

BUDOWANIE ŚWIADOMOŚCI CYBERBEZPIECZEŃSTWA W KONTEKŚCIE NAJNOWSZYCH ZAGROŻEŃ





FAN CHMURY
PASJONAT CYBERBEZPIECZEŃSTWA
AUDYTOR BEZPIECZEŃSTWA TELEINFORMATYCZNEGO



FAN OPEN SOURCE
BADACZ ZABEZPIECZEŃ
TESTER PENETRACYJNY



(ISC)^{ZS}

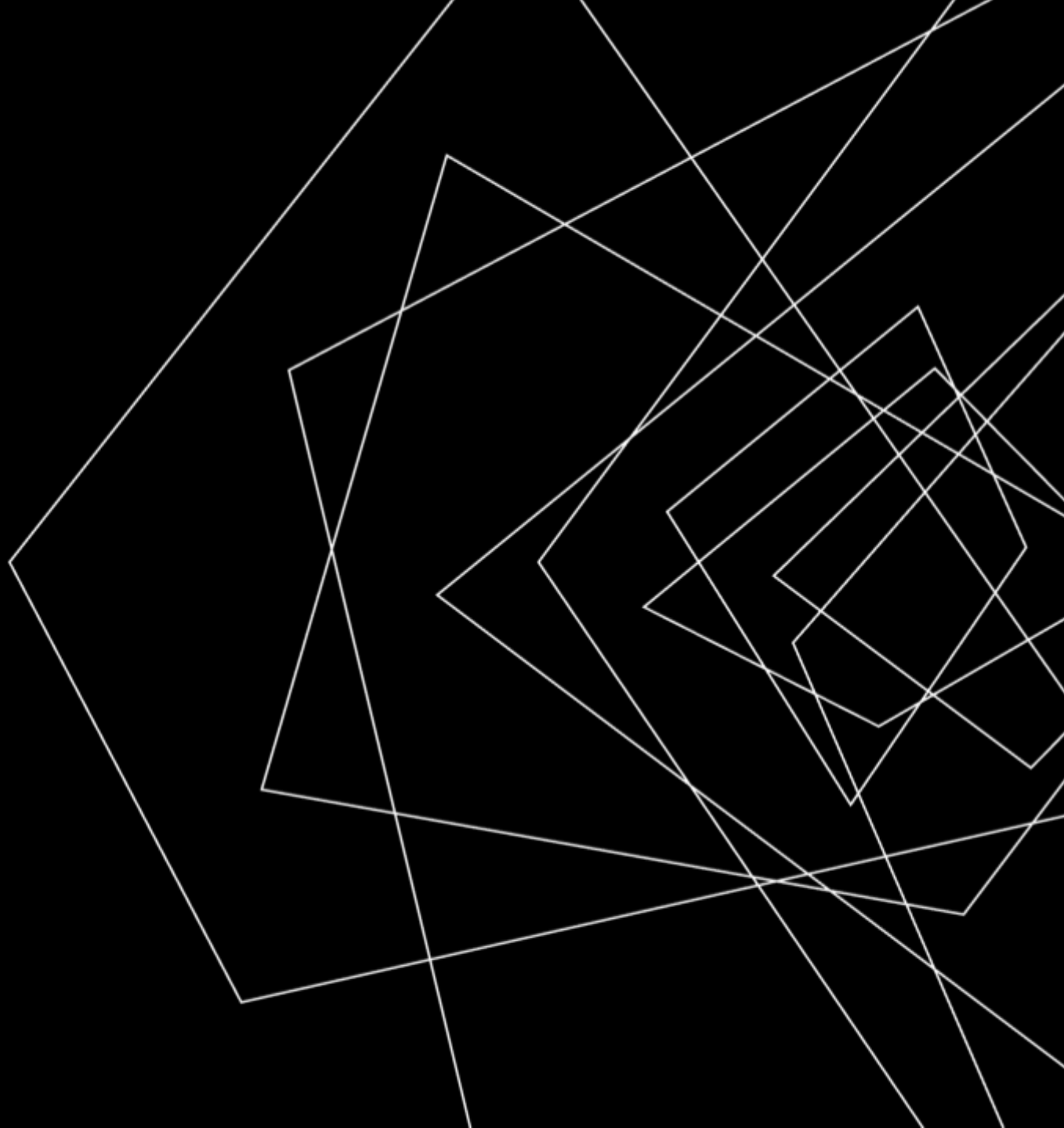


OFFENSIVE
security



AGENDA

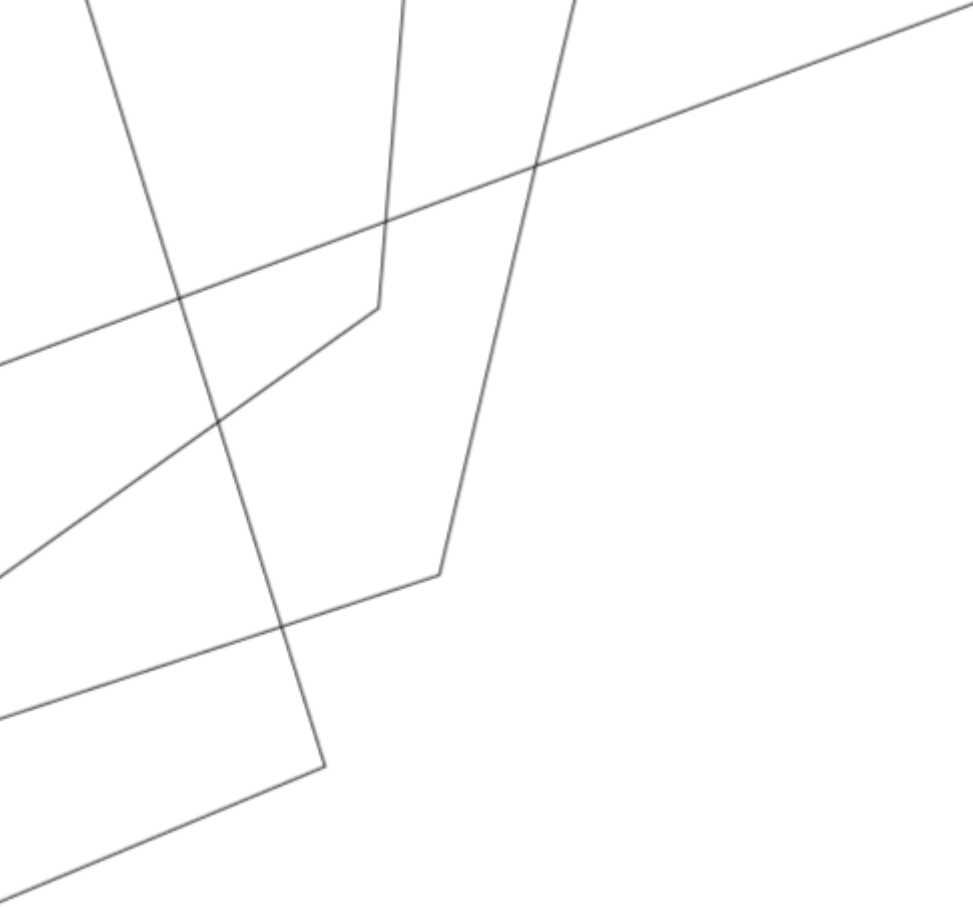
- Zagrożenia
- Cyberświadomość





STATYSTYKI

- W 2024 roku odnotowano ponad 113 600 poważnych incydentów cybernetycznych w Polsce (Ministerstwo Cyfryzacji).
- Wzrost o 100% liczby zgłoszonych incydentów w pierwszym półroczu 2024 r. w porównaniu z 2023 (ponad 400 tys. zgłoszonych).
- Najwięcej ataków miało charakter phishingu, socjotechniki oraz ransomware.
- Ponad 68% firm doświadczyło przynajmniej jednego incydentu w 2023 r., jednak tylko 26% ma procedury reagowania.



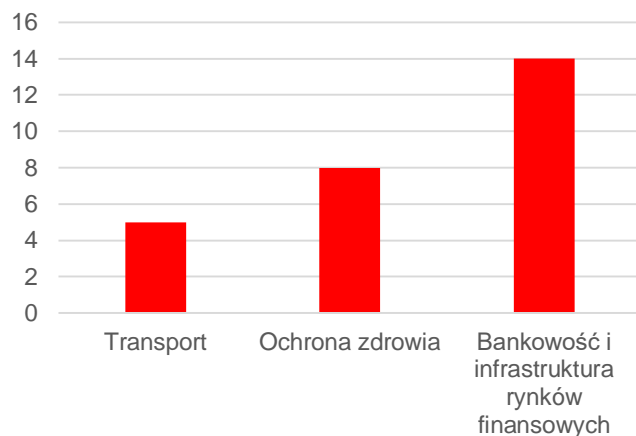
Zgłoszenia zagrożeń cyberbezpieczeństwa 550 049

Nowe incydenty cyberbezpieczeństwa 211 029

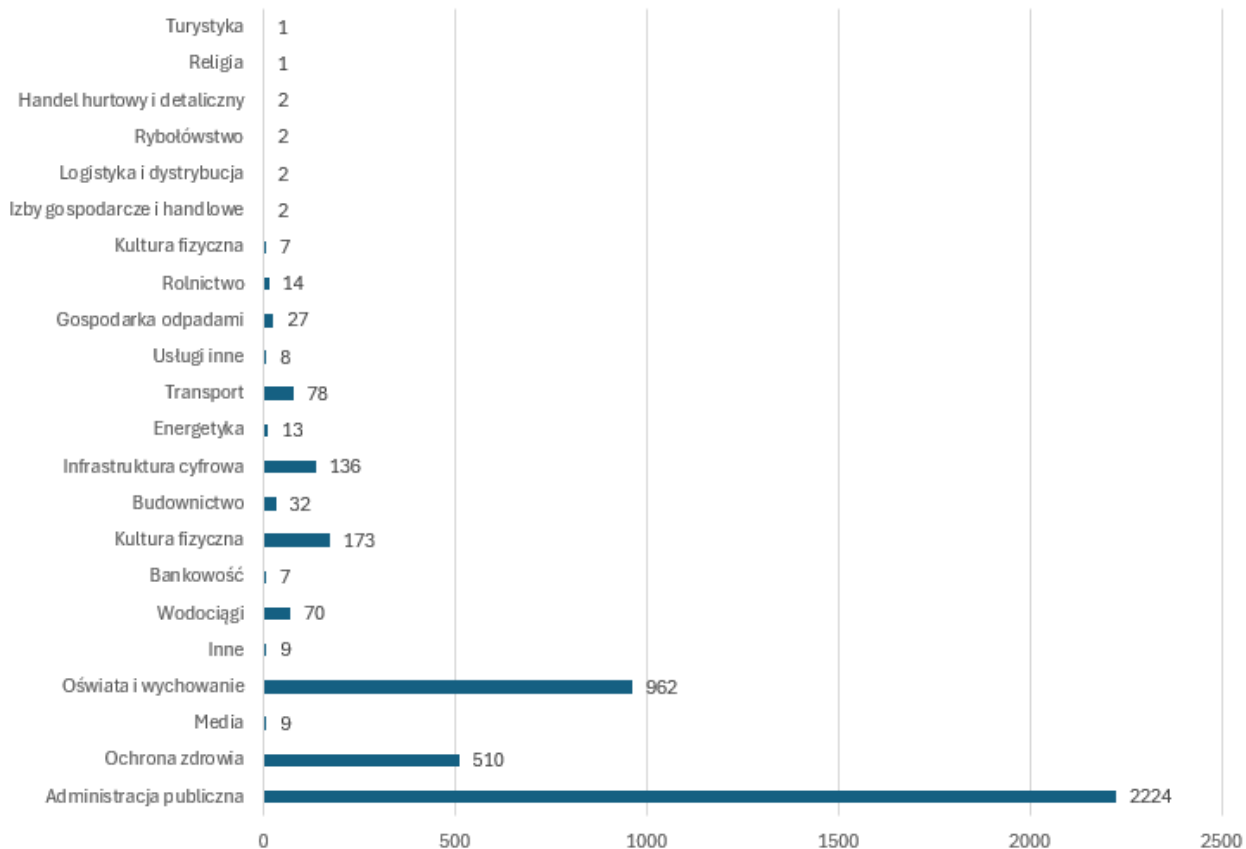
STATYSTYKI OBSŁUŻONYCH
INCYDENTÓW PRZEZ ZESPÓŁ
CERT POLSKA:

01.01.2025-30.10.2025

Incydenty poważne



Incydenty istotne



STATYSTYKI OBSŁUŻONYCH
INCYDENTÓW PRZEZ ZESPÓŁ
CERT POLSKA:

01.01.2025-30.10.2025



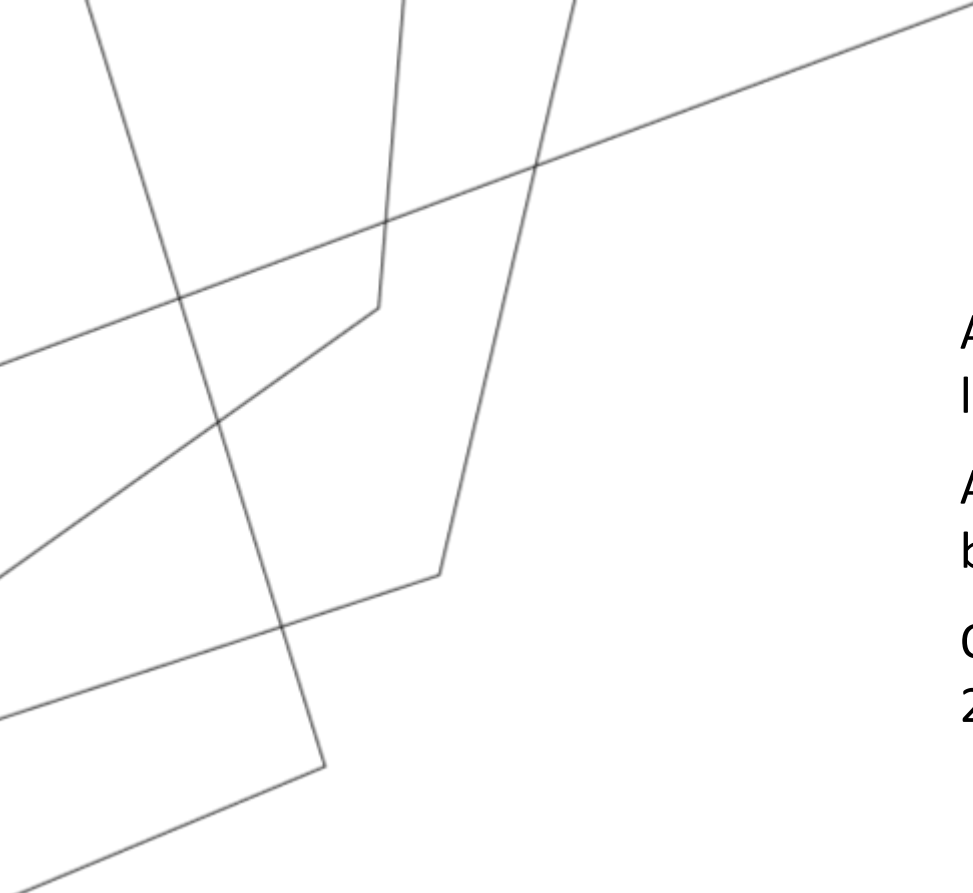
NAJWIĘKSZE ZAGROŻENIA

Phishing i socjotechnika - główne metody włamań do systemów i wyłudzenia danych.

Ransomware ataki na infrastrukturę krytyczną, m.in. szpitale i systemy wodociągowe.

Wycieki danych - cyberatak na biuro podróży ITAKA (październik 2025).

Wzrost działań grup hakerskich sponsorowanych przez Rosję i Białoruś.



Atak hakerski na spółkę Nowa Itaka skutkował wyciekiem danych logowania części klientów.

Akcja wykrywania i reagowania prowadzona przez NASK i służby bezpieczeństwa.

Ostrzeżenia dla klientów: zmiana haseł, wzmocnienie zabezpieczeń 2FA, monitoring wycieków na bezpiecznedane.gov.pl.

WYCIEK DANYCH

Standard	Standard	Standard	Standard
email_canonical	enabled	salt	password
valud...com	t		\$2y\$13\$6QW0xeIC.UnJ0DUXnnkT
olga...@gmail.com	t		\$argon2id\$v=19\$m=65536,t=4,
locke...com	t		\$argon2id\$v=19\$m=65536,t=4,
marek...com.pl	t		\$argon2id\$v=19\$m=65536,t=4,
irena...com.pl	t		\$argon2id\$v=19\$m=65536,t=4,
micha...@gmail.com	t		\$argon2id\$v=19\$m=65536,t=4,
aleks...a.pl	t		\$argon2id\$v=19\$m=65536,t=4,
pipi...89@gmail.com	t		\$argon2id\$v=19\$m=65536,t=4,
dami...k94@wp.pl	t		\$argon2id\$v=19\$m=65536,t=4,
magda...@gmail.com	t		\$argon2id\$v=19\$m=65536,t=4,
patry...ta@wp.pl	t		\$argon2id\$v=19\$m=65536,t=4,
wyso...@gmail.com	t		\$argon2id\$v=19\$m=65536,t=4,
katar...ka@o2.pl	t		\$2y\$13\$MzbMZoT7PZu41ZgsFN90
glowa...@gmail.com	t		\$2y\$13\$YPW1gRJ3ujTE1LM5572F
korel...onet.pl	t		\$2y\$13\$KKfHtejf0TFKLCTQMsQU

Ważna informacja dotycząca bezpieczeństwa danych w Strefie Klienta

31-10-2025, aktualizacja 04-11-2025

Szanowni Państwo,

informujemy, że Nowa Itaka spółka z o.o. padła ofiarą ataku hakerskiego. Nieuprawniona osoba / grupa osób uzyskała dostęp do części danych osobowych użytkowników posiadających konta w Strefie Klienta (takich jak adres e-mail, opcjonalnie imię i nazwisko, opcjonalnie numer telefonu). **Podkreślamy, że osoby nieuprawnione nie uzyskały dostępu do danych dotyczących rezerwacji (w tym danych finansowych, informacji o uczestnikach wyjazdów, czy numerów PESEL) oraz haseł do kont – te dane są bezpieczne.**

Do jakich danych uzyskano dostęp w wyniku ataku?

1. Wśród danych, które zostały pozyskane przez osobę nieuprawnioną, znajdują się: adresy e-mail, opcjonalnie imiona i nazwiska, opcjonalnie numery telefonów oraz hashe haseł powiązane z zarejestrowanymi kontami użytkowników. Co ważne, na podstawie tych danych nie ma możliwości bezpośredniego zalogowania się do Strefy Klienta ani do innych systemów.
2. Obecnie wiemy, że dane dotyczą grupy 10 tysięcy użytkowników, potencjalnie skala wycieku może być większa.

WYCIEK DANYCH



Krzysztof Gawkowski ✓

@KGawkowski



Show translation

⚠️ KOLEJNY ATAK HAKERSKI ⚠️

Ostrzeżenie dla klientów serwisu Supergrosz (prowadzonego przez AIQLABS sp. z o.o.). W wyniku incydentu bezpieczeństwa dane części użytkowników trafiły w ręce przestępców.

Nad sprawą pracuje już CSIRT KNF i CSIRT NASK. Powiadomiony został Prezes Urzędu Ochrony Danych Osobowych. Służby państwa szukają sprawców.

Sytuacja jest bardzo poważna bo wśród danych, które zostały pozyskane przez osobę nieuprawnioną, znajdują się [m.in.](#): adresy e-mail, imiona i nazwiska, informacje o narodowości, numery PESEL, dane dotyczące dowodu osobistego, adresy zamieszkania lub pobytu oraz adresy do korespondencji, numery telefonów, informacje o pozostawaniu w związku małżeńskim, informacje o liczbie dzieci, dane dotyczące statusu zawodowego, nazwa, adres, NIP oraz telefon do pracodawcy, zadeklarowana branża, deklarowany dochód, numery rachunków bankowych, identyfikator w portalu Facebook.

RMF24 › Fakty › Polska › Wyciekły m.in. numery PESEL. Atak hakerski na serwis z pożyczkami online

Wyciekły m.in. numery PESEL. Atak hakerski na serwis z pożyczkami online

Opracowanie: Maciej Nycz

Niedziela, 2 listopada (10:29)

Aktualizacja: Niedziela, 2 listopada (11:33)



Posłuchaj artykułu

Dźwięk wygenerowany automatycznie

Podkład



2:29

Hakerzy wykradli dane części użytkowników serwisu SuperGrosz, oferującego pożyczki online. Jak informuje minister cyfryzacji, chodzi m.in. o numery PESEL, adresy i numery telefonów.

WYCIEK DANYCH

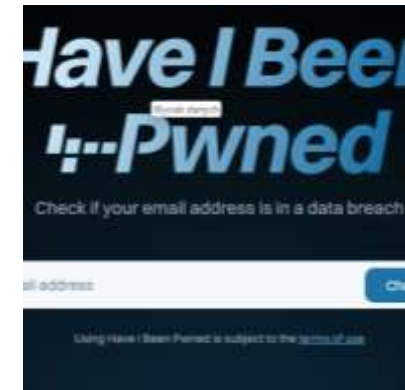
WYCIEK DANYCH



<https://bezpiecznedane.gov.pl/>



<https://info.mobywatel.gov.pl/>



<https://haveibeenpwned.com/>

PHISHING

security@govministry.pl
security@govministry.pl

Reply Forward Archive Junk Delete More

Pilna weryfikacja kontaktów w ramach Krajowego Programu Cyberbezpieczeństwa 2024-2028 12:32

Szanowni Państwo,

wg rozdzielnika

W związku z podwyższeniem standardów bezpieczeństwa informacyjnego, prosimy o dokonanie sprawdzenia pliku załączonego do niniejszej komunikacji SMS pod kątem zawartości danych osobowych pracowników.

W przypadku stwierdzenia obecności Państwa danych w załączonym dokumencie, prosimy o podjęcie następujących działań zapobiegawczych:

- należy niezwłocznie zmienić wszystkie hasła i dane logowania, unikając stosowania słabych haseł na różnych kontaktach i platformach.
- prosimy sprawdzić, czy do Państwa/Pana kontaktują się pracownicy urzędów i instytucji należące do Państwa/Pana.
- w celu ochrony danych osobowych należy unikać ich wdrażania w komunikacji internetowej, które mogą wywołać wątpliwości co do ich autentyczności i bezpieczeństwa.

Termin na przesłanie informacji: 48 godzin.


Adres e-mail kontaktowy: security@govministry.pl

Termin na przesłanie informacji: 48 godzin.

Z upoważnienia Ministra Cyfryzacji

Paweł Olszewski
Sekretarz Stanu

> 1 attachment: database_part.xlsx size unknown Save



Polska zajmuje wysokie miejsce na liście najbardziej atakowanych krajów UE (3. miejsce w Europie).

Codziennie 20-50 prób ataku na infrastrukturę krytyczną (szpitale, systemy wodne, administrację).

Rozbijanie grup sabotażystów przez polskie służby.

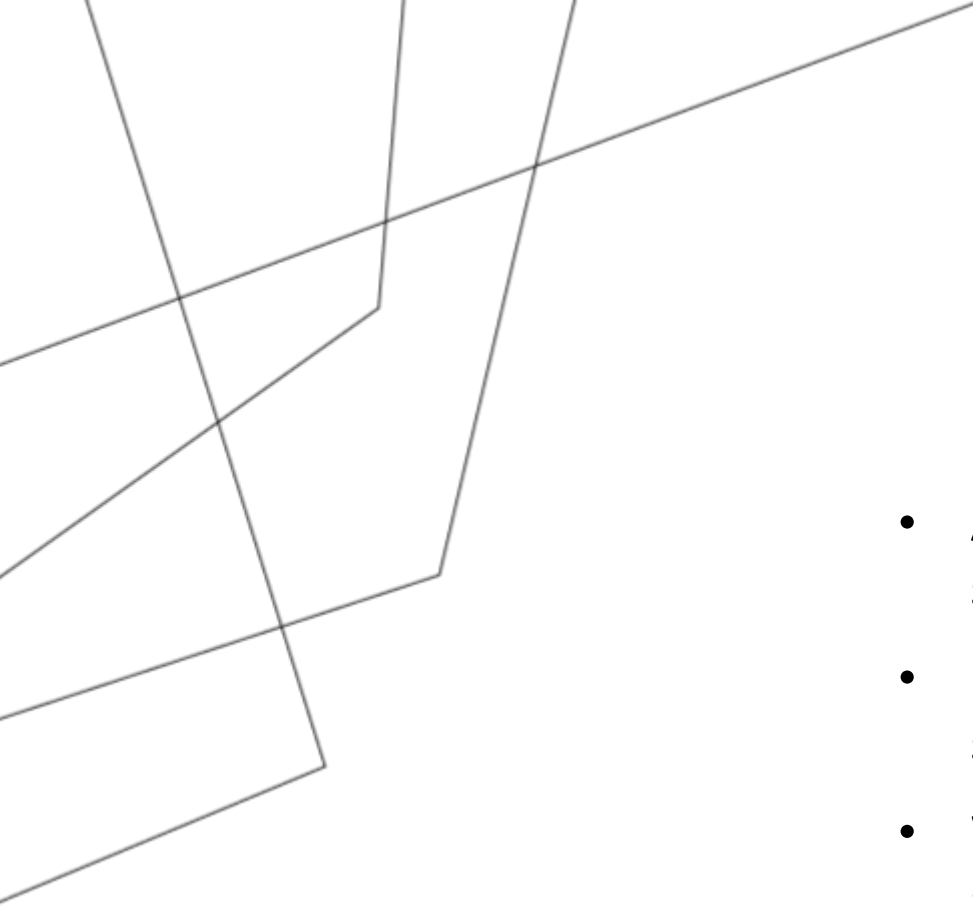
STATE SPONSORED



Funkcjonariusze CBZC rozpracowali międzynarodową grupę przestępczą



Foto: Centralne Biuro Zwalczania Cyberprzestępczości



- AI umożliwia bardziej zaawansowane phishingi i ataki socjotechniczne oparte na deep fake i automatyzacji.
- Przestępcy wykorzystują boty AI do generowania spersonalizowanych wiadomości i dezinformacji.
- Wyzwanie dla organizacji – konieczność edukacji i aktualizacji systemów zabezpieczeń pod kątem nowych technologii.

AI

BEZPIECZEŃSTWO TO...



A MOŽE...?



KRAJOBRAZ CYBERBEZPIECZEŃSTWA W POLSCE



1 na 5

Co piąty polski pracownik padł ofiarą cyberataku



52%

pracowników nie wie, jak zareagować na zagrożenie cyberatakiem



41%

Polskich firm nie korzysta z oprogramowania antywirusowego!



32%

firm w Polsce regularnie przeprowadza testy bezpieczeństwa IT



52%

pracowników polskich firm w ciągu ostatnich 5 lat, nie brało udziału w szkoleniu z cyberbezpieczeństwa

CZY MOŻESZ ZRESETOWAĆ MI HASŁO?

Sierpień 2023

- telefon do IT Cognizant z prośbą o restart hasła
- brak weryfikacji dzwoniącego, wyłączenie MFA, brak informacji do Clorox o zmianie hasła
- i jeszcze raz to samo ;)
- dostęp do AD, odpalenie ransomware
- atakujący - Scattered Spider



CZY MOŻESZ ZRESETOWAĆ MI HASŁO?

Efekt ataku

- 380 mln \$ utraconych przychodów
- 49 mln \$ kosztów usunięcia ataku
- 6 tygodni przerwy w dostawach

A w tym roku?

- **Pozew przeciwko Cognizant na kwotę 380 mln \$ za rażące zaniedbania**



POLACY NIE GĘSI... WŁASNE WYCIEKI MAMY

Październik 2022

Grupa Hunters publikuje 6 TB danych z firmy AIUT

- własność intelektualna
- NDA
- CV, prywatne dokumenty
- skany paszportów
- hasła do ponad 100 kont

The logo for AIUT, consisting of the lowercase letters 'aiut' in a bold, blue, sans-serif font. The letters are closely spaced and have a slight shadow effect.

POLACY NIE GĘSI... WŁASNE WYCIEKI MAMY

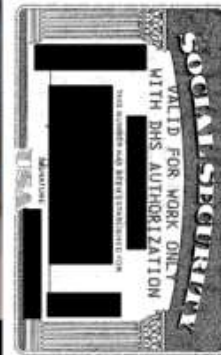
1	Passwords		
2	Company	Username	Passwords
3	Amazon	@aiut.com	
4	Best Buy	@aiut.com	
5	Ebay	@aiut.com	
6	Advantech	@aiut.com	
7	Allied Electronics	@aiut.com	
8	BuyRexroth	@aiut.com	
9	Digi-Key	@aiut.com	
10	Digi-Key	@aiut.com	
11	Grainger	@aiut.com	

Rozmowa 2009, godz.

Dostępność w pracy:
 Oczekiwania finansowe:
 Posiada prawo jazdy + auto
 Wiedza komputerowa: dobra
 Wiedza sieciowa: przyzwoita

CURRICULUM VITAE

Imię i nazwisko:
 Adres zamieszkania:
 Numer telefonu:



UMOWA NAJMU

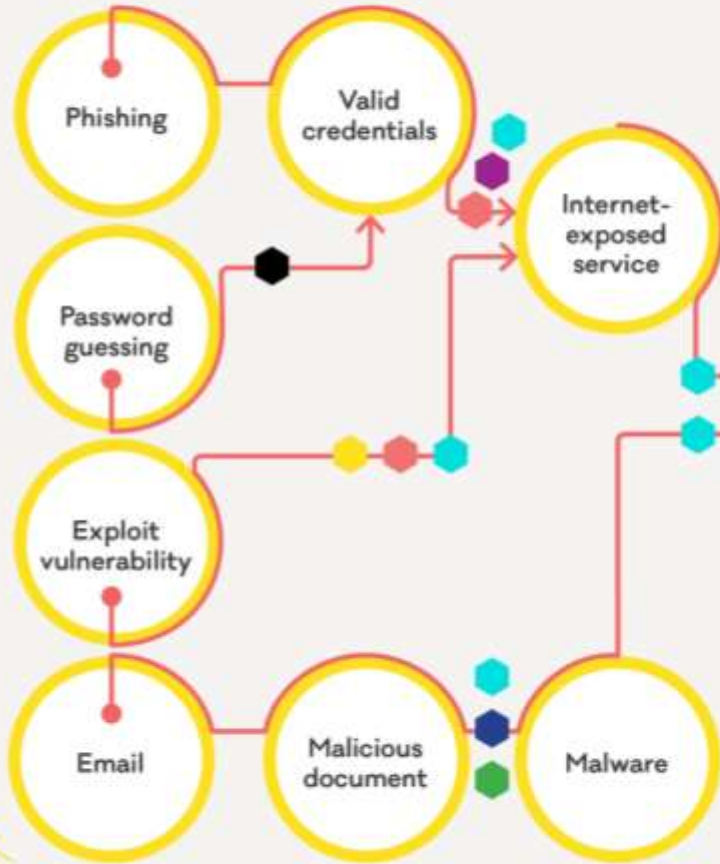
W dniu r. w pomiędzy:
 zamieszkałym w identyfikującym się numerem PESEL: zwaną dalej „Najemcą”,
 a
 zamieszkałym w identyfikującym się numerem PESEL: Zwanym dale „Wynajmującym”, zawarto umowę następującej treści:

LIFECYCLE OF A RANSOMWARE INCIDENT

How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.

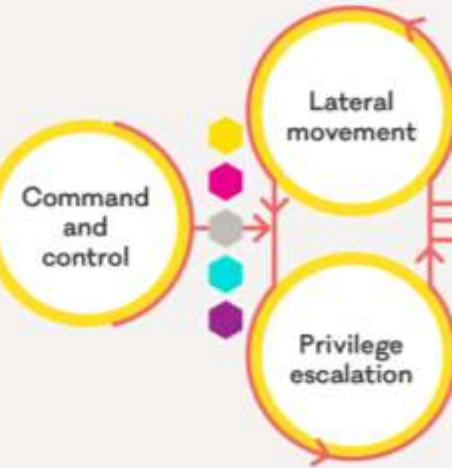
INITIAL ACCESS

Attacker looks for a way into the network



CONSOLIDATION AND PREPARATION

Attacker attempts to gain access to all devices



IMPACT ON TARGET

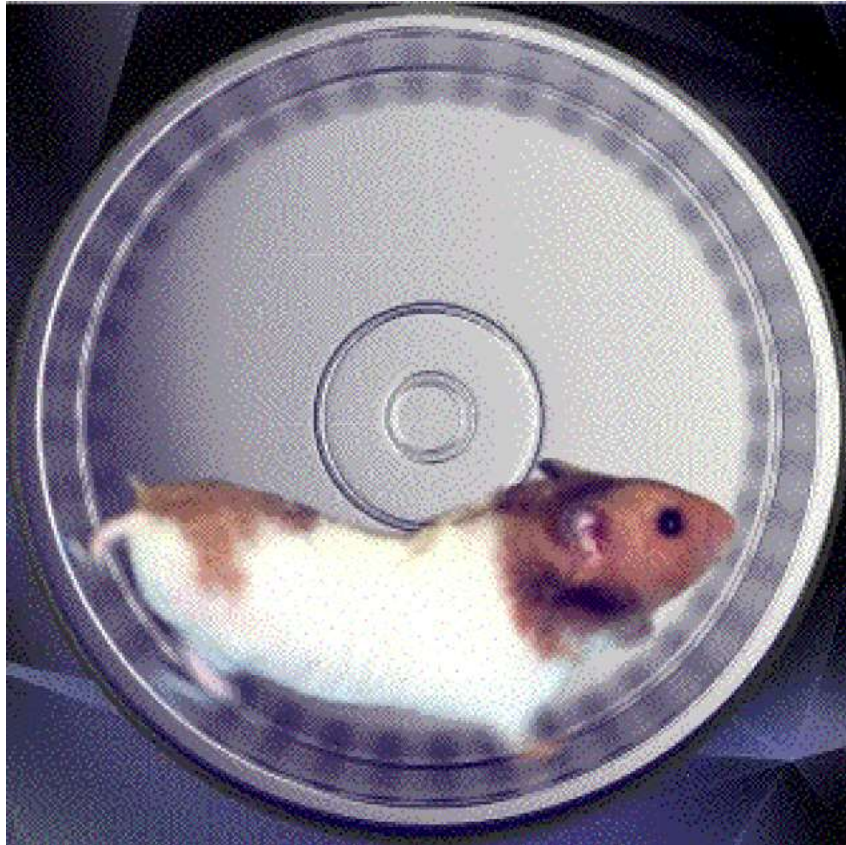
Attacker steals and encrypts data, then demands ransom



CRITICAL CONTROLS KEY

- | | | | | |
|---------------------------|--------------------------|----------------------|----------------------|------------------------------|
| Internet-exposed services | Patching | MFA | Network segmentation | Principle of least privilege |
| Backups | Application allowlisting | Logging and alerting | Disable macros | Password manager |

CYBERSECURITY AWARENES



- ISO/IEC 27001
każda organizacja wdrażająca ISO 27001 musi utrzymywać sformalizowany program szkoleń
- Ustawa o KSC
nakłada obowiązek cyklicznych szkoleń zarówno dla kadry zarządzającej jak i pracowników
- DORA
sektor finansowy musi prowadzić obowiązkowe i udokumentowane szkolenia dla pracowników, zarządu i dostawców
- GDPR/RODO
regularne i udokumentowane szkolenia dla osób przetwarzających dane osobowe

KULTURA CYBERBEZPIECZEŃSTWA

Strategiczny plan budowania świadomości cyberbezpieczeństwa

- wizja i misja
- cele i zadania strategiczne
- podejście szkoleniowe i plany działania
- taktyki pomagające w realizacji celów
- wskaźniki i raportowanie

KULTURA CYBERBEZPIECZEŃSTWA

Elementy programu budowy świadomości cyberbezpieczeństwa

- Rola i wpływ na organizację
- Aktualny stan zgodności
- Dostępność materiałów i zasobów

KULTURA CYBERBEZPIECZEŃSTWA

Ustalanie priorytetów planów budowania świadomości

- Działania uświadamiające
 - Komunikaty na ekranach logowania, wygaszaczach ekranu
 - Plakaty, biuletyny z poradami ds. cyberbezpieczeństwa
- Nauka przez doświadczenie
 - Testy phishingowe, gry symulacyjne
- Szkolenia
 - Stacjonarne
 - Online, podcasty

KULTURA CYBERBEZPIECZEŃSTWA



DLACZEGO DAJEMY SIĘ ZŁAPAĆ?

- Uśpienie naszej czujności poprzez uwiarygodnienie oszusta.
- Perfekcyjne scenariusze rozmów.
- Nasza niewiedza.
- Zasada "dowolnego uzasadnienia"
- Brak wystarczającej uwagi i izolacja ofiary
- Głos lub ton wiadomości oszusta jest „sympatyczny”, to osoba "taka jak ja"



TO JAK SIĘ NIE DAĆ ZŁAPAĆ?

- Pobieraj oprogramowanie wyłącznie z zaufanych, legalnych i oficjalnych źródeł.
- Nie ufaj reklamom w mediach społecznościowych, szczególnie zachęcających do pobrania oprogramowania.
- Nie wykonuj komend, kodu, którego działania nie znasz lub nie rozumiesz.
- Wybierz inny menadżer haseł niż ten wbudowany w przeglądarkę.
- Dbaj o bezpieczeństwo swoich danych, szczególnie jeśli chronią Twoje pieniądze.
- Weryfikuj informacje i oferty – krytyczne myślenie i zasada ograniczonego zaufania to najlepsze narzędzia w walce z oszustami.
- Korzystaj z rozwiązań MFA.



DZIĘKUJEMY

Tomasz Wiertelak

Wiktor Sędkowski