OSIĄGNIĘCIA, WYZWANIA, MOŻLIWOŚCI

18-20 czerwca 2024 r.

Krajowa Sieć Obszarów Wiejskich

CDR

Program Rozwoju Obszarów Wiejskich na lata 2014-2020

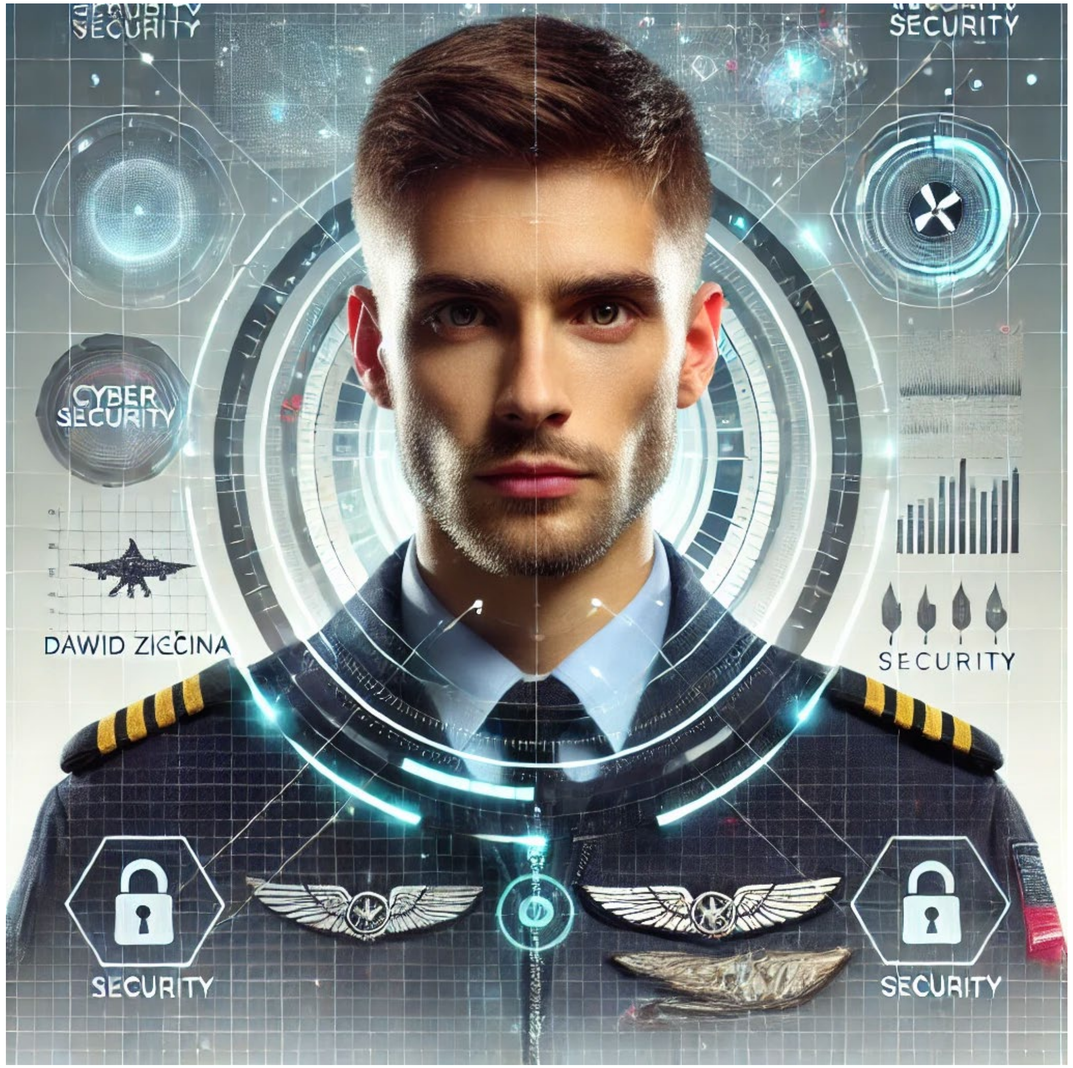
Europejski Fundusz Rolny na rzecz Rozwoju Obszarów Wiejskich: Europa Inwestująca w obszary wiejskie.
Instytucja Zarządzająca Programem Rozwoju Obszarów Wiejskich na lata 2014–2020 – Minister Rolnictwa i Rozwoju Wsi.
Operacja współfinansowana ze środków Unii Europejskiej w ramach Schematu II Pomocy Technicznej „Krajowa Sieć Obszarów Wiejskich" Programu Rozwoju Obszarów Wiejskich na lata 2014–2020.

Dawid Zięcina

Bezpieczeństwo Lokalnych Grup Działania w sieci

Europejski Fundusz Rolny na rzecz Rozwoju Obszarów Wiejskich: Europa Inwestująca w obszary wiejskie.
Instytucja Zarządzająca Programem Rozwoju Obszarów Wiejskich na lata 2014–2020 – Minister Rolnictwa i Rozwoju Wsi.
Operacja współfinansowana ze środków Unii Europejskiej w ramach Schematu II Pomocy Technicznej „Krajowa Sieć Obszarów Wiejskich" Programu Rozwoju Obszarów Wiejskich na lata 2014–2020.

Czy leci z nami pilot?



Cyberincydent a katastrofa lotnicza

- *łańcuch zdarzeń*
- *czynnik ludzki*
- *złożoność systemów*
- *procedury i protokoły*
- *szybkość reakcji*
- *konsekwencje*
- *analiza „post-mortem”*

Najpopularniejsze typy cyberataków

Phishing

Malware

Socjal Engineering

Pozostałe

Źródło: Raport KPMG „Barometr cyberbezpieczeństwa 2024”

Najpopularniejsze typy cyberataków

Kradzież danych

Szkodliwe oprogramowanie

Inżynieria społeczna

Pozostałe

Najpopularniejsze typy cyberataków

Kradzież danych

Szkodliwe oprogramowanie

Inżynieria społeczna

Pozostałe

Phishing – przebieg ataku

Phishing – przebieg ataku

- *podszywanie się*
- *wzbudzenie emocji*
- *nakłonienie do akcji*
- *wyłudzenie informacji*
- *wykorzystanie skradzionych informacji*

Phishing – obrona przed atakiem

- menedżer haseł (np. KeePass) $
- uwierzytelnienie dwuskładnikowe $
- e-persona $
- ochrona urządzeń (np. ESET) $
- ochrona przed fałszywymi stronami (np. OpenDNS) $
- Bezpieczna wymiana informacji (np. NordVPN) $

Phishing – mnie to nie dotyczy?

Phishing – mnie to nie dotyczy?

Phishing – mnie to nie dotyczy?

Phishing – mnie to nie dotyczy?

jan.kowalski@mf.gov.pl

jan.kowalski@yandex.ru

Phishing – mnie to nie dotyczy?

https://www.allegro.pl

https://www.alleqro.pl

Phishing – mnie to nie dotyczy?

https://www.allegro.pl

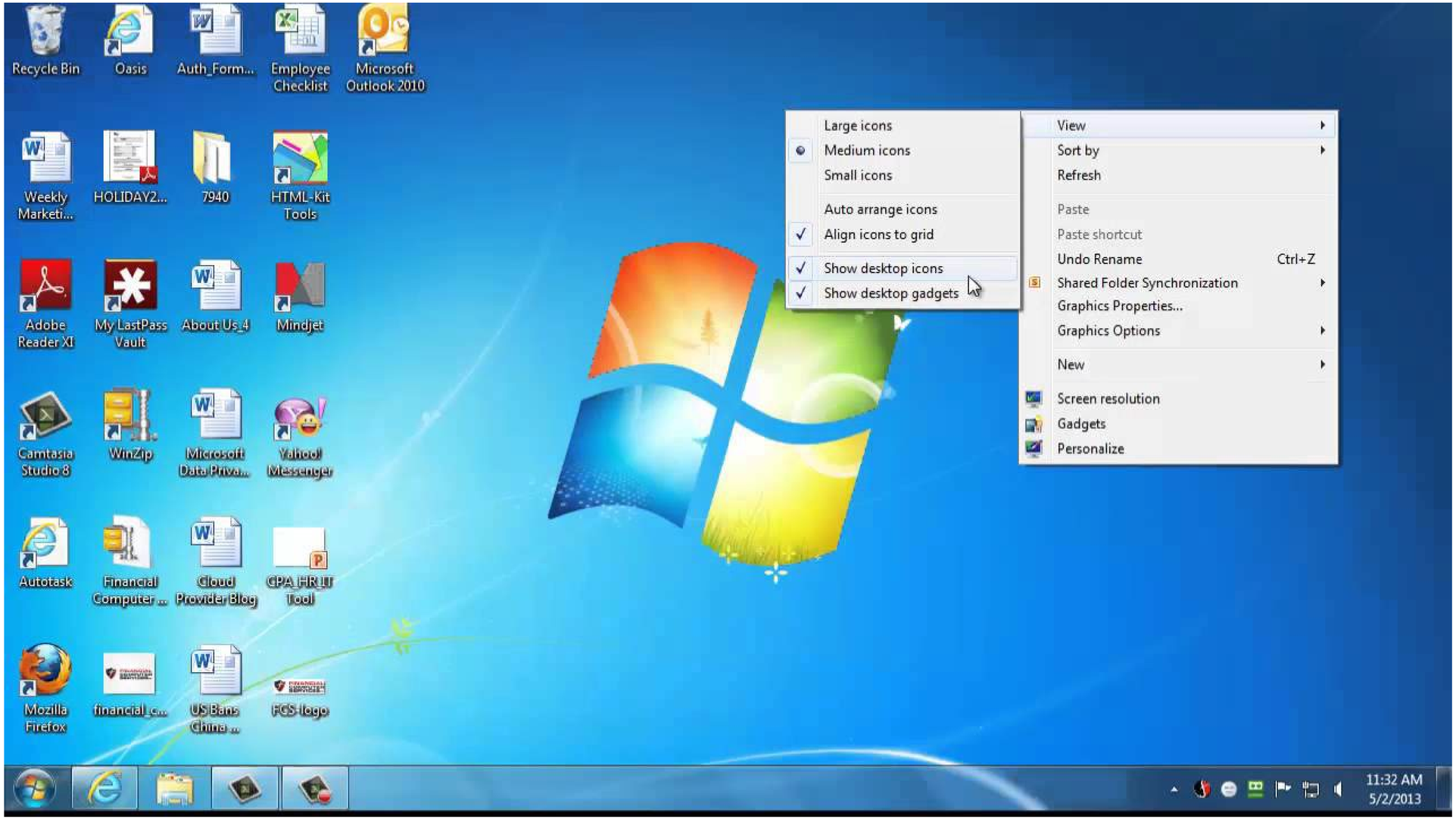
https://www.allegro.pl-allegro.fm

Phishing – mnie to nie dotyczy?

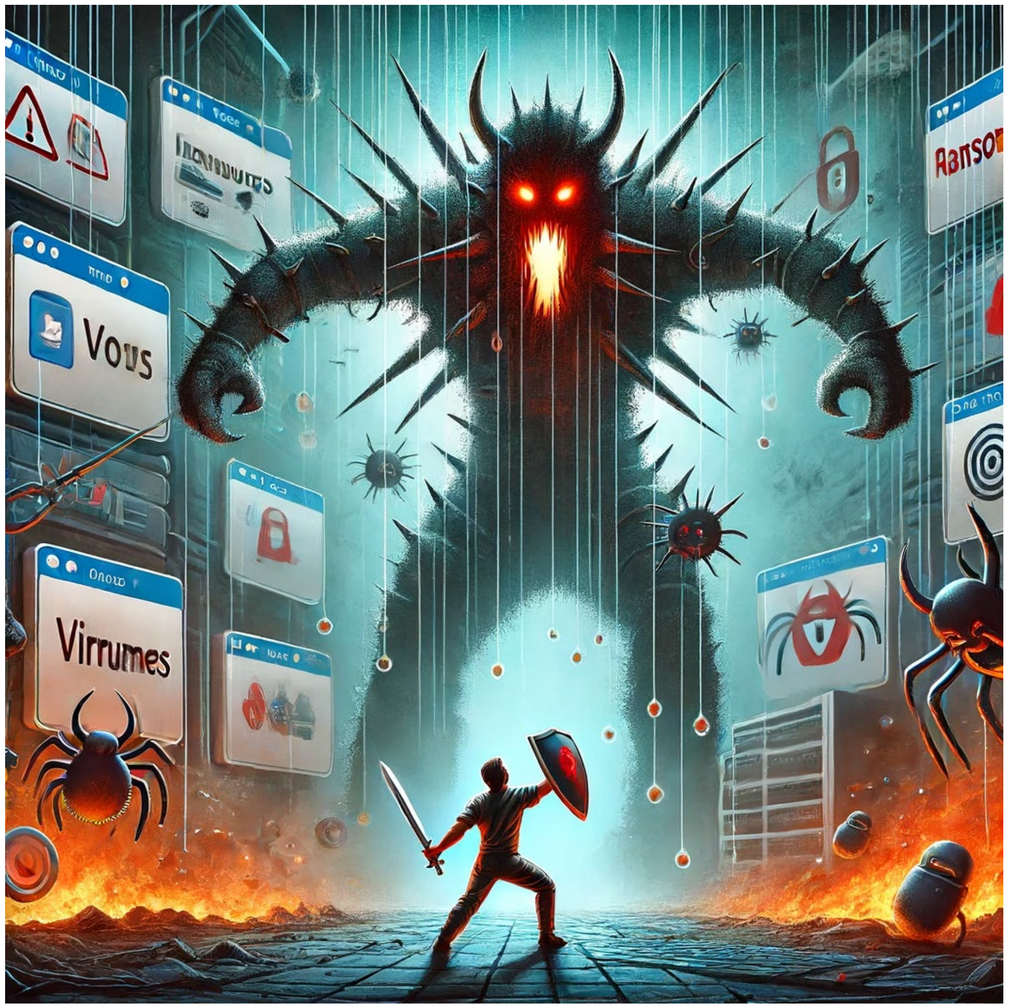
https://www.allegro.pl

https://www.allegro.pl

Malware – przebieg ataku

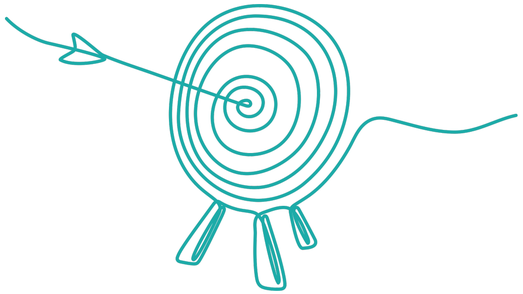


Malware – przebieg ataku



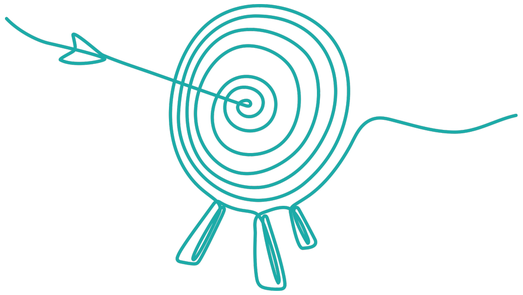
- załącznik w mailu
- link w wiadomości
- zainfekowane strony www
- aplikacje z niezaufanego źródła
- nośniki fizyczne (np. pendrive)
- luki w oprogramowaniu lub konfiguracji

Malware – cel ataku



- zarobek finansowy
- kradzież danych
- pozyskanie zasobów (komputer, energia elektryczna)
- kontrola nad systemem
- manipulacja i dezinformacja
- zakłócenie działalności

Malware – obrona przed atakiem



- aktualna wersja oprogramowania $/$
- instalowanie aplikacji z zaufanych źródeł $/$
- ochrona urządzeń (np. ESET) $/$
- twórz kopię bezpieczeństwa swoich danych (np. Acronis) $
- stosuj zalecenia dotyczące ochrony przed phishingiem

Socjotechnika – przebieg ataku

phishing

Jedna z najczęstszych form ataków socjotechnicznych, gdzie atakujący wysyłają fałszywe e-maile lub wiadomości SMS, które wyglądają, jakby pochodziły od zaufanych źródeł, takich jak banki, firmy technologiczne czy instytucje rządowe. Celem jest skłonienie ofiary do podania poufnych informacji, takich jak dane logowania, numery kart kredytowych czy dane osobowe.

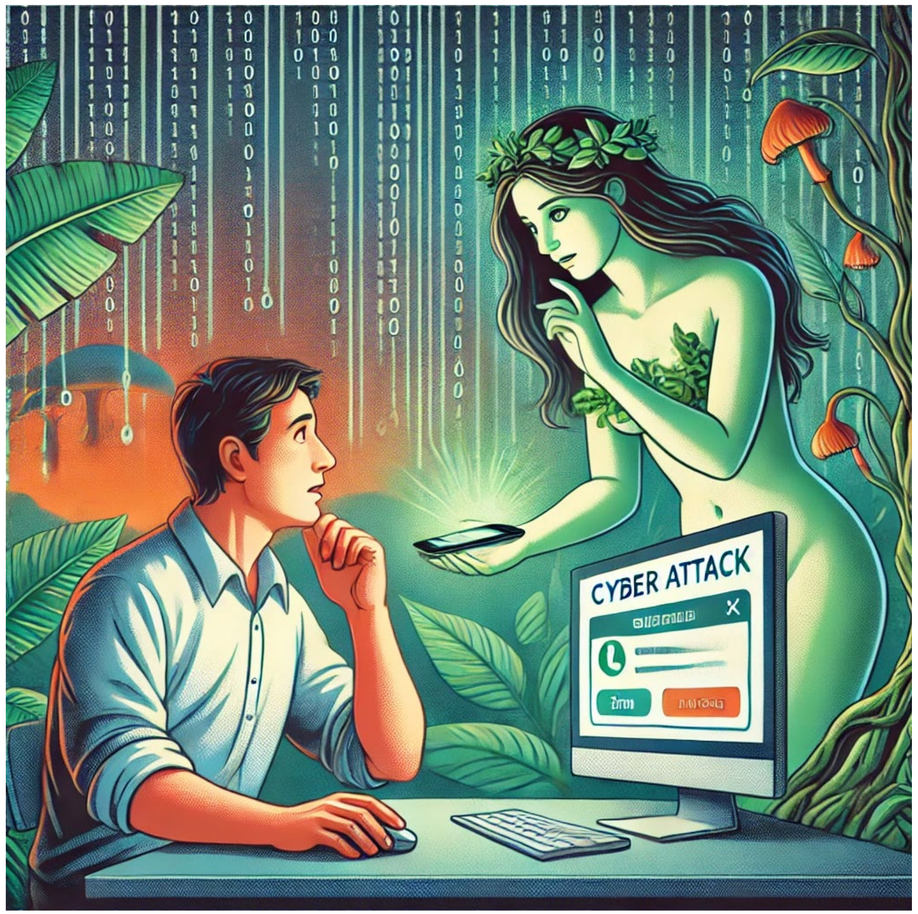
Socjotechnika – przebieg ataku

pretexting

Polega na tworzeniu fałszywego pretekstu, aby skłonić ofiarę do ujawnienia poufnych informacji. Atakujący podszywa się pod zaufaną osobę lub instytucję, tworząc wiarygodny scenariusz, aby zdobyć zaufanie ofiary.

Scenariusz: dzwoni pracownik banku celem wykonania transferu pieniędzy po rzekomym ataku.

Socjotechnika – przebieg ataku



baiting

Polega na kuszeniu ofiary fałszywą obietnicą lub nagrodą, aby skłonić ją do wykonania określonej akcji, takiej jak pobranie złośliwego oprogramowania.

Scenariusz: atakujący zostawia zainfekowany pendrive w miejscu publicznym, licząc na to, że ktoś go podłączy do swojego komputera, co spowoduje zainstalowanie malware.

Socjotechnika – przebieg ataku

shoulder surfing

Shoulder surfing to technika, w której atakujący obserwuje ofiarę, aby zdobyć poufne informacje, takie jak hasła czy numery PIN, poprzez podglądanie przez ramię.

Scenariusz: atakujący obserwuje ofiarę wprowadzącą PIN na bankomacie.

Socjotechnika – przebieg ataku

vishing

Forma phishingu, która wykorzystuje rozmowy telefoniczne do wyłudzenia informacji osobistych. Atakujący podszywa się pod zaufaną instytucję lub osobę, aby skłonić ofiarę np. do ujawnienia poufnych informacji.

Scenariusz: atakujący dzwoni do ofiary, udając znajomego i prosi o szybką pożyczkę pieniędzy.

Socjotechnika – obrona przed atakiem

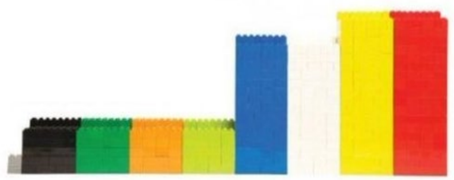
- śledzenie bieżących kampanii (np. CyberAlerty)
- alternatywne kanały komunikacji
- ustalony i przećwiczony sposób weryfikacji rozmówcy
- weryfikacja informacji

UważAI co zostawiasz w sieci

Dane/Informacje…

…przygotowanie/sortowanie

…prezentacja



…analiza

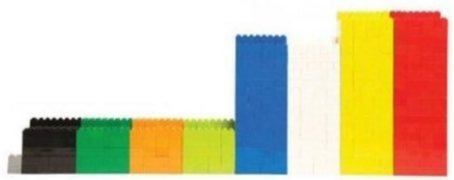
…przedstawiające rzeczywistość

UważAI co zostawiasz w sieci

Dane/Informacje…
https://haveibeenpwned.com $

…przygotowanie/sortowanie
https://dehashed.com $/$

…prezentacja
https://www.shodan.io/ $



…analiza

…przedstawiające rzeczywistość

Gdzie zgłosić incydent?

- Policja
- SMS -> 8080
- https://incydent.cert.pl/
- Bank, instytucja, dostawca usługi
- UODO 606-950-000

DZIĘKUJĘ
ZA UWAGĘ

Dawid Zięcina

Krajowa Sieć
Obszarów Wiejskich

www.ksow.pl