Bezpieczeństwo sieci

O hakerach, atakach i włamaniach.
Jak się przed nimi bronić?

Prowadzenie: Marcin Chlebowski

CCIE #21714 Security [Eximo Project, VDIBox, F5Wizard]

Eximo Project Sp. z o.o.
Bydgoszcz, ul. Poznańska 31
tel: (52) 56 84 440
fax: (52) 56 84 430
eximo@eximoproject.pl

Kim jesteśmy?

Eximo Project Sp. z o.o.
Bydgoszcz, ul. Poznańska 31
tel: (52) 56 84 440
fax: (52) 56 84 430
eximo@eximoproject.pl

PROJECT eximo
www.eximoproject.pl

- Oferujemy rozwiązania w oparciu o najwyższe standardy obowiązujące na rynku nowych technologii.
- Doświadczenie kadry inżynierskiej związane z realizacją wymagających projektów z zakresu bezpieczeństwa, infrastruktury sieciowej, budowy systemów e-commerce, systemów wirtualizacji dają gwarancję niezawodności proponowanych rozwiązań.
- Kładziemy szczególny nacisk na jakość świadczonych usług oraz niezawodność proponowanych produktów. Indywidualne podejście do potrzeb odbiorców procentuje budową optymalnego środowiska informatycznego każdej firmy.

Czym się zajmujemy?

Eximo Project Sp. z o.o.
Bydgoszcz, ul. Poznańska 31
tel: (52) 56 84 440
fax: (52) 56 84 430
eximo@eximoproject.pl

PROJECT eximo
www.eximoproject.pl

Zakres usług:

- ✓ Bezpieczeństwo systemów IT
- ✓ Rozwiązania sieciowe
- ✓ Systemy serwerowe
- ✓ Outsourcing IT w obszarach
- ✓ Usługi doradcze i szkoleniowe
- ✓ System monitoringu (F5wizard)
- ✓ Systemy wirtualizacji

Nasze Data Center:

- ✓ Zabezpieczenia energetyczne
- ✓ Kontrola dostępu i ochrony
- ✓ Systemy klimatyzacyjne
- ✓ Całodobowy monitoring dostępności
- ✓ Całodobowa opieka techniczna
- ✓ Łącza o wysokiej przepustowości
- ✓ Niezawodność

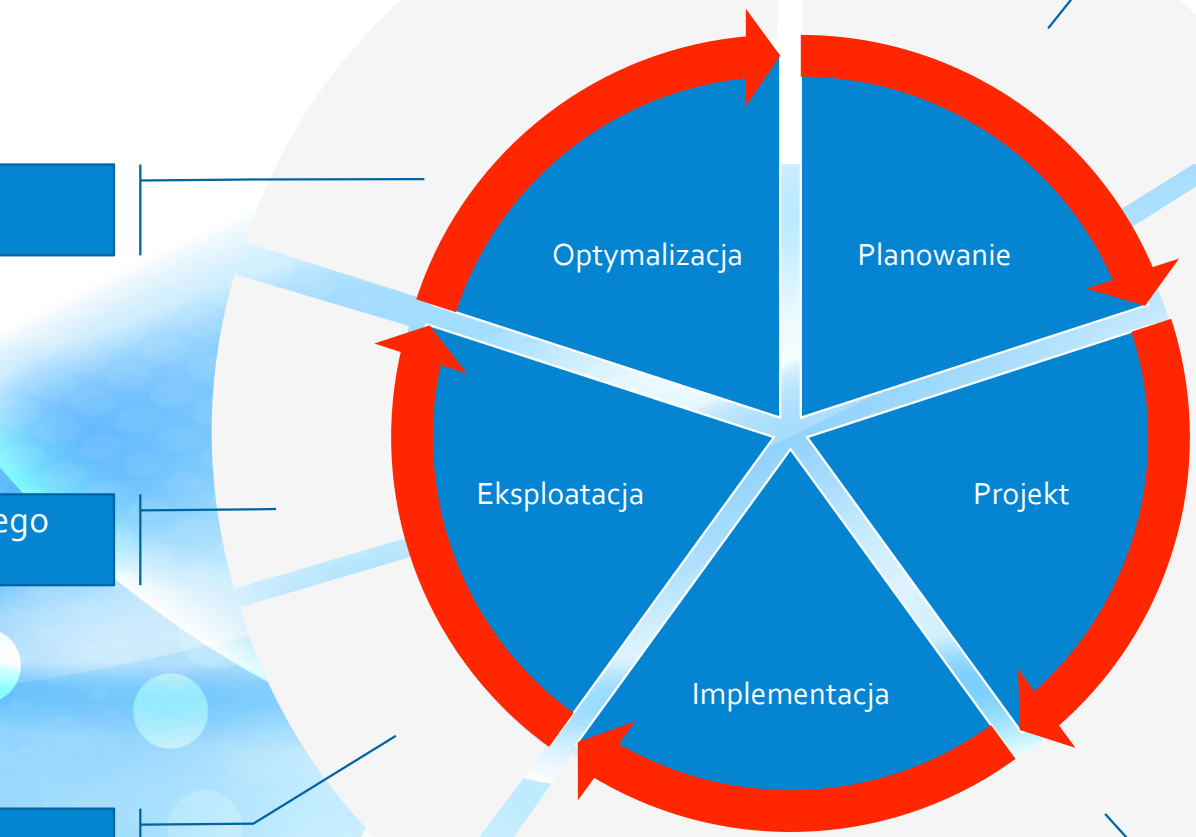
O bezpieczeństwie

Czym jest bezpieczeństwo informatyczne? Jakie są jego atrybuty?

Bezpieczeństwo teleinformatyczne jest związane ze spełnianiem pewnych jego własności, zwanych atrybutami bezpieczeństwa. Są to:

- **Integralność**
- **Poufność**
- **Dostępność**
- **Autentyczność**
- **Rozliczalność**
- **Niezawodność**

Cykl życia usługi bezpieczeństwa



- Strategia i ocena
- Optymalizacja bezpieczeństwa
- System wczesnego ostrzegania
- Zdalne zarządzanie
- Wdrożenie i migracja

Cykl życia usługi (ITIL)

- Zarządzanie strategią dla usług IT
- Zarządzanie portfelem usług
- Zarządzanie finansami dla usług IT
- Zarządzanie popytem
- Zarządzanie relacjami z biznesem

- Koordynacja projektowania
- Zarządzanie katalogiem usług
- Zarządzanie poziomem usług
- Zarządzanie dostępnością
- Zarządzanie pojemnością
- Zarządzanie ciągłością usług IT
- Zarządzanie bezpieczeństwem informacji
- Zarządzanie dostawcami

- Planowanie i wsparcie przekazania
- Zarządzanie zmianami
- Zarządzanie komponentami usług i konfiguracją
- Zarządzanie wersjami i wdrożeniami
- Weryfikacja i testowanie usług
- Ocena zmian
- Zarządzanie wiedzą

- Zarządzanie zdarzeniami
- Zarządzanie incydentami
- Realizacja wniosków o usługę
- Zarządzanie problemami
- Zarządzanie uprawnieniami dostępu

7-stopniowy proces doskonalenia

- Identyfikacja strategii dla poprawy
- Definicja co będzie mierzone
- Zbieranie danych: kto, jak, kiedy?
- Przetworzenie danych
- Analiza informacji i danych
- Prezentacja i użycie informacji
- Wdrożenie działań naprawczych

Atak na wirtualną walutę

Kradzież Bitcoin przez wstrzykiwanie tras BGP

Co udało się osiągnąć:

- Przechwycenie ruchu „górników bitcoin”,
- Kradzież mocy obliczeniowej w celu kradzieży bitcoin.

Jak przebiegał atak:

- Na ślad ataku trafili badacze z Della. Atakującemu, który kontrolował router znajdujący się w serwerowni jednego z kanadyjskich ISP, udało się za pomocą wstrzykniętych przez siebie prefiksów BGP **przekierować na swoje serwery ruch związany z „kopaniem kryptowaluty”**. Przechwycony ruch pochodził z 57 podsieci od 19 ISP. Wśród ofiar znalazły się serwerownie Amazon, DigitalOcean i OVH. *[niebezpiecznik.pl]*

Atak na wirtualną walutę

Kto stoi za tym atakiem?

- Fałszywe trasy BGP były wstrzykiwane przez router jednego z kanadyjskich ISP. Badacze nie podają jego nazwy, bo nie są pewni, czy za atakiem stał jeden z pracowników ISP, czy router został zhakowany przez kogoś z zewnątrz.
- Mógł to także być były pracownik firmy, który chciał się zemścić na byłym pracodawcy.

Jak się zabezpieczyć:

- Aplikacje powinny używać do komunikacji protokół SSL, nie tylko aby ruch nie mógł być podsłuchany ale również do identyfikacji hostów za pomocą odcisków SSL.

Nie ma systemów idealnych

[Holding finansowy JP Morgan Chase]

Kradzież danych z JP Morgan Chase

- W trakcie kontroli sieci JP Morgan Chase spostrzeżono, zapewne w skutek analizy logów związanych z obciążeniem sieci, że z bankowych serwerów od dłuższego czasu wypływają dane.

Co udało się osiągnąć włamywaczom:

- Wykradziono dane 76 milionów amerykańskich gospodarstw domowych (65% wszystkich gospodarstw w USA) oraz informacje o 7 milionach firm.
- Zdobyto wewnętrzne informacje na temat użytkowników JP Morgan Chase – informacje o systemach Big Data - przetwarzających dane o przelewach i aktywności finansowej celem utworzenia spersonalizowanego „profilu" klienta.

Nie ma systemów idealnych

[Holding finansowy JP Morgan Chase]

Jak się włamano:

- Atakujący wykorzystali nieznany dotąd atak na jedną z głównych stron świadczących usługi bankowe JP Morgan.
- Poprzez lukę w stronie wprowadzono do sieci JP Morgan złośliwe oprogramowanie, które obeszło reguły firewalla i było w stanie niezauważone wyprowadzać przez 2 miesiące dane z firmy.
- Do czasu interwencji administratorów, cały system bezpieczeństwa sieci JP Morgan Chase, na który firma wyłożyła w samym 2014 roku 250 milionów dolarów, nie wykazał żadnych anomalii.

Wnioski:

- Bez względu na ilość środków przeznaczonych na bezpieczeństwo, nie można zbudować systemu idealnego, i nie należy polegać jedynie na zaimplementowanych rozwiązaniach. Systemu powinny podlegać okresowemu przeglądowi administratorów.

[niebezpiecznik.pl]

Energia na celowniku

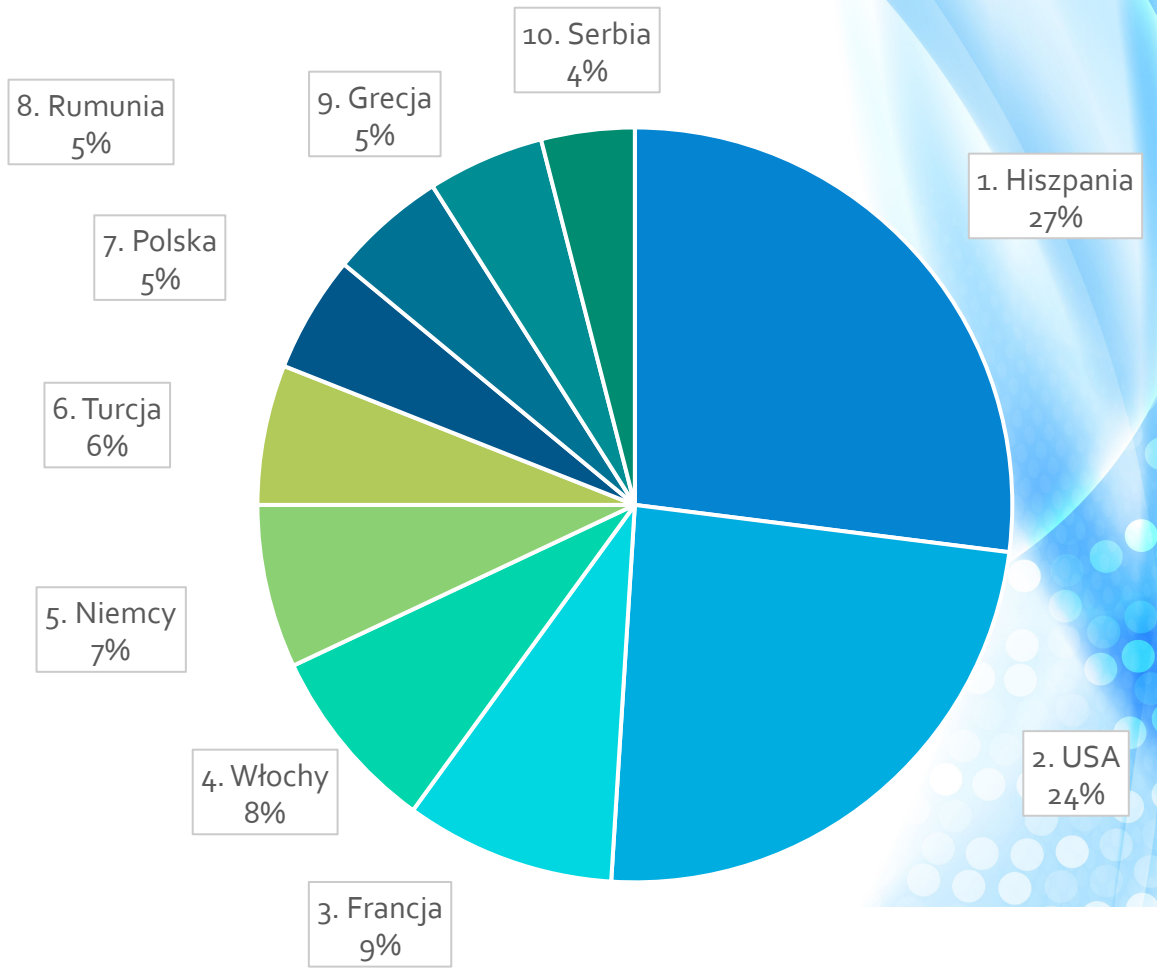
Ataki informatyczne na firmy z sektora energetycznego

Dragonfly to nazwa grupy, która trojanami infekuje komputery należące do firm z sektora.

Za większością publicznie ujawnionych tego typu ataków stoją Chińczycy.

Dragonfly to prawdopodobnie Rosjanie.

Procentowy podział na kraje zarażonych systemu sektora energetycznego przez Dragonify



Energia na celowniku

Jak się przebiegała infekcja:

- **Trojan (Havex)** jest podrzucany metodą wodopoju **(Watering Hole)**. Atakujący włamują się na strony zazwyczaj niewielkich firm - producentów oprogramowania wspierającego systemy ICS wykorzystywane do zarządzania sieciami w większych firmach energetycznych. Następnie podmieniają oryginalne oprogramowanie (np. sterownik) na „zainfekowaną".

Kiedy ofiara połknie przynętę, trojan jest zainteresowany przede wszystkim:

- książką kontaktów z Outlooka
- danymi dostępowymi do VPN

Jak się zabezpieczyć:

- Podpisywać oprogramowanie, kluczami szyfrującymi, sprawdzać sumy kontrolne aplikacji, stosować systemy IPS. *[niebezpiecznik.pl]*

Wszystko za grę…

Włamanie do Microsoft, Valve, Epic i Activision i Zombie

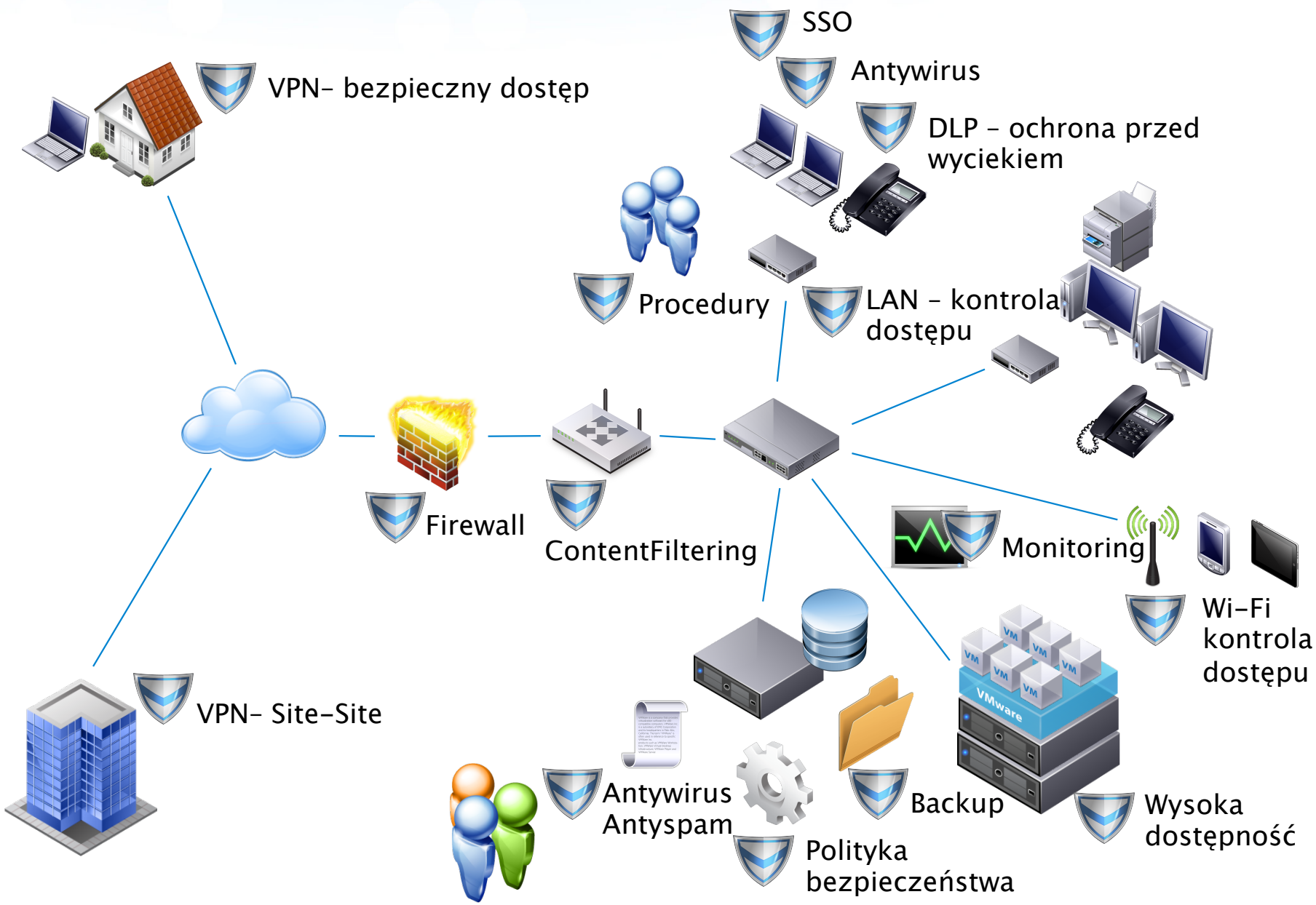
Co udało się osiągnąć włamywaczom:

- dostęp przez wiele miesięcy do wewnętrznych serwisów Microsoftu (Game Development Network Portal oraz PartnerNet)
- wykradzenie dokumentacji technicznej i kodów źródłowych oprogramowania Xbox One na wiele miesięcy przed premierą
- dostęp do sieci Epic Games, Valve i Activision Blizzard
- wykradzenie gry Gears of War 3 na ponad pół roku przed premierą
- wykradzenie gry Call of Duty: Modern Warfare 3 na kilka tygodni przed premierą
- dostęp do sieci firmy Zombie Studios, opracowującej symulator wojskowego helikoptera dla armii USA
- dostęp do wojskowej sieci i wykradzenie z niej kodu symulatora helikoptera

Główni oskarżeni to Amerykanie i Kanadyjczycy: Nathan Leroux – 20 lat, Sanadodeh Nesheiwat - 28 lat, David Pokora – lat 22 i Austin Alcala – lat 18. (Działali od 3 lat). *[zaufanatrzeciastrona.pl]*

Gdzie jest to bezpieczeństwo ?

[Przykład średniej firmy]



Firmy informatyczne oferujące produkty z zakresu bezpieczeństwa IT

1. Firewall
2. Systemy wykrywania i prewencji włamań - IPS
3. Sieci VPN w tym SSL VPN
4. Systemy kontroli treści
5. Systemy ochrony stacji roboczych
6. Systemy ochrony urządzeń mobilnych
7. Zabezpieczenie poczty elektronicznej
8. Autoryzacja i uwierzytelnianie
9. Zintegrowane rozwiązania bezpieczeństwa – UTM
10. Systemy zarządzania bezpieczeństwem
11. Systemy antywirusowe
12. Systemy ochrony danych (archiwizacja/backup)
13. Systemy zasilania awaryjnego UPS
14. Systemy kontroli dostępu
15. Bezpieczeństwo aplikacji i danych
16. Szyfrowanie informacji i baz danych

Pytania ?

Dziękuję za uwagę.

Kontakt:
marcin.chlebowski@eximoproject.pl