VECTOR® SOLUTIONS | BE ABLE

We integrate Hybrid IT solutions. Together

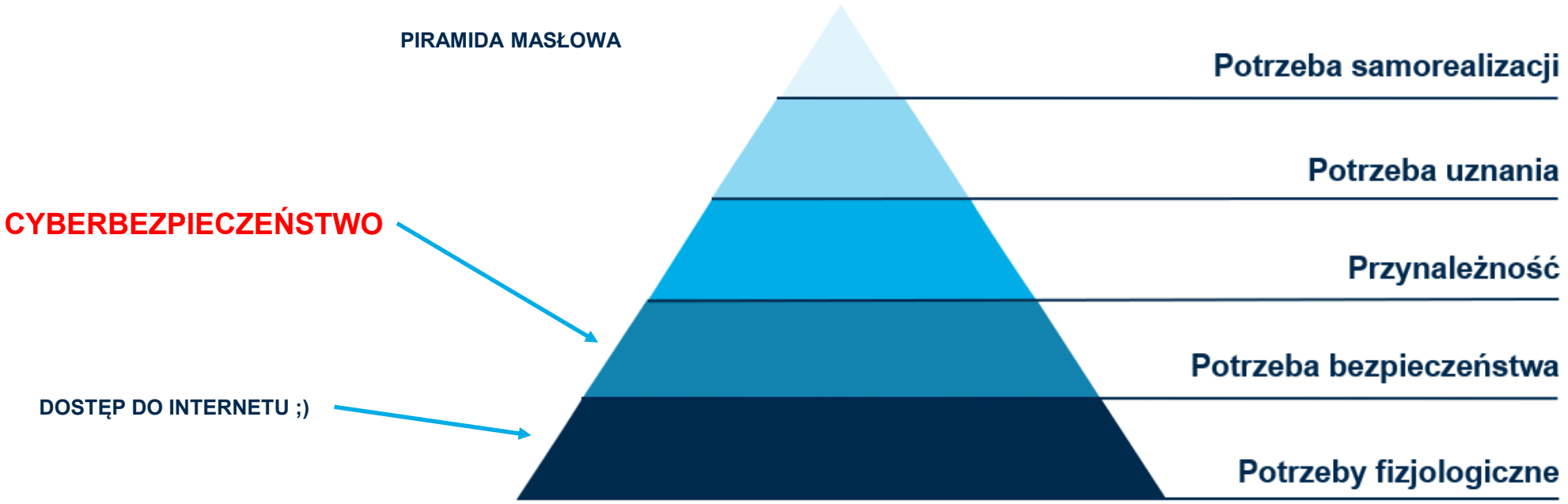
vectorsolutions.net

Jak zbudować strategię Cyberbezpieczeństwa w obliczu NIS2 ?

MACIEJ CICHY
Solutions Management Director
Hybrid IT

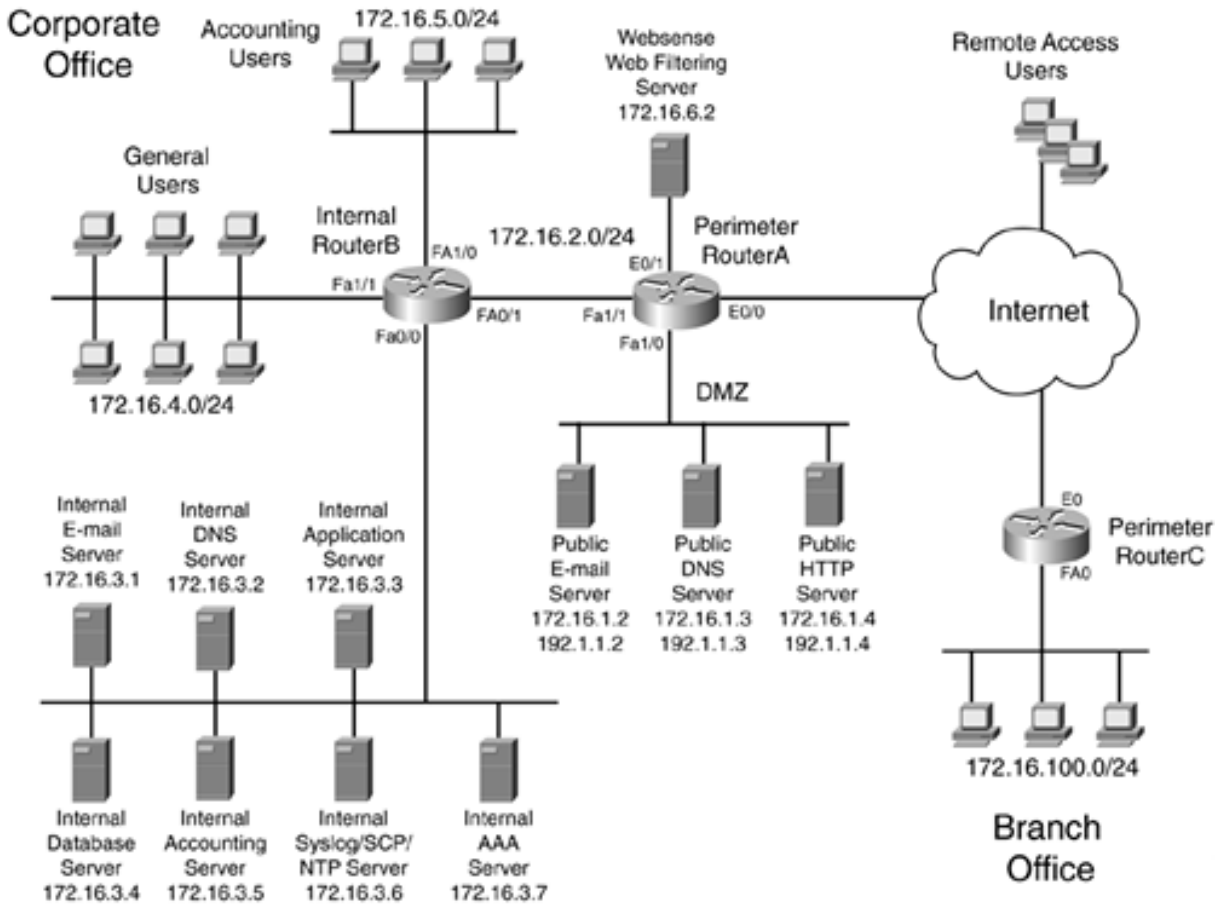
BEZPIECZEŃSTWO

To stan dający poczucie pewności i gwarancję jego zachowania oraz szansę na doskonalenie. Bezpieczeństwo to jedna z podstawowych potrzeb.

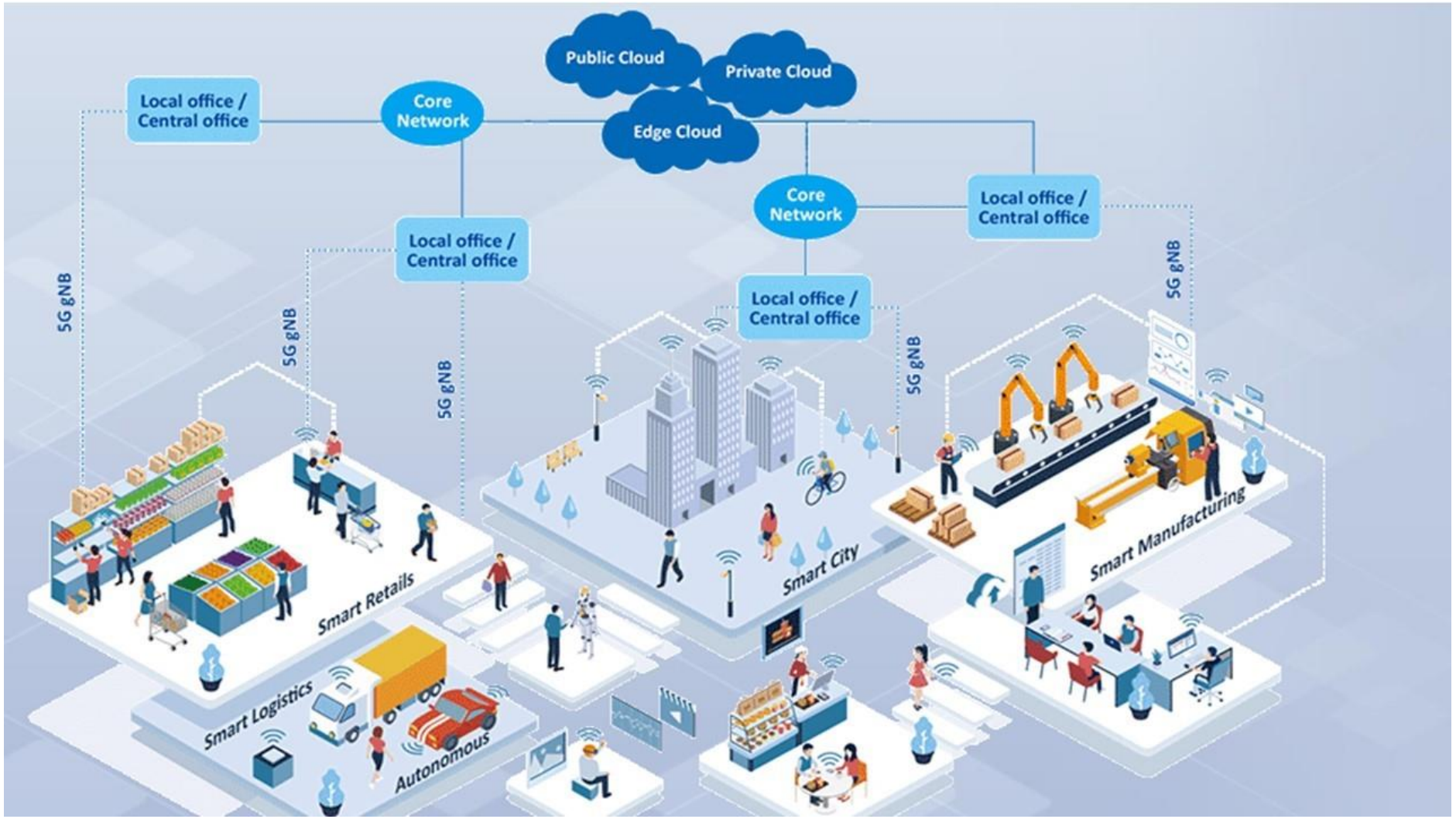


WALKA DOBRA ZE ZŁEM

OGÓLNA ARCHITEKTURA IT DO 2015 ROKU



WSPÓŁCZESNA ARCHITEKTURA IT



NAJCZĘŚCIEJ WYSTĘPUJĄCE INCYDENTY

Ransomware

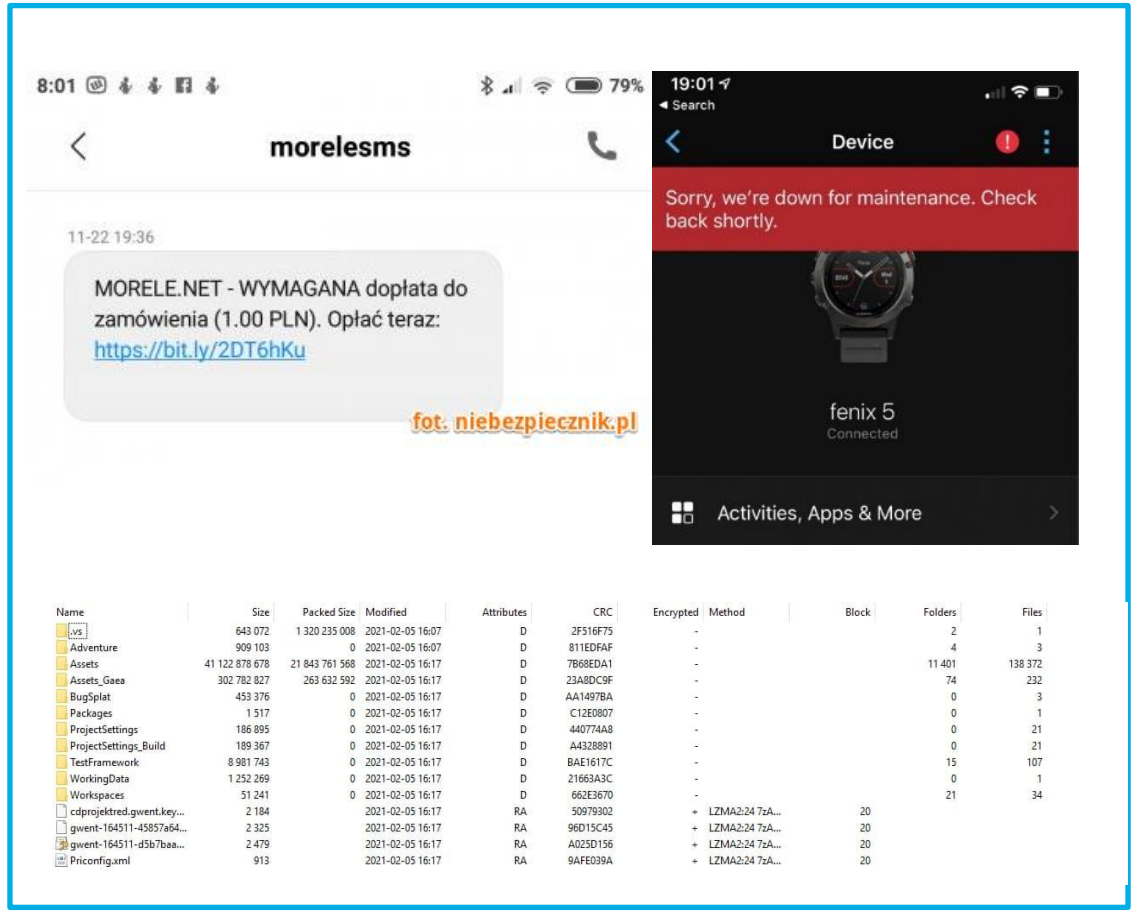
- Centrum Zdrowia Matki Polki
- Garmin - WastedLocker, okup $10M
- Media Markt i Saturn – Hive

Kradzież danych osobowych

- Morele.net - UODO nałożyło 3M PLN
- e-TOLL (Imię i nazwisko, e-mail, tel, PESEL, NIP)

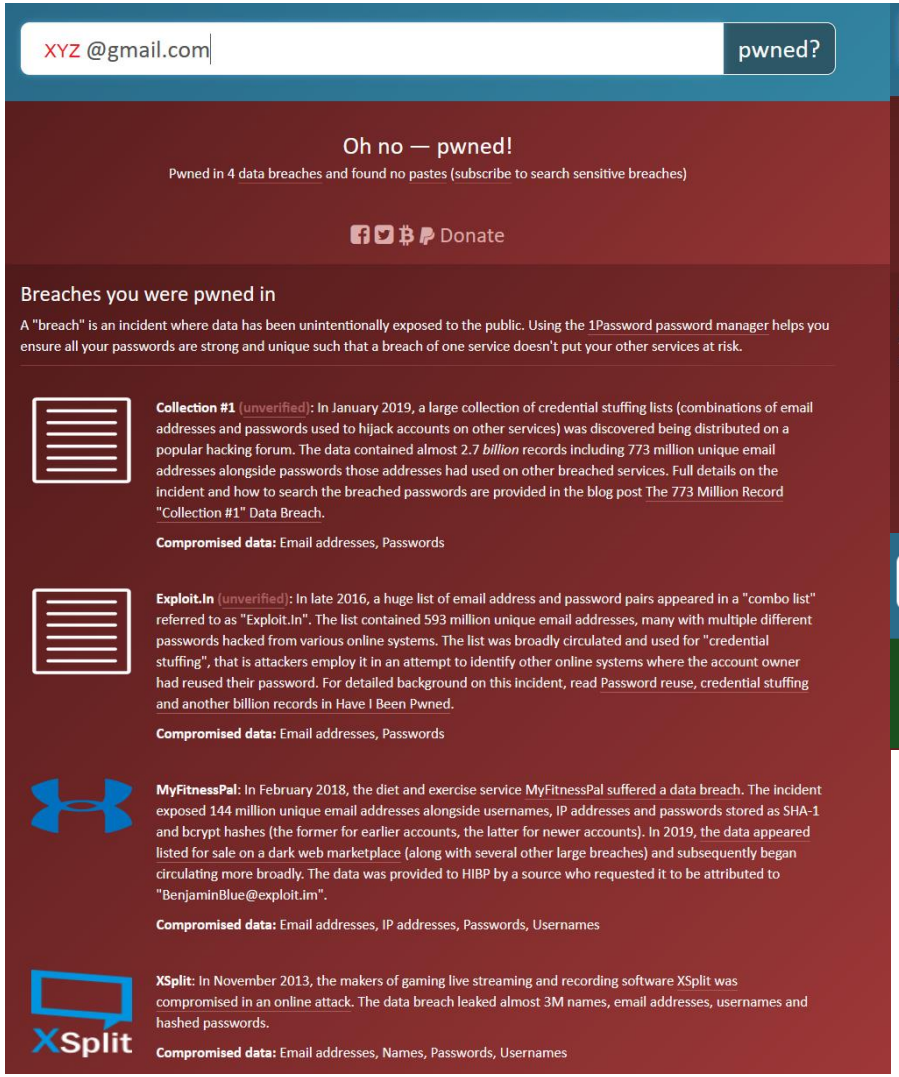
Kradzież własności intelektualnej

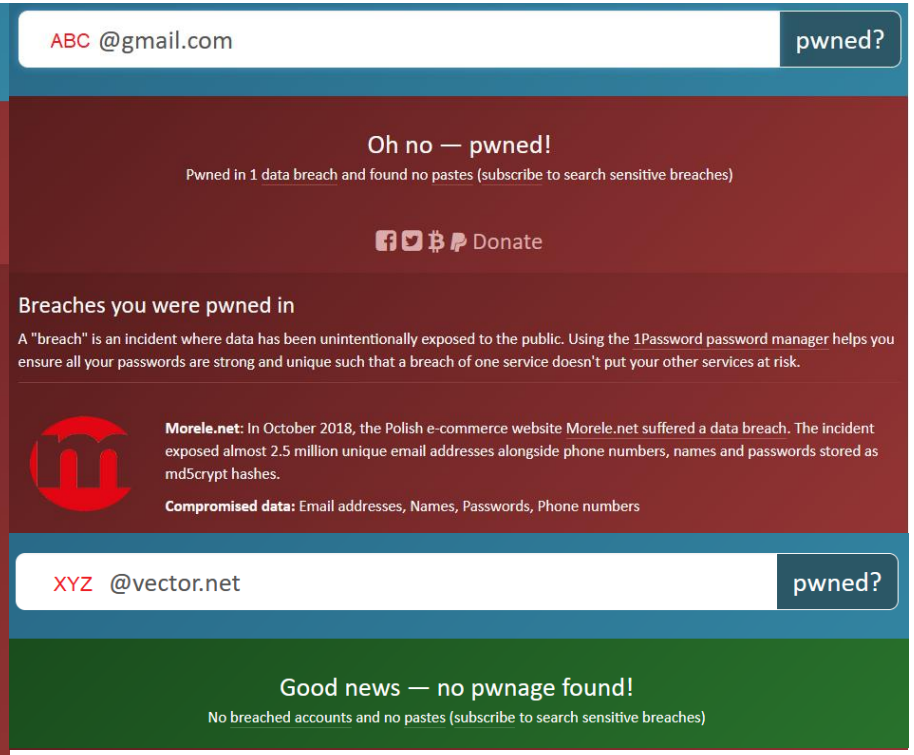
- CD Projekt – wyciekły kody źródłowe

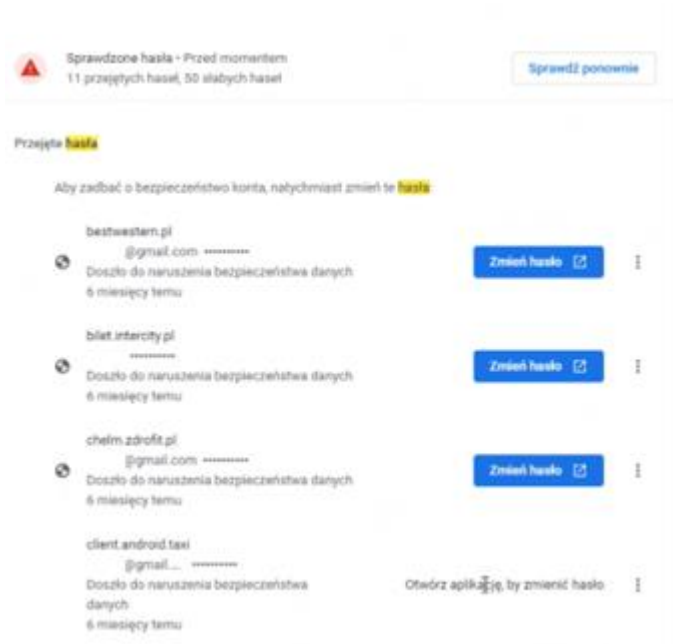


Name	Size	Packed Size	Modified	Attributes	CRC	Encrypted	Method	Block	Folders	Files
.vs	643 072	1 320 235 008	2021-02-05 16:07	D	2F516F75	-			2	1
Adventure	909 103	0	2021-02-05 16:07	D	811EDFAF	-			4	3
Assets	41 122 878 678	21 843 761 568	2021-02-05 16:17	D	7B68EDA1	-			11 401	138 372
Assets_Gaea	302 782 827	263 632 592	2021-02-05 16:17	D	23A8DC9F	-			74	232
BugSplat	453 376	0	2021-02-05 16:17	D	AA1497BA	-			0	3
Packages	1 517	0	2021-02-05 16:17	D	C12E0807	-			0	1
ProjectSettings	186 895	0	2021-02-05 16:17	D	440774A8	-			0	21
ProjectSettings_Build	189 367	0	2021-02-05 16:17	D	A4328891	-			0	21
TestFramework	8 981 743	0	2021-02-05 16:17	D	BAE1617C	-			15	107
WorkingData	1 252 269	0	2021-02-05 16:17	D	21663A3C	-			0	1
Workspaces	51 241	0	2021-02-05 16:17	D	662E3670	-			21	34
cdprojektred.gwent.key...	2 184		2021-02-05 16:17	RA	50979302	+	LZMA2:24 7zA...	20		
gwent-164511-45857a64...	2 325		2021-02-05 16:17	RA	96D15C45	+	LZMA2:24 7zA...	20		
gwent-164511-d5b7baa...	2 479		2021-02-05 16:17	RA	A025D156	+	LZMA2:24 7zA...	20		
Priconfig.xml	913		2021-02-05 16:17	RA	9AFE039A	+	LZMA2:24 7zA...	20		

A CZY TWOJE DANE JUŻ WYCIEKŁY?







Serwis PWND

Menadżer haseł Google Chrome

Czy użytkownik o tym wie?

KARY UODO

Uniwersyteckie Centrum Kliniczne Warszawskiego Uniwersytetu Medycznego	**10 tys. PLN**	Art. 34 RODO	06.07.2022	https://www.uodo.gov.pl/decyzje/DKN.5131.34.2021
Główny Geodeta Kraju	**100 tys. PLN**	Art. 31 RODO Art. 58 RODO	15.07.2020	https://uodo.gov.pl/decyzje/DKE.561.3.2020
Fortum Marketing and Sales Polska S.A	**4,9 mln PLN**	Art. […] RODO	19.01.2022	https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020
Bank Millennium	**363 tys. PLN**	Art. 33 RODO	14.10.2021	https://uodo.gov.pl/pl/138/2211 https://uodo.gov.pl/decyzje/DKN.5131.16.2021 https://uodo.gov.pl/pl/138/2420
Szkoła w Gdańsku	**0 PLN**	Art. 5 RODO Art. 9 RODO	04.03.2020	https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018 http://orzeczenia.nsa.gov.pl/doc/2A2CFDE9D2
Krajowa Szkoła Sądownictwa i Prokuratury	**100 tys. PLN**	Art. 28 RODO Art. 32 RODO	11.02.2021	https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020 https://uodo.gov.pl/pl/138/1909
Główny Geodeta Kraju	**60 tys. PLN**	Art. 4 RODO	06.07.2022	https://uodo.gov.pl/pl/138/2411 https://www.uodo.gov.pl/decyzje/DKN.5131.27.2022

RANSOMWARE W POLSCE

Komenda Wojewódzkiej
Państwowej Straży Pożarnej w Łodzi

**Atak na serwer WWW,
zaszyfrowane dane z żądaniem okupu**

Urząd Gminy
w Lututowie

**Atak na infrastrukturę,
zaszyfrowane dane z żądaniem okupu**

Urząd Gminy
Kościerzyna

Cyberprzestępcy dostali się do sieci, z której korzystają wszystkie jednostki organizacyjne podlegające do Urzędu Gminy Kościerzyna, zaszyfrowali wszystkie dane, Hakerzy żądają okupu w kryptowalucie

Urząd Marszałkowski
Województwa Małopolskiego

**Atakujący zażądał zapłaty okupu,
utracone dane**

Instytut Centrum Zdrowia
Matki Polki

Szczególnie bolesny atak dla możliwości operacyjnych jednego z najważniejszych szpitali w Polsce

**Koszt ataku dla polskich firm
to średnio 1,49 mln zł – ustalił Sophos**

DYREKTYWA NIS 2

2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy:

a) politykę analizy ryzyka i bezpieczeństwa systemów informatycznych;

b) obsługę incydentu;

c) ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzanie kryzysowe;

d) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;

e) bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie;

f) polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;

g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa;

h) polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania;

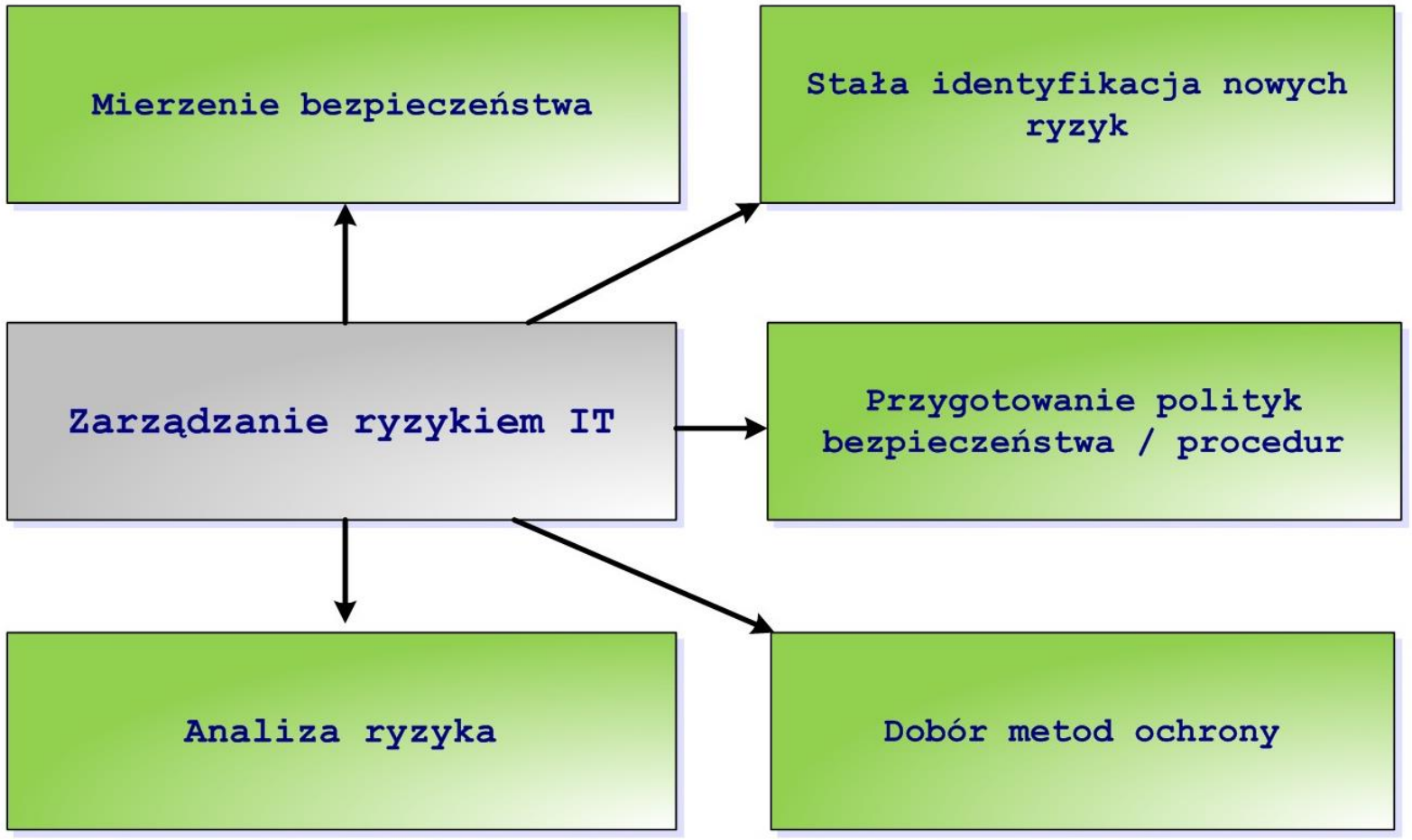
i) bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami;

j) w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

- Zbiór rekomendacji dla przedsiębiorstw
- Właściwie każda organizacja publiczna na liście
- Po lewej obowiązki
- Poza tym główny obowiązek, to raportowanie incydentów do CSIRT, którego jeszcze nie ma i nie posiadamy regulaminów, jak to robić

NIS2 2.A, 2.F

ANALIZA RYZYKA

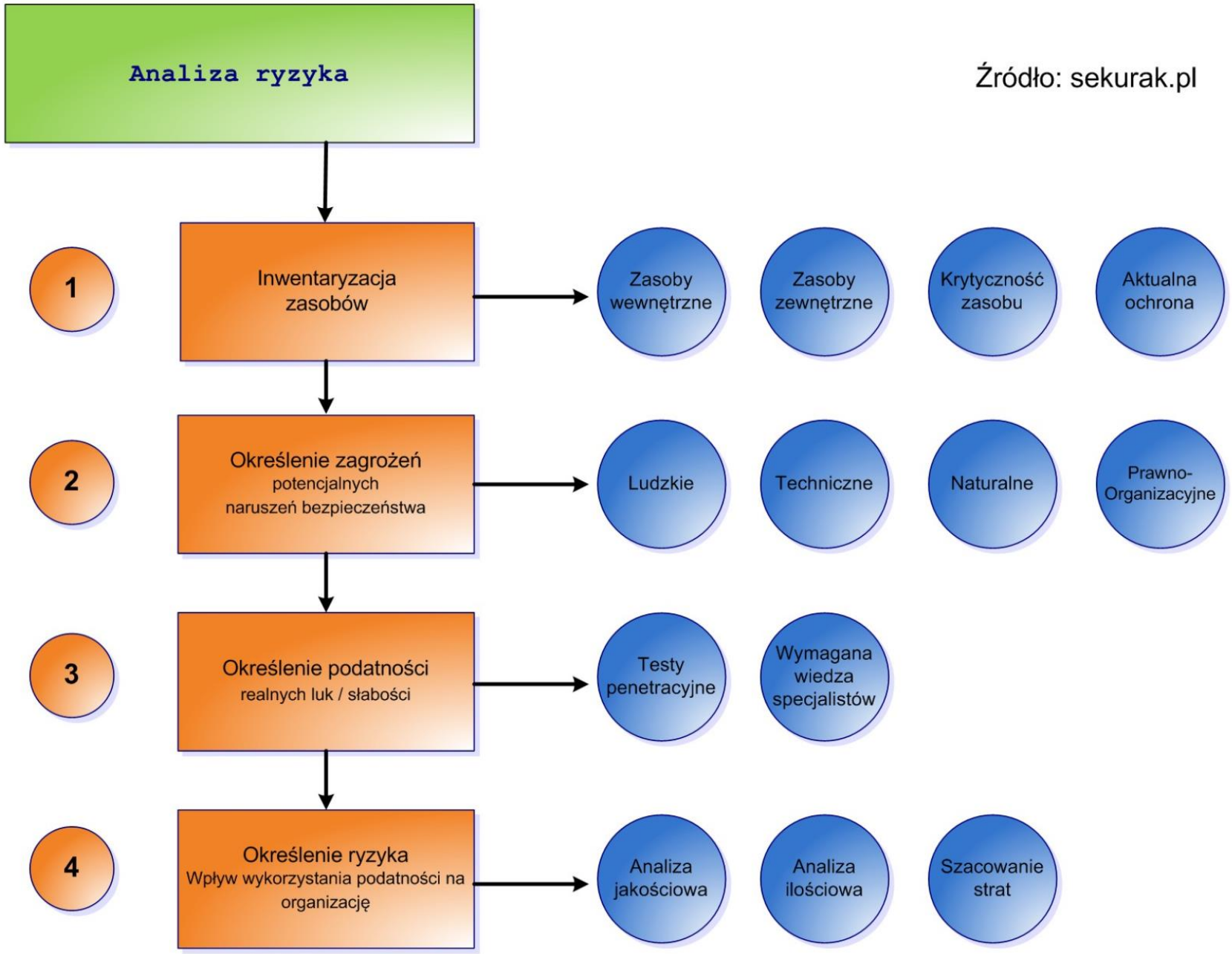


NIS2 2.A, 2.F

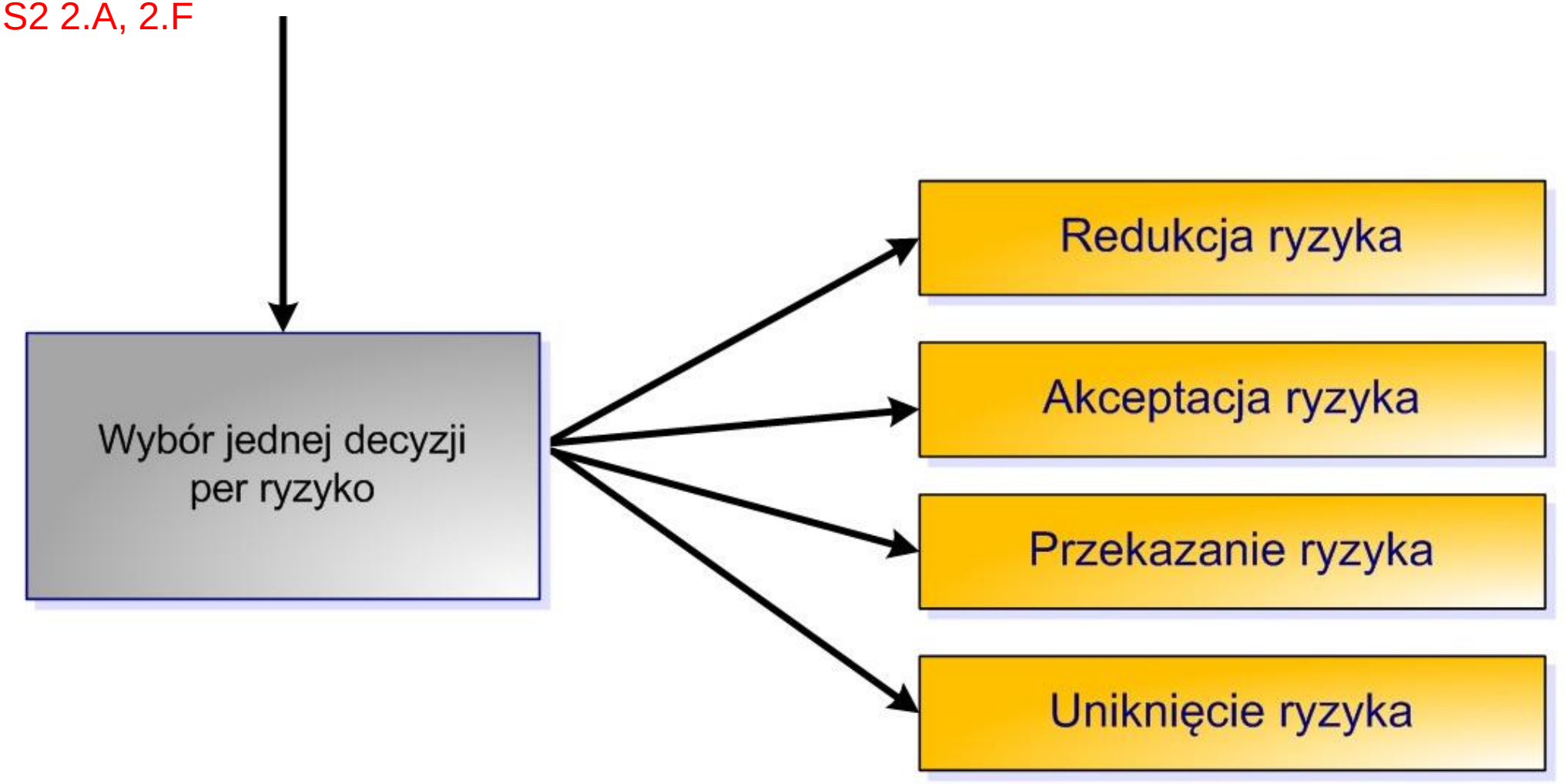
RYZYKA PRZYKŁADY

- zalanie, pożar, kataklizm,
- wyciek/ujawnienie danych,
- DDoS,
- fizyczna awaria nośników danych,
- awaria okablowania,
- awaria zasilania,
- nieautoryzowane fizyczne uzyskanie dostępu do istotnego pomieszczenia z przetwarzanymi danymi,
- zagubienie / kradzież sprzętu zawierającego istotne dane,
- malware,
- użycie pirackiego oprogramowania,
- brak odpowiednich zapisów umownych gwarantujących bezpieczeństwo,
- zagrożenia płynące z innych systemów, na których nasz zasób bazuje

NIS2 2.A, 2.F


Analiza ryzyka
Źródło: sekurak.pl
1
Inwentaryzacja zasobów
Zasoby wewnętrzne
Zasoby zewnętrzne
Krytyczność zasobu
Aktualna ochrona
2
Określenie zagrożeń potencjalnych naruszeń bezpieczeństwa
Ludzkie
Techniczne
Naturalne
Prawno-Organizacyjne
3
Określenie podatności realnych luk / słabości
Testy penetracyjne
Wymagana wiedza specjalistów
4
Określenie ryzyka Wpływ wykorzystania podatności na organizację
Analiza jakościowa
Analiza ilościowa
Szacowanie strat

NIS2 2.A, 2.F

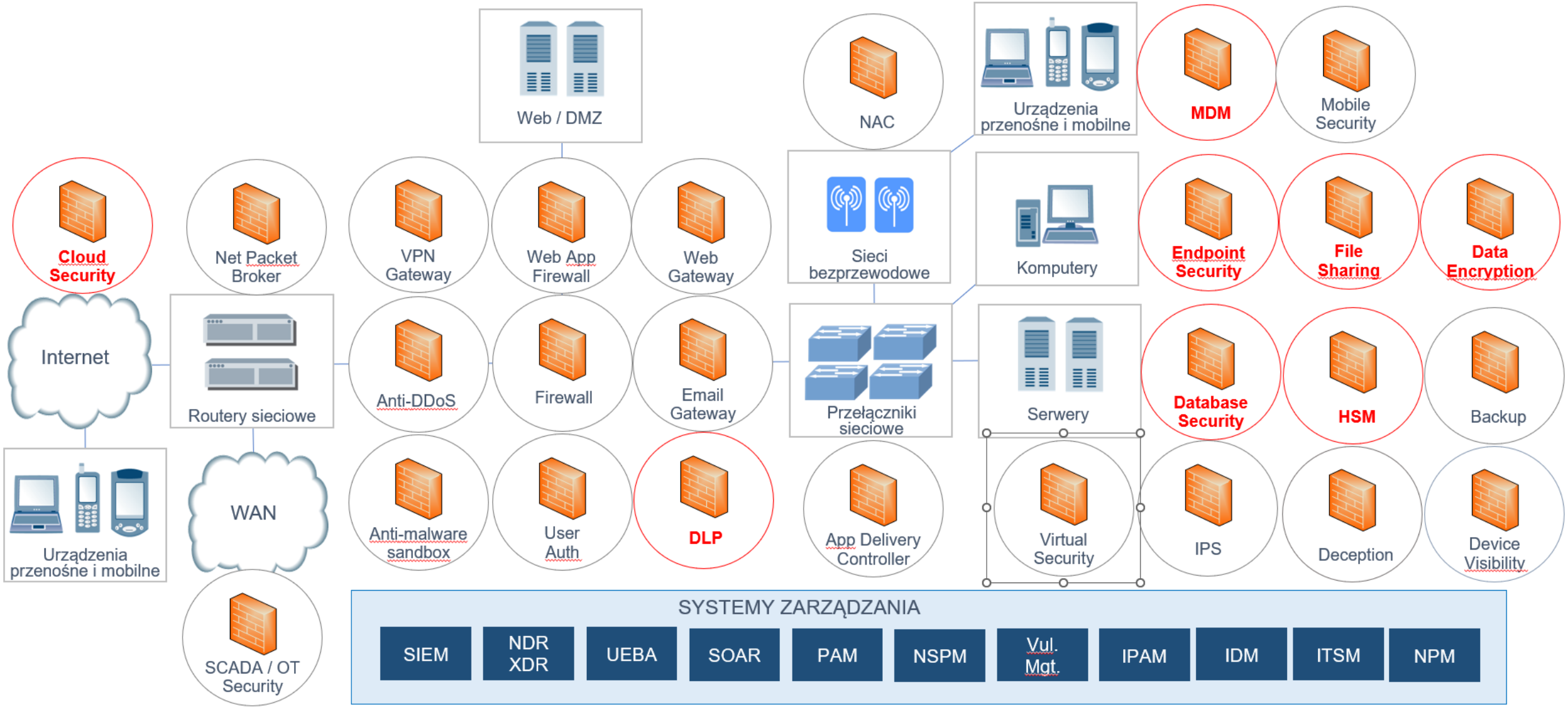

Wybór jednej decyzji per ryzyko
Redukcja ryzyka
Akceptacja ryzyka
Przekazanie ryzyka
Uniknięcie ryzyka

NIS2 2.A, 2.F

DLACZEGO POTRZEBNA JEST ANALIZA?

Ocena skutków jest formalną, określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie, której odpowiada administrator danych, przed przetwarzaniem.

Wyniki analizy ryzyka stanowią podstawę zaprojektowania odpowiednich mechanizmów kontroli dla systemów informatycznych eksploatowanych w organizacji.



Źródło: Clico

CIS CONTROLS v8

- Critical Security Controls
- Priorytetyzacja zagrożeń
- Grupy IG

CIS Center for Internet Security®
Creating Confidence in the Connected World.

CIS CRITICAL SECURITY CONTROLS IMPLEMENTATION GROUPS

IG1

- Niezbędne podstawy bezpieczeństwa
- Każdy podmiot powinien zastosować
- Niski koszt i niski próg wejścia

IG2

- Zespoły utrzymujące IT wymagane
- Zbiory danych / złożoność operacyjna jednostki

IG3

- Eksperci cyberbezpieczeństwa wymagani
- Ograniczenia wpływ wyrafinowanych ataków

CIS Control 1: Inwentaryzacja i kontrola zasobów firmowych (sprzętowych)

NIS2 2.E

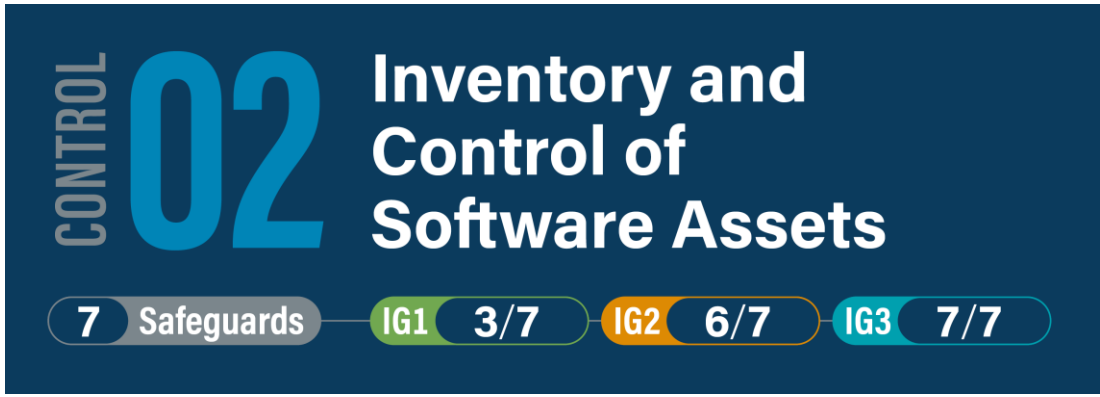
- Trzeba wiedzieć
  - Co się ma
  - Kto ma prawo używać i na jakich zasadach

- IG1:
  - Establish and maintain a comprehensive enterprise asset inventory
  - Address unauthorized assets

CIS Control 2: Inwentaryzacja i kontrola zasobów oprogramowania

NIS2 2.E

- Inwentarz oprogramowania
  - Wersja
  - Licencja
  - Gdzie zainstalowane



- IG1:
  - Establish and maintain an up-to-date software inventory.
  - Ensure authorized software is currently supported
  - Address unauthorized software

CIS Control 3: Zabezpieczenie danych

NIS2 2.C

- Identyfikujemy
- Klasyfikujemy
- Zabezpieczamy
- Utrzymujemy
- *Niszczymy (§Brakowanie danych§)

- IG1:
  - Establish and maintain a data management process
  - Establish and maintain a data inventory
  - Configure data access control lists
  - Enforce data retention according to your data management process
  - Securely dispose of data and ensure the disposal methods and processes match data sensitivity
  - Encrypt data on end-user devices like laptops and phones

CIS Control 4: Bezpieczna konfiguracja sprzętu i oprogramowania

NIS2 2.I

- Dobre praktyki
  - Podczas wytwarzania
  - Podczas utrzymywania
- Bezpieczeństwa sprzętu i oprogramowania

- IG1:
  - Establish and maintain a secure configuration process
  - Establish and maintain a secure configuration process for network infrastructure
  - Configure automatic session locking on enterprise assets after defined periods of inactivity
  - Implement and manage firewalls on servers
  - Implement and manage firewalls on end-user devices
  - Securely manage enterprise software and assets
  - Manage default accounts on enterprise software and assets

CIS Control 5: Zarządzanie kont użytkowników

NIS2 2.I

- Zarządzanie kontami użytkowników
  - Ograniczanie uprawnień!
  - Centralizacja!

- IG1:
  - Establish and maintain a list of accounts
  - Use unique passwords
  - Disable dormant accounts (accounts that haven't been used for at least 45 days)
  - Restrict admin privileges to dedicated admin accounts

CIS Control 6: Zarządzanie kontroli dostępu

NIS2 2.I, 2.J

- Uprawienia użytkowników
  - Procesy i dobre praktyki

- IG1:
  - Establish an access-granting proces
  - Establish an access-revoking proces
  - Require multi-factor authentication (MFA) for externally-exposed accounts
  - Require MFA for remote network access
  - Require MFA for administrative access

MFA WYMAGANE W REKOMENDACJI NIS2 !!

CIS Control 7: Ciągłe zarządzanie podatnościami

NIS2 2.A, 2.E

- Łatamy dziury
- Śledzimy listę podatności

- IG1:
  - Establish and maintain a vulnerability management process
  - Establish and maintain a remediation process
  - Perform automated operating system patch management
  - Perform automated application patch management

CIS Control 8: Zarządzanie logów audytowych

NIS2 2.B

- Co robić z logami?
- 5W 1H co, kto, kiedy, gdzie, dlaczego i jak

- IG1:
  - Establish and maintain an audit log management process
  - Collect audit logs
  - Ensure adequate audit log storage

CIS Control 9: Zabezpieczenie poczty elektronicznej i przeglądarek Web

NIS2 2.G, 2.I

- Email i WWW
  - Popularny wektor ataku
  - Człowiek najsłabsze ogniowo
  - Filtracja

- IG1:
  - Ensure only fully supported email clients and browsers are used
  - Use Domain Name System (DNS) filtering services

Bardzo mało firm filtruje DNS !!

CIS Control 10: Ochrona przed złośliwym oprogramowaniem

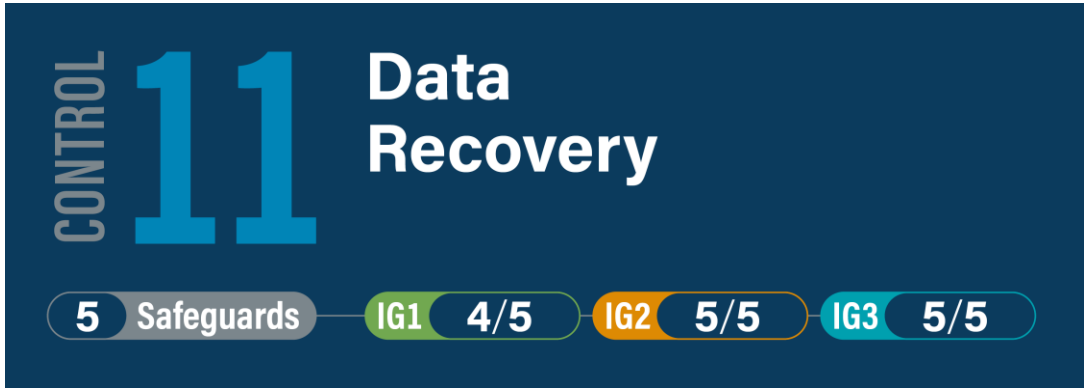
- Czy każdy ma AV?
- Ransomware
- APT

- IG1:
  - Deploy and maintain anti-malware software
  - Configure automatic anti-malware signature updates
  - Disable autorun and auto-play for removable media

CIS Control 11: Zapewnianie zdolności odzyskiwania danych

NIS2 2.C

- Backupy



- IG1:
  - Implement an automated backup process
  - Protect recovery data
  - Establish and maintain isolated copies of backup data

CIS Control 12: Zarządzanie infrastrukturą sieci

NIS2 2.E, 2.I

- Bez sieci nie ma ataków!
- Bez sieci nie ma firmy!

- IG1:
  - Establishes guidelines for managing network devices

CIS Control 13: Monitorowanie sieci i zabezpieczeń

NIS2 2.A, 2.B

- Sieć trzeba:
  - Monitorować
  - Chronić
  - Analizować
  - Zarządzać dostępem
  - Logować
- IG1
  - Brak

CIS Control 14: Wdrożenie programu szkoleń i budowania kultury bezpieczeństwa

NIS2 2.G

- Człowiek to najsłabsze ogniwo
- Szkolenia
- Socjotechniki
- Good practices
- Skutki nieumyślnej ekspozycji danych
- Rozpoznawanie incydentów
- Dostrzeganie luk bezpieczeństwa
- User Awerness dostosowane do roli
- IG1:

— **DUŻO**

Budowa kultury organizacji:
Użytkownik powinien być nagrodzony za zgłoszenie incydentu bezpieczeństwa ! Jak już się stało trzeba działać. Nie wiemy = nie działamy.

CIS Control 15: Zarządzanie dostawcami usług

NIS2 2.D

- Inwentaryzacja z uwzględnieniem:
  - Wymogów bezpieczeństwa
  - Monitorowania

- IG1:
  - Establish and maintain a list of service providers

CIS Control 16: Zapewnianie bezpieczeństwa aplikacji

NIS2 2.C, 2.H

- Jeśli wystawiamy:
  - WAF
  - A05:2021 – Security Misconfiguration
  - A02:2021 – Cryptographic Failures
- Jeśli tworzymy:
  - A04:2021 – Insecure Design
  - A08:2021 – Software and Data Integrity Failures
  - A06:2021 – Vulnerable and Outdated Components

- IG1:
  - Brak

CIS Control 17: Reagowanie i zarządzanie incydentami

NIS2 2.B

- Obsługiwanie incydentów jest kluczowe
- RODO, NIS2 i inne literki!!!
- Obowiązek raportowania incydentów!!
- Down time – można zredukować

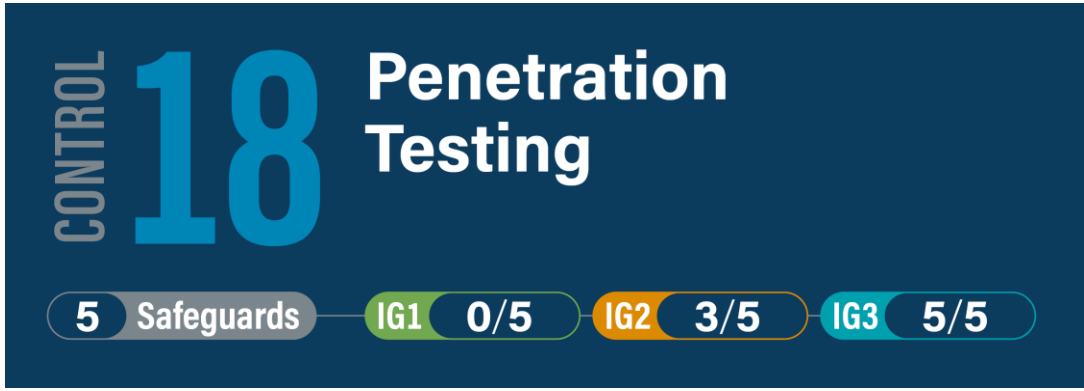
- IG1:
  - Designate personnel to manage incident handling
  - Establish and maintain contact information for reporting security incidents
  - Establish and maintain an enterprise process for reporting incidents

CIS Control 18: Testy penetracyjne

NIS2 2.F

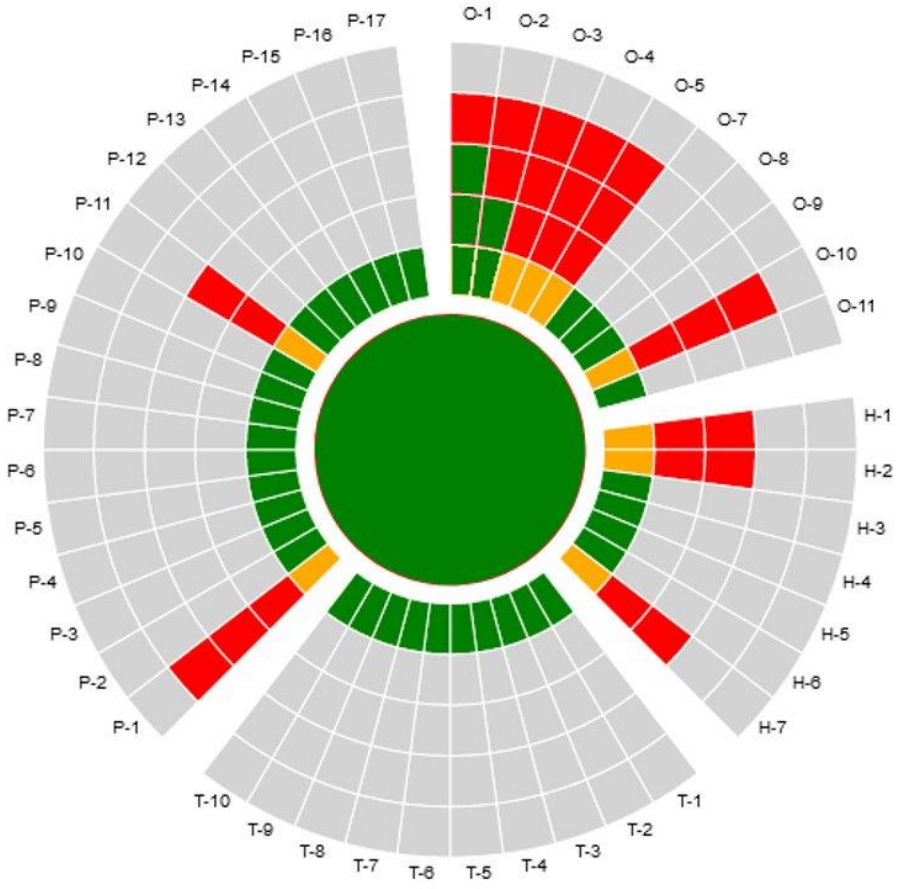
- Czy jesteśmy bezpieczni?
- Nie czekamy na złośliwe testy/ataki
  - Samokontrola!

- IG1:
  - Brak



JAK TO ZEBRAĆ W CAŁOŚĆ?

- Strategia = zebranie wszystkich powyższych
- Weryfikujemy kontrolki, określamy najsłabsze strony, zarządzamy ryzykiem
- Inwestujemy, wdrażamy rozwiązania
- Następnie wracamy do wykresu, audytujemy bezpieczeństwo
- I tak dalej, i tak dalej
- Cyberbezpieczeństwo = proces ciągły



CO JEŚLI NIE SPEŁNIAMY?!

- Bycie bezpieczną organizacją nie musi oznaczać, że wszystkie reguły CIS muszą być przestrzegane
- Zaimplementowanie wszystkich kontrolek CIS nie musi oznaczać ze jesteśmy bezpieczni!
- Zapewnianie bezpieczeństwa ma charakter iteracyjny
- Bezpieczeństwo to proces
- Bycie bezpiecznym w 2022 nie oznacza ze jest się bezpiecznym w 2023

ŚWIADOMOŚĆ PRACOWNIKA

Człowiek to często najsłabszy element łańcucha bezpieczeństwa

Proste pytania:

- Czy stosujemy inne hasła w różnych serwisach?
- Czy blokujemy komputer?
- Czy otwieramy każdy plik z poczty?
- Jakie hasła używamy?
- Czy nasz tel. jest bezpieczny?
- Kiedy odbyłem ostatnie szkolenie o tematyce bezpieczeństwa?

Najpopularniejsze hasła na świecie:

- 123456,
- 123456789,
- Qwerty,
- password,
- 111111.

VECTOR SOLUTIONS

OSTATNIE PROJEKTY:

Dostawa i uruchomienie klastra Firewalli NGFW Checkpoint Maestro, wraz z ochroną urządzeń końcowych Harmony Endpoint i usługami SASE Harmony Connect

DLA: Dużego operatora telkomunikacyjnego

Dostawa i wdrożenie sieci automatycznej opartej na rozwiązaniu Cisco SDA wraz z wdrożeniem polityki bezpieczeństwa sieci ZTNA i kontrolą dostępu do sieci NAC

DLA: Jednostki publicznej szczebla wojewódzkiego

Dostarczenie klastra macierzy dyskowych IBM FlashSystem 7300 replikujących się między dwoma centrami danych o pojemności skutecznej 500TB dla współdzielonych usług IT

DLA: Warszawskiego operatora usług Data Center

Projekt, dostawa i konfiguracja trzypoziomowej fabryki przełączającej wykorzystującej standard BGP EVPN dla Data Center na bazie przełączników i routerów Huawei

DLA: Ogólnopolskiego operatora usług Data Center

Dostawa i konfiguracja firewalli Palo Alto wraz z oprogramowaniem Panorama, wdrożenie polityki bezpieczeństwa sieciowego wsparcie serwisowe

DLA: Publicznej jednostki ratownictwa medycznego

OPINIE KLIENTÓW:

„W przypadku usług IT niezbędni są zarówno dostawcy, jak i sprawdzony partner biznesowy, który przeprowadza wdrożenie, trasfer wiedzy oraz wspomaga instytucje w zarządzaniu oprogramowanie. Współpracujemy z VECOTR SOLUTIONS i jest to bardzo dobry partner, certyfikowany w zakresie rozwiązań, których używamy.”

Robert Targos

Zastępca Dyrektora, LCIT

„Jesteśmy zadowoleni z przebiegu współpracy. Zamówienie zostało zrealizowane w ustalonym terminie, a dostarczony sprzęt spełnia wymagania jakościowe. Inżynierowie VECTOR SOLUTIONS wykazali się profesjonalizmem i zorientowaniem na potrzeby Klienta, a także służą pomocą i wiedzą w zakresie dostarczonych rozwiązań.”

Paweł Sokołowski

Dyrektor Pionu urządzeń konsumenckich, Cyfrowy Polsat

„Zdecydowaliśmy się na współpracę z VECTOR SOLUTIONS ze względu na dobre doświadczenia związane z tym integratorem. Gwarantuje on rzetelne i profesjonalne podejście, a także zastosowanie urządzeń, które rzeczywiście będą wspierać nasz biznes”

Radosław Potera

CTO, Atman

REFERENCJE:

UNIWERSYTET MEDYCZNY W ŁODZI

NETIA

CANAL+

atman

NASK

CYFROWY POLSAT

LUBELSKIE CENTRUM INNOWACJI I TECHNOLOGII

VECTOR SOLUTIONS

Łódzki Urząd Wojewódzki w Łodzi

inea

CISCO Partner Premier Integrator

HUAWEI Enterprise Partner VAP

veeAM PROPARTNER Gold Reseller

DELL

rubrik

CHECK POINT

f5

Hewlett Packard Enterprise

IBM

paloalto NETWORKS

vectorsolutions.net

Kontakt

MACIEJ CICHY
SOLUTIONS MANAGEMENT
DIRECTOR
HYBRID IT

M +48 693 668 456

T +48 58 77 17 419

E m.cichy@vector.net

We integrate Hybrid IT solutions. Together

Poznaj szczegóły

vectorsolutions.net

vectorsolutions.net