WZROST POZIOMU BEZPIECZEŃSTWA SEKTORA OCHRONY ZDROWIA

WNIOSKI Z WDRAŻANIA PROJEKTU CYBERSZPITALI,

DOŚWIADCZENIA Z WALKI W CYBERPRZESTRZENI

STRUKTURA PODMIOTÓW SEKTORA ZDROWIA

Podmioty sektora zdrowia

- **Podmioty lecznicze (26 tys.)**
  - 874 szpitale
  - 25 tys. ambulatoriów, w tym 8,7 tys. POZ
  - 40 podmiotów leczniczych utworzonych przez MSWiA
- **Indywidualne i grupowe praktyki zawodowe (193 tys.)**
- **Apteki (14 tys.), Hurtownie farmaceutyczne (424)**
- **Jednostki i organy podległe lub nadzorowane MZ (81)**
- **Operatorzy usług kluczowych w rozumieniu KSC (256)**

Tylko 1,2 tys. podmiotów działa w formie SPZOZ, pozostałe to działalności gospodarcze i spółki

Poza sektorem: 127 podmiotów leczniczych utworzonych przez MON

BADANIE ANKIETOWE

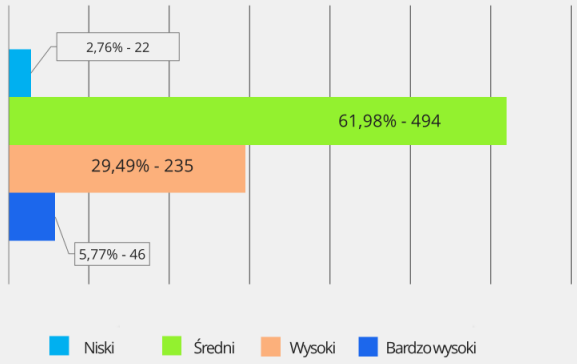
W jednostce jest dedykowana osoba odpowiedzialna za ochronę danych osobowych (ZA.1.1)	**OCH.4.1** - Kopie zapasowe informacji są sporządzane, utrzymywane i testowane.	Anomalie i zdarzenia (CM.1)	**CM.1.1** - Wykryte zdarzenia są analizowane aby zrozumieć cele i metody ataku.
W jednostce jest dedykowana osoba odpowiedzialna za bezpieczeństwo fizyczn (Za.1.2)			**CM.1.2** - Dane o zdarzeniach są pozyskiwane oraz ...u źródeł i czujników.
W jednostce jest dedykowana osoba odpowiedzialna za cyberbezpieczeństwo (ZA.1.3)			...monitorowana w celu wykrywania ...rzeń cyberbezpieczeństwa. (SIEM)
Osoby odpowiedzialne za cyberbezpieczeństwo, ochronę danych osobowych podlegają bezpośrednio pod kierownika jednostki (ZA.1.4)			...sko fizyczne jest monitorowane w celu ...alnych zdarzeń cyberbezpieczeństwa.
Dyrektor jednostki odbył szkolenie w zakr... cyberbezpieczeństwa w ciągu ostatniego (ZA.2.1) Podać datę szkolenia w dolnej cz...			...ść personelu jest monitorowana w celu ...alnych zdarzeń związanych z ...twem.
Dyrektor jednostki cyklicznie przegląda ra... oceny ryzyka w...			...kod jest wykrywany.
Dyrektor jednc... zintegrowanyn... bezpieczeństw...			...yzowany kod mobilny jest wykrywany (np. ...t).
Dyrektor jednc... bezpieczeństw... cyberbezpieczeń...			...ść zewnętrznego dostawcy usług jest ...alu wykrywania potencjalnych zdarzeń
			...kątem ...eń i
			...ości.

TAK
NIE
NIE WIEM

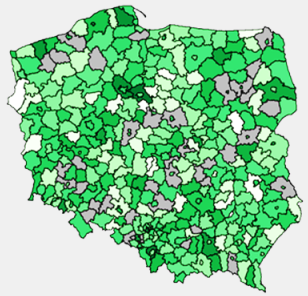
Plan poprawy cyberbezpieczeństwa sektora ochrony zdrowia

Stan cyberbezpieczeństwa w szpitalach (04.2022 r.)

Poziom dojrzałości systemu cyberbezpieczeństwa, n=797



Rozkład przestrzenny poziomu dojrzałości



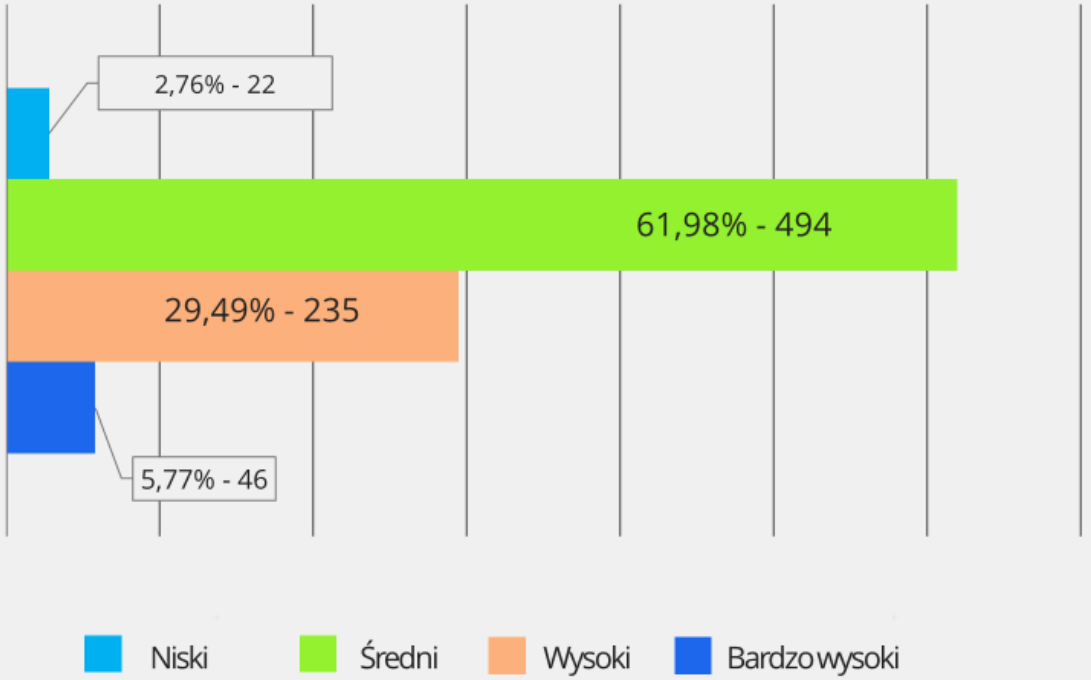
Mediana,
ciemny kolor – poziom wysoki,
jasny – niski poziom

7

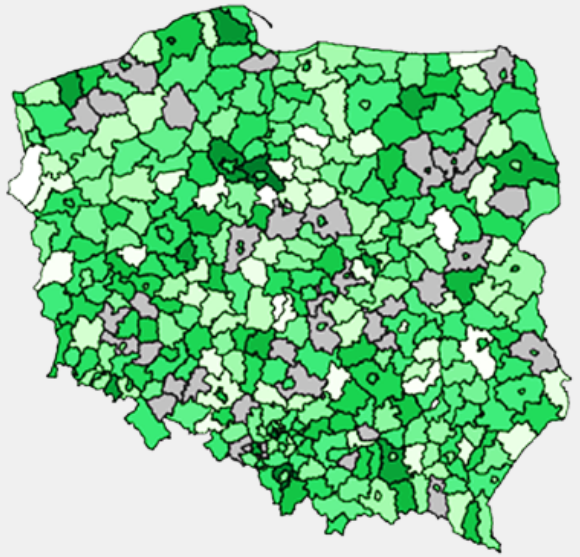
Ankieta: 127 pytań; 9 kategorii; 83% odpowiedzi

Stan cyberbezpieczeństwa w szpitalach (04.2022 r.)

Poziom dojrzałości systemu cyberbezpieczeństwa, n=797



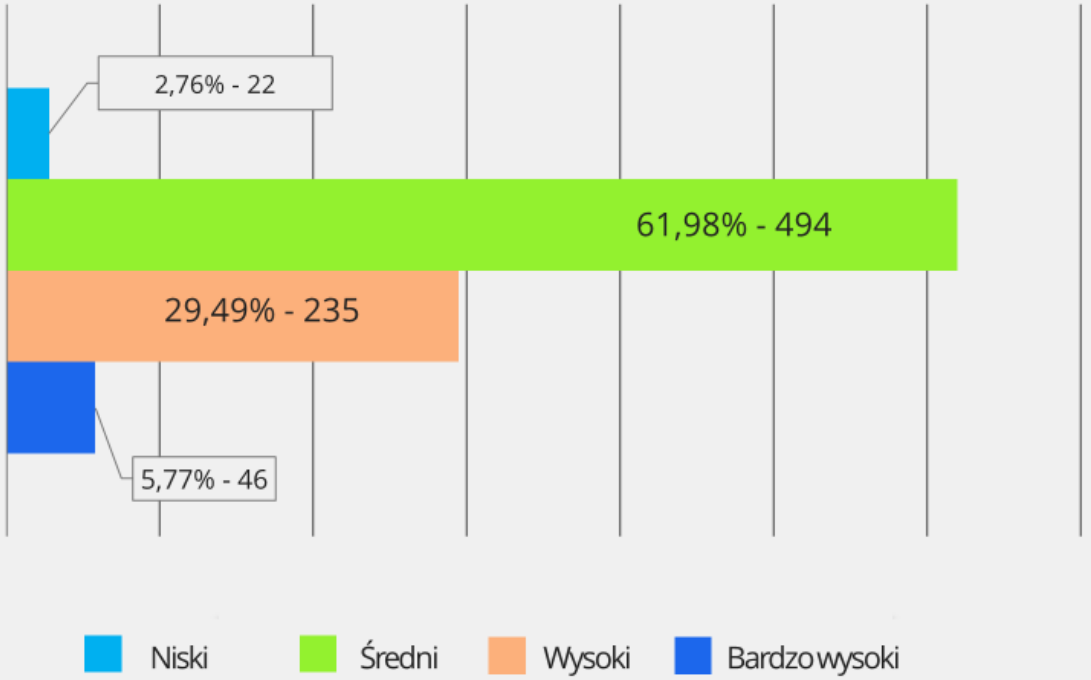
Rozkład przestrzenny poziomu dojrzałości



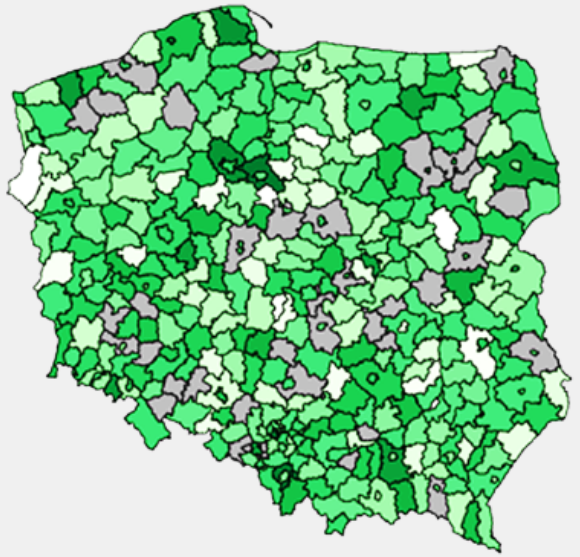
Mediana,
ciemny kolor – poziom wysoki,
jasny – niski poziom

Stan cyberbezpieczeństwa w szpitalach (04.2022 r.)

Poziom dojrzałości systemu cyberbezpieczeństwa, n=797



Rozkład przestrzenny poziomu dojrzałości



Mediana,
ciemny kolor – poziom wysoki,
jasny – niski poziom

STAN CYBERBEZPIECZEŃSTWA W SZPITALACH (04.2022 R.)

57% brak dokumentacji SZBI (zatem również procedur w zakresie kopii zapasowych)

81% nie ma planu zarządzania podatnościami

68% brak odmiejscowionych kopii bezpieczeństwa

53% brak dedykowanego stanowiska ds. cyberbezpieczeństwa

80% nie weryfikuje umów z partnerami w zakresie bezpieczeństwa

92% brak podwójnego uwierzytelniania kont

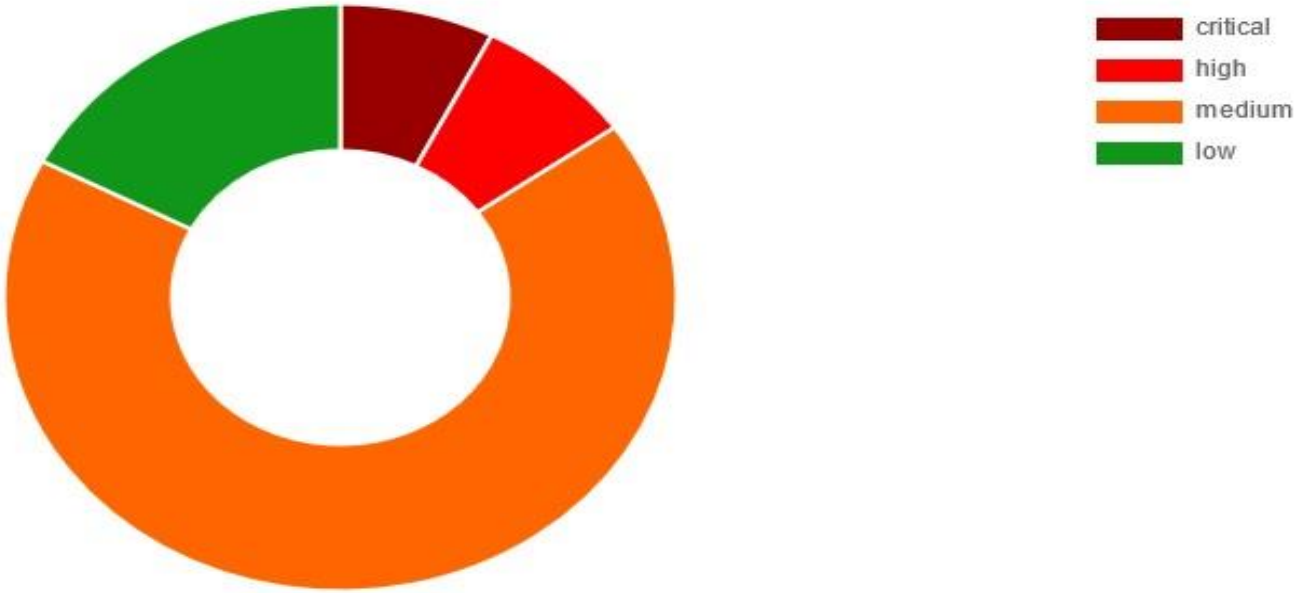
86% kierownik jednostki nie odbył szkolenia w zakresie cyberbezpieczeństwa

Ataki weryfikują nadmierny optymizm przy wypełnianiu ankiet

SYTUACJA PRZED ATAKIEM **W SZPITALU**

CRITICAL	HIGH	MEDIUM	LOW	INFO
191	199	1735	445	12219

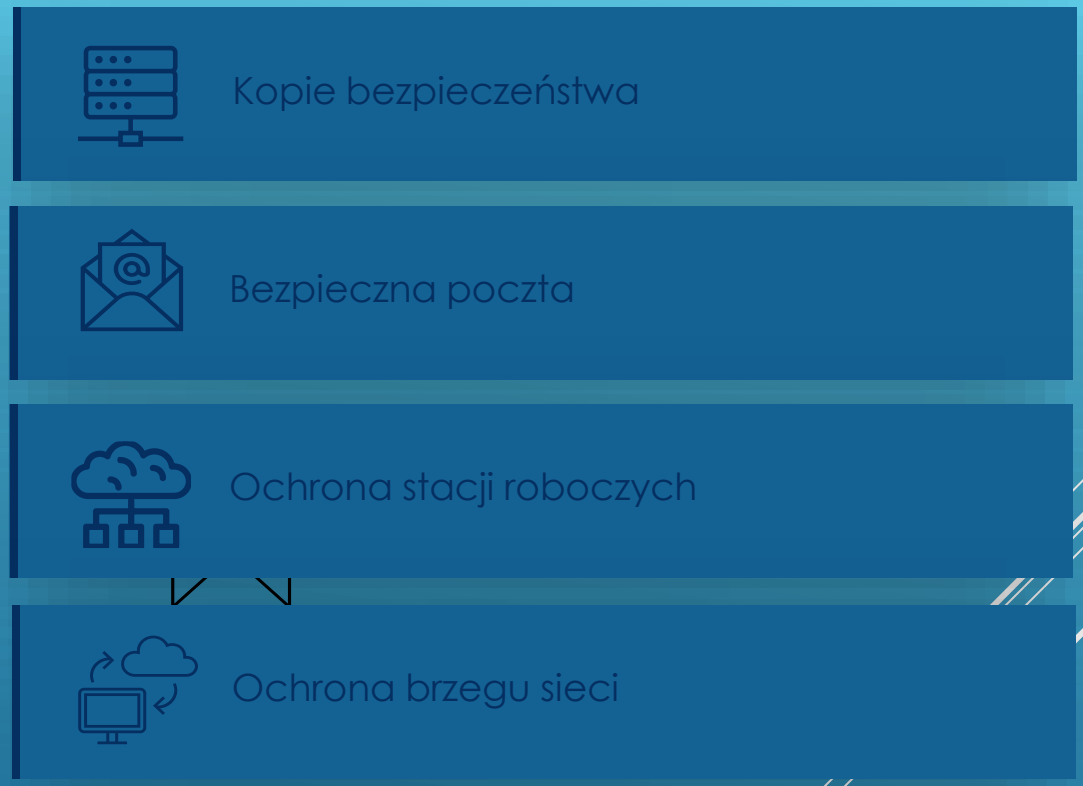
Podatność według stopnia ciężkości



Rekomendacje w zakresie budowy systemów cyberbezpieczeństwa

- Priorytety działań
- Rekomendacje w zakresie architektury cyberbezpieczeństwa (podstawowej i docelowej)
- Rekomendacje w zakresie funkcjonalności komponentów bezpieczeństwa
- Wymagania dotyczące wykonania usługi skanowania podatności
- Dokument opublikowany w kwietniu 2022 r.

Wskazane priorytety



Źródło: Plan działania w zakresie cyberbezpieczeństwa w ochronie zdrowia, CeZ, 2022 r.

ZMIANA W SZPITALACH (04.2023 R.)

57% -> 45% brak dokumentacji SZBI (zatem również procedur w zakresie kopii zapasowych)

81% -> 71% nie ma planu zarządzania podatnościami

68% -> 50% brak odmiejscowionych kopii bezpieczeństwa

53% -> 47,3 % brak dedykowanego stanowiska ds. cyberbezpieczeństwa

80% - > 80% nie weryfikuje umów z partnerami w zakresie bezpieczeństwa

92% -> 91% brak podwójnego uwierzytelniania kont

86% -> 72% kierownik jednostki nie odbył szkolenia w zakresie cyberbezpieczeństwa

Ataki weryfikują nadmierny optymizm przy wypełnianiu ankiet

DECYZJE OUK STATUS (04.2023 R.)

239 decyzji

235 (98,3%) wskazano osoby odpowiedzialne za cyberbezpieczeństwo

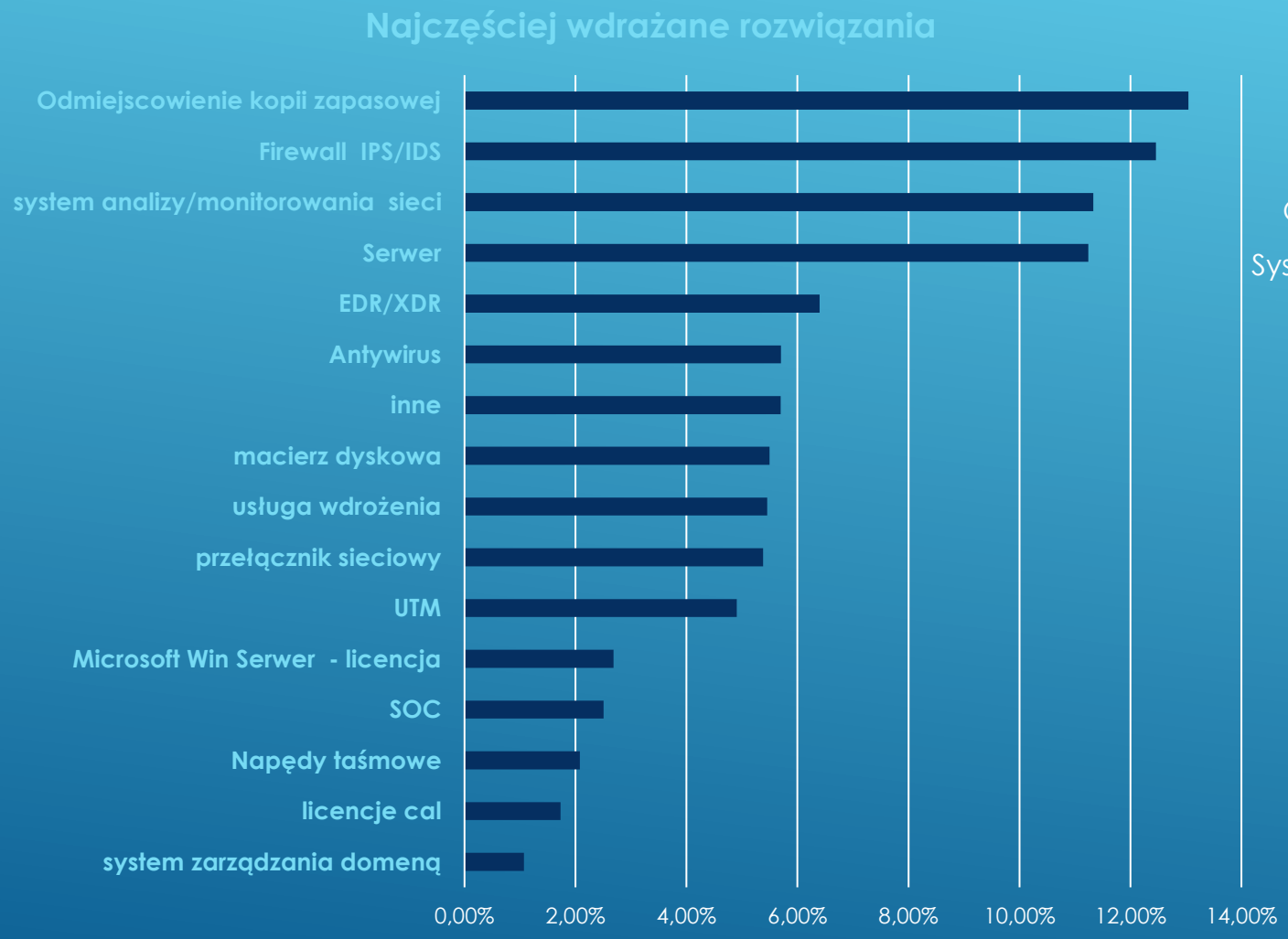
51 Podmiotów ma obowiązek przedstawienia audytu KSC

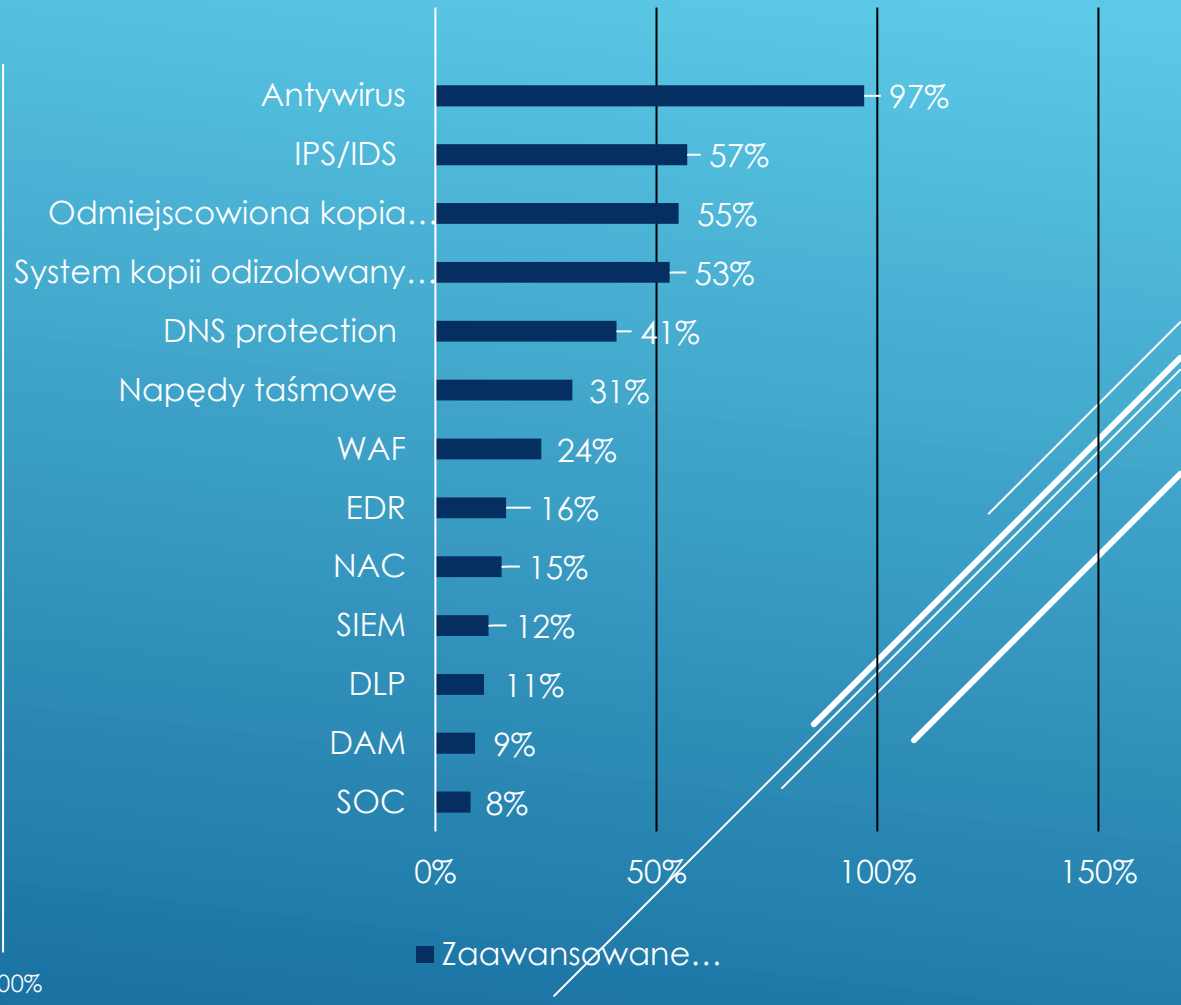
67,5 % **podmiotów zrealizowało wymagania art. 8 p. 2, 3, 5 i 6 oraz art. 10 p. 1, 2 i 3 ust. KSC**

32,5 % **podmiotów NIE zrealizowało wymagań art. 8 p. 2, 3, 5 i 6 oraz art. 10 p. 1, 2 i 3 ust. KSC**

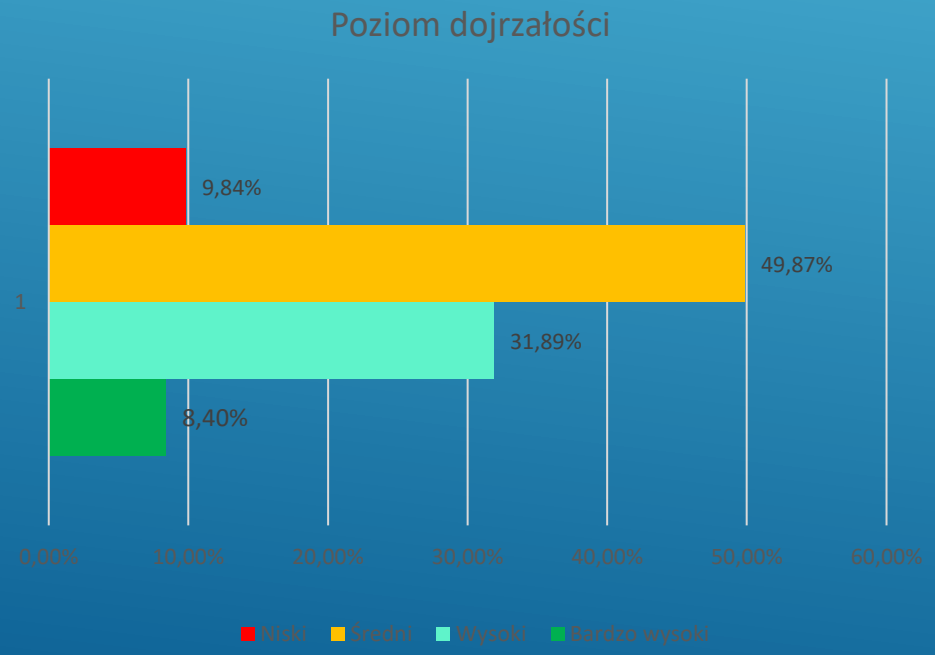
37 (72,5 %) liczba audytów KSC przesłanych do MZ

Statystyka nowych systemów w szpitalach

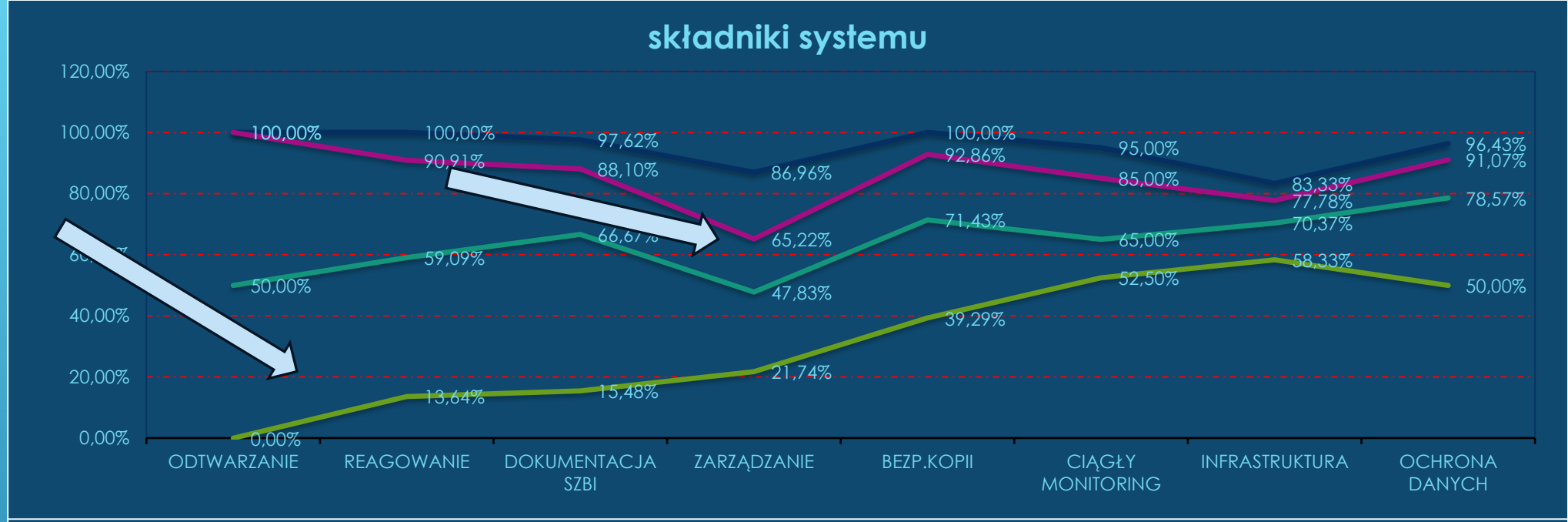


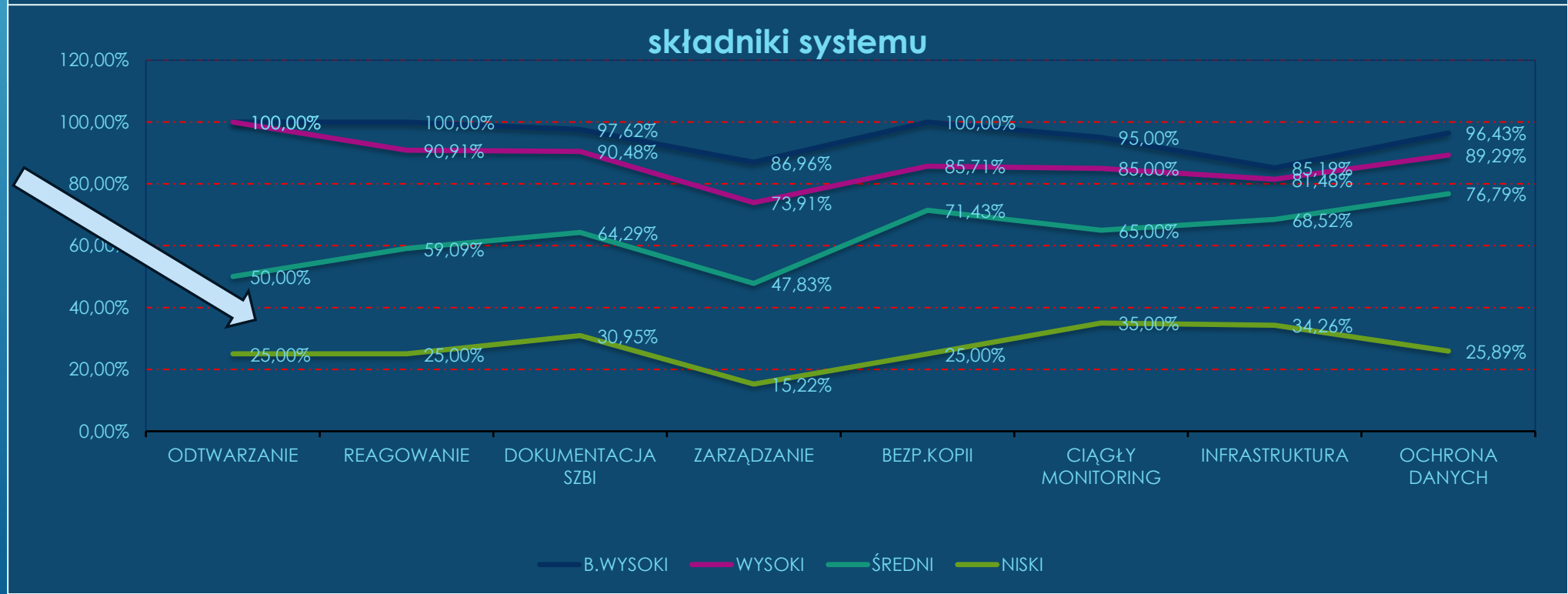



Poziom dojrzałości
2,76%
61,98%
29,49%
5,77%
1
0,00%
10,00%
20,00%
30,00%
40,00%
50,00%
60,00%
70,00%
Niski
Średni
Wysoki
Bardzo Wysoki


Poziom dojrzałości
9,84%
49,87%
31,89%
8,40%
1
0,00%
10,00%
20,00%
30,00%
40,00%
50,00%
60,00%
Niski
Średni
Wysoki
Bardzo wysoki

Statystyka nowych systemów w szpitalach





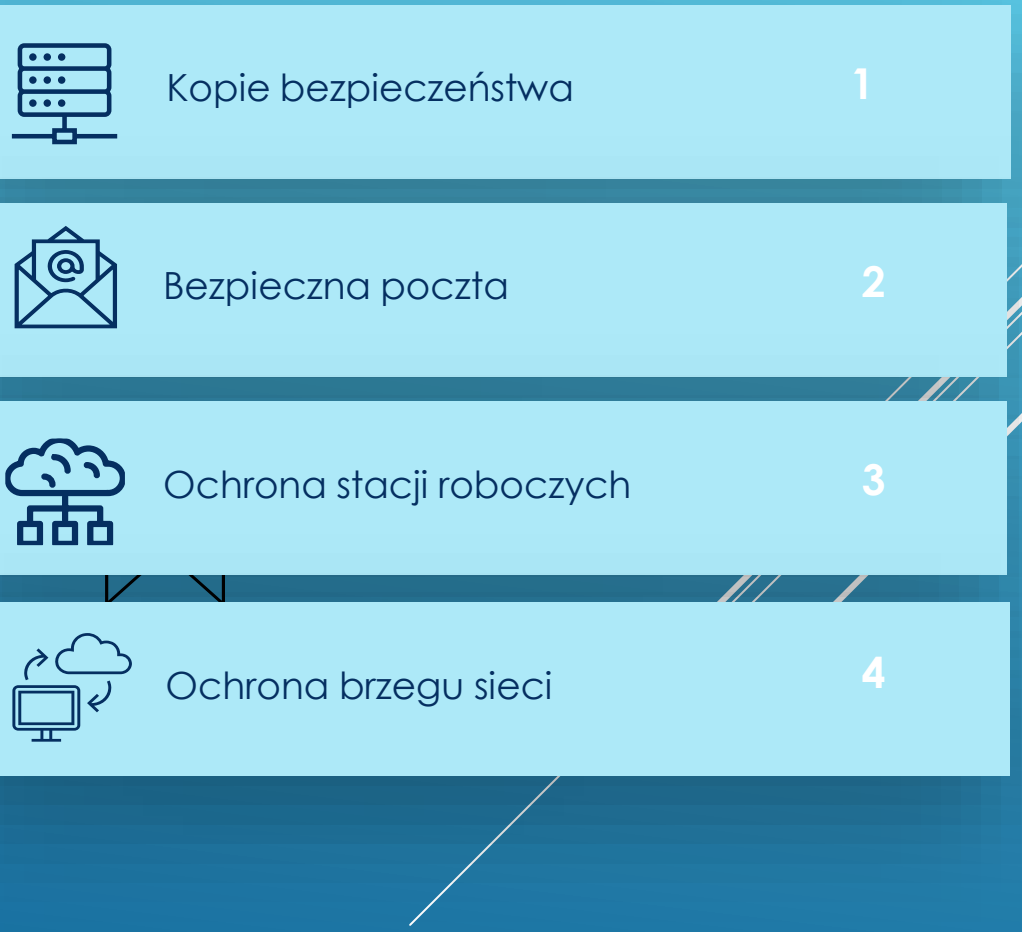
Zmiana podejścia w 2023 – rekomendacje – obligatoryjna kolejność budowy systemów cyberbezpieczeństwa

- Priorytety działań
- Rekomendacje w zakresie architektury cyberbezpieczeństwa (podstawowej i docelowej)
- Rekomendacje w zakresie funkcjonalności komponentów bezpieczeństwa
- Wymagania dotyczące wykonania usługi skanowania podatności
- Dokument opublikowany w kwietniu 2023 r.

Segmentacja sieci

Wieloskładnikowe uwierzytelnianie

Wskazane priorytety



Źródło: Plan działania w zakresie cyberbezpieczeństwa w ochronie zdrowia, CeZ, 2022 r.

CSIRT CEZ
- PRZYGOTOWANIE 2022/2023 R.
- URUCHOMIONY 12’ 2023 R.

- Formalne dokumenty powołujące CSIRT sektorowy, formalne poinformowanie sektora
- Zapewnienie bezpiecznego kanału do zgłaszania incydentów
- Listy kontaktowe do OUK. Komunikacja do OUK. Komunikacja z innymi zespołami cyberbezpieczeństwa
- Komunikacja z CSIRT poziomu krajowego

ZADANIA REALIZOWANE W CSIRT CEZ

Wsparcie w obsłudze incydentów:
(LPR Warszawa, Pajęczno, Giżycko, PSSE Jędrzejów, ICZMP Łódź, CZD Warszawa, USK Łódź)

Przygotowywanie rekomendacji: zalecenia dotyczące ochrony anty DDOS, kopii zapasowych, bezpiecznej korespondencji elektronicznej oraz haseł

Przygotowanie oraz rozsyłanie ostrzeżeń wraz z zaleceniami: **4 wysyłki w 2022 r.**

(5432 e-maile)

Wymiana informacji o zagrożeniach z CSIRT poziomu krajowego – **informacje o atakach w ochronie zdrowia**

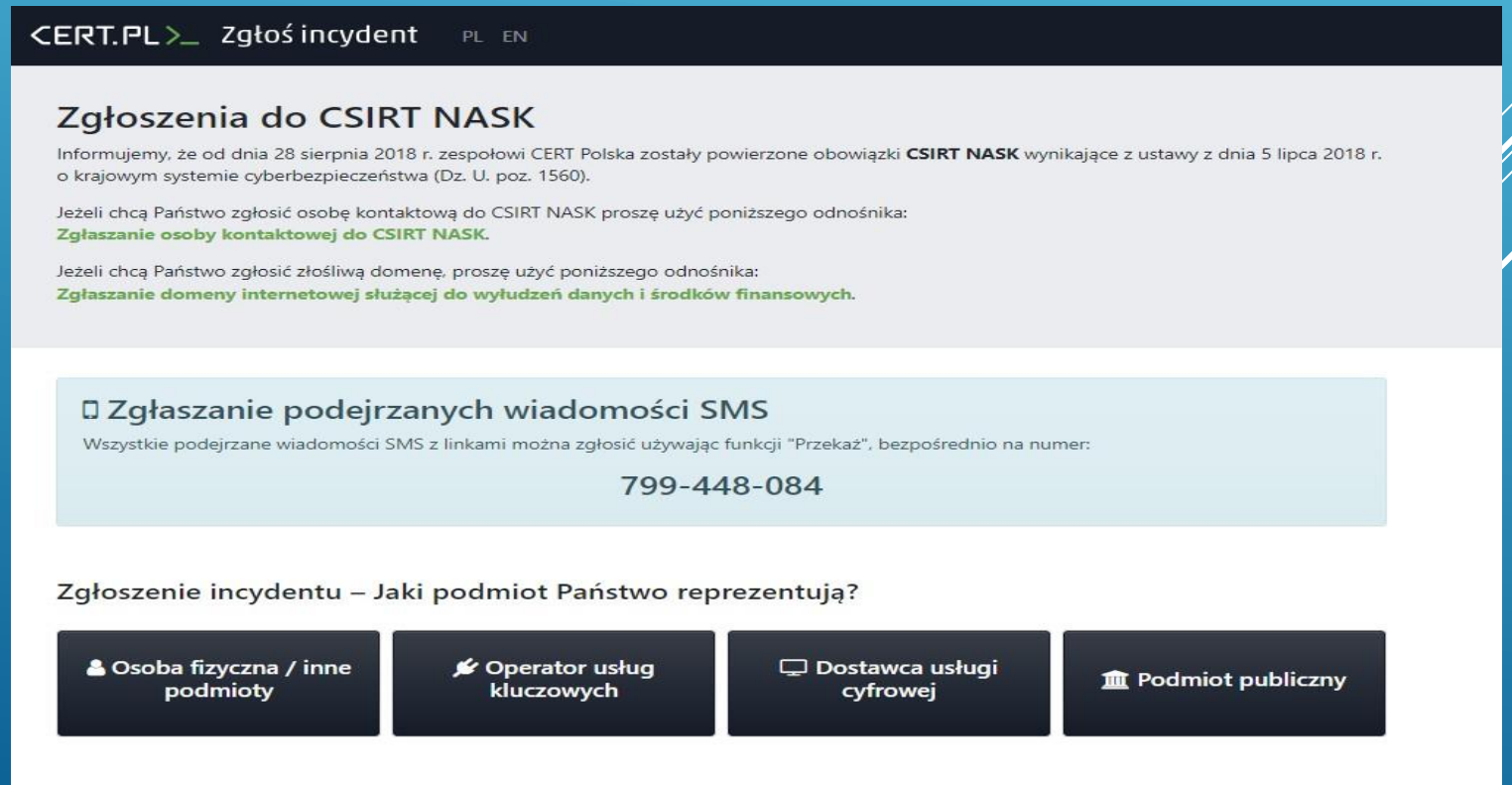
Testy podatności stron na żądanie – **rekonesans w 5 podmiotach**

Cyberkaretka CeZ

Jakie są te incydenty Bezpieczeństwa ?

INCYDENT

- zapewnia zarządzanie, zgłaszania i obsługi incydentu w podmiocie publicznym
- https://incydent.cert.pl
- zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;



ATAKI HAKERSKIE (INCYDENTY) PRZYPADKI PRAWDZIWE

PIERWSZE POWAŻNE INCYDENTY RANSOMWARE W POLSCE – 2021

SZPITAL W SOCHACZEWIE – 2021

Wpływ incydentu na funkcjonowanie szpitala:

Koronawirus
(obsługa doraźna z wydzielonej jednostki z dostępem do Internetu)
Szczepienia Brak możliwości rejestracji uprawnionych do szczepień w r
szczepień.
Badania Brak możliwości wystawienia elektronicznych zleceń na wykon
koronawirusa.
Administracja (część szara)
Infomedica Brak możliwości obsługi kadrowo-płacowej.
Brak możliwości generowania dokumentacji dokumentów do ZUS i US.
Brak możliwości rozliczenia wynagrodzeń pracowników szpitala.
Płatnik Brak możliwości rozliczeń z ZUS.
Usługi opieki zdrowotnej (część biała)
[redacted] Brak możliwości elektronicznej obsługi pacjentów (w tym nawet
odbywa się to z wykorzystaniem dokumentacji wyłącznie papierowej.
Brak możliwości sprawdzenia uprawnień pacjenta (system eWUS).
Brak możliwości wystawienia e-recepty.
Brak możliwości wystawienia i zaczytania e-skierowania.
Brak możliwości rozliczeń z NFZ, które umożliwiają finansowanie działal
szpitala (rozliczania kosztów działalności szpitala i refundacji
z NFZ za wykonane usługi).
Brak możliwości wywiązania się z obowiązków sprawozdawczych do NF
zakresie m.in. statystyk medycznych, w tym kolejek (m.in. oczekujące, w
miejsca, pacjentów onkologicznych [redacted]).
PAX (powiązany z [redacted])
Brak możliwości elektronicznej obsługi diagnostyki obrazowej (RTG, TK,
Mammograf) i czytania obrazów na stacjach opisowych w wysokiej
rozdzielczości.
[redacted] **(system apteczny)**
Brak możliwości dystrybucji elektronicznej leków (wyłącznie papierowe
zlecenia).

MAŁOPOLSKI URZĄD MARSZ. – 2021

Atak hakerski na urząd marszałkowski. Atakujący zażądał okupu. Ma chodzić o miliony euro. Sprawę bada policja

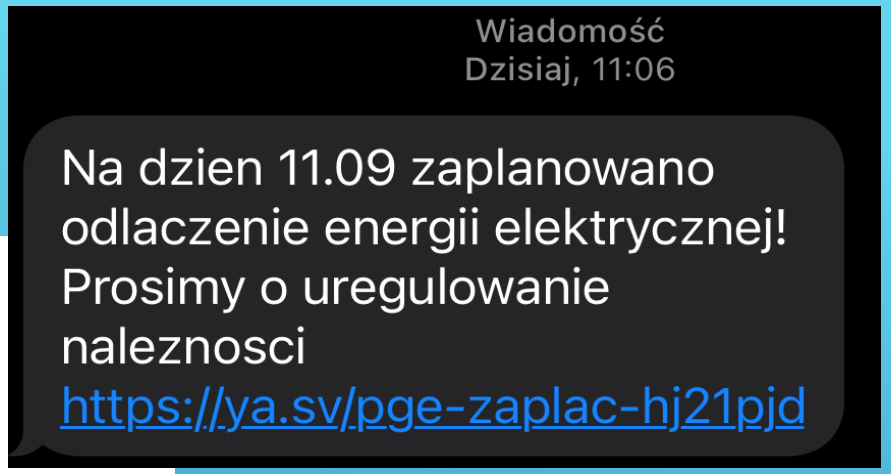
Bartosz Dybała 11 lutego 2021, 11:45

Doszło do ataku hakerskiego na urząd marszałkowski https://www.malopolska.pl/

Policja bada sprawę ataku hakerskiego na Urząd Marszałkowski Województwa Małopolskiego. Incydent doprowadził do utraty dostępności danych osobowych, m.in. klientów urzędu. Za jej przywrócenie atakujący zażądał zapłaty okupu: ma chodzić o miliony euro. - W tej chwili przyjmujemy formalne zawiadomienie o przestępstwie od pracownika urzędu. Chodzi o przestępstwo przeciwko ochronie informacji - mówi nam rzecznik małopolskiej policji.

INCYDENTY – 2021

LokiBot – kradnie dane logowania do banków, podszywa się pod komunikatory, a na końcu blokuje urządzenie domagając się okupu.



Ministerstwo Finansów

Paragon podatkowy.xlsx
343 KB

Rejestr podatkowy.xlsx
343 KB

Dobry dzień,

Ma to na celu poinformowanie Cię o rozbieżności w Twojej ewidencji podatkowej. Odwiedź swój bank lub jakikolwiek urząd skarbowy w Twojej okolicy z załączonym ewidencją podatkową.

W załączniku znajduje się dokumentacja podatkowa, zaległe płatności i numer referencyjny sprawy podatkowej.

Dochód krajowy Administracja
Rząd Polski

Phone: +48 22 364 44 66
Email: info@gove.pl
website: www.gov.pl
Address: Świętokrzyska 12 00-916 Warszawa NIP 5260250274 Regon 000002217. Poland

OSZUKANE MAILE

Afera mailowa. Tajne informacje na mailach Dworczyka

wyborcza.pl

NIE MA WOLNOŚCI BEZ SOLIDARNOŚCI

Nie ma już wątpliwości: Michał Dworczyk jako szef kancelarii premiera przekazywał za pośrednictwem prywatnej poczty mailowej informacje, które powinny mieć nadaną klauzulę tajności. Chodzi o instrukcje dla Agencji Wywiadu i Służby Wywiadu Wojskowego.

92% lekarzy w Polsce nie stosuje podwójnego uwierzytelniania

Ziobro straszy Morawieckiego mailami Dworczyka. Trzy śledztwa prokuratury

Poufna Rozmowa publikuje hasło i login ze "skrzynki Dworczyka". KPRM nie zmieniła ich od trzech lat

CYBERBEZPIECZEŃSTWO 05.05.2023, 17:20

Bolesław Breczko

• Generator haseł to przydatne narzędzie. Zdjęcie ilustracyjne (Shutterstock)

92% lekarzy w Polsce nie stosuje rotacji uwierzytelniania

OSZUKANE MAILE?

Afera mailowa. Tajne informacje na mailach Dworczyka

CEL : KOMPROMITACJA

INFORMACJE MILTARNE
PROŚBY O PRACĘ + CV
ROZMOWY POLITYCZNE
KORESPONDENCJA SŁUŻBOWA

92% lekarzy w Polsce
nie stosuje
podwójnego uwierzytelniania

OSZUKANE MAILE?

JAK SIĘ OBRONIĆ ?

TYLKO WIEDZĄ!

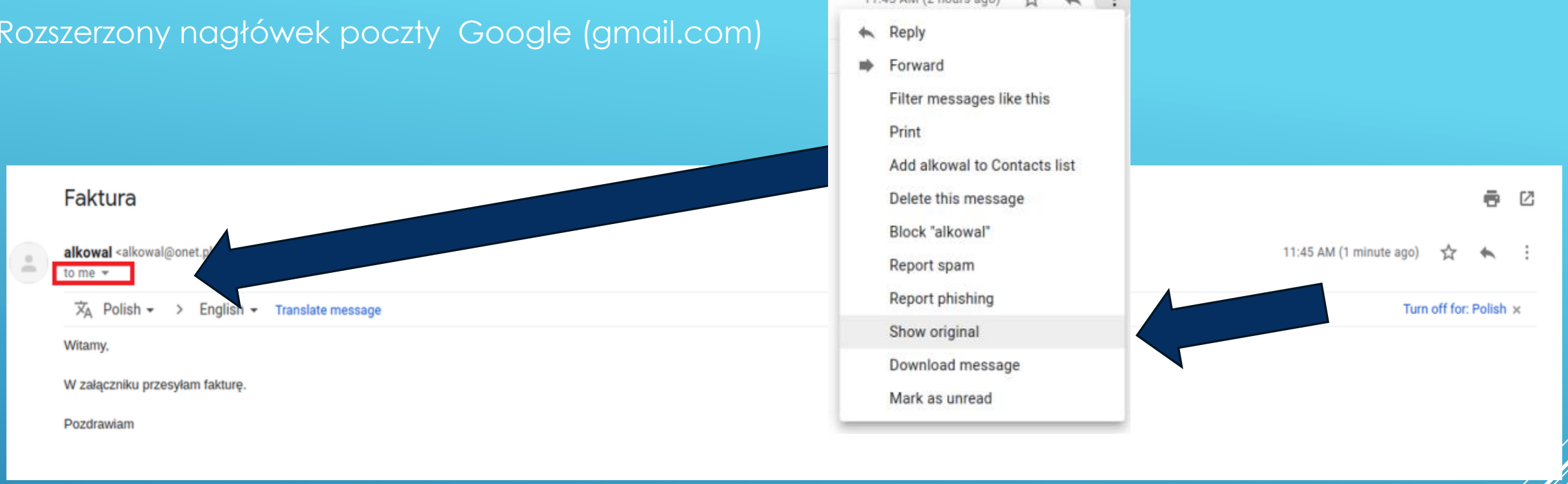
KLUCZEM JEST ANALIZA NAGŁÓWKA ROZSZERZONEGO.

Rozszerzony nagłówek poczty WP

Źródło : FUNDACJA bezpieczna cyberprzestrzeń

https://www.cybsecurity.org/pl/jak-zobaczyc-naglowki-wiadomosci-e-mail-na-roznych-pocztach/

Rozszerzony nagłówek poczty Google (gmail.com)



Źródło : FUNDACJA bezpieczna cyberprzestrzeń

https://www.cybsecurity.org/pl/jak-zobaczyc-naglowki-wiadomosci-e-mail-na-roznych-pocztach/

Rozszerzony nagłówek poczty MS Outlook

Nagłówki wiadomości

Received: from mx.poczta.onet.pl (unresolved [10.175.36.31]: 42712)
by ps18 (Ota) with LMTP id 47222DDED9C4E
for <alkowal@onet.pl>; Thu, 27 Jun 2019 16: 46: 30 +0200 (CEST)
Received: from localhost (emkei.cz [46.167.245.210])
(using TLSv1.2 with cipher ADH-AES256-GCM-SHA384 (256/256 bits))
(No client certificate requested)
by mx.poczta.onet.pl (Onet) with ESMTPS id 45ZN521tgKzDRRyf1
for <alkowal@onet.pl>; Thu, 27 Jun 2019 16: 46: 30 +0200 (CEST)
Received: by localhost (Postfix, from userid 33)
id 84205C2EE9; Thu, 27 Jun 2019 16: 46: 27 +0200 (CEST)
To: alkowal@onet.pl
Subject: Faktura
From: "Orange" <info@orange.pl>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: info@orange.pl
Reply-To: info@orange.pl
Content-Type: text/plain; charset=utf-8
Message-Id: <20190627144627.84205C2EE9@localhost>
Date: Thu, 27 Jun 2019 16: 46: 27 +0200 (CEST)
X-ONET_PL-MDA-Version: 1.0.25
X-ONET_PL-MDA-Info: 018 38309 47222DDED9C4E 0.521097
X-ONET_PL-MDA-From: info@orange.pl
X-ONET_PL-MDA-Spam: NO

Jak rozpoznać fałszywego maila?

- **Spójrz w nagłówki „Received” – w powyższym przykładzie wiadomość została wysłana z serwera o adresie 46.167.245.210 (emkei.cz).**
- **Sprawdź adres w polu „From” (czy adres nadawcy jest zgodny z oczekiwanym).**
- **Porównaj adres e-mail z pola „From” i „Reply-To”. Jeśli adresy są różne, możemy podejrzewać próbę oszustwa.**

FUNDACJA bezpieczna cyberprzestrzeń

Źródło :
https://www.cybsecurity.org/pl/jak-zobaczyc-naglowki-wiadomosci-e-mail-na-roznych-pocztach/

Nagłówek zmanipulowany

Mail pokrzywdzonego

Mail kontrolowany przez sprawcę

Mail podmiotu pod który się podszyto

Mail z którego wysłano wiadomość - może być to mail sprawcy lub osoby pokrzywdzonej włamaniem na konto poczty elektronicznej

```
Received: from mx.poczta.onet.pl (unresolved [10.174.34.83]:47784)
        by ps25.m5r2.onet (Ota) with LMTP id 2C7AD2E8F61F0
        for <abc@poczta.onet.pl>; Wed, 11 Oct 2017 05:57:22 +0200 (CEST)
Received: from acc153.rev.netart.pl (acc153.rev.netart.pl [77.55.54.153])
        by mx.poczta.onet.pl (Onet) with ESMTP id 3yBgD20S4HzGJR
        for <abc@poczta.onet.pl>; Wed, 11 Oct 2017 05:57:22 +0200 (CEST)
X-Virus-Scanned: by amavisd-new using ClamAV (21)
X-Spam-Flag: NO
X-Spam-Score: 0.711
X-Spam-Level:
X-Spam-Status: No, score=0.711 tagged_above=-10 tests=[HTML_IMAGE_ONLY_20=0.7,
        HTML_MESSAGE=0.001, T_HEADER_FROM_DIFFERENT_DOMAINS=0.01]
        autolearn=disabled
Received: from [192.168.25.1] (free-125-19.mediaworksit.net [95.140.125.19])
        by wertaz.nazwa.pl (Postfix) with ESMTP id 2BAF837F4AE
        for <abc@poczta.onet.pl>; Tue, 10 Oct 2017 23:31:19 +0200 (CEST)
Reply-To: <adwokatchojka@0.pl>
From:"Kancelaria Adwokacka - Jerzy Chojka" <kancelaria@adwokatchojka.pl>
To: "abc" <abc@poczta.onet.pl>
Subject:=?utf-8?B?IFBvd2lhZG9taWVuaWUgbyBwcnplasSZY2l1IHdpZXJ6eXRlbG5vxZtjaSBuYWxlxbzEhWNlaiBkbyBUd29qZWogZmlybXk=?=
Message-ID: <580c0b55fe7ad24984fd34d5eb1cc03d@9971GHPJ77>
Date: Tue, 10 Oct 2017 23:21:22 +0200
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0001_52FE4741.CCECCF4B"
Disposition-Notification-To: adwokatchojka@0.pl
X-Priority: 3
X-Mailer: Office Outlook 2016
X-ONET_PL-MDA-SEGREGATION: 0
X-ONET_PL-MDA-Version: 1.0.25
X-ONET_PL-MDA-Info: 025 25405 2C7AD2E8F61F0 0.501615
X-ONET_PL-MDA-From: xyz@xyz.pl
X-ONET_PL-MDA-Spam: NO
```

Źródło: prezentacja „Wybrane aspekty cyberprzestępczości" prof.ucz. Dr hab. Inż. Agnieszka Gryszczyńska

ŚLEDZENIE CZYLI JAK DUŻO O NAS WIEDZĄ „INTERNETY”

Jak namierzono adres ministra Niedzielskiego? (Niebezpiecznik.pl)

Wiedzieli gdzie mieszka i będą go odwiedzać “nie raz, nie dwa”

na 4 minutowym materiale widać jak grupa osób z kamerami towarzyszy ministrowi Niedzielskiemu od klatki wejściowej aż do windy, a kiedy ta rusza, grupa wbiega schodami na piętro, na którym mieszka minister. Wtedy minister sięga po telefon a nagrywający opuszcza budynek, stwierdzając: “Wiemy dokładnie gdzie on mieszka i będziemy tutaj nie raz, nie dwa”

Źródło : https://niebezpiecznik.pl/post/minister-adam-niedzielski-adres/

Jak namierzono adres ministra Niedzielskiego? (Niebezpiecznik.pl)

Wiedzieli gdzie mieszka i będą go odwiedzać “nie raz, nie dwa”

Osobowe Źródła Informacji

Źródło : https://niebezpiecznik.pl/post/minister-adam-niedzielski-adres/

Jak namierzono adres ministra Niedzielskiego? (Niebezpiecznik.pl)

Wiedzieli gdzie mieszka i będą go odwiedzać “nie raz, nie dwa”

jeszcze jedno zagrożenie związane z prywatnością VIP-ów, chociaż ten problem w zasadzie dotyczy każdej osoby, co do której wiemy, że kiedyś będzie w określonym miejscu i czasie, tak jak właśnie Pan minister, np. w Sejmie, dzieci w szkole itp..

Chodzi o możliwość …**śledzenia takiej osoby aż do miejsca zamieszkania**.
Zgubienie ogona, zwłaszcza w mieście, na szczęście nie jest trudne.

Źródło : https://niebezpiecznik.pl/post/minister-adam-niedzielski-adres/

Jak namierzono adres ministra Niedzielskiego? (Niebezpiecznik.pl)

Miejsce swojego zamieszkania zdradził sam Niedzielski. Na Twitterze

Na podstawie powyższego można **całkiem nieźle** oszacować miejsce, z którego minister w weekend ruszył na rowerową przejażdżkę. Oczywiście, start wcale nie musiał znajdować się w bloku, w którym mieszka Pan minister. Ale mógł. Więc na wszelki wypadek ocenzurowaliśmy punkt początku i końca tej trasy zielonym prostokątem, żeby nie został uwieczniony w naszym artykule, jeśli Pan minister zdecyduje się kiedyś usunąć tego twita. Przy okazji przypomnijmy, że podobną wpadkę parę lat temu zaliczyli żołnierze — biegali z aplikacjami i w ten sposób zdradzili lokalizację wielu obiektów wojskowych, nawet tych, których nie było jeszcze na mapach…

Źródło : https://niebezpiecznik.pl/post/minister-adam-niedzielski-adres/

Jak namierzono adres ministra Niedzielskiego? (Niebezpiecznik.pl)

Księgi wieczyste też zdradzają, gdzie ktoś mieszka

Dzięki Księgom Wieczystym można ustalić też wiele innych informacji o "figurancie", m.in. **PESEL, informacje o ew. kredycie i banku a także informacje dotyczące związku małżeńskiego**

Wyszukiwanie numeru księgi wieczystej po numerze działki
Zdobądź numer księgi wieczystej poprzez wyszukiwanie na podstawie numeru działki. Wystarczy wpisać w pasek wyszukiwania numer działki. Wyszukiwanie numeru księgi wieczystej po numerze działki to jedna z dwóch metod szukania numeru dostępnych na portalu.

Identyfikator działki
Wyszukanie numeru księgi wieczystej po identyfikatorze działki odbywa się po wpisaniu pełnej formy tego identyfikatora mającej postać sekwencji cyfr WWPPGG_R.XXXX.NDZ/Y np.: 320906_5.0211.161/2.
W identyfikatorze poszczególne cyfry oznaczają:
•WW: kod województwa
•PP: kod powiatu
•GG: kod gminy
•R: typ gminy, gdzie gmina miejska to 1, wiejska 2, gmina miejsko-wiejska 3, miasto w gminie miejsko-wiejskiej 4, obszar wiejski w gminie miejsko-wiejskiej 5, dzielnice m.st. Warszawy 8, delegatury oraz dzielnice innych gmin miejskich 9
•XXXX to numer ewidencyjny obrębu jednostki ewidencyjnej
•NDZ/Y to numer działki.

Jak uzyskać numer działki?
Skąd można wziąć numer działki? Są dwie opcje:
•Uzyskanie go w wydziale ewidencji gruntów
•Znalezienie online na portalu GeoPortal.gov.pl.

Gdy już zdobędziesz numer księgi wieczystej

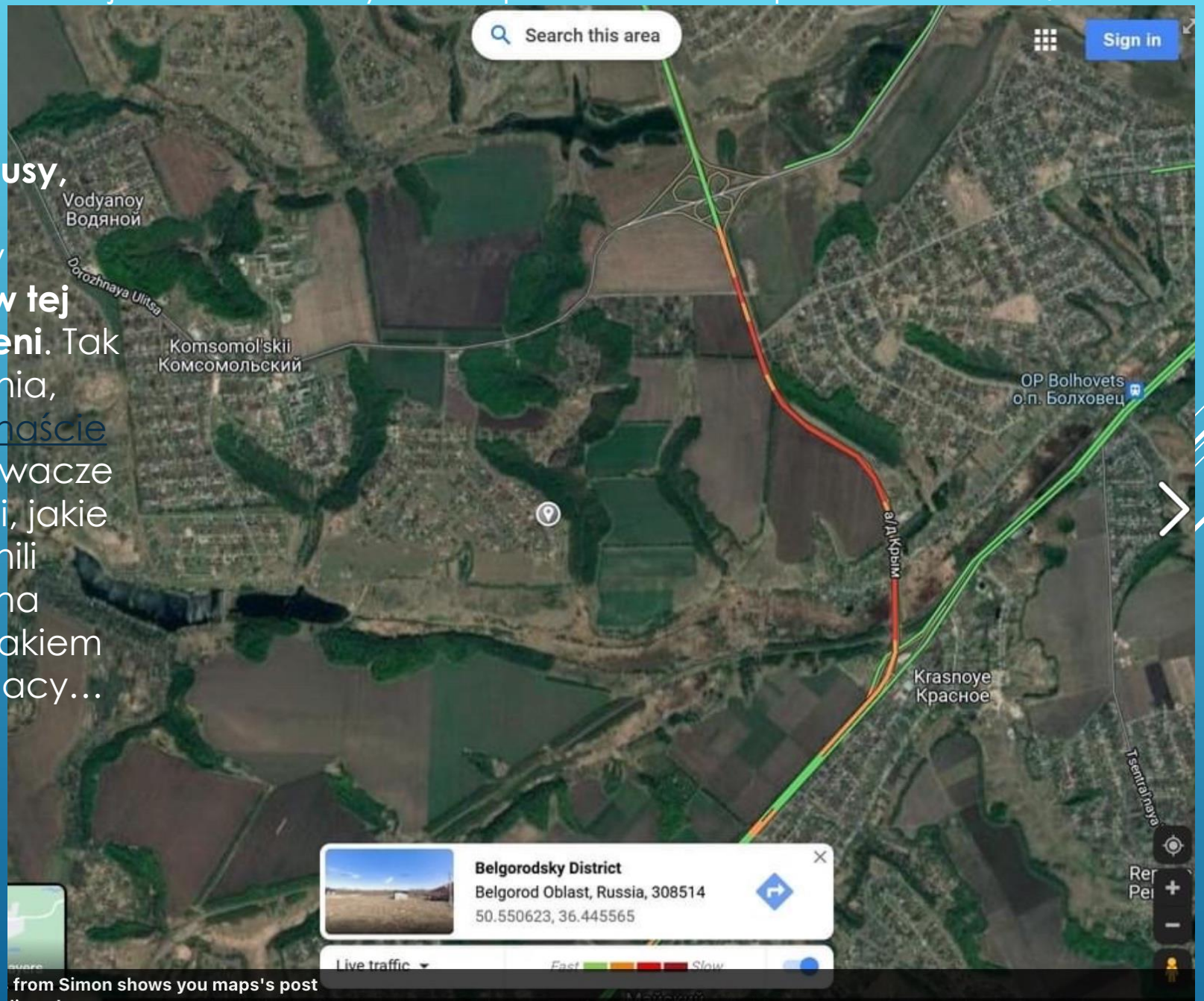
Kiedy już wyszukasz numer księgi wieczyste po numerze działki, masz otwartą drogę do przejrzenia treści księgi wieczystej. Księgi są jawne i dostępne online. Przeglądanie księgi wieczystej jest darmowe, a pobranie dokumentu kosztuje 20 zł brutto plus opłaty manipulacyjne przelewu elektronicznego. W sądzie rejonowym pobranie księgi wieczystej kosztuje 30 zł za każdy wypis.

https://www.znajdzksiege.pl/dzialki/?utm_source=adwords&utm_medium=cpc&utm_term=ksi%C4%99ga%20wieczysta%20po%20numerze%20dzia%C5%82ki&utm_campaign=dzialki&gclid=EAIaIQobChMI3ZXG6PuJgwMVsBoGAB2ukQ0VEAAYASAAEgJn_fD_BwE

https://niebezpiecznik.pl/post/wojna-rosji-z-ukraina-a-cyberbezpieczenstwo-w-polsce-kilka-rad/

Wojna to nie tylko bomby, to także wirusy, ddosy i deface

Bombardowanie Ukrainy zaczęło się w środku nocy, ale **pierwszą fazą ataku w tej wojnie były działania w cyberprzestrzeni**. Tak naprawdę zaczęły się one już 15 stycznia, kiedy informowaliśmy o ataku na kilkanaście sieci rządowych (tzw. **Deface**). Włamywacze używając narzędzi powiązanych z tymi, jakie wykorzystują rosyjscy hakerzy, podmienili treści rządowych stron internetowych na komunikat. Treść sugerowała, że za atakiem mają stać nieprzychylni Ukraińcom Polacy…



PRZYKŁADOWE ATAKI 2022 - 24

FAŁSZYWE PŁATNOŚCI	MORELE.NET
RANSOMWARE W LPR	LPR WARSZAWA
RANSOMWARE W SZPITALU	CZMP ŁÓDŹ
RANSOMWARE W SZPITALU	GIŻYCKO
WYCIEK DANYCH	ALAB
WŁAMANIA DO ZUS/RPWDL/P1	CEZ/ZUS
FAŁSZOWANIE RECEPT	CEZ
ATAKI DDOS	CEZ 09'23
ATAKI DDOS	CEZ 01'24

Fałszywe płatności
MORELE.NET

MORELE. NET

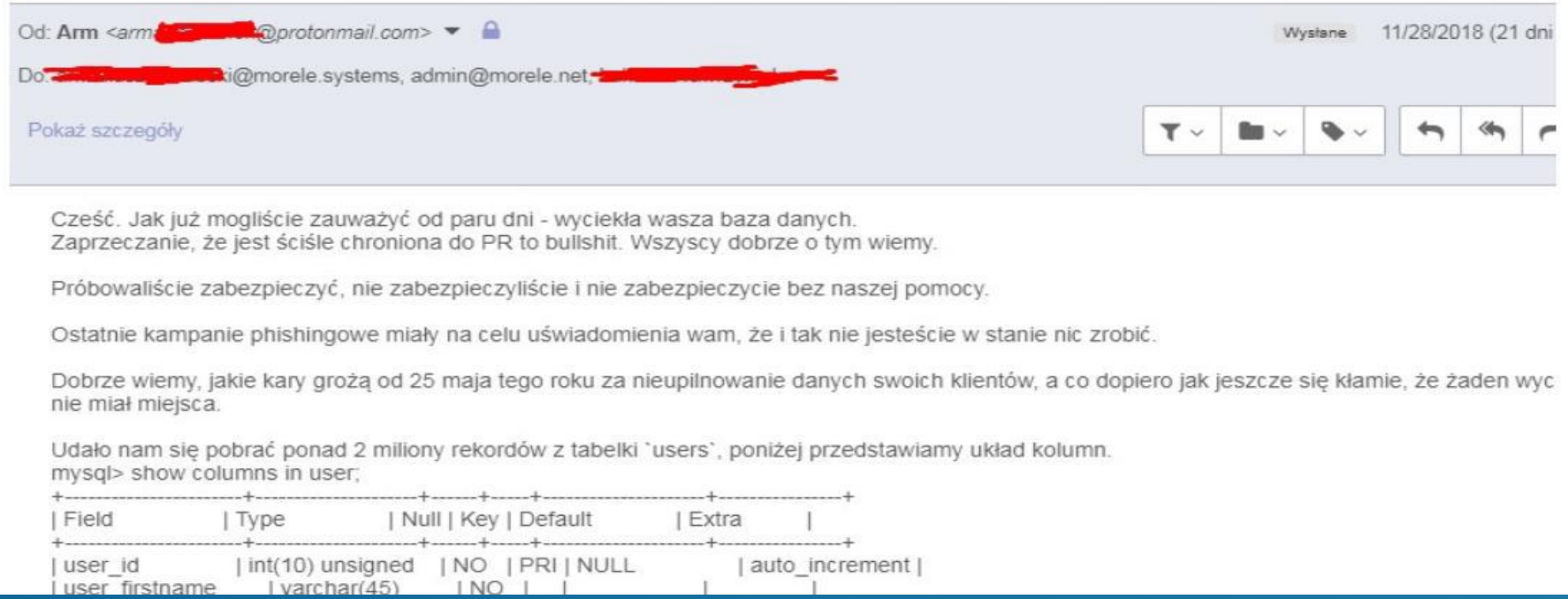
HISTORIA BY XARM

xArm
4 mies. temu dodał

Cześć wykopkowicze. Ostatnio natknąłem się na pewien otwarty serwer i był to serwer morele net, niezabezpieczone żadne porty, otwarty phpmyadmin i najcudowniejszy framework na świecie, który jest wystawiany na światło dzienne.

Udało mi się całą bazę danych, całe 2.2 mln danych użytkowników, do tego kilkadziesiat tysiecy peseli, pare tysiecy zeskanowanych dowodów osobistych, zazwyczaj były to dwie strony.

Przykładowy log z bazych danych wygląda nastepująco(wykop nie usuwaj proszę)
(2478371,'J****','Boj**uk','jboj**uk@interia.pl','$1
$owLbC*****DRkZJMh78U7g1','510***509',3,3,32**,722**43,3,3,'2018-10-0923:56:58','2018-10-1333:00:08',0)


Od: Arm <arm[redacted]@protonmail.com> Wysłane 11/28/2018 (21 dni
Do: [redacted]@morele.systems, admin@morele.net; [redacted]
Pokaż szczegóły

Cześć. Jak już mogliście zauważyć od paru dni - wyciekła wasza baza danych.
Zaprzeczanie, że jest ściśle chroniona do PR to bullshit. Wszyscy dobrze o tym wiemy.

Próbowaliście zabezpieczyć, nie zabezpieczyliście i nie zabezpieczycie bez naszej pomocy.

Ostatnie kampanie phishingowe miały na celu uświadomienia wam, że i tak nie jesteście w stanie nic zrobić.

Dobrze wiemy, jakie kary grożą od 25 maja tego roku za nieupilnowanie danych swoich klientów, a co dopiero jak jeszcze się kłamie, że żaden wyc nie miał miejsca.

Udało nam się pobrać ponad 2 miliony rekordów z tabelki `users`, poniżej przedstawiamy układ kolumn.
mysql> show columns in user;

Field	Type	Null	Key	Default	Extra
user_id	int(10) unsigned	NO	PRI	NULL	auto_increment
user_firstname	varchar(45)	NO			

http://www.wykop.pl/artykul/4704903/morele-net-historia-by-xarm/

Prawie 3 milionowa kara dla Morele.net za naruszenie RODO – do kasacji. Spółka wygrała w NSA

11 LUTEGO 2023, 20:18 | W BIEGU | KOMENTARZY 31

TAGI: RODO, UODO, WYCIEK

Sprawa rozpoczęła się w 2018 roku, kiedy doszło do dużego wycieku danych użytkowników (~2.2 milionów rekordów). UODO nałożyło wtedy dość wysoką karę pieniężną, którą później podtrzymał Wojewódzki Sąd Administracyjny:

> *Dziś WSA w Warszawie potwierdził zasadność kary nałożonej przez Prezesa UODO na spółkę https://t.co/5oS4Wilqar. Szczegóły dot. nałożenia kary na https://t.co/5oS4Wilqar dostępne są pod linkiem: https://t.co/p31iYETNj9*
>
> *— Urząd Ochrony Danych Osobowych (@UODOgov_pl) September 3, 2020*

Jak jednak donosi właśnie Dziennik Gazeta Prawna:

Wyrok w sprawie skargi kasacyjnej złożonej przez spółkę Morele.net zapadł na posiedzeniu niejawnym, dlatego nie wiadomo na razie, jakimi motywami kierował się Naczelny Sąd Administracyjny i jakie zarzuty uwzględnił. Jak jednak potwierdził Dziennik Gazeta Prawna uchylono zarówno wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie, który w 2020 r. utrzymał karę nałożoną na spółkę, jak i samą decyzję prezesa Urzędu Ochrony Danych Osobowych. Kara została więc wyeliminowana z obrotu prawnego.

~ms

Komentarze

policjant z majami
11 lutego, 2023 | 9:00 pm

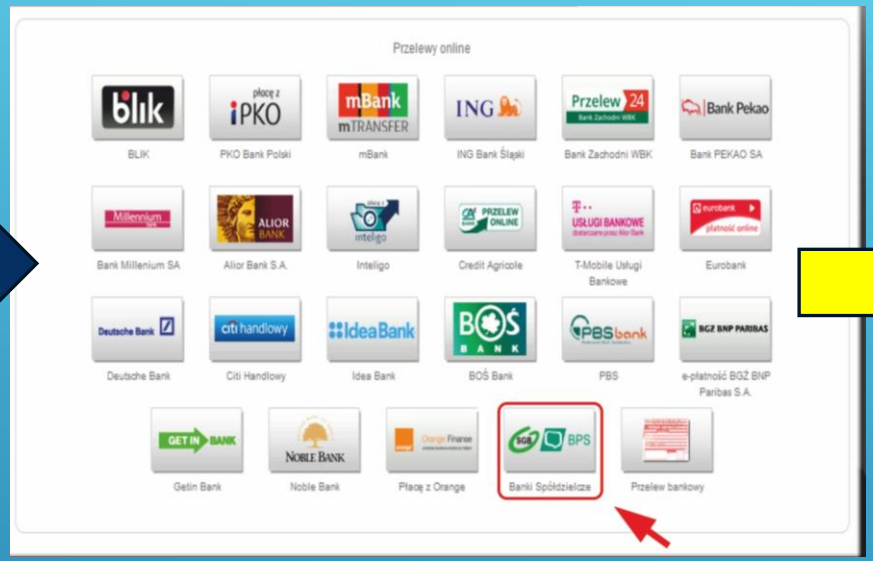
Czyli przepisy o RODO to fikcja? Przeciez ten wyciek powstal przez zaniebania firmy z tego pamiętam.

Odpowiedz

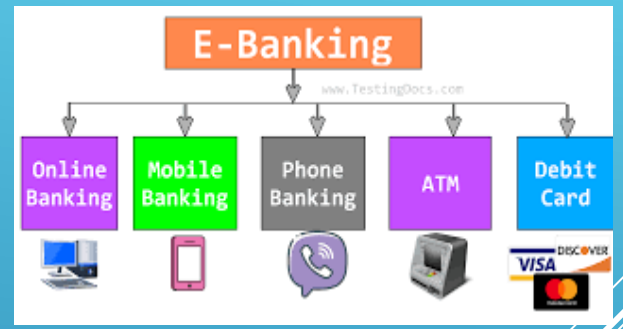
Sklep

Koszyk

płatność



Bank



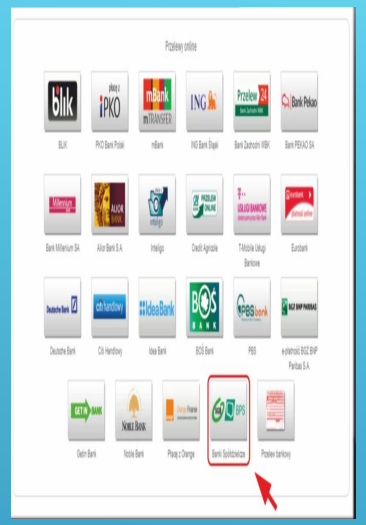
Towar

Potwierdzenie płatności

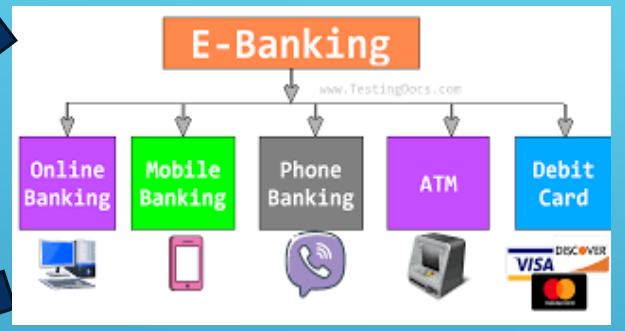
Sklep

Koszyk

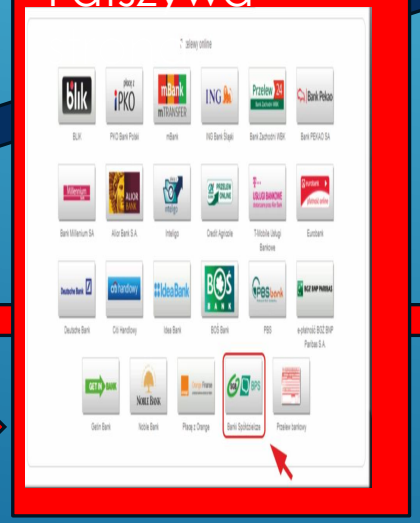
płatność



Bank

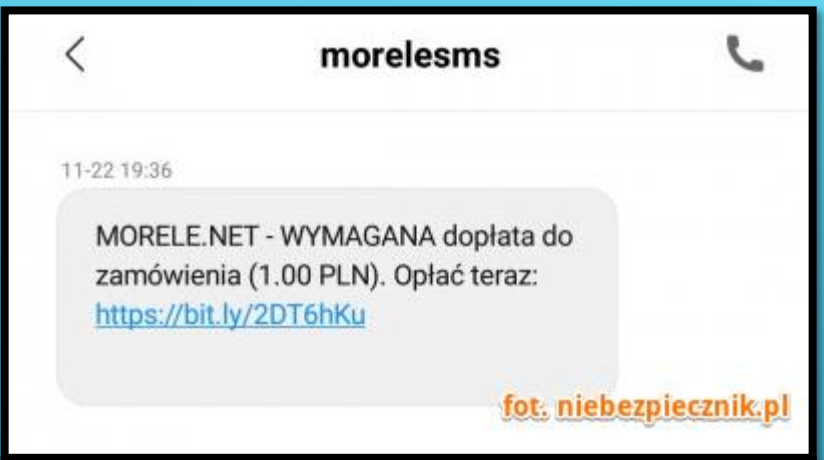


Fałszywa



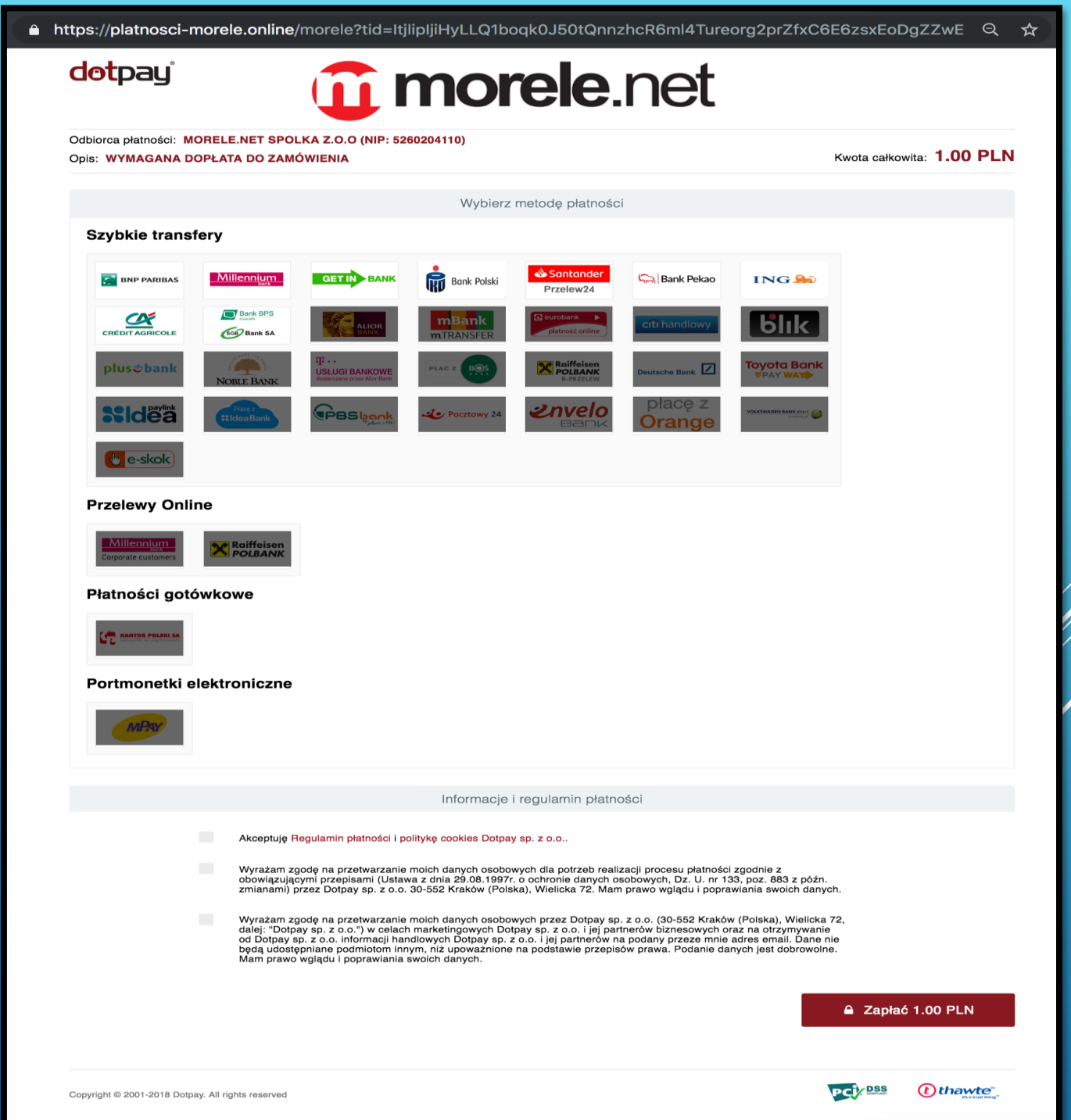
Przelew do słupa na cały stan konta!

Fałszywe uzupełnienie płatności


morelesms
11-22 19:36
MORELE.NET - WYMAGANA dopłata do zamówienia (1.00 PLN). Opłać teraz: https://bit.ly/2DT6hKu
fot. niebezpiecznik.pl


morelenet
fot. niebezpiecznik.pl
środa, wczoraj
Użytkowniku! Wymagana dopłata do twojego zamówienia na MORELE.NET. Dopłata na kwote 1.00 PLN - Dopłać teraz: http://bit.ly/2DAEJbD
21:08


morele24
Użytkowniku! Wymagana dopłata do zamówienia na MORELE.NET na kwotę 1.00 PLN. Ureguluj zaległą kwotę teraz: http://bit.ly/2zBfZxl
Od : morele24
26 Lis 2018 19:55
fot. niebezpiecznik.pl


https://platnosci-morele.online/morele?tid=ItjlipljiHyLLQ1boqk0J50tQnnzhcR6ml4Tureorg2prZfxC6E6zsxEoDgZZwE
dotpay
morele.net
Odbiorca płatności: MORELE.NET SPOLKA Z.O.O (NIP: 5260204110)
Opis: WYMAGANA DOPŁATA DO ZAMÓWIENIA
Kwota całkowita: 1.00 PLN
Wybierz metodę płatności
Szybkie transfery
BNP PARIBAS
Millennium
GETIN BANK
Bank Polski
Santander Przelew24
Bank Pekao
ING
CRÉDIT AGRICOLE
Bank BPS
Bank SA
ALIOR BANK
mBank mTRANSFER
eurobank płatność online
citi handlowy
blik
plus bank
NOBLE BANK
USŁUGI BANKOWE
Raiffeisen POLBANK E-PRZELEW
Deutsche Bank
Toyota Bank PAY WAY
paylink Idea
IdeaBank
PBS bank
Pocztowy 24
envelo BANK
płacę z Orange
e-skok
Przelewy Online
Millennium Corporate customers
Raiffeisen POLBANK
Płatności gotówkowe
KANTOR POLSKI SA
Portmonetki elektroniczne
mPay
Informacje i regulamin płatności
Akceptuję Regulamin płatności i politykę cookies Dotpay sp. z o.o..
Wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb realizacji procesu płatności zgodnie z obowiązującymi przepisami (Ustawa z dnia 29.08.1997r. o ochronie danych osobowych, Dz. U. nr 133, poz. 883 z późn. zmianami) przez Dotpay sp. z o.o. 30-552 Kraków (Polska), Wielicka 72. Mam prawo wglądu i poprawiania swoich danych.
Wyrażam zgodę na przetwarzanie moich danych osobowych przez Dotpay sp. z o.o. (30-552 Kraków (Polska), Wielicka 72, dalej: "Dotpay sp. z o.o.") w celach marketingowych Dotpay sp. z o.o. i jej partnerów biznesowych oraz na otrzymywanie od Dotpay sp. z o.o. informacji handlowych Dotpay sp. z o.o. i jej partnerów na podany przeze mnie adres email. Dane nie będą udostępniane podmiotom innym, niż upoważnione na podstawie przepisów prawa. Podanie danych jest dobrowolne. Mam prawo wglądu i poprawiania swoich danych.
Zapłać 1.00 PLN
Copyright © 2001-2018 Dotpay. All rights reserved
PCI DSS
thawte

Uwaga na SMS-y proszące o dopłatę 1 PLN do zamówienia w sklepach Grupy Morele.

Otrzymaliśmy od Państwa niepokojące informacje o smsach, które przychodzą na Państwa nr telefonów, w których są Państwo nakłaniani do zapłaty dodatkowej kwoty (w dotychczasowych przypadkach smsy mówiły o kwocie 1 PLN) do złożonego zamówienia w sklepach GRUPY MORELE. **Informujemy, że nie jesteśmy nadawcą tych smsów i jest to prawdopodobnie próba oszustwa i wyłudzenia**.

Tego typu ataki miały już miejsce - przestępcy mogą się podszywać pod firmę kurierską (np. DHL, Paczkomaty24) lub system płatności.

Nigdy nie wysyłamy smsów do Klientów z prośbą o dopłatę do zamówienia. Nie wysyłają ich również w naszym imieniu firmy kurierskie, ani żadne inne, związane z nami podmioty. Najprawdopodobniej jest to próba wyłudzenia pieniędzy. Bardzo prosimy o ignorowanie ich oraz w żadnym wypadku nie klikanie w link wysyłany smsem.

Nie jesteśmy źródłem danych, nasza baza danych jest ściśle chroniona. Wiadomości najprawdopodobniej wysyłane są losowo, a ich zbieżność z Państwa zamówieniami to wynik masowości całego procederu. Sprawę zgłaszamy również na Policję.

Więcej informacji o tym procederze znajdą Państwo w artykule.

Morele nie zapłaci gigantycznej kary za wyciek danych. NSA obciążył UODO

Sklep internetowy Morele.net nie zapłaci prawie 3 mln zł kary za wyciek danych, do którego doszło w 2018 r. Naczelny Sąd Administracyjny zobowiązał natomiast Urząd Ochrony Danych Osobowych do zwrócenia portalowi 65 tys. zł za kosztów postępowania.

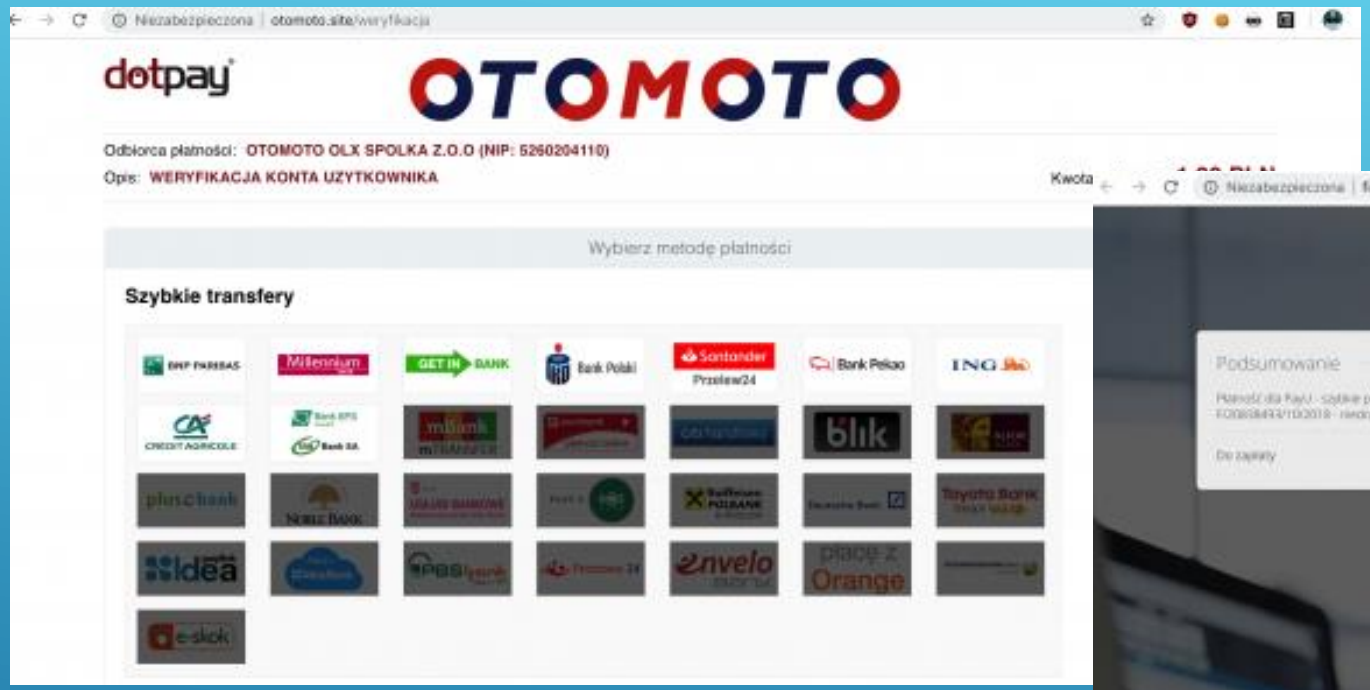
Publikacja: 29.03.2023 12:02

Foto: Adobe Stock

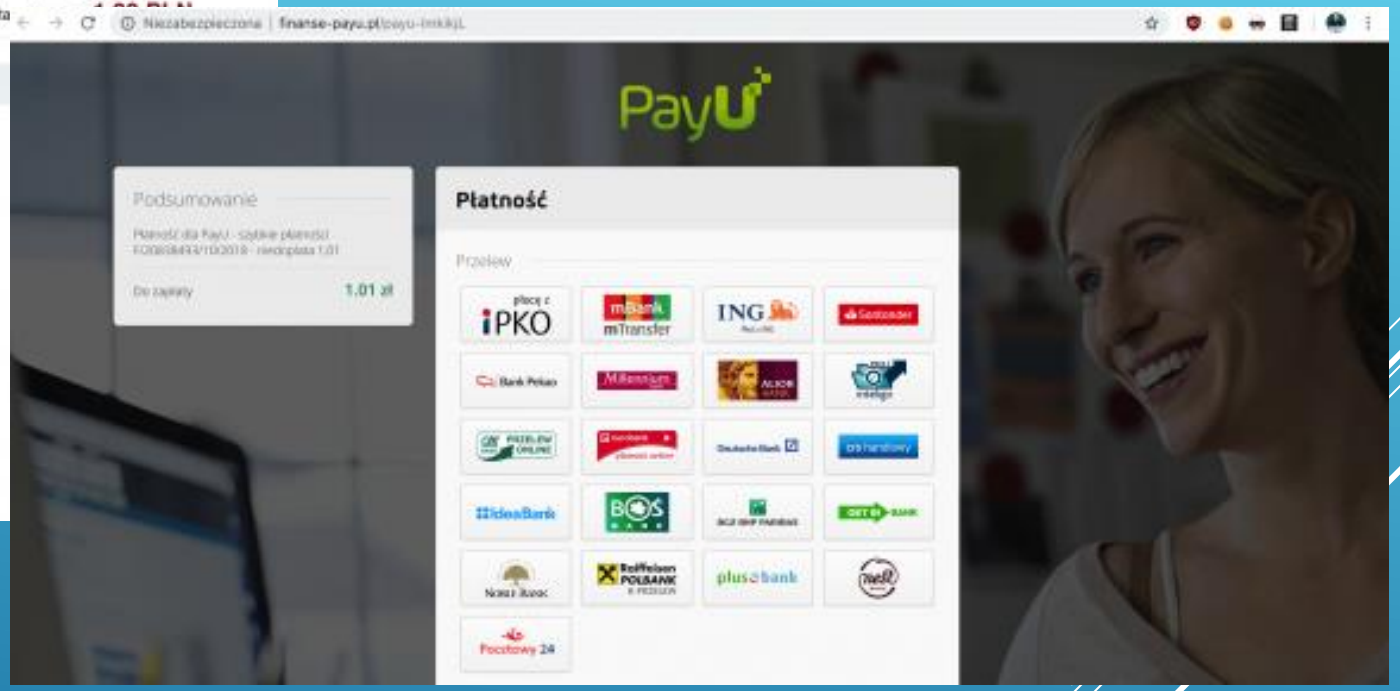
dgk

O prawomocnym wyroku NSA, który zapadł w lutym 2023 r., informuje serwis Niebezpiecznik.pl, który ujawnił ogromny wyciek danych w Morele.net w listopadzie 2018 r.

INNE FAŁSZYWE „SZYBKIE PŁATNOŚCI”



http://otomoto.site/weryfikacja



http://finanse-payu.pl

INNE FAŁSZYWE „SMS”

Ania masz płatność blikiem?

Tak

Oplacisz mi cos bo mam juz limit? Odesle Ci szybkim przelewem z nawiazka za pomoc

Nie na sprawy, daj dane, nr telefonu

Wiesz co mam juz dane wpisane na stronie to mi tylko kod podasz

Dasz rade dwa razy po 500?

poniedziałek, 8 stycznia

DHL: Przesyłka PL258626323BD podlega opłatom celnym (2,99 zł), przejdź do https://dhl24.com.pl, aby wznowić dostawę.

Blik

Text Message
Today 19:08

BLIK. Ktos wyslal ci przelew na telefon 450zl, skorzystaj z ponizszego linku do odbioru srodkow:
https://4.fo/blik

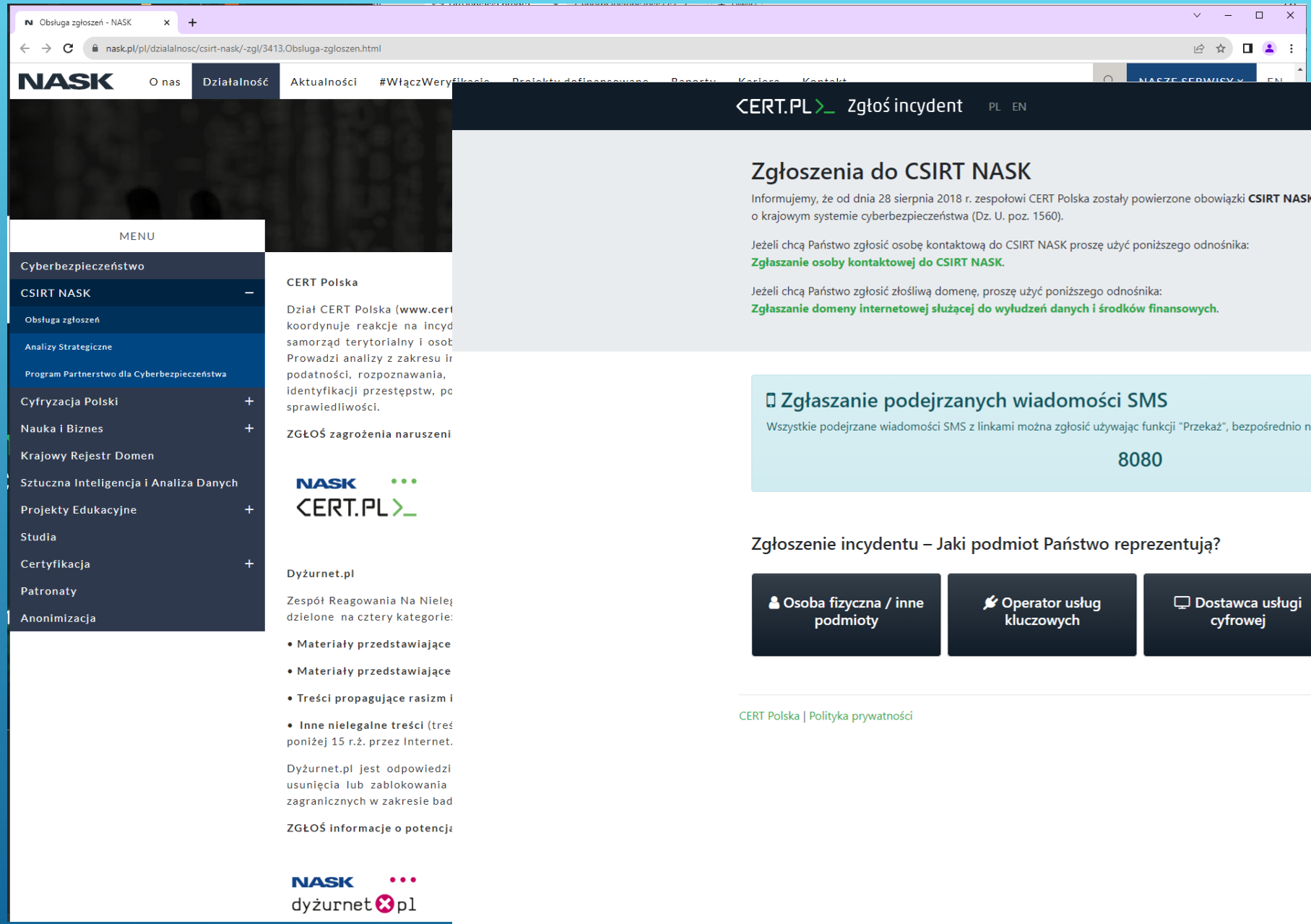
środa, 16 marca 2022

PGE-obrot: Na dzien 16.03 zaplanowano odlaczenie energii elektrycznej! Prosimy o uregulowanie naleznosci: https://4.fo/fy3rtj2 07:22

Masz niezaplacony mandat karny !
W dn. 13.04.2021 sprawa zostanie skierowana do sadu.
Kwota: 10,00 PLN
Zaplac teraz: https://urzadkarny.net/193827 16:27

Komornik powiadamia
o rozpoczęciu postępowania
z tytułu nieuregulowania długu
w kwocie 2,37 PLN.

Istnieje możliwość dobrowolnej spłaty tu dluznik-pl.tk/154431


Obsługa zgłoszeń - NASK
nask.pl/pl/dzialalnosc/csirt-nask/-zgl/3413,Obsluga-zgloszen.html
NASK
O nas
Działalność
Aktualności
MENU
Cyberbezpieczeństwo
CSIRT NASK
Obsługa zgłoszeń
Analizy Strategiczne
Program Partnerstwo dla Cyberbezpieczeństwa
Cyfryzacja Polski
Nauka i Biznes
Krajowy Rejestr Domen
Sztuczna Inteligencja i Analiza Danych
Projekty Edukacyjne
Studia
Certyfikacja
Patronaty
Anonimizacja
CERT Polska
Dyżurnet.pl
ZGŁOŚ informacje o potencj

CERT.PL Zgłoś incydent
PL EN
Zgłoszenia do CSIRT NASK
Informujemy, że od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki CSIRT NASK wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).
Jeżeli chcą Państwo zgłosić osobę kontaktową do CSIRT NASK proszę użyć poniższego odnośnika:
Zgłaszanie osoby kontaktowej do CSIRT NASK.
Jeżeli chcą Państwo zgłosić złośliwą domenę, proszę użyć poniższego odnośnika:
Zgłaszanie domeny internetowej służącej do wyłudzeń danych i środków finansowych.
Zgłaszanie podejrzanych wiadomości SMS
Wszystkie podejrzane wiadomości SMS z linkami można zgłosić używając funkcji "Przekaż", bezpośrednio na numer:
8080
Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?
Osoba fizyczna / inne podmioty
Operator usług kluczowych
Dostawca usługi cyfrowej
Podmiot publiczny
CERT Polska | Polityka prywatności

RANSOMWARE W LPR LPR WARSZAWA

Atak na LPR

14 lutego 2022

Szyfrowanie Dokumentacji

Algorytm szyfrowania to **AES** o kluczu **256** bitowym.

Teoretyczny czas odszyfrowywania to **$3x10^{51}$** lat*

Przy założeniu sprawdzania 10^{18} kluczy na sekundę.

Atak typu Ransomware – wirus/aplikacja Mallware ETAPY :

Krajowe Centrum Monitorowania Ratownictwa Medycznego

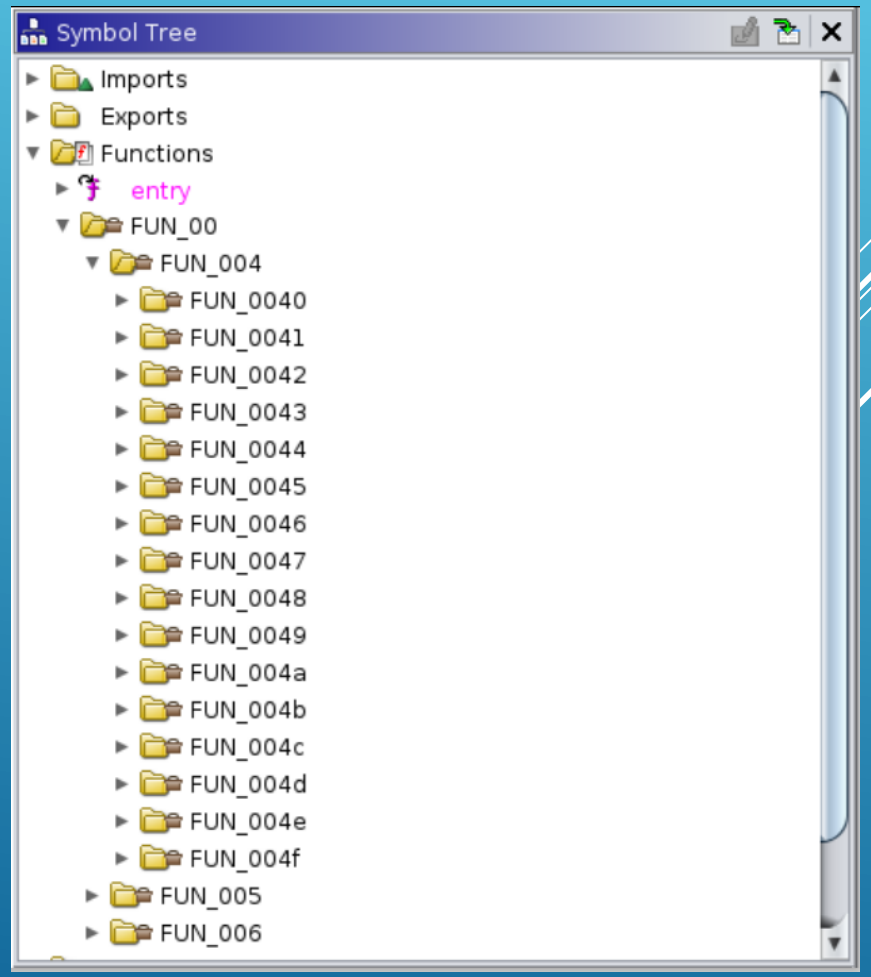
PIERWSZY – ZARAŻENIE - poprzez celowany atak na usługę serwera pocztowego. Zaatakowano serwer pocztowy „LOTUS" wykorzystując podatność umożliwiającą przejęcie kontroli nad serwerem, który jako zaufany członek domeny (AD) „otworzył" dostęp do pozostałych hostów w domenie w tym do wszystkich końcówek użytkowników.

DRUGI – DYSTRYBUCJA – po przejęciu metod dostępu do końcówek i serwerów sieci lokalnej LPR należy założyć iż szkodliwe oprogramowanie zostało rozprowadzone do wszystkich stacji dostępnych w sieci. Infekowane byłu stacje z systemem WINDOWS lub WINDOWS SERWER jednak nie można wykluczyć, że hosty z systemem linux mogą służyć jako stacje pośredniczące w dystrybucji oprogramowania szkodliwego.

TRZECI etap – USUWANIE BACKUPU – w LPR zastosowano nieodmijscowioną kopię bezpieczeństwa na dedykowane urządzenie dyskowe QNAP (macierz z 4 dyskami). Dane z dysków zostały usunięte w dniu ataku co utrudnia (na razie nie ma informacji o odzyskaniu kopii) odtworzenie danych z kopii bezpieczeństwa. Może to być niemożliwe.

CZWARTY – SZYFROWANIE – prawdopodobnie między piątkiem a niedzielą rozpoczął się ostatni etap ataku ransomware – szyfrowanie zarażonych stacji. Zaszyfrowane stacje udostępniają jedynie plik tekstowy z informacją o wysokości okupu. Należy pamiętać, iż w przypadku ataków ransomware oprócz samego zaszyfrowania danych dochodzi także do wycieków danych – te pomimo zapłacenia okupu nigdy nie wracają do właściciela i mogą zostać opublikowane bądź sprzedane w każdym momencie po ataku.

a. Skutek ataku
   i. – wyciek danych i utrata kontroli nad ich dystrybucją.
   ii.– utrata kopii zapasowych i ew. archiwów poprzez wykasowanie zawartości nośników
   iii.– zaszyfrowanie stacji roboczych i serwerów – uniemożliwienie pracy
b. Zasięg ataku - sieć lokalna i zasoby LPR. Wg. relacji P. Pawła Bąkały KCMRM nie zostało zaatakowane i centrum monitorowania pracuje.



```
10 undefined8 davV_z4M.Cm2rihik(void)
11
12 {
13   undefined8 uVar1;
14   longlong unaff_R14;
15   undefined8 local_30;
16   undefined8 uStack40;
17   code *local_20;
18   undefined8 *puStack24;
19   code **local_10;
20
21   if (*(undefined **)(ulonglong *)(unaff_R14 + 0x10) <= &stack0xfffffffffffffff8 &&
22       &stack0xfffffffffffffff8 != *(undefined **)(ulonglong *)(unaff_R14 + 0x10)) {
23     local_20 = davV_z4M.Cm2rihik.func1;
24     puStack24 = &local_30;
25     local_10 = &local_20;
26     runtime.makeslice(0x300000);
27     uStack40 = 0x300000;
28     VL8ntQFo.DSZ9f39L();
29     local_30 = 0x300000;
30     (**local_10)();
31     return 0;
32   }
33   runtime.morestack_noctxt();
34   uVar1 = davV_z4M.Cm2rihik();
35   return uVar1;
36 }
37
```

Przełom

```
puVar11 = (undefined8 *)register0x00000020;
if (*(ulonglong *)(unaff_R14 + 0x10) <= (longlong)&local_5da + 2U &&
    (longlong)&local_5da + 2U != *(ulonglong *)(unaff_R14 + 0x10)) {
  puVar11 = &local_658;
  local_250 = time.Now();
  if (local_250 < 0) {
    unaff_RBX = ((ulonglong)(local_250 << 1) >> 0x1f) + 0xdd7b17f80;
  }
  local_4b0 = (undefined4 *)
              ((longlong)(int)((uint)local_250 & 0x3fffffff) + unaff_RBX * 1000000000 +
              -0x5e4dfc14c2e60000);
  math/rand.(*Rand).Seed();
  uVar5 = davV_z4M.Cm2rihik();
  if (_DAT_008413c0 == 0) {
    *in_RAX = uVar5;
  }
```

Symbol Tree

- c
- d
- DMTZQkvC.
- e
- f
- FUN_00
- go
- I9CkVdRz.
- i
- log.
- LTz1qNb5.
- m
  - ma
    - main.main
    - math
  - memeqbody
  - mfkf5hcf.
- net.
- os
- path
- r
- s
- t
- unicode

postgres | encrypted_files | *<postgres> Script ×

```
select
ROUND(decrypted / 1024 / 1024 / 1024 / 1024, 2) as decrypted_tb,
ROUND(total / 1024 / 1024 / 1024 / 1024, 2) as total_tb,
ROUND(decrypted * 100 / total, 2) percentage_decrypted
from (
select
sum(filesize) filter (where decrypted) DECRYPTED,
sum(filesize) TOTAL
from encrypted_files ef
)r;
```

Results 1 ×

select ROUND(decrypt | Enter a SQL expression to filter results

Grid | Text

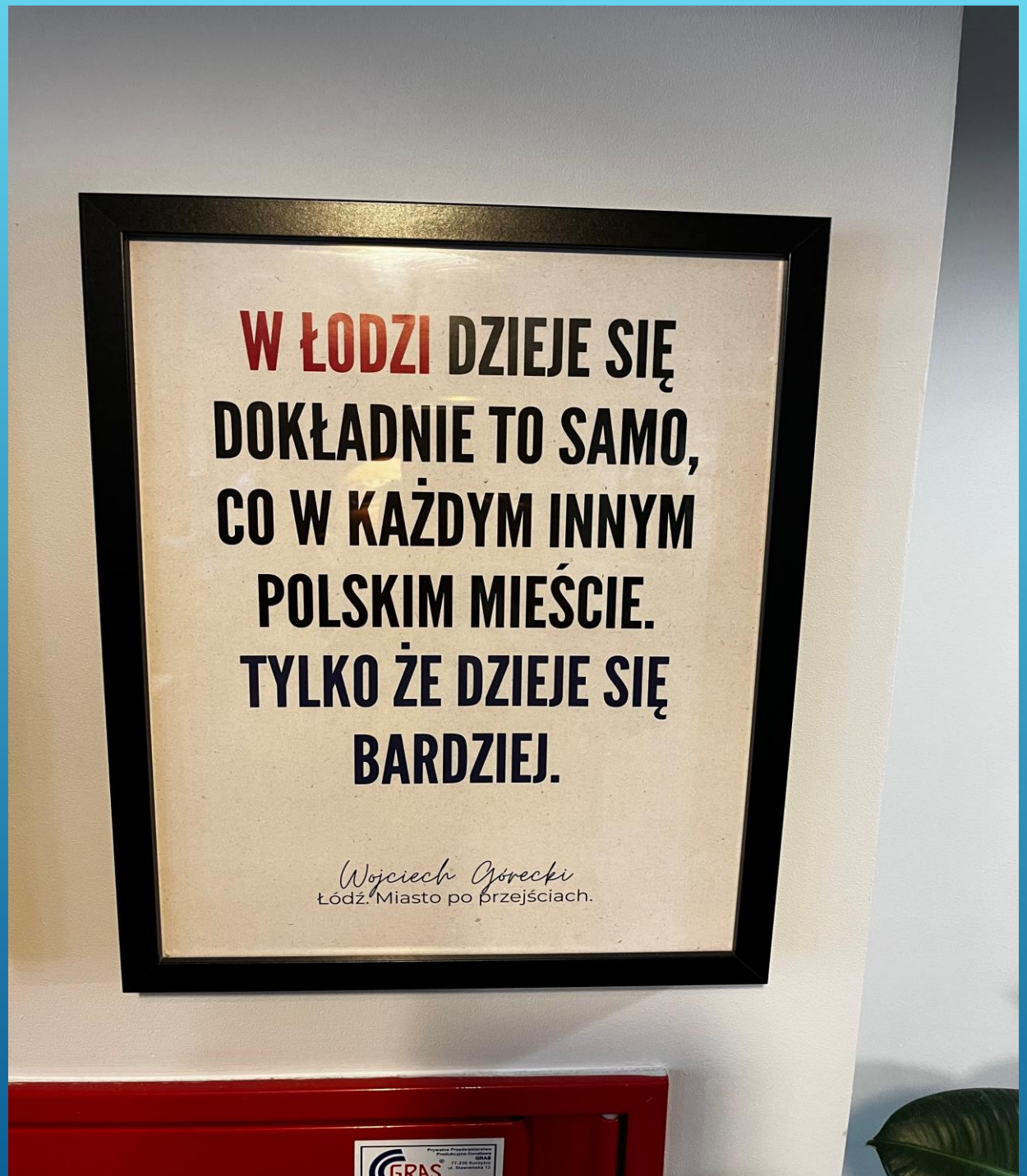
	decrypted_tb	total_tb	percentage_decrypted
1	2.08	2.09	99.67

Value ×

2.08

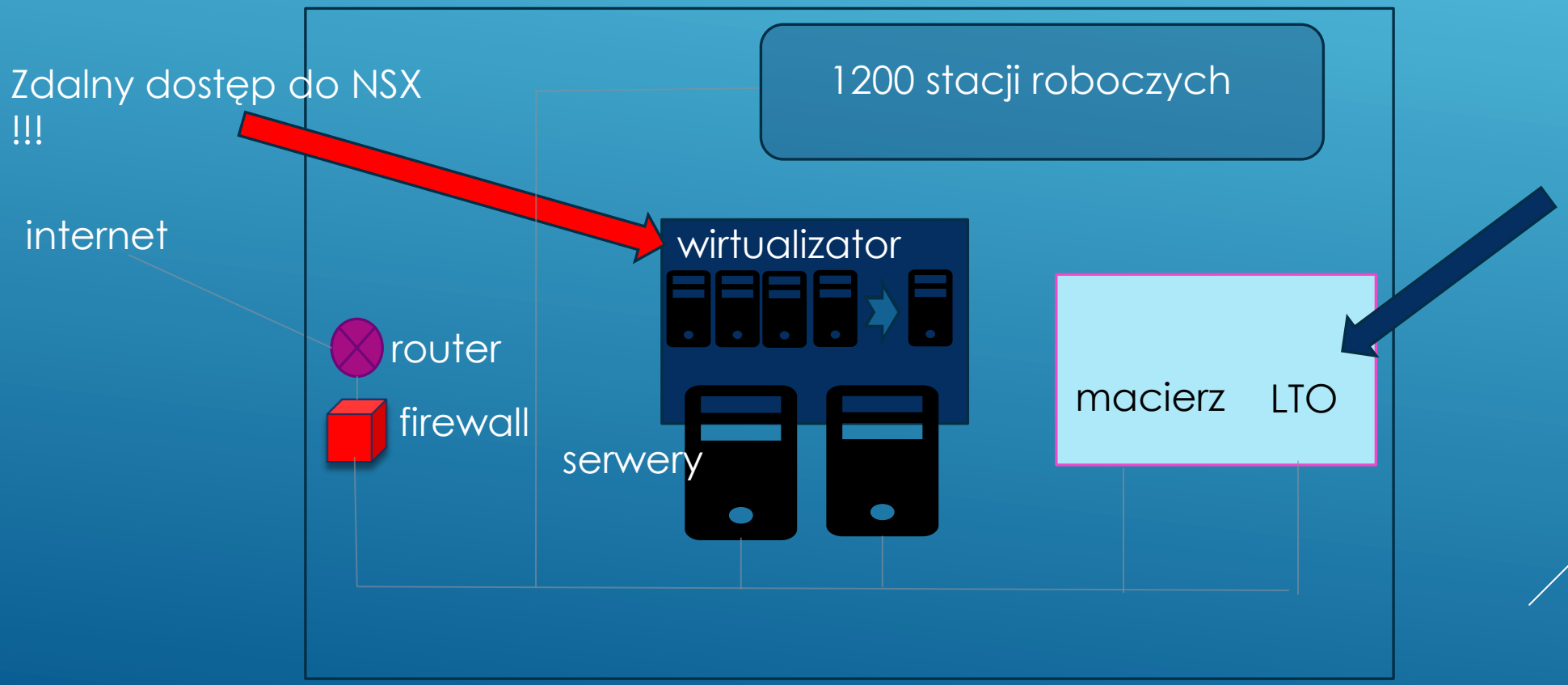
Koniec

RANSOMWARE W SZPITALU CZMP ŁÓDŹ


W ŁODZI DZIEJE SIĘ
DOKŁADNIE TO SAMO,
CO W KAŻDYM INNYM
POLSKIM MIEŚCIE.
TYLKO ŻE DZIEJE SIĘ
BARDZIEJ.
Wojciech Górecki
Łódź. Miasto po przejściach.

Infrastruktura zastana:

1. Na brzegu sieci stoi router – bez logów, wyłącznie ACL
2. Serwery na wszystkich portach wystawione do sieci Internet
3. Segmentacja sieci na poszczególne VLAN`y bez ograniczenia ruchu pomiędzy podsieciami = segmentacja na papierze
4. Ruch do Internetu bez ograniczeń
5. Antywirus na stacjach roboczych
6. Brak ochrony zasobów serwerowych



SYSTEMY IT W SZPITALACH

SYSTEM OPROGRAMOWANIA DLA SZPITALA

SYSTEM KADROWO-PŁACOWY;

LABORATORIUM;

APTEKA;

SYSTEMY DIAGNOSTYKI OBRAZOWEJ.

WSZYSTKIE NA SERWERACH WIRTUALNYCH

a. Skutek ataku
   i. – wyciek danych i utrata kontroli nad systemami.
   ii.– brak kopii zapasowych możliwych do odczytania i ew. archiwów poprzez zaszyfrowanie zawartości nośników
   iii.– zaszyfrowanie stacji roboczych i serwerów – uniemożliwienie pracy
b. Zasięg ataku - sieć lokalna i zasoby serwerowe szpitala.

c. Wektor ataku – przełamanie zabezpieczeń podmiotu trzeciego i wykorzystanie danych logowania do szpitala. Podmiot od kilku miesięcy nie miał już umowy o współpracę ze szpitalem.

Re: Instytut Centrum Zdrowia Matki Polki (ICZMP) - status 10.11.2022

MP

Masiarz Paweł <p.masiarz@mz.gov.pl>
Do Grzegorz Lewczuk; Łożyński Roman
DW Węcławik Piotr; Kikosicki Paweł; Matyjasik Piotr; Piotr Bednarski

Odpowiedz | Odpowiedz wszystkim | Prześlij dalej | ...

pt. 11.11.2022 07:58

1. HIS – system uruchomiony. Trwa konfiguracja wydruków. SOR+Izba Przyjęć w szpitalu już działa w oparciu o system na 16 stanowiskach roboczych. Dane i konta użytkowników odzyskane. HIS z wydrukami uruchomiony w SOR, IZBIE PRZYJĘĆ, Zakład Patomorfologii, uruchomiony moduł do rozliczeń z NFZ (dział FK). Prace nad pozostałymi końcówkami systemu w toku (konfiguracja wydruków). Uruchomiono kolejnych 30 stanowisk roboczych (zakład patomorfologii + dodatkowe stanowiska SOR + dodatkowe stanowiska Izba Przyjęć) **uruchomiono komputery w AOS (6 sztuk) (poradnie - w pełni można realizować zadania podstawowe - porady lekarskie, recepty, skierowania, EDM)**

   Uruchomiona Klinika Neonatologii (stacja lekarska/pielęgniarska/sekretariat zostały uruchomione) skanujemy kolejne krytyczne oddziały jednostki do uruchomienia:
   1. Kliniki Ginekologii Bud A - skanowanie dzisiaj do uruchomienia 11.11(10 stanowisk)
   2. Kliniki Położnictwa Bud A - skanowanie dzisiaj do uruchomienia 11.11(10 stanowisk)
   3. Klinika Pediatrii - Prof. Zeman na Bud B - skanowanie 11.11.2022
   4. Kardiologia Bud B i A - budynek A dzisiaj - budynek B skanowanie 11.11.2022

2. LAB – system całkowicie zaszyfrowany, brak backupu danych. System należy zainstalować na nowo. – nie uruchomiony Dane odszyfrowano, trwa rozpoznawanie zakresu odzyskanych danych (baza danych (silnik bazy), jej lokalne kopie)

3. PACS (obrazówka) – dane odzyskane. Od 6.11 trwa odtwarzanie powiązań między obrazami i ich indeksami. System uruchomiony. Dane są dostępne. Trwają kolejne prace konfiguracyjne. (CGM konfiguruje dalej środowisko - podpinanie przestrzeni z obrazami. Konieczne jest również przeadresowywanie tych zasobów wraz z poprowadzeniem do nich sieć VLAN.) **połączono udziały z obrazami**

   11.11 zakończy się weryfikacja i wykonane zostanie podłączenie portów aparatów. Infrastruktura PACS będzie już dostępna w sieci szpitala.

4. Apteka – system zaszyfrowany w całości. System jeszcze nie oddany do użytku. Spis z natury w aptece zakończony . **Dostarczono 4 stanowiska - obecnie jeszcze trwa konfiguracja systemu, import kontrahentów/stanów magazynowych/słowników Clininet (HIS) - 9 listopada wg producenta przewidywany jest start aplikacji.**
   pracownicy firmy MCArt przygotowują wsparcie stanowiskowe dla personelu Apteki. prace zgodnie z harmonogramem skonfigurowano bazę danych oraz jesteśmy w trakcie importu danych z FK oraz HIS.
   ze względu na konieczne korekty w bilansie czas do uruchomienia w całości został wydłożony do 13.11.2022
   TRwa WERYFIKACJA IMPORTÓW
   MOŻNA WPROWADZAĆ FAKTURY
5. System FK, Kadry-płace –**system uruchomiony i funkcjonuje na 15 stanowiskach roboczych.**
6. Usługi podstawowe sieci LAN – DHCP,DNS – wykonano usługi działają
7. Usługi podstawowe domena użytkowników (AD) – reinstalacja serwera wykonana, import użytkowników z M365 wykonany trwa odtwarzanie struktury katalogów rekonfiguracja ok 1900 kont trwa migracja stacji roboczych na One Drive.
8. Repozytorium EDM – zaszyfrowane w całości. Brak możliwości odzyskania danych w wersji z repozytorium. Konieczne ponowne generowanie dokumentów i ponowne podpisanie cyfrowe. Po zakończeniu odzyskiwania Laboratorium podjęta zostanie próba odszyfrowania danych EDM – w ciągu 48 godzin.
9. Przeprowadzono szkolenie osób zarządzających w zakresie cyberbezpieczeństwa – 7.11.2022 (Jeremi Olechnowicz) - **zrealizowane**

Stan stacji roboczych szpitala

1. Przygotowanie na wyczyszczenie 1200 stanowisk roboczych z infekcji - migracja plików do chmury MS (OneDrive) - w procesie kluczowe stanowiska kadry zarządzającej (kierownicy klinik) - zakończono migrację - część administracyjnej: Kadry/Płace/Księgowość. pozostali realizowani będą w dalszych etapach wymiany czystych stanowisk pracy

   - wymieniono 4 komputery (Izba Przyjęć, pielęgniarka naczelna) **+ 15 komputerów (Apteka, SOR/Izba Przyjęc/Zakład Patomorfologii) + 30 komputerów + 10 komputerów + 3 PC**

   - przeskanowano 60 komputerów. **+ 20 stanowisk + 40 PC**

Roman Łożyński

RANSOMWARE W SZPITALU GIŻYCKO

Status na 2022-07-19 godz.:13:00

Otrzymanie informacji o ataku na podmiot.

W dniu 2022-07-19, około godziny 13.00 Departament Bezpieczeństwa otrzymał informację o możliwym skutecznym ataku na szpital w Giżycku - Szpital Giżycki sp. z o.o.

Po kilku telefonach udało się skontaktować z jedynym informatykiem w szpitalu, który był akurat w trakcie prac w serwerowni. Informatyk potwierdził udany atak, który zaszyfrował:

- serwer plików na serwerze z OS Windows Server;

- serwery z OS Windows Server oraz stojący na nich system kopii zapasowych, w tym same kopie zapasowe;

- inne serwery z OS Windows Server;

Początkiem ataku mogła być stacja robocza na Szpitalnym Oddziale Ratunkowym – antywirus podobno „coś" wykrył na niej. W opinii informatyka udało się atak przerwać w trakcie szyfrowania. Systemy stojące na OS rodziny Linux nie zostały dotknięte tym atakiem. Dane medyczne były przechowywane właśnie na tych serwerach. W trakcie rozmowy informatyk stwierdził, że nadal próbuje uzyskać dostęp do kopii zapasowych.

Wszystkie pozostałe systemy, które w opinii Informatyka nie zostały dotknięte atakiem ransomware zostały poddane skanowaniu antywirusowemu.

Alarmujące w tym incydencie jest iż podmiot ten wypełniając w okresie 04.2022 – 06.2022 ankietę badającą dojrzałość podmiotu w kontekście cyberbezpieczeństwa zaznaczył odpowiedzi:

W91. INFRASTRUKTURA (IN), Kopia zapasowa (IN.5), IN.5.1 Kopia odmiejscowiona

TAK

96/1

W92. INFRASTRUKTURA (IN), Kopia zapasowa (IN.5), IN.5.2 Napęd taśmowy (biblioteka taśmowa)

TAK

97/1

W93. INFRASTRUKTURA (IN), Kopia zapasowa (IN.5), IN.5.3 System kopii zapasowej izolowany od środowisk produkcyjnych

TAK

Niniejszy incydent wskazuje, iż kopia zapasowo nie była izolowana od środowiska produkcyjnego, nie ma także pewności czy faktycznie skutecznie były stosowane biblioteki taśmowe oraz nie było kopii odmiejscowionych lub jeśli są to nie pozwalają one na skuteczną odbudowę środowisk.

Ten przypadek może wskazywać na naginanie rzeczywistości w odpowiedziach ankietowych. Obraz poziomu cyberbezpieczeństwa w sektorze zdrowia uzyskany dzięki ankiecie może więc być zakłamany poprzez tuszowanie bądź naginanie stanu faktycznego.

Status na 2022-08-08 godz.: 15:00

- NASK jest w trakcie analizy próbki malware aczkolwiek szanse na uzyskanie kluczy szyfrujących oceniane są na niskie.

- Odzyskanie plików z shadow copy bez postępów. Informatyk podejmuje kolejne próby.

Status na 2022-08-11 godz.: 16:00

- NASK - Brak postępu w analizie malware.

- Odzyskanie plików z shadow copy bez postępów. Informatyk podejmuje kolejne próby.

- Podmiot zakupił aplikację typu OCR. Utracone dokumenty będą odzyskiwać z wersji wydrukowanych.

- Informatyk wprowadza dodatkowe konfiguracje ograniczające skutki ewentualnego ponownego ataku.

przez NFZ.

5. Wnioski

Posiadany w podmiocie backup nie był skonfigurowany zgodnie z najlepszymi praktykami. Był w tej samej podsieci więc nie był izolowany od środowiska produkcyjnego. Nie było też kopii na bibliotekach taśmowych oraz nie było kopii odmiejscowionych. Utracono całą kopię zapasową danych przetrzymywaną na systemie Windows Server. Szczęśliwie nie było tam kopii danych białych.

Pomimo wsparcia zespołu CSIRT NASK nie udało odzyskać kluczy szyfrujących, tym samym nie udało się odszyfrować danych.

WYCIEK DANYCH ALAB

CYBERBEZPIECZEŃSTWO

Atak na ALAB Laboratoria. Zagrożone dane nawet 200 tysięcy pacjentów

MICHAŁ GÓRSKI
07.12.2023 16:30

Fot. CyberDefence24.pl

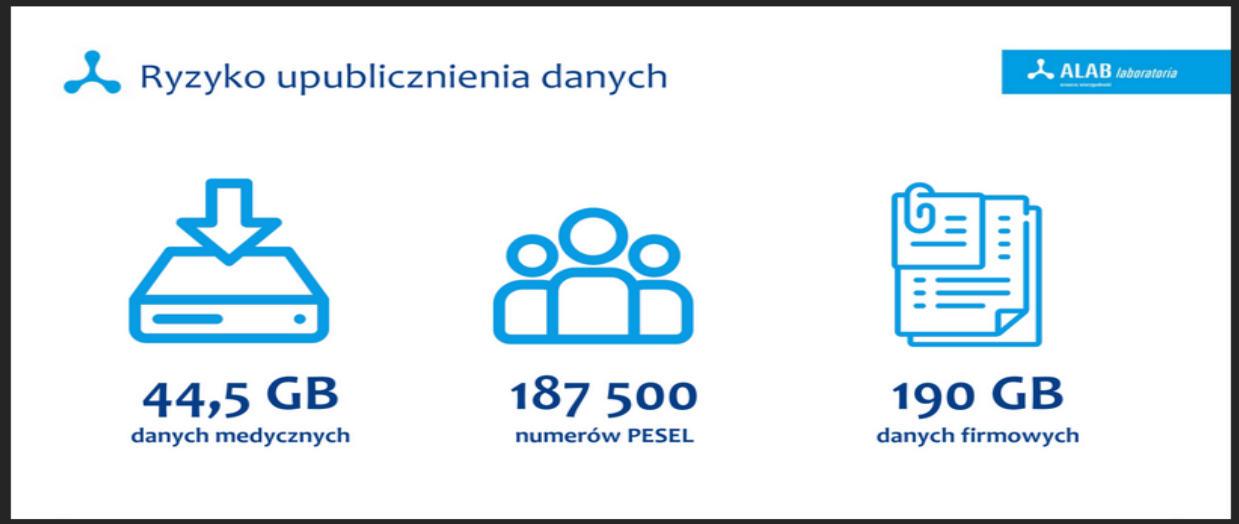
Firma ALAB Laboratoria kika dni temu oficjalnie potwierdziła wyciek danych. Wcześniej nieoficjalnie było wiadomo, że dotyczy to ponad 55 tys. różnych badań. Jak wynika z informacji CyberDefence24, „w najgorszym scenariuszu upublicznieniem danych osobowych i wyników badan laboratoryjnych zagrożonych jest nawet 200 tys. pacjentów", na co wskazuje dr Seweryn Dmowski z ALAB Laboratoria.

czwartek zorganizował śniadanie prasowe, na którym odsłonił niektóre kulisy incydentu. Bardzo chwalimy to podejście – dzięki otwartości można własną katastrofę zamienić w lepszą naukę dla innych podmiotów, z korzyścią dla całego społeczeństwa. Ręce składają się do oklasków, ale z oklaskami poczekajmy.

Skala wycieku

Zacznijmy od informacji najważniejszej, na którą wszyscy czekają, czyli ile danych wyciekło. Spekulacje były zatrważające – ALAB sam ogłaszał, że przeprowadza miliony badań rocznie. Na szczęście wszystko wskazuje na to, że włamywacze odnieśli jedynie umiarkowany sukces, ponieważ zgodnie z informacjami ALAB-u wykradli dane 187 500 osób. To dużo, ale też dużo mniej, niż można się było spodziewać.

Dlaczego włamywacze nie sięgnęli po więcej informacji? Okazuje się, że w trakcie włamania dostali się tylko do jednego z serwerów przechowujących dane pacjentów. Znaleźli tam 44,5 GB danych medycznych, z których fragment opublikowali w listopadzie w ramach szantażu. Ukradli także 190 GB danych firmowych, ale te są mniejszym zmartwieniem dla naszych czytelników.



Czy możemy zaufać tym szacunkom ALAB-u? Wszystko wskazuje na to, że tak – rozmiar wykradzionych danych zgadza się z zakresem informacji przechowywanych na zaatakowanym serwerze. Większość klientów ALAB-u może zatem spać w miarę spokojnie.

https://zaufanatrzeciastrona.pl/post/co-stalo-sie-w-alab-ie-czyli-jakie-zabezpieczenia-nie-chronia-przed-hakerami/

ásku zakładek, aby mieć do nich szybki dostęp. Zarządzaj zakładkami...

Przebieg ataku

Chronologia zdarzeń udostępniona przez ALAB zaczyna się około godziny 1 rano 19 listopada 2023. Pojawiają się wtedy problemy z dostępem do usług Microsoft Office 365. Ok. 2:30 okazuje się, że problem leży w niedostępnym kontrolerze domeny. IT przystępuje do przywrócenia kontrolera domeny z kopii bezpieczeństwa, co kończy ok. 3:50. Wtedy też zauważono pierwsze oznaki szyfrowania danych i podjęto decyzję o wyłączeniu systemów. Od 4:00 pracują wszyscy dyżurni administratorzy i od 4:30 zaczyna się odzyskiwanie danych z backupów. O 5:06 wezwana na pomoc zostaje firma CyberBLOCK. O 8:00 zbiera się zarząd firmy wraz z Komitetem Bezpieczeństwa. O 11:36 zostaje odczytana notatka z żądaniem okupu. O 20:43 firma dowiaduje się, że część danych została umieszczona w sieci. Prawdziwość wykradzionych danych potwierdza o godzinie 23:00.

21 listopada ALAB zgłasza naruszenie bezpieczeństwa informacji do UODO, powiadamia policję i zespół CERT Polska. 27 listopada, kilkanaście godzin po naszym artykule, pojawia się publiczny komunikat o incydencie.

Ujawnienie przebiegu ataku oraz szybkie zgłoszenie incydentu do UODO i do CERT Polska to bardzo pozytywne działanie – za to także należy ALAB pochwalić.

Nie negocjujemy z terrorystami

Skoro już ALAB chwalimy, to jeszcze trzeci powód, by to zrobić – ALAB odmówił zapłacenia okupu. To zawsze trudna decyzja, ale odcięcie źródeł dochodu przestępców przebywających najczęściej w dzikich krajach, jak Rosja, poza zasięgiem naszej jurysdykcji, to jeden z niewielu mechanizmów mogących ograniczyć skalę problemu ransomware. Oklaski zatem należne.

Zaraz, czegoś tu brakuje

Teraz napiszmy, czego nie wiemy. Harmonogram zdarzeń pokazany przez ALAB zaczyna się długo po samym ataku. Co działo się przed 19 listopada? Jak włamywacze dostali się do sieci? Jak ją penetrowali? Dlaczego nikt ich nie zauważył, zanim ukradli dane? Dlaczego nawet proces kradzieży łącznie ponad 200 GB danych nie został zauważony i zatrzymany? Na te pytania niestety nie znamy odpowiedzi. Zapytaliśmy oczywiście o to ALAB, lecz od od wczoraj trwa tam kontrola UODO i firma nie jest najwyraźniej skłonna do opisywania tych zdarzeń w prasie, woli przekazać swoją wiedzę bezpośrednio kontrolerom.

WŁAMANIA DO ZUS/RPWDL/P1 CEZ/ZUS


RPWDL
Rejestr Podmiotów Wykonujących Działalność Leczniczą
Zaloguj się
Strona główna
Wyszukiwarki
Pliki do pobrania
Informacje o rejestrze
Polityka prywatności
Deklaracja dostępności
Częste pytania (FAQ)
Kontakt
Wyszukiwanie Podmiotów Leczniczych
Wyszukiwanie Praktyk Zawodowych Lekarzy i Lekarzy Dentystów
Wyszukiwanie Praktyk Zawodowych Pielęgniarek i Położnych
Wyszukiwanie Praktyk Zawodowych Fizjoterapeutów
Aktualności
1 2 3 4 5 6 7 8 9 10 ... » »»
Start nowego rejestru praktyk zawodowych Diagnostów Laboratoryjnych
Szanowni Państwo,
już 10 listopada bieżącego roku startuje nowy rejestr praktyk zawodowych Diagnostów Laboratoryjnych. Wynika to z wejścia w życie ustawy o Medycynie Laboratoryjnej z dnia 15 września 2022 roku (Dz.U. z 2023 r. poz. 2125) w zakresie RPWDL. Do obsługi nowego rejestru zostanie uruchomiony system w wersji 2.0: rpwdl2.ezdrowie.gov.pl (strona została uruchomiona 10 listopada 2023 roku). Pozostałe rejestry zarówno podmiotów leczniczych jak i praktyk zawodowych lekarzy, pielęgniarek i fizjoterapeutów nadal będą obsługiwane przez dotychczasowy system: rpwdl.ezdrowie.gov.pl.
Instrukcje obsługi nowego systemu można zobaczyć klikając następujące odnośniki:
Instrukcja użytkownika systemu RPWDL 2.0 dla praktyk zawodowych Diagnostów Laboratoryjnych
Instrukcja użytkownika systemu RPWDL 2.0 dla osób niezalogowanych
Filmy wizualizujące obsługę systemu dostępne są również na platformie You Tube: filmy instruktażowe RPWDL 2.0 Centrum e-Zdrowia
dodano [2023-10-27] , zaktualizowano [2023-11-10]
Aktualizacja systemu RPWDL 1.0 w dniu 9 listopada
Szanowni Państwo,
informujemy, że ze względu na aktualizację systemu RPWDL 1.0 związaną z uruchomieniem nowej wersji systemu (RPWDL 2.0) w dniu 9 listopada br. w godzinach 16:00 – 18:00 system może być niedostępny.
Więcej informacji o uruchomieniu RPWDL 2.0 można przeczytać w tym komunikacie.
Przepraszamy za utrudnienia
dodano [2023-11-03] , zaktualizowano [2023-11-06]
Badanie opinii o portalu ezdrowie
Chcemy poznać Twoją opinię o portalu e-zdrowie.gov.pl, żeby lepiej dostosować go do Twoich potrzeb. Jak z niego korzystasz? Co powinniśmy zmienić, żeby ułatwiał Ci poruszanie się w systemie ochrony zdrowia i wspierał w pracy? Podziel się Twoją opinią. Możesz to zrobić do 27 października.
Wypełnij krótką ankietę.
dodano [2023-10-16] , zaktualizowano [2023-10-16]
Aktualizacja systemu RPWDL w dniu 13 września
Szanowni Państwo,
informujemy, że w związku z aktualizacją systemu RPWDL w dniu 13 września br. w godzinach 17:00 – 19:00 system może być niedostępny.
Ten serwis korzysta z plików cookies. Brak ograniczenia lub wyłączenia cookies w przeglądarce internetowej oznacza zgodę na takie korzystanie (szczegółowe informacje znajdują się w Polityce cookies)

Rejestr Podmiotów Wykonujących Działalność Leczniczą

RPWDL jest elektronicznym rejestrem prowadzonym zgodnie z ustawą o działalności leczniczej. W części publicznej Rejestru użytkownik może uzyskać informacje na temat podmiotów wykonujących działalność leczniczą, w tym:

- Podmiotów leczniczych
- Praktyk zawodowych lekarzy i lekarzy dentystów
- Praktyk zawodowych pielęgniarek i położnych

W części dostępnej po zalogowaniu, Rejestr umożliwia między innymi:

- tworzenie wniosków:
- o wpis podmiotu do Rejestru;
- o wpis zmian w Rejestrze;
- o wykreślenie podmiotu z Rejestru;
- wysłanie drogą elektroniczną podpisanego wniosku w formie elektronicznej
- pobranie zaświadczeń
- przechowywanie i późniejszy dostęp do wniosków roboczych oraz wniosków podpisanych i wysłanych drogą elektroniczną

Administratorem danych osobowych użytkowników w systemie Rejestr Podmiotów Wykonujących Działalność Leczniczą są organy prowadzące rejestr wskazane w art. 106 ustawy o działalności leczniczej:

- wojewoda właściwy dla siedziby albo miejsca zamieszkania podmiotu leczniczego — w odniesieniu do podmiotów leczniczych,
- okręgowa rada lekarska właściwa dla miejsca wykonywania praktyki zawodowej lekarza — w odniesieniu do tych praktyk,
- okręgowa rada pielęgniarek i położnych właściwa dla miejsca wykonywania praktyki zawodowej przez pielęgniarkę — w odniesieniu do tych praktyk.

•Natomiast administratorem systemu, tj. podmiotem odpowiedzialnym za techniczno-organizacyjną obsługę jest Centrum e-Zdrowia z siedzibą w Warszawie, ul. Stanisława Dubois 5A, 00-184 Warszawa.

……Aby skutecznie wystawić receptę, konieczne wykonanie jest kolejnego etapu.

…..W drugim etapie przestępcy pozyskali login i hasło do systemu RPWDL, posługując się wykradzionymi danymi do uwierzytelnienia. Najczęściej hasła i loginy do systemów są zapisywane w przeglądarkach internetowych na komputerach lekarzy, skąd są wykradane przez złośliwe oprogramowanie. Po zalogowaniu do RPWDLa przestępcy dopisują do danego podmiotu leczniczego osobę lekarza, którego certyfikat ZUS ZLA został wykradziony. ….

Wnioski:
-słabość systemu ZUS PUE, brak obligatoryjnego logowania 2FA,
-słabość systemu RPWDL, brak obligatoryjnego logowania 2FA.
…….
Istnieją prawne zapisy regulujące sposób logowania się do niektórych systemów CEZ
- brak weryfikacji relacji lekarza i podmiotu w trakcie przyjmowania recept.

……Wszystkie konta użytkowników powiązanych z kontami 7 placówek w RPWDL zostały zablokowane. Uniemożliwi ponowne zawnioskowanie o certyfikaty dostępu do P1……

FAŁSZOWANIE RECEPT

CEZ

92% lekarzy w Polsce nie stosuje podwójnego uwierzytelniania

RPWDL
Brak wieloskładnikowego uwierzytelniania

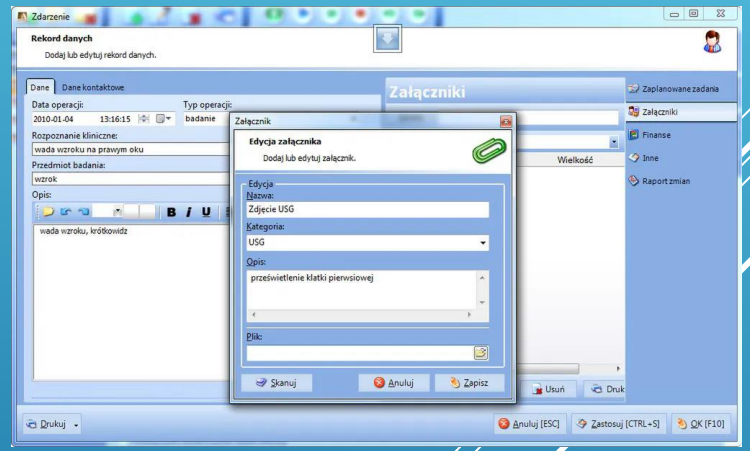
Aplikacja w podmiocie

Certyfikat podmiotu

PUE ZUS
Brak wieloskładnikowego uwierzytelniania

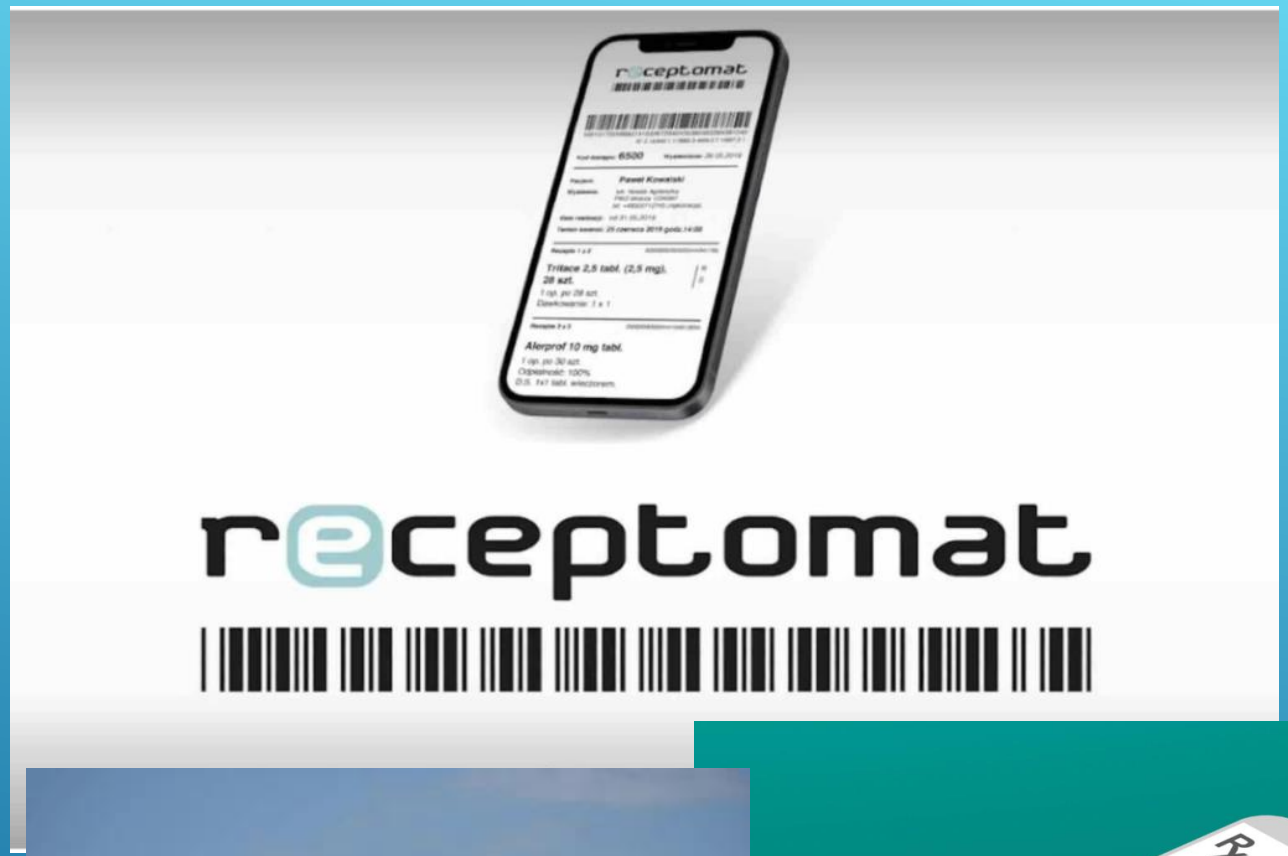
E - recepta

API P1

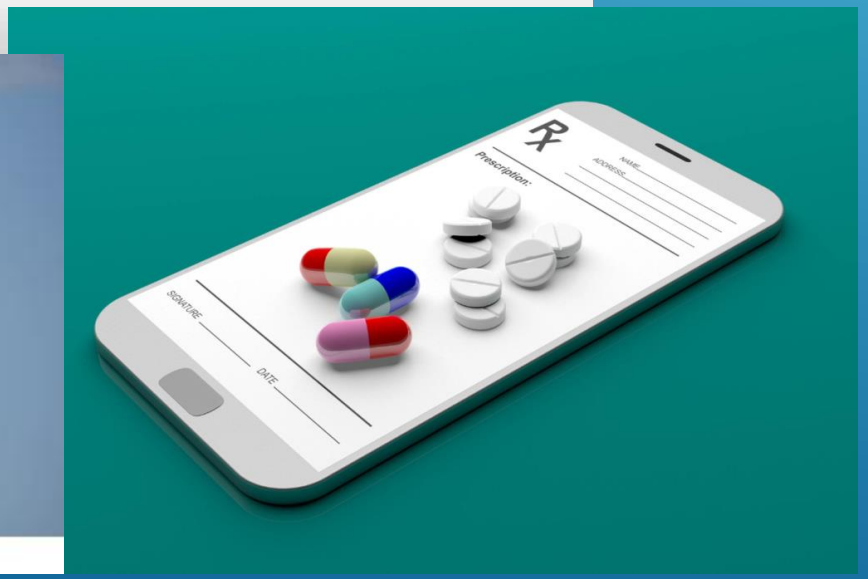


Certyfikat lekarza (npwz)

Wnioski:
-słabość systemu ZUS PUE, brak obligatoryjnego logowania 2FA,
-słabość systemu EPLOZ, brak obligatoryjnego logowania 2FA.
- obligatoryjne 2FA w EPLOZ skutkuje zmianą logowania dla kilku innych aplikacji w CEZ. Istnieją prawne zapisy regulujące sposób logowania się do niektórych systemów CEZ
- brak weryfikacji relacji lekarza i podmiotu w trakcie przyjmowania recept.


receptomat


receptomat®
shutterstock.com · 2325784265

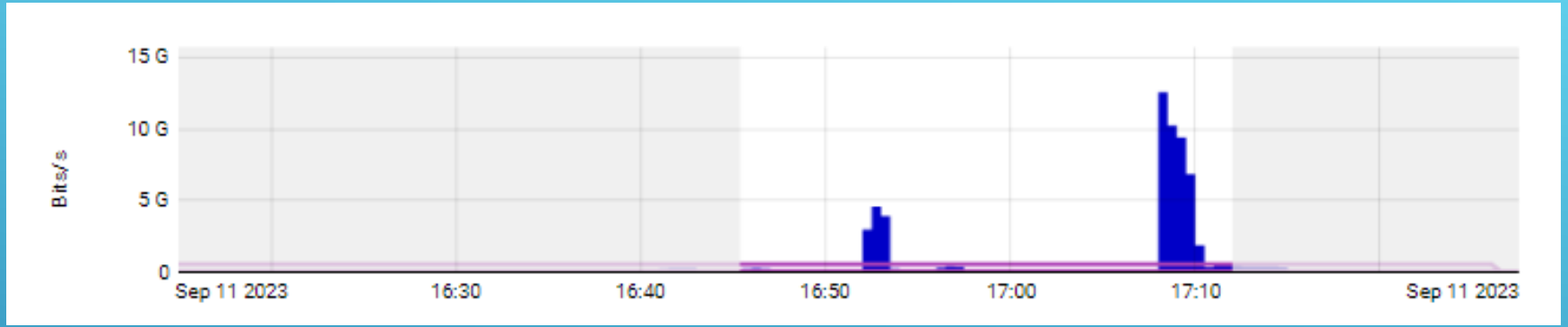

Rx
Prescription
SIGNATURE
DATE


12:37
receptomat
Niedobór Witaminy D
wyszukaj lek...
Decyduje Lekarz
Nasi lekarze na podstawie wywiadu dobiorą odpowiedni dla Ciebie lek.
Wybieram
Dekristol
cholecalciferolum
kapsułki miękkie
Wybieram
Dekristol Pro
cholecalciferolum
kapsułki twarde
Wybieram
Wybierz Przypadłość i Lek

PRZYKŁADOWE ATAKI 2022 - 24

ATAKI DDOS	CEZ 09’23
ATAKI DDOS	CEZ 01’24

11.09.2023



Atak DDoS (ang. Distributed Denial of Service) na **pacjent.gov.pl** miał miejsce w dniu 11.09.2023. Celem atakujących było spowodowanie niedostępności pacjent.gov.pl lub utrudnienie w dostępu do niej, przez wysycenie liczby wolnych sesji podłączeniowych.

Atak został wykryty automatycznie przez narzędzie antyddos operatora łącza ATMAN, które zarejestrowało znaczny wzrost ruchu przychodzącego na stronę internetową pacjent.gov.pl. Ruch ten charakteryzował się wieloma źródłami i był znacznie wyższy niż zazwyczaj. Ruch przekroczył próg blackholing 5 GBps, po którym operator łącza odcina cały ruch przychodzący do danego adresu IP.

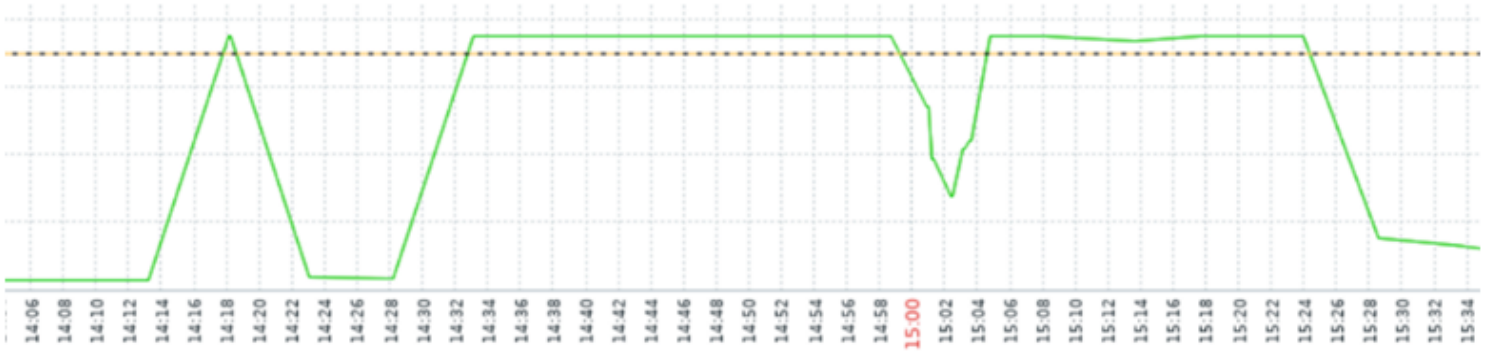
Metody ataku to : General flood All, SC:CPS - ATM1-CSIOZ-00569UDP, SC:network flood IPv4 UDP, SC:network flood IPv4 UDP-FRAG, SC:DOSS-SSL-ClearText, SC:SYN Flood HTTPS

II. Typ ataku

Atak DDoS jest typem ataku aplikacyjnego, w którym hakerzy wykorzystują rozproszone zasoby, takie jak botnety lub losowo generowane IP nadawcy, aby przeciążyć infrastrukturę aplikacyjną i uniemożliwić dostęp do strony internetowej pacjent.gov.pl.

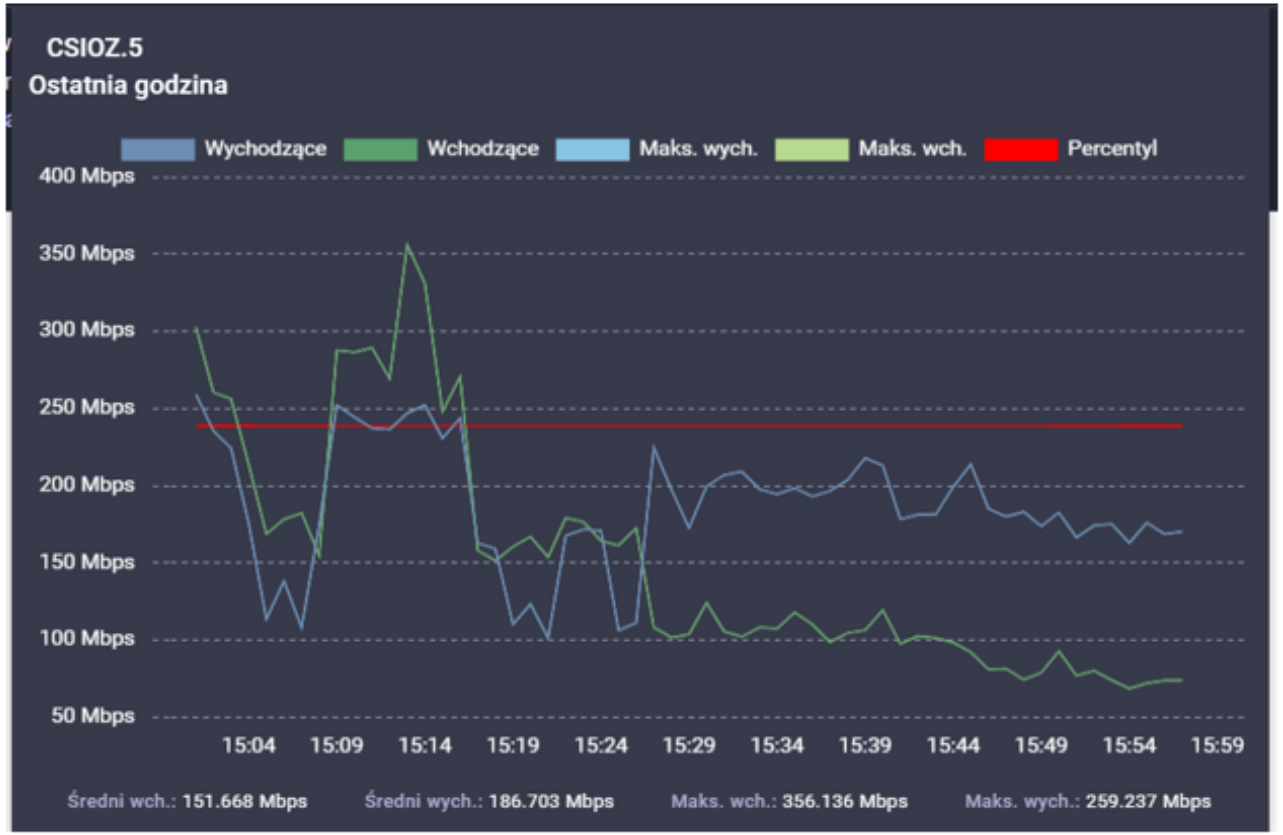
III. Czas trwania ataku

Atak rozpoczął się 13.09.2023 godz. 14:13 i trwał przez 71 min. **Niedostępność strony lub utrudnienia dla użytkowników trwały łącznie 45 minut**. Linia zielona ponad progiem oznacza wyczerpanie limitu sesji – niedostępność strony lub problemy w dostępie do niej.



IV. Wykrywanie ataku

Atak został wykryty automatycznie przez narzędzie antyddos operatora łącza ATMAN, które zarejestrowało znaczny wzrost ruchu przychodzącego na stronę internetową pacjent.gov.pl. Ruch ten charakteryzował się wieloma źródłami i był znacznie wyższy niż zazwyczaj. Ruch przekroczył próg alarmowy 200 kpps (ang. kilopackets per second – tysiące pakietów na sekundę)



V. Wpływ na działalność firmy

Atak DDoS spowodował czasową niedostępność strony internetowej pacjent.gov.pl lub utrudnienia w jej działaniu, co wpłynęło na zdolność do obsługi klientów online. Przywrócenie dostępności strony zajęło około 45 min. W czasie trwania ataku został osiągnięty limit połączeń do IKP (pacjent.gov.pl) który ustawiony jest na urządzeniach F5 na 75 tyś co mogło spowodować niedostępność portalu dla nowych połączeń.

VI. Środki zaradcze

CEZ natychmiast podjął działania w celu zneutralizowania ataku. Środki zaradcze, które zostały podjęte, obejmowały:

- Automatyczne skierowanie ruchu atakującego na serwery ochrony DDoS celem jego oczyszczenia.
- Przeanalizowano wpływ ataku na infrastrukturę przez [redacted]
- Prewencyjnie włączono mechanizmy oczyszczania ruchu po stronie operatora łącza dla IP pacjent.gov.pl
- włączenie strony statycznej pacjent.gov.pl w przypadku niedostępności CMSa. Prace i testy nad tą zmianą trwają przy wsparciu inżyniera F5 (na ten moment testy nie przechodzą pozytywnie scenariusza).

VII. Identyfikacja atakujących

Identyfikacja źródeł ataku DDoS i osób odpowiedzialnych za ten incydent jest nie możliwa z uwagi na rozproszony charakter ataku. Źródłowe IP uczestniczące w ataku są wybierane losowo i nie stanowią prawdziwego adresu nadawcy ataku.

VIII. Rekomendacje

W celu zapobieżenia przyszłym atakom DDoS, rekomendujemy podjęcie następujących kroków:

- rozważenie zwiększenia limitu sesji dla pacjent.gov.pl do 100 tyś. na F5
- włączenie ochrony antyddos w trybie transparentnym przed atakami aplikacyjnymi na urządzaniach F5 w P1.
- na urządzeniach F5 ustawiono blokowanie adresów generujących największy ruch o wartości 500% TPS.

IX. Podsumowanie

Atak DDoS na pacjent.gov.pl był poważnym incydentem, który miał negatywny wpływ na działanie strony. Działania podjęte przez CEZ pomogły w szybkim przywróceniu dostępności strony, ale należy wdrożyć kolejne mechanizmy ochronę antyddos na urządzaniach F5.

ATAK DDOS CEZ 01’24

Raport z Ataku DDoS na DNS MZ 14-17.01.2024- Podsumowanie

Data raportu: 19.01.2024

[redacted]

Wydział Centrum Operacji Bezpieczeństwa

I. Wprowadzenie

W dniach 14-17.01.2024, z różną intensywnością wystąpił atak DoS (ang. Denial of Service) na usługę DNS (ang. Domain Name System) Ministerstwa Zdrowia.

II. Typ ataku

UDP flood to atak DDoS z użyciem protokołu UDP na usługę DNS. Atak może zostać zainicjowany poprzez wysłanie dużej liczby pakietów UDP na losowe porty zdalnego hosta, tym wypadku port numer 53 serwerów DNS.

Dla dużej liczby pakietów UDP, system ofiary jest zmuszony odpowiadać wieloma pakietami ICMP Destination Unreachable, stając się w końcu nieosiągalnym dla innych klientów. Atakujący może również spreparować adres nadawcy pakietów UDP, aby zwrotne pakiety ICMP nie docierały do niego oraz ukrywając przez to również swoją tożsamość.

Atakujący podszywając się pod adresy IP z całego świata wysyłał pytania o rozwiązanie nie istniejących nazw poddomen z domeny MZ.GOV.PL.

III. Czas trwania ataku

Atak rozpoczął się 14-01-2024 godz. 23:00 i trwał przez 4 dni z różną intensywnością. **Atak nie zakłócił dostępu do stron obsługiwanych przez serwery DNS dla klientów z Polski**. Wykres poniżej obrazuje wzrost liczby pakietów (linia pomarańczowa).

IV. Wykrywanie ataku

Atak został wykryty automatycznie przez SOC CEZ, który zarejestrował znaczny wzrost ruchu przychodzącego w postaci pakietów UDP w narzędziu SIEM. Pakiety były kierowane do dwóch serwerów DNS MZ ipso.mz.gov.pl (109.197.164.20) oraz ubik.mz.gov.pl (109.197.164.36). Ruch ten charakteryzował się jednym źródłem ataku.

Na skutek zwiększonego ruchu z adresu IP 223.220.161.94 Chiny do serwerów DNS MZ polityka antyddos skonfigurowana na firewallu ograniczyła również prawidłowy ruch DNS. Polityka ddos dla parametru udp_flood miała blokować przekroczenie wartości 1k dla adresu źródłowego. Po przeanalizowaniu działania, polityka ddos dla parametru udp_flood blokowała dostęp do serwera po przekroczeniu 1k nie tylko atakującemu, ale również innym adresom, które chciały skorzystać z usługi (na okres 60s). Polityka została przełączona w tryb monitoringu (do zbierania logów w SIEM). Dodatkowo włączono parametr udp_flood w tryb blokowania wyłącznie dla określonych krajów takich jak: Chiny, Rosja.

V. Wpływ na działalność firmy

Atak nie zakłócił dostępu do stron obsługiwanych przez serwery DNS dla klientów z Polski. Serwery DNS nieprzerwanie realizowały zapytania o strony należące do MZ przez cały czas trwania ataku.

VI. Środki zaradcze

CEZ natychmiast przystąpił do analizy wykrytego ataku oraz przez cały czas monitorował stan serwerów DNS. Środki zaradcze, które zostały podjęte obejmowały wielowarstwową ochronę:

- automatyczne skierowanie ruchu atakującego na serwery ochrony DDoS/DoS celem jego oczyszczenia (ochrony antyDDoS operatora sieci). Próg uruchomienia czyszczenia jest wyznaczony na poziom 30k pakietów/s oraz włączenie czasowej geoblokady adresów IP spoza Polski;
- ochrona na urządzeniach brzegowych Firewall CEZ/MZ – polityka ochronna UDP flood i geoblokada;
- mechanizm blokujący na serwerach DNS fail2ban;
- przeanalizowano wpływ ataku na infrastrukturę MZ i CEZ.

VII. Identyfikacja atakujących

Zidentyfikowano źródło ataku, adres IP 223.220.161.94 należący do ChinaNet Qinghai Province Network (Xining, Qinghai)

VIII. Rekomendacje

Brak możliwości zapobieganiu podobnych ataków na serwery DNS. Zastosowanie wielowarstwowej ochrony ruchu przychodzącego do serwerów DNS w poprawny sposób ochroniło usługę przed niedostępnością dla klientów końcowych z terytorium Polski.

NO I WRESZCIE PODSUMOWANIE!

SYTUACJA PO ATAKU **W SZPITALU**

Brak skutecznej kopii zapasowej

Usługi ochrony sieci wyłączone

Zaszyfrowane zasoby wymagają odszyfrowania przez inżynierów

W IT zbyt mała obsada

Incydent wpłynął na udzielanie świadczeń zdrowotnych

Stan cyberbezpieczeństwa w szpitalach – weryfikacja

SYSTEM	WERSJA, AKTUALIZACJA	KOPIA ZAPASOWA		
		Wykonywana codziennie	Odmiejscowiona	Weryfikacja odtwarzania
HIS	1.11.08	TAK	taśma	10.12.2022
LABORATORIUM LIS	xxxxx	NIE	NIE	xxxx
APTEKA	xxxxx	xxxx	xxxx	xxxx
PACS	xxxxx	xxxx	xxxx	xxxx
EDM	xxxxx	xxxx	xxxx	xxxx
FK, Kadry	xxxxx	xxxx	xxxx	xxxx
AD, DNS	xxxxx	xxxx	xxxx	xxxx
wirtualizator	xxxxx	xxxx	xxxx	xxxx

DOFINANSOWANIE CYBERBEZPIECZEŃSTWA PODMIOTÓW LECZNICZYCH 2022-2023 ->500 MLN; 2024 – 400 MLN

Projekt obejmuje finansowanie zakupów teleinformatycznych

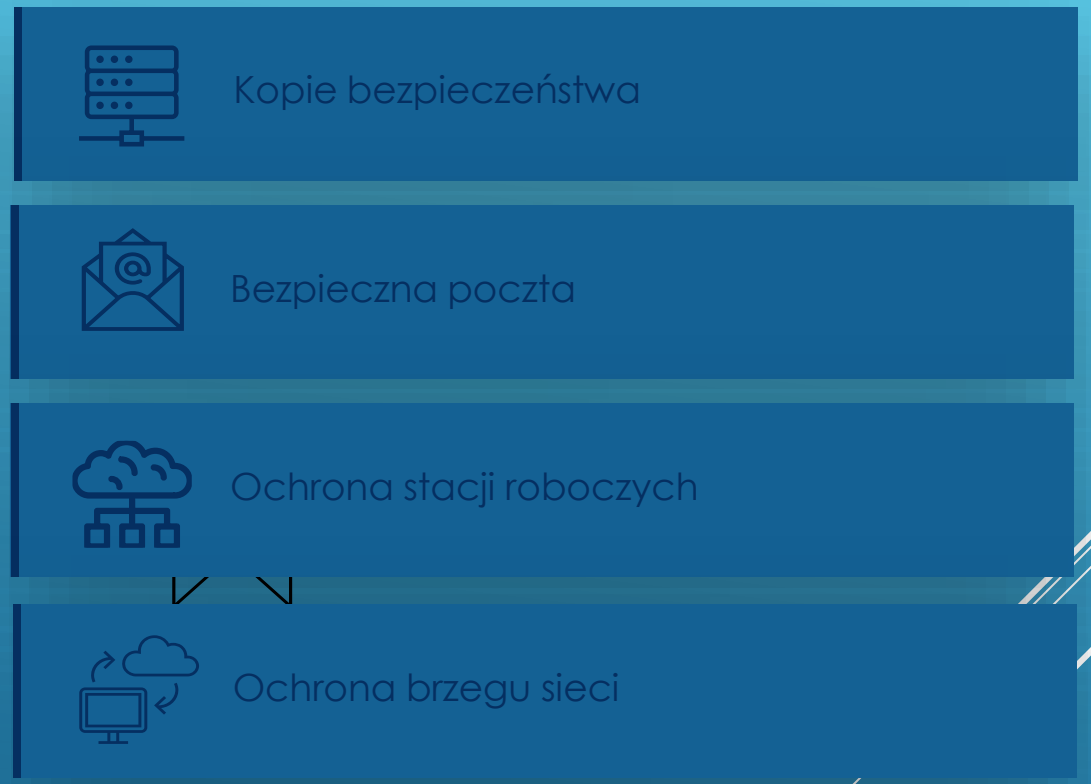
cel: **Podniesienie poziomu cyberbezpieczeństwa**

- Szpital może wnioskować o dofinansowanie od 300 do 900 tys. zł (w zależności od wysokości kontraktu z NFZ)
- Warunkiem zwrotu kosztów jest wynik audytu, który wykaże podniesienie poziomu cyberbezpieczeństwa
- Podstawa: polecenie Ministra Zdrowia z 29 kwietnia br.

Rekomendacje w zakresie budowy systemówcyberbezpieczeństwa

- Priorytety działań
- Rekomendacje w zakresie architektury cyberbezpieczeństwa (podstawowej i docelowej)
- Rekomendacje w zakresie funkcjonalności komponentów bezpieczeństwa
- Wymagania dotyczące wykonania usługi skanowania podatności
- Dokument opublikowany w kwietniu 2022 r.

Wskazane priorytety



CSIRT CEZ - WSPARCIE SEKTORA - PRZYGOTOWANIE 2022 R. - REALIZACJA 2023 R.

- Formalne dokumenty powołujące CSIRT sektorowy, formalne poinformowanie sektora
- Zapewnienie bezpiecznego kanału do zgłaszania incydentów
- Listy kontaktowe do OUK. Komunikacja do OUK. Komunikacja z innymi zespołami cyberbezpieczeństwa
- Komunikacja z CSIRT poziomu krajowego
- Największe wyzwanie:
  brak etatów dla podstawowego zespołu

CYBERKARTEKA WSPARCIE DLA SZPITALI

Skanowanie infrastruktury placówek medycznych - detekcja podatności słabości w systemach widocznych w sieci Internet

Rekonesans dla witryn/hostów

Cyberkaretka

Metody przeprowadzania skanów dla placówek w oparciu o narzędzia open-source – testy i ich zakres.

1. Testy wykonywane są metodą autorską w oparciu o darmowe rozwiązania dostępne w Internecie, m.in..:
   - poprawności komunikacji SSL,
   - skanowanie portów, DNS,
   - skanowanie OSINT/rekonesans (zbieranie informacji, np. o nagłówkach serwerów, informacji w kodzie aplikacji dot. wersji bibliotek i komponentów systemów),
   - skanowanie pod kątem podatności.
2. Skany mają charakter nieinwazyjny, wykonywane są za zgodą placówki w terminie dogodnym dla zainteresowanego,
3. Skany mają na celu zebranie jak największej liczby informacji, które można pozyskać w sieci Internet na temat danej adresacji/domeny,
4. W ramach badań nie wykonuje się weryfikacji/exploitacji wykrytych podatności,
5. Zebrane informacje poddawane są analizie, powstaje raport z rekomendacjami.

csirt
Centrum e-Zdrowia

Wykrywane podatności/słabości. Stan początkowy.

Co znaleźliśmy w sieci internet o danej placówce.

Wynik działania Nmapa | Porty / Hosty | Topologia | Szczegóły hosta | Skany

Port	Protokół	Stan	Usługa	Wersja
53	tcp	open	domain	
80	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443	tcp	open	http	Microsoft IIS httpd 7.5

https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-3427/version_id-456828/Microsoft-Internet-Information-Services-7.5.html

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2010-2730	Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to execute arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability."

Fingerprinted CMS & Vulnerabilities

WordPress 5.5.11

The fingerprinted CMS version is vulnerable to publicly known vulnerabilities. Urgently update to the most recent version when it becomes available.

CVSSv3.1 Score	Vulnerability CVE-ID CVE	Vulnerability Type
5.3 Medium	CVE-2022-3590	CWE-918 - Server-Side Request Forgery (SSRF)

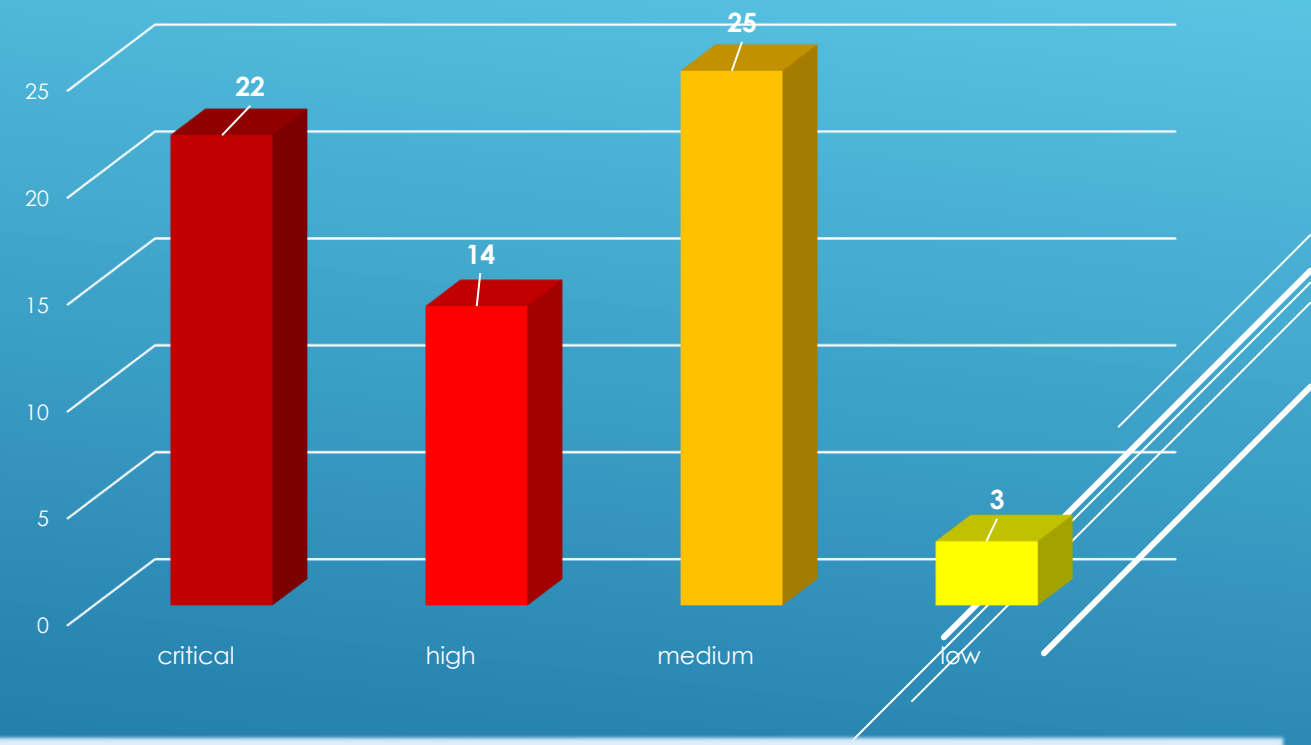
Fingerprinted CMS Components & Vulnerabilities

jQuery 1.12.4

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version 3.6.4.

CVSSv3.1 Score	Vulnerability CVE-ID CVE	Vulnerability Type
5.5 Medium	CVE-2020-11022	CWE-79 - Cross-site scripting

Suma zidentyfikowanych podatności



Security Report Summary

F

Site:	
IP Address:	
Report Time:	19 Apr 2023 06:19:37 UTC
Headers:	✖ Strict-Transport-Security ✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy

Wykrywane podatności/słabości. Stan po mitygacji (reskan).

Jak słabości i podatności zostały usunięte i zmitygowane.

Wynik działania Nmapa | Porty / Hosty | Topologia | Szczegóły hosta | Skany

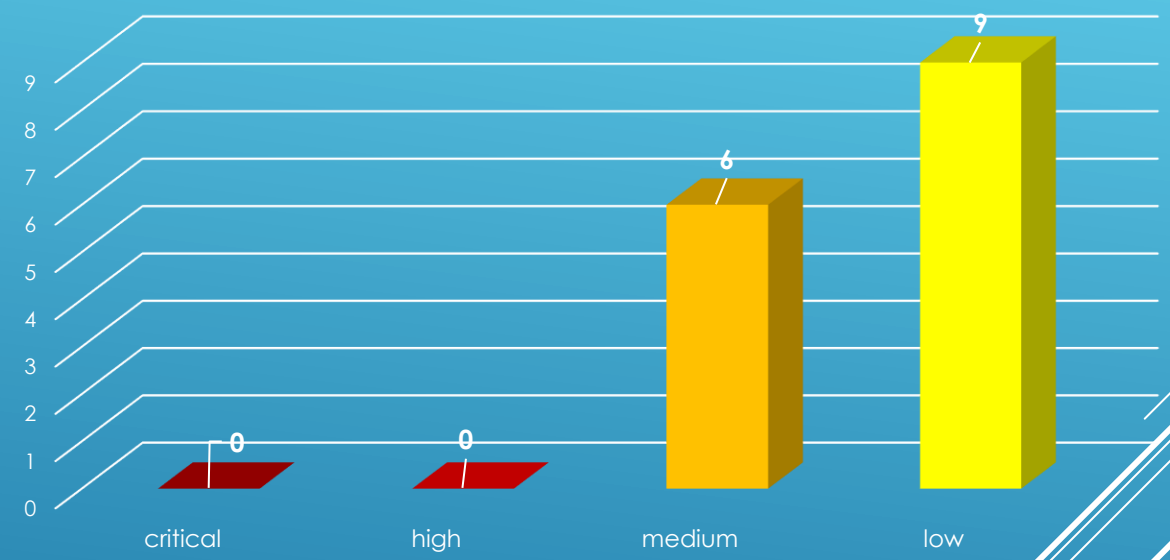
Port	Protokół	Stan	Usługa	Wersja
53	tcp	open	domain	
80	tcp	open	http	Apache httpd
113	tcp	closed	ident	
443	tcp	open	http	Apache httpd

Fingerprinted CMS & Vulnerabilities

WordPress

The fingerprinted CMS version is up2date, no security issues were found.

Suma zidentyfikowanych podatności



Security Report Summary

A

Site:

IP Address:

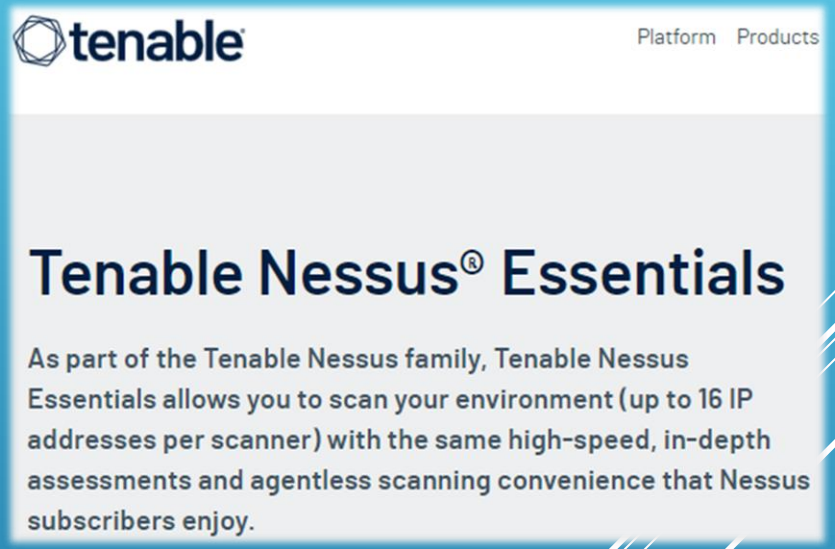
Report Time: 07 Jul 2023 11:09:08 UTC

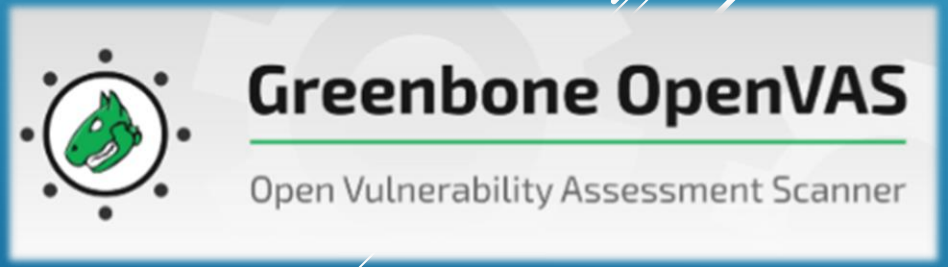
Headers: Strict-Transport-Security | Content-Security-Policy | X-Frame-Options | X-Content-Type-Options | Referrer-Policy | Permissions-Policy

Warning: Grade capped at A, please see warnings below.

O co warto zadbać pod kątem cyberbezpieczeństwa bez ponoszenia dodatkowych kosztów – przykłady.

2. Regularne aktualizacje i skany infrastruktury oraz usuwanie/mitygacja podatności.





Wybrane darmowe narzędzia umożliwiające rekonesans/weryfikację podatności.

1. Testy komunikacji TLS witryn/certyfikaty/nagłówki: https://www.ssllabs.com/ssltest/
2. Testy nagłówków witryn: https://securityheaders.com/
3. Raporty witryn (site report, tls, IP, historia): https://sitereport.netcraft.com/
4. Skanowanie portów: https://nmap.org/
5. Skanery aplikacji (www, mobilnych, API itp.): https://www.immuniweb.com/websec/
6. Strony na WordPress: https://wpsec.com/
7. Strony na Joomla: https://hackertarget.com/joomla-security-scan/
8. Maszyna, dokumentacja, środowiska do testów: https://www.kali.org/docs/
9. Skany podatności aplikacji – ZAP (Zed Attack Proxy): https://www.zaproxy.org/
10. Skany podatności – OpenVas/GVM/Greenbone z dystrybucji Kali: https://www.kali.org/tools/gvm/
11. Skany podatności – NESSUS Essentials (ograniczenie do 16 IP) https://www.tenable.com/products/nessus/nessus-essentials
12. Recon DNS: https://dnsspy.io/scan lub https://dnsdumpster.com/
13. Recon – co zaindeksowano w Internecie na temat naszych IP, domen itp.: https://www.shodan.io/dashboard

Wybrane płatne narzędzia do skanowania podatności i testów aplikacji.

1. **Tenable** (Nessus, s.c.+, i.o): skaner występuje w dwóch wariantach – darmowym (Nessus Essentials) i płatnym, różnica między nimi polega na feedach, które subskrybujemy, możliwości licencji w zależności od wybranego pakietu (wersja s.c.+ wspiera również procesy zarządzania ryzykiem, w tym priotetyzacji mitygacji wykrytych zagrożeń, compliance) - Tenable® - The Exposure Management Company

2. **Qualys:** platforma oferuje wiele funkcjonalności, takich jak skanowanie podatności, zarządzanie ryzykiem, zgodność z wymaganiami regulacyjnymi i wiele innych (badanie komunikacji SSL, certyfikatów itp.) - IT Security and Compliance Platform | Qualys, Inc.

3. **Acunetix:** skaner podatności stron internetowych, które oferuje wiele funkcjonalności, takich jak skanowanie podatności, zarządzanie ryzykiem, zgodność z wymaganiami regulacyjnymi i wiele innych (automatyzacja zadań, tworzenie ticketów, weryfikacja compliance) Acunetix | Web Application Security Scanner

4. **Burp Suite Professional:** narzędzie do ręcznego i automatyczngo testowania bezpieczeństwa aplikacji internetowych, działa jak proxy, w wersji płatnej dostęp do funkcji skanera i w pełni odblokowany moduł Intruder oraz możliwość zapisywania sesji. Obsługa wymaga większej wiedzy od użytkownika. Często użytkowany przez pentesterów. Burp Suite Professional - PortSwigger

5. **SNYK:** platforma, która oferuje zarówno statyczne (SAST), jak i dynamiczne (DAST) testowanie bezpieczeństwa aplikacji. Narzędzia SAST/DAST są możliwe do zintegrowania w procesie CI/CD (proces skanowania jest uruchamiany już na etapie wytwarzania aplikacji/kodu przez developerów) Snyk | Developer security | Develop fast. Stay secure. | Snyk

CERT Polska – projekt Artemis

Artemis – wykrywanie podatności systemów internetowych.

Artemis pomaga sprawdzać bezpieczeństwo systemów udostępnianych w internecie przez podmioty, które zgodnie z ustawą o KSC (Krajowym Systemie Cyberbezpieczeństwa), znajdują się we właściwości CSIRT NASK. W ramach prowadzonych projektów skanowane są określone grupy stron w poszukiwaniu podatności bezpieczeństwa i błędów konfiguracyjnych.

Dlaczego CERT Polska prowadzi skanowanie stron?

Zespół CERT Polska działa w strukturach NASK – Państwowego Instytutu Badawczego. Od wejścia w życie ustawy z dn. 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa zespół realizuje część zadań CSIRT NASK, zgodnie z art. 26 tej ustawy.

W jaki sposób wybierane są systemy do skanowania?

Wyznacznikiem jest ustawa o KSC. Zgodnie z jej zapisami CERT Polska pomaga dbać o cyberbezpieczeństwo m.in.:

- szkół,
- szpitali,
- instytutów badawczych,
- uczelni,
- jednostek samorządu terytorialnego

1. Źródło: https://cert.pl/skanowanie/

Dziękuję za uwagę

Roman Łożyński
CIRF

Wykorzystane materiały :

KPRM
KANCELARIA PREZESA RADY MINISTRÓW

Ministerstwo Cyfryzacji

Ministerstwo Finansów

cez Centrum e-Zdrowia