Bezpieczeństwo…

… czy komuś na nim zależy?

Wiesław Kasprzak

Ekspert Blue Energy Sp. z o.o.

wieslaw.kasprzak@grupablue.pl

kom. 601 809 918

www.grupablue.pl

Seminarium, Bezpieczeństwo sieci OT

Poznań, 23 maja 2017r.

Infrastruktura krytyczna - prawo

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2013 r. poz. 1166 oraz z 2015 r. poz. 1485) definiuje infrastrukturę krytyczną jako **systemy** oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, **urządzenia, instalacje**, **usługi kluczowe** dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

RCB
Rządowe Centrum Bezpieczeństwa

Infrastruktura krytyczna - prawo

ochrona infrastruktury krytycznej (wg Ustawy) – należy przez to rozumieć wszelkie działania zmierzające do zapewnienia **funkcjonalności, ciągłości działań i integralności infrastruktury** krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków **oraz szybkiego odtworzenia tej infrastruktury** na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie;

RCB
Rządowe Centrum Bezpieczeństwa

Infrastruktura krytyczna - zadania

Bezpieczna eksploatacja obiektów i instalacji

Remonty obiektów i instalacji….

Mamy rok 2017

Bezpieczeństwo systemów kluczowych dla obiektów i instalacji

Wymagania bezpieczeństwa - separacja

- **RCB – Standardy i dobre praktyki ochrony infrastruktury krytycznej - Automatyka przemysłowa w sektorze ropy i gazu**
  - K-4.1 Architektura sieci
    - Systemy firewall oraz DMZ
    - Reguły okresowo przeglądane
    - Każda zmiana dokumentowana
    - Dostęp do Internetu zablokowany
  - K-4.2 – Bezpieczeństwo sieci bezprzewodowych
    - Sieci bezprzewodowe odseparowane w sposób fizyczny
  - 4.1 – Architektura sieci – defense-in-depth –
  - Stosowanie segmentacji pomiędzy sieciami lub strefami bezpieczeństwa
  - LAN biznesowy to strefa niezaufana
  - Element pośredniczący – DMZ
  - Narzędzia kontroli ruchu
  - 4.7 – Monitorowanie systemów OT (systemy klasy SIEM, IDS).

Wymagania bezpieczeństwa - separacja

- **Rodzina norm ISA 62443 (International Society of Automation)**
  - **ISA-62443-3-3 – 2013 (dawniej ISA 99)**

9.3 SR 5.1 – Network segmentation

9.3.1 Requirement

The control system shall provide the capability to logically segment control system networks from non control system networks and to logically segment critical control system networks from other control system networsk

9.3.3 Requirement enhancements

(1) Physical network segmentation

(2) Independence from non-control system networks

(3) Logical and phisical isolation of critical networks

Wymagania bezpieczeństwa - separacja

- **Rodzina norm ISA 62443 (International Society of Automation)**
  - **ISA-62443-3-3 – 2013 (dawniej ISA 99)**

9.4 SR 5.2 – Zone boundary protection

9.4.1 Requirement

The control system shall provide the capability to monitor and control communications at zone boundaries to enforce to compartmentalization defined in the risk-based zones and conduits model.

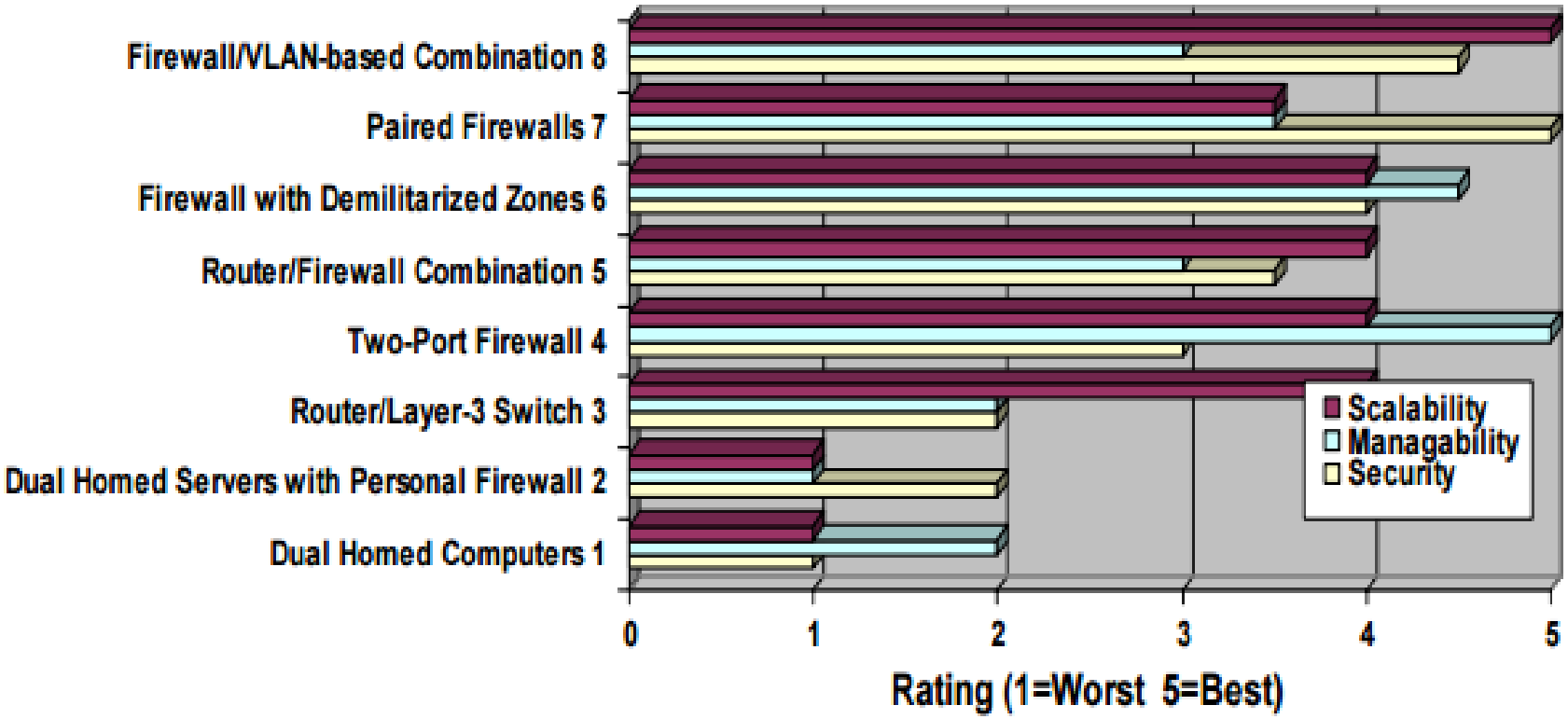
9.4.3 Requirement enhancements

(1) Deny by default, allow by exception

(2) Island mode

(3) Fail close

Wymagania bezpieczeństwa - separacja

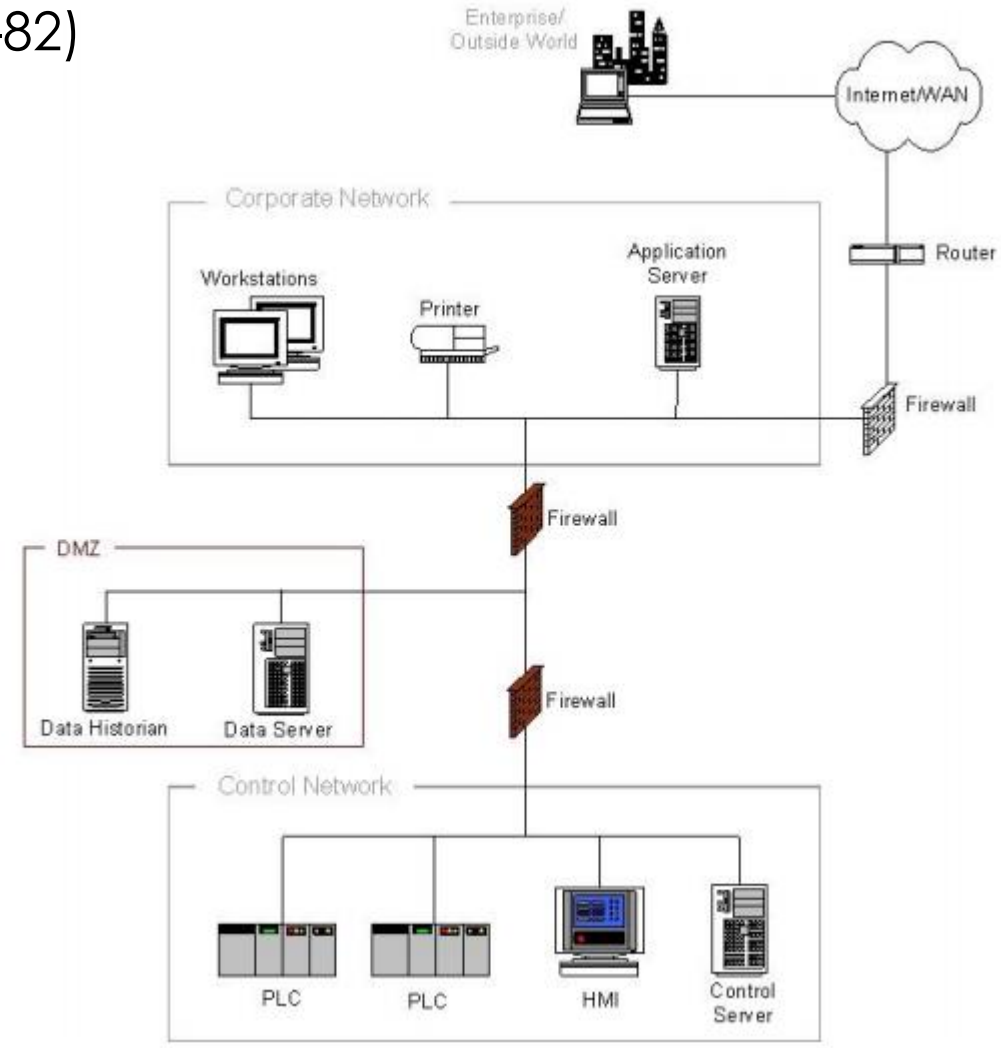


Źródło: CPNI.GOV.UK, 2004r.

CPNI
Centre for the Protection of National Infrastructure

Wymagania bezpieczeństwa - separacja

- Jedno z rozwiązań (NIST 800-82)
  - Utrzymanie firewall
  - Zarządzanie zmianą
  - Uzasadnienie reguł
  - Regularne audyty
  - Stały monitoring logów
  - Błędy….



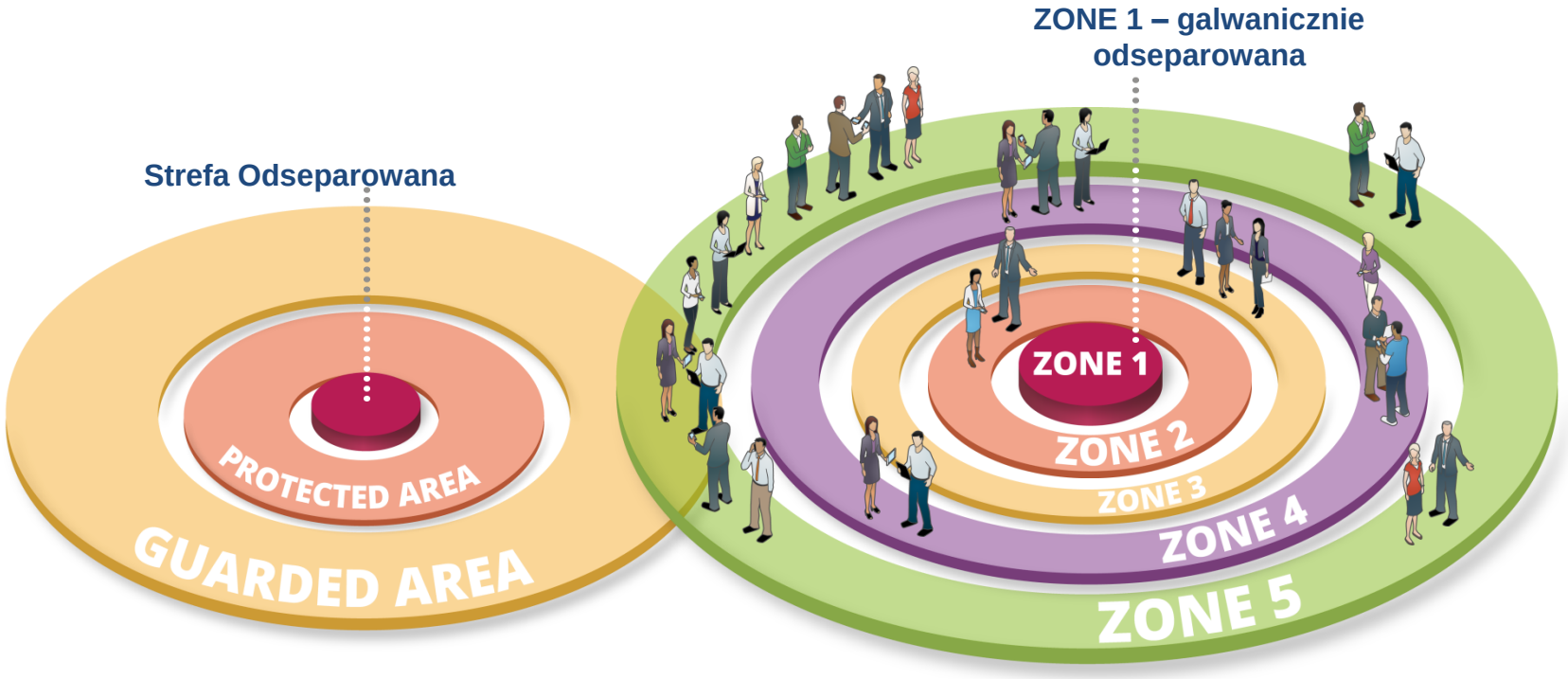
Wymagania dla bezpieczeństwa systemów SCADA

- ISA-62443 (ISA)
- Good Practice Guide, Process Control and SCADA Security (CPNI)
- NIST 800-82 Guide to Industrial Control Systems (ICS) Security (NIST US)
- ISO/IEC 27001 (ISO)
- RCB – podręcznik i wytyczne

- **5.4. Zwiększenie bezpieczeństwa teleinformatycznego usług kluczowych i cyfrowych oraz infrastruktury krytycznej**
- **5.5.Opracowanie i wdrożenie standardów oraz dobrych praktyk bezpieczeństwa sieci i systemów informatycznych**

Separacja – Defence-in-Depth

Koncepcja standardowa vs DiD



Separacja – Firewall

- Pierwsze rozwiązania to koniec lat 80 początek 90.
- DEC Seal – 1991 rok.

Technologia, która ma już 27 lat….

Obecne zagrożenia

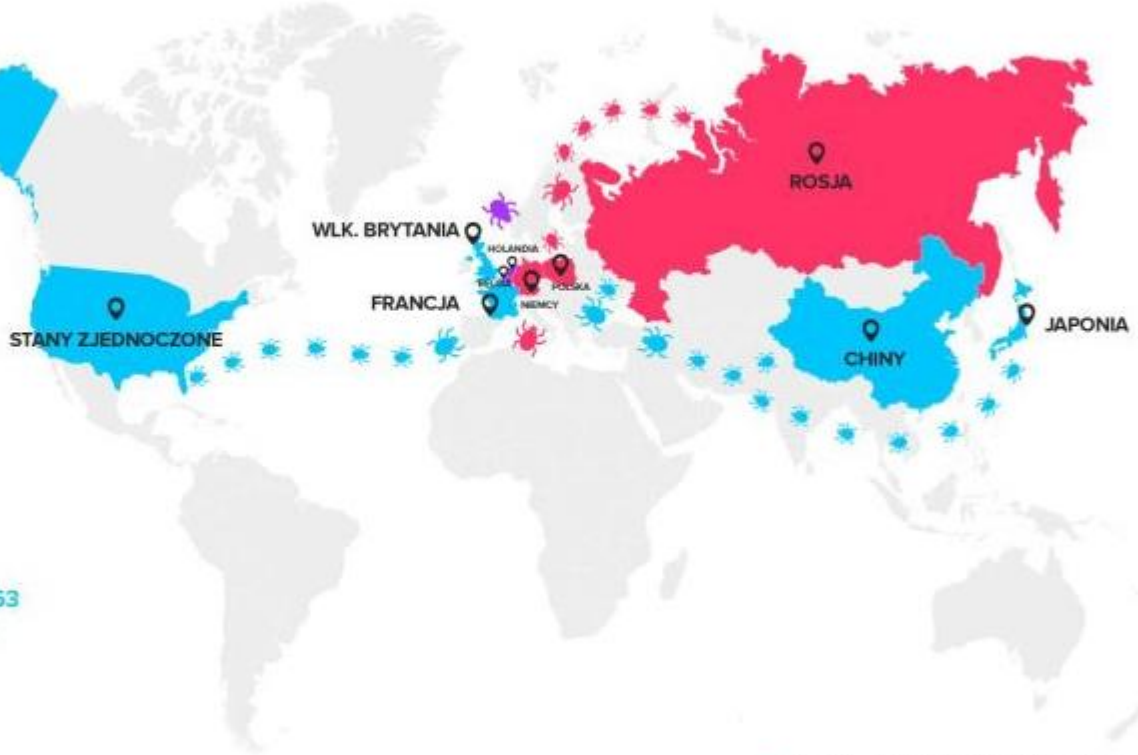
- KRLD – elitarne grupy hakerów
- ROSJA -
- CHINY 12 operacyjnych biur Armii Ludowej, jednostka 61398 – 10 mln osób
- Przestępcy…..
  - 2007 rok Estonia
  - 2008 rok Gruzja
  - 2014 rok Sony Pictures Entertainment
  - 2014 rok Tajlandia
  - 2015 rok Korea Południowa
  - 2016 rok Ukraina
  - 2016 rok Parlament RFN
  - 2017 rok USA, Francja
  - 2017 rok – cały świat

Rzeczpospolita Polska
Ministerstwo
Spraw Zagranicznych

KANCELARIA PREZESA RADY MINISTRÓW
THE CHANCELLERY OF THE PRIME MINISTER

Komisja
Nadzoru
Finansowego

SKĄD POCHODZĄ CYBERATAKI NA POLSKĘ? TOP 10



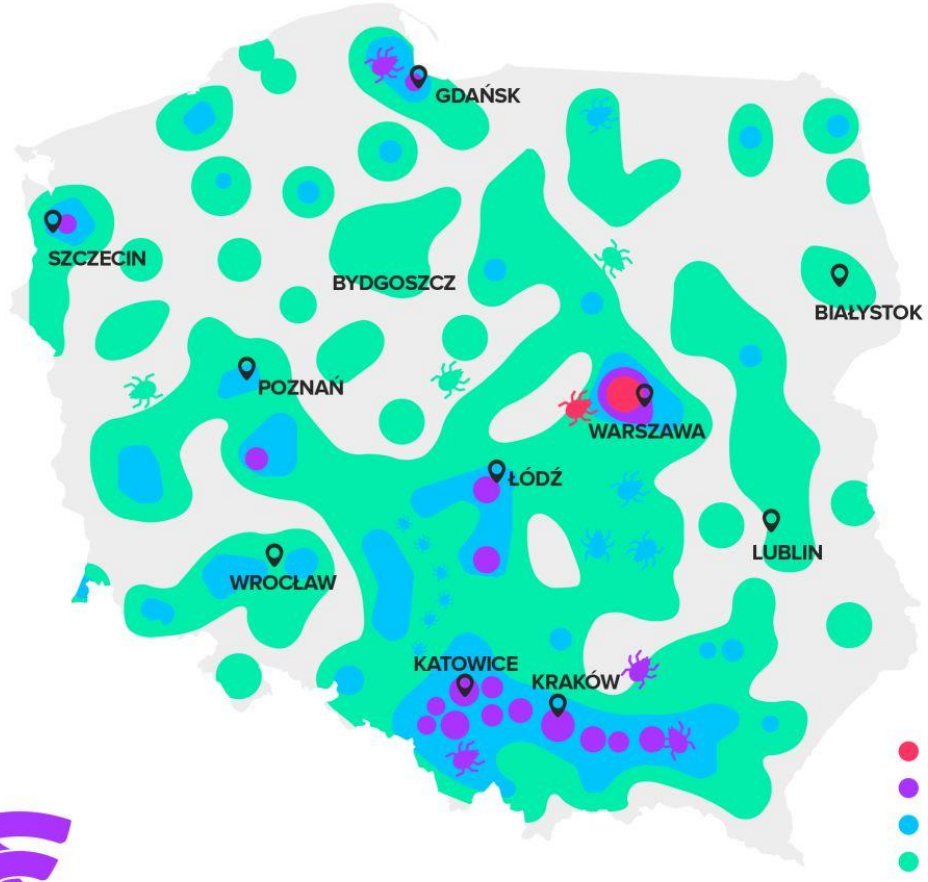
1. ROSJA **65 493**
2. NIEMCY **13 390**
3. POLSKA **11 628**
4. HOLANDIA **6 732**
5. BELGIA **4 824**
6. CHINY **463**
7. JAPONIA **199**
8. FRANCJA **187**
9. STANY ZJEDNOCZONE **163**
10. WIELKA BRYTANIA **135**

F-Secure.

- Średnio od 10 001 do 100 000 prób ataków dziennie
- Średnio od 1001 do 10 000 prób ataków dziennie
- Średnio do 1000 prób ataków dziennie

Dane z sieci Honeypot uzyskane pomiędzy październikiem 2016 i marcem 2017, 10.2016-03.2017

NAJCZĘŚCIEJ ATAKOWANE
MIEJSCA W POLSCE



F-Secure.

Dane z sieci Honeypot uzyskane pomiędzy październikiem 2016 i marcem 2017, 10.2016-03.2017

Obecne zagrożenia – jak bronią się inne kraje

- US Cyber Command – 6000 specjalistów, miliadry dolarów inwestycji
- Korea Południowa – 1000 specjalistów
- Singapur – 104 mln USD
- Wietnam – 40 mln USD
- Polska……..

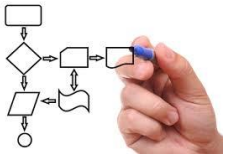
STRATEGIA CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ NA LATA 2017–2022

Podsumowując

- Zagrożenie istnieje
- Jak się zabezpieczyć wiemy
- Wymagania prawne istnieją i będą coraz bardziej precyzyjne
- Firewall – wymaga nakładów i opieki

STRATEGIA CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ NA LATA 2017–2022

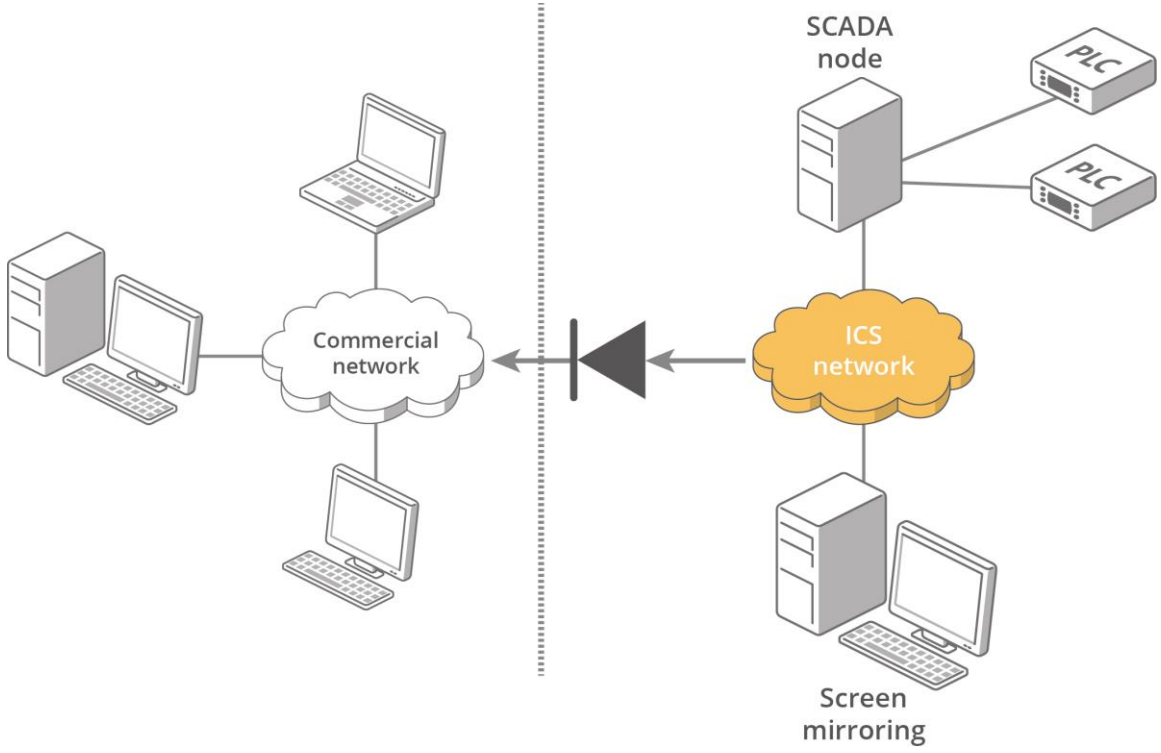
Ministerstwo Cyfryzacji



A może by tak zastosować coś innowacyjnego……

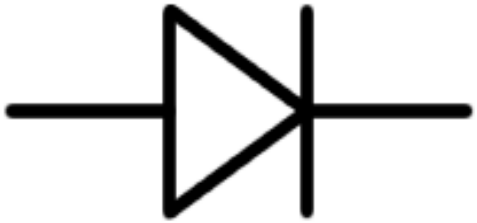
Innowacyjne metody separacji sieci

- Data Diode
  - Komunikacja UDP „tylko w jedną stronę” z zastosowaniem medium światłowodowego (nadajnik, odbiornik)



Innowacyjne metody separacji sieci

Dioda – elektroniczny komponent który przepuszcza ładunek wyłącznie w jednym kierunku.



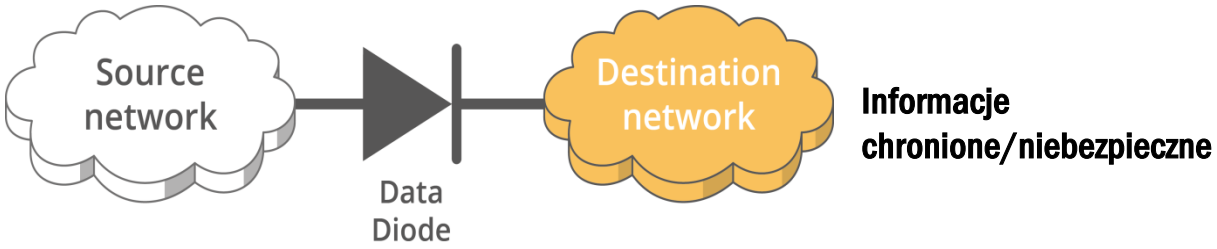
Innowacyjne metody separacji sieci

Dioda Danych – sieciowy komponent który przepuszcza dane wyłącznie w jednym kierunku.

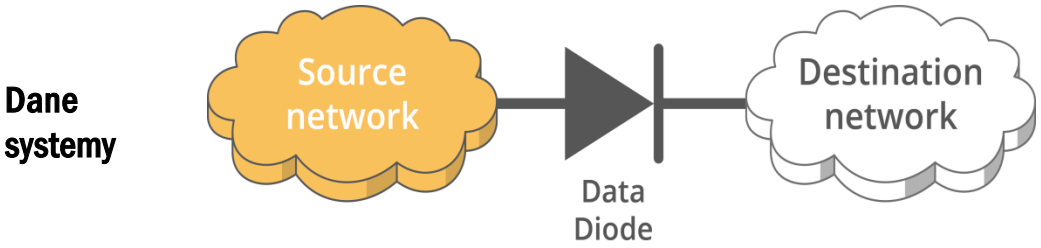
advenica

Innowacyjne metody separacji sieci

- **Chronimy poufność**
  - gdy wyciek informacji doprowadzi do katastrofy

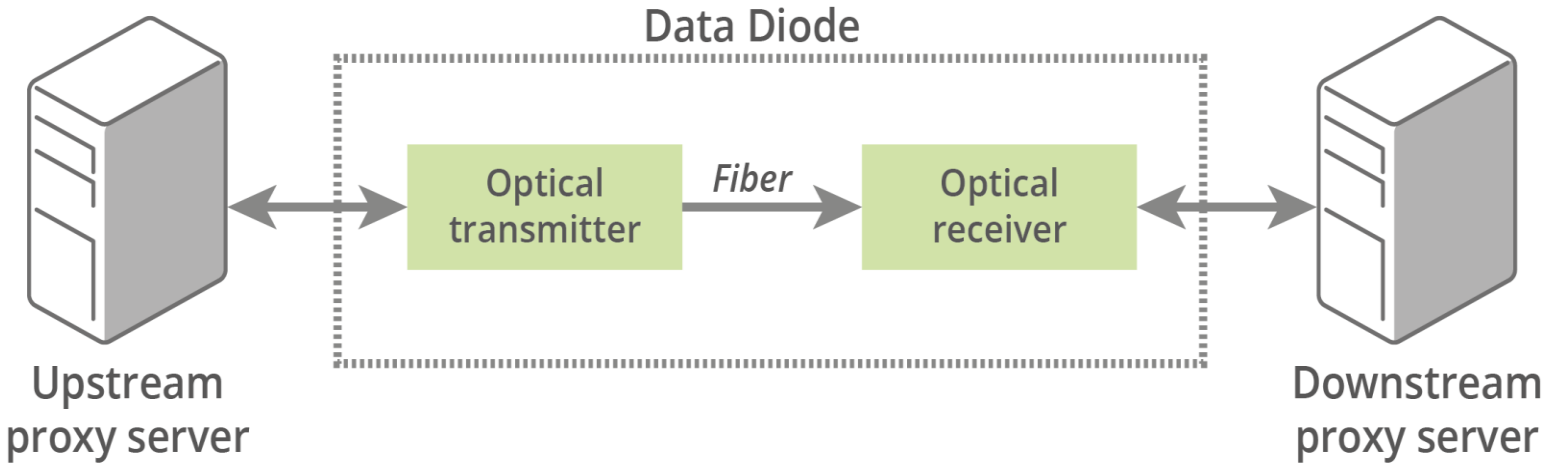


- **Chronimy integralność**
  - gdy modyfikacja danych/systemów doprowadzi do katastrofy



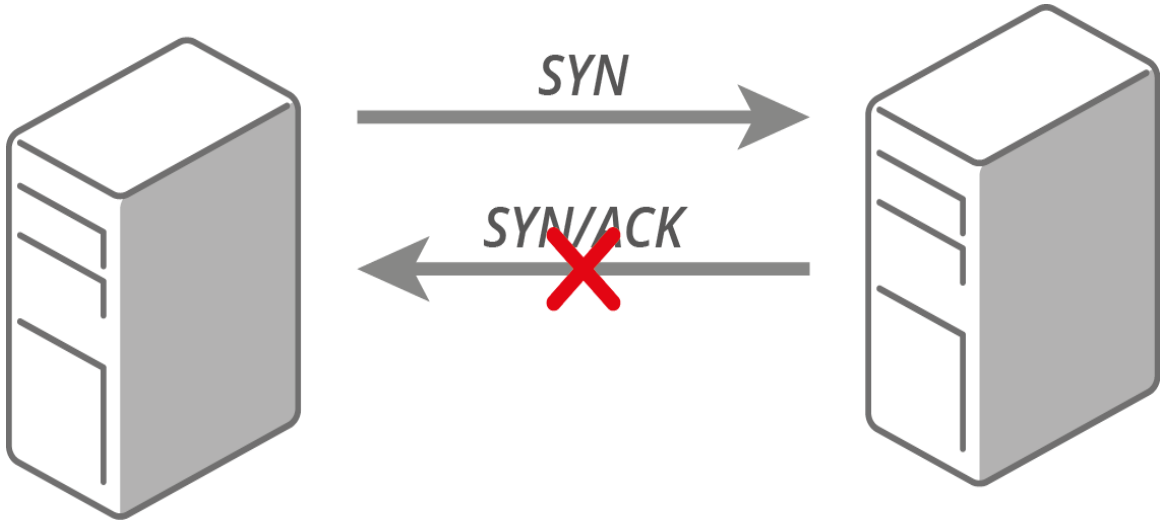
advenica

Innowacyjne metody separacji sieci



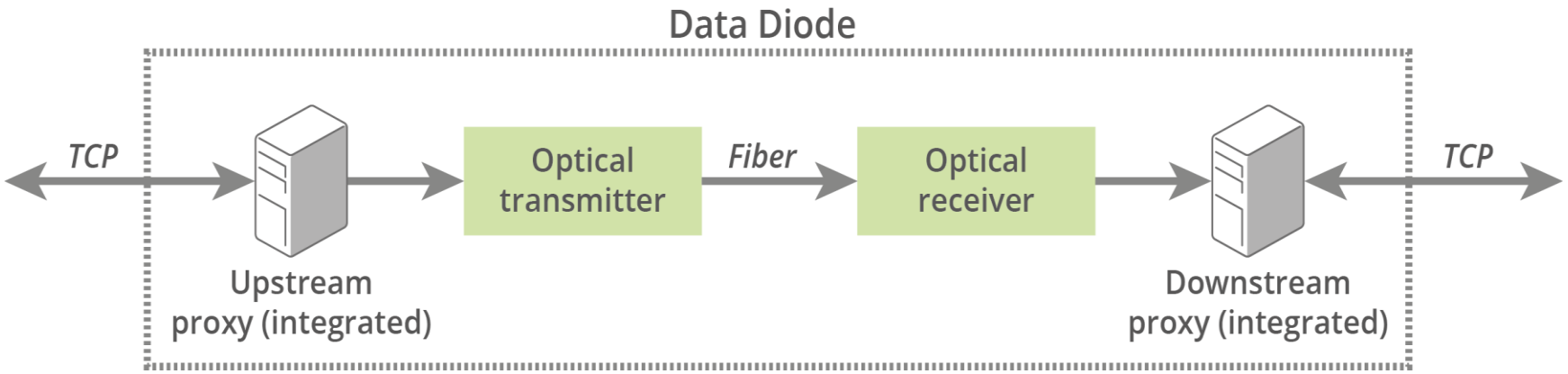
advenica

Innowacyjne metody separacji sieci



advenica

Innowacyjne metody separacji sieci



Innowacyjne metody separacji sieci

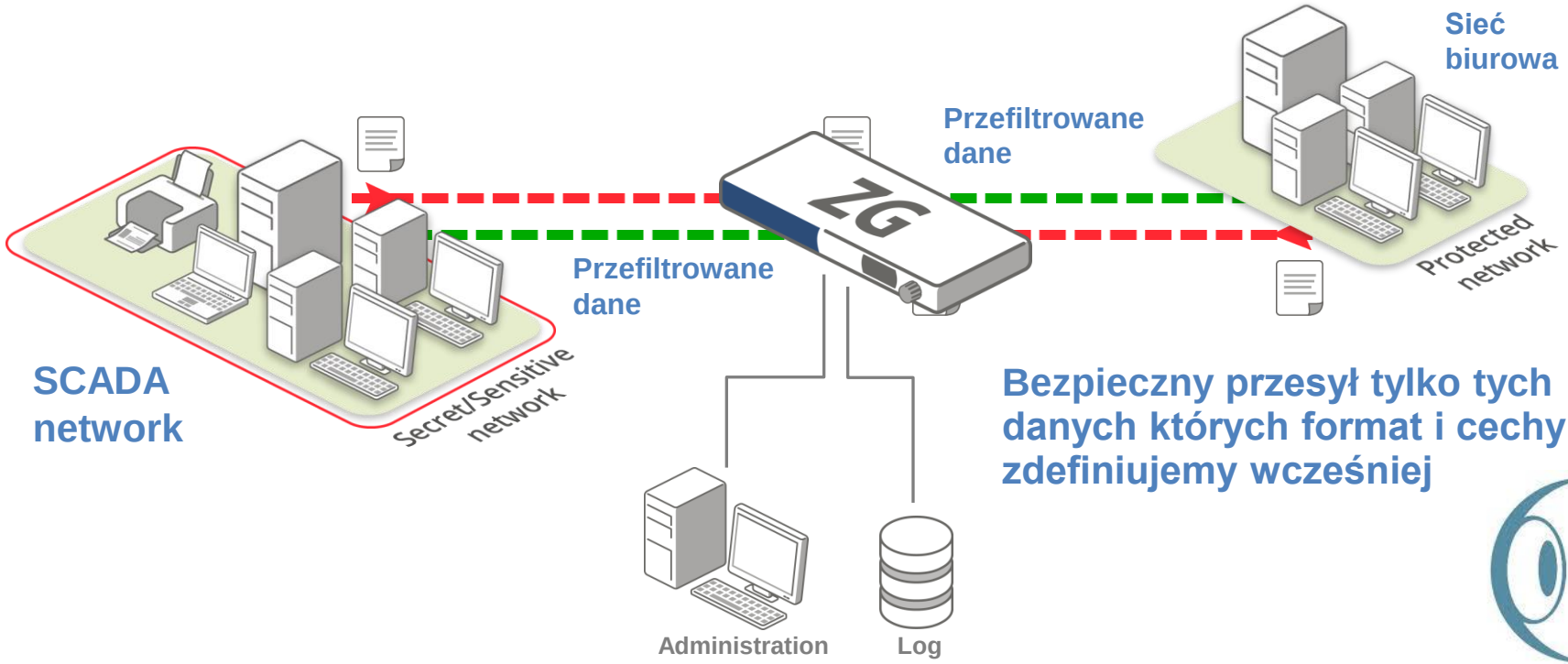
- Diody Danych

Tel-Ster sp. z o.o.
www.tel-ster.pl

Pierwsze w Polsce rozwiązanie TelDiode gotowe do wdrożenia

Innowacyjne metody separacji sieci

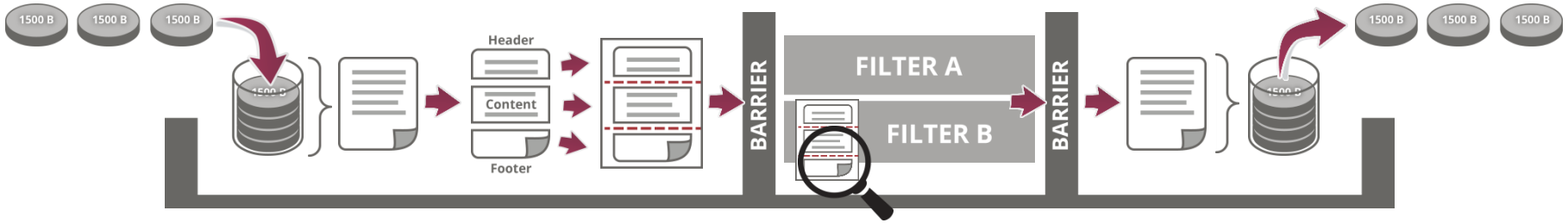
- Filtr danych
  - Przesyłamy dwustronnie tylko te dane których cechy na warstwie aplikacji dokładnie zdefiniujemy



advenica

Innowacyjne metody separacji sieci

- Data Filter
  - Zasada działania polega na złożeniu całości informacji w urządzeniu, porównaniu jej ze zdefiniowanym wzorcem i w przypadku zgodności wysłanie informacji dalej.

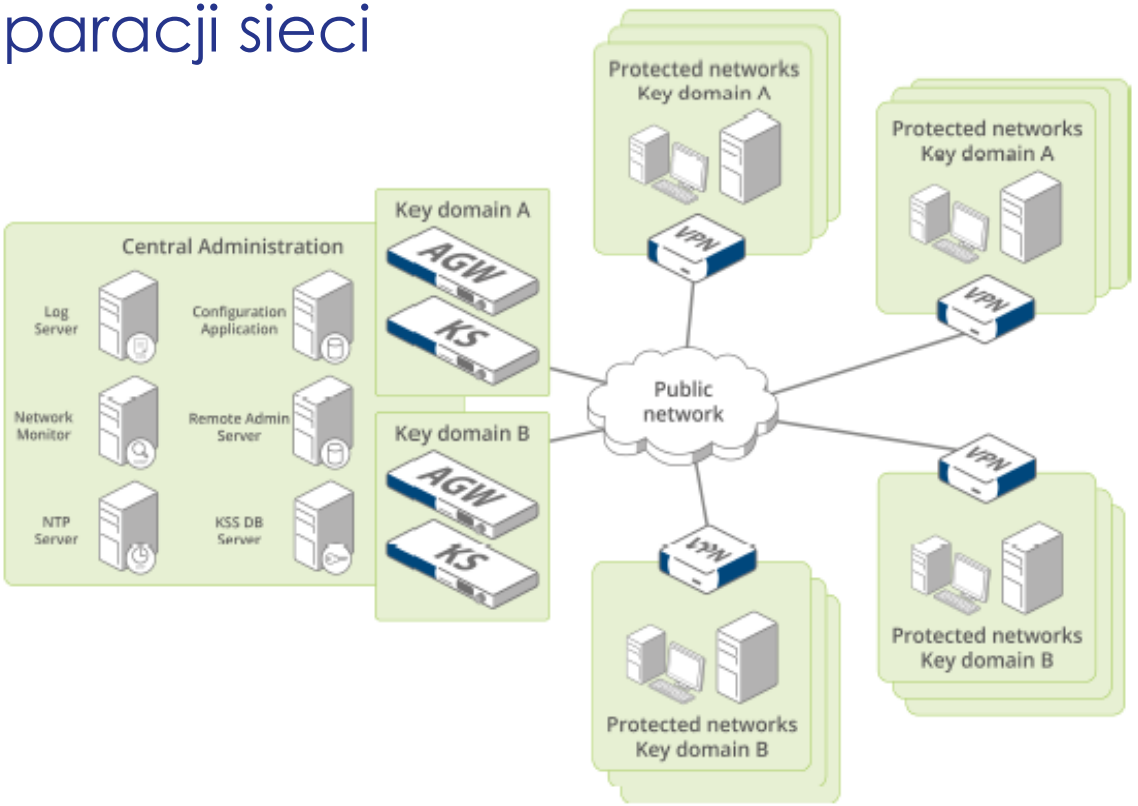


  - Przykład dla wiadomości e-mail. Podobna zasada ma zastosowanie dla wszystkich protokołów o znanym (ustandaryzowanym formacie)

advenica

Innowacyjne metody separacji sieci

- VPN Securi Connect



Podstawowe zalety:

- Dynamiczna wymiana kluczy między urządzeniami – nawet co kilka minut.
- Dzielenie transmisji na losowe długości pakietów.
- Zarządzanie odseparowane od przesyłanych danych
- Wersje 19” oraz portable

advenica

Innowacyjne metody zabezpieczenia

- Szyfratory 2 warstwy

Podsłuch za grosze

FCD 10B Cena około 200$

Podstawowe zalety

- Szyfrowanie w warstwie 2, transparentne dla wyższych warstw OSI
- Prędkości 1, 10, 100 GBit – dla najbardziej wydajnych zastosowań
- Opóźnienia transmisji poniżej 2µs
- Łatwa instalacja i konfiguracja urządzeń nie wymagająca zmiany adresacji sieci
- Szyfrowanie wyłącznie sprzętowe – wysoka wydajność i bezpieczeństwo

gemalto
security to be free

CN 9000 series

CN 6000 series

CN 8000 series

CN 4000 series

Specjaliści w separacji sieci

Blue energy sp. z o.o.
http://grupablue.pl
Audyty i konsulting bezpieczeństwa

Tel-Ster sp. z o.o.
http://www.tel-ster.pl
Pierwsze w Polsce rozwiązanie TelDiode gotowe do wdrożenia

Advenica AB
https://advenica.com/
Światowy lider w bezpieczeństwie i separacji sieci

Dziękuję za uwagę

Wiesław Kasprzak

Ekspert Blue Energy
wieslaw.kasprzak@grupablue.pl
kom. 601 809 918

Blue energy Sp. z o.o.
ul. Towarowa 35,
61-896 Poznań
tel. 61-643-51-98
fax. 61-859-59-01
NIP: 7781473428 KRS: 0000060682
www.grupablue.pl