej generacji
  - Dostęp do ponad 20 laboratoriów badawczych CBPIO

Eksperymentalna przestrzeń badań interakcji użytkowników z usługami sieciowymi nowej generacji (living labs)
Eksperymentalny usługowy węzeł obsługi laboratoriów i dostępu zdalnego Lab(IT)aaS
Laboratorium bezpieczeństwa cyberprzestrzeni i ochrony infrastruktur krytycznych
Laboratorium integracji technologii ICT z otoczeniem
Laboratorium integracji technologii komunikacyjnych
Laboratorium integracji usług sieciowych z sieciami IOT i naukowego wykorzystania infrastruktur społecznościowych
Laboratorium otwartego sprzętu sieciowego
Laboratorium przetwarzania i przesyłania sieciowych multimediów 3D
Laboratorium sieci definiowanych programowo (PL-LAB2020)
Laboratorium sieci optycznych o programowalnej optyce 100/400/1000G
Laboratorium symulacji i zintegrowanego sterowania zasobami w multidomenowych ekosystemach sieciowych
Laboratorium technologii informacyjnych przyjaznych środowisku - „Green ICT"
Laboratorium technologii interfejsów głosowych dla usług nowej generacji
Laboratorium technologii oprogramowania usługowego
Laboratorium telemedycyny
Laboratorium usług nowych mediów UHD w sieciach optycznych
Laboratorium wirtualne dla e-Nauki
Laboratorium wizualizacji i interakcji
Laboratorium zarządzania centrami danych i systemami efektywnymi energetycznie


Wykorzystajmy
sieć PIONIER oraz
doświadczenie
Konsorcjum
PIONIER dla
potrzeb polskiej
edukacji!


Amsterdam
Genewa (CERN)
Géant
Światowy Internet
Rosja
Litwa
Niemcy
Niemcy
Republika Czeska
Słowacja
Białoruś
Ukraina
GDAŃSK
GRONOWO
OGRODNIKI
KOSZALIN
OLSZTYN
SZCZECIN
BYDGOSZCZ
KUŹNICA BIAŁOSTOCKA
KOŁBASKOWO
TORUŃ
BIAŁYSTOK
POZNAŃ
SŁUBICE
ZIELONA GÓRA
WARSZAWA
GUBIN
ŁÓDŹ
PUŁAWY
RADOM
WROCŁAW
LUBLIN
CZĘSTOCHOWA
OPOLE
KIELCE
GLIWICE
KRAKÓW
HREBENNE
CIESZYN
RZESZÓW
ZWARDOŃ

Pytania

Dziękujemy za uwagę!

Dane kontaktowe, dalsze informacje

- Autorzy prezentacji
  - gerard.frankowski@man.poznan.pl
  - tomasz.nowocien@man.poznan.pl
- PCSS
  - www.pcss.pl
  - office@man.poznan.pl
- PIONIER
  - www.pionier.net.pl

Poznańskie Centrum Superkomputerowo - Sieciowe

afiliowane przy Instytucie Chemii Bioorganicznej PAN,

ul. Noskowskiego 12/14, 61-704 Poznań,
tel : (+48 61) 858-20-00, fax: (+48 61) 852-59-54,
e-mail: office@man.poznan.pl, http://www.pcss.pl