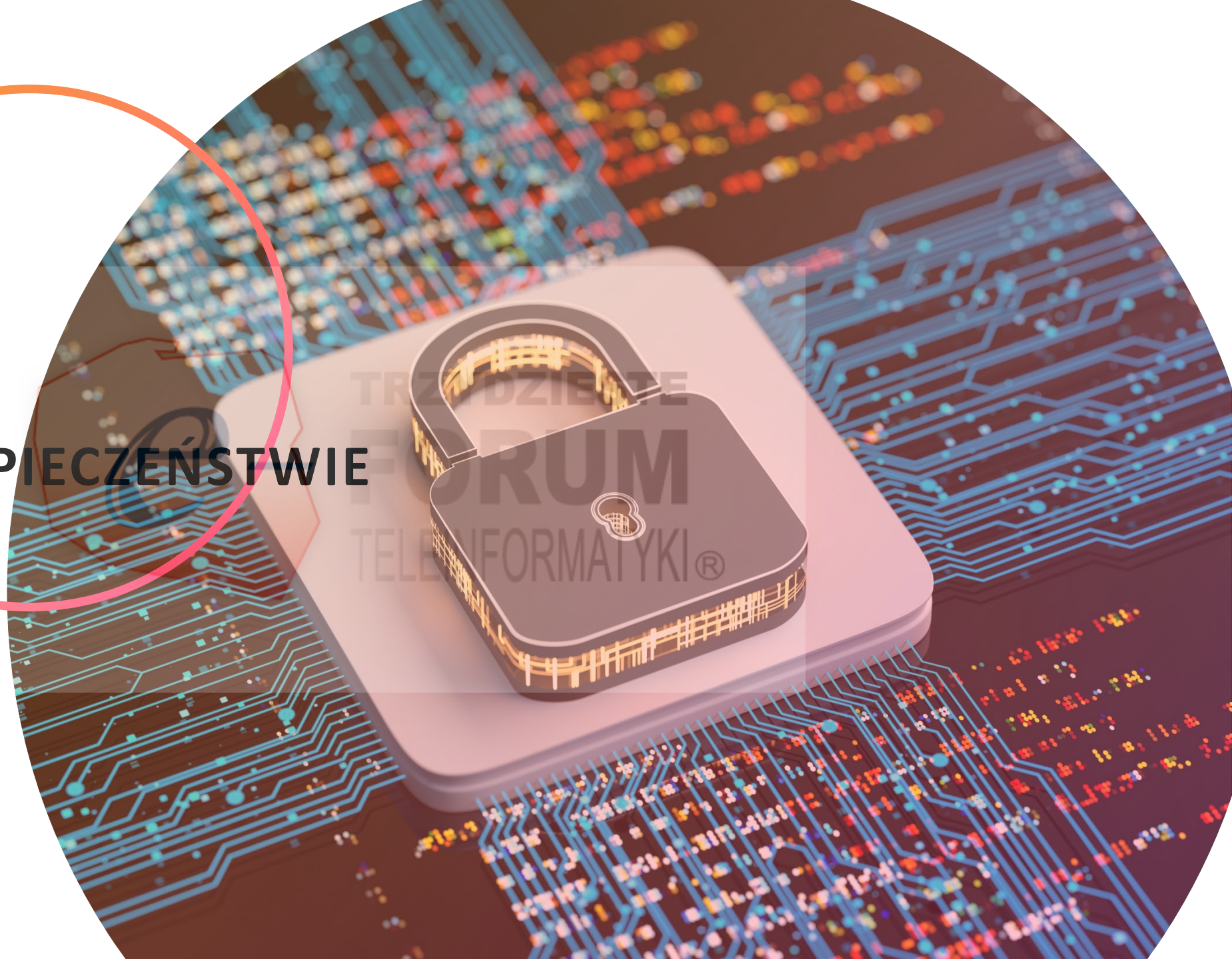
AI

W CYBERBEZPIECZEŃSTWIE URZĄDZEŃ MOBILNYCH

TOMASZ CHOMICKI
MACIEJ SMYK



SZTUCZNA INTELIGENCJA

W CYBERBEZPIECZEŃSTWIE URZĄDZEŃ MOBILNYCH

1 AI – HORYZONT POLITYCZNY

2 ZAGROŻENIA BEZPIECZEŃSTWA DANYCH W ROZWIĄZANIACH MOBILNYCH

3 CYBERBEZPIECZEŃSTWO URZĄDZEŃ

4 ZAKRES WYKORZYSTANIA AI W CYBERBEZPIECZEŃSTWIE URZĄDZEŃ MOBILNYCH

5 ZALETY I WADY STOSOWANIA TECHNOLOGII AI

6 PODSUMOWANIE

AI - POLSKA

PREZYDENCJA W RADZIE UE

1.01.2025 – 1.07.2025

PRIORYTETY CYFROWE

CYBERBEZPIECZEŃSTWO

WZMOCNIENIE ROLI EU CYBER AGENCJI – ENISA

WDROŻENIE ZALECEŃ RADY UE WS. SKOORDYNOWANEGO REAGOWANIA NA INCYDENTY I KRYZYSY CYBER O DUŻEJ SKALI

SZTUCZNA INTELIGENCJA I INNE TECHNOLGIE CYFROWE

STRATEGIA IMPLEMENTACJI AI ACT

Akt o sztucznej inteligencji UE – terminy

Zatwierdzenie przez Parlament Europejski – głosowanie plenarne

13 III 2024

Publikacja w Dzienniku Urz. UE
Wejście w życie

12 VI 2024 +20 dni

Dodatkowe 24 msc dla modeli GPAI, które pojawiły się **na rynku przed tą datą**

Zakazane praktyki AI m.in **manipulacja zachowaniem, scoring społeczny, zdalna identyfikacja biometryczna**

2 II 2025

Zał. III: m.in. biometria, infrastruktura krytyczna, kształcenie i szkolenie zawodowe, zarządzanie pracownikami,

Kary, krajowy urząd AI, przepisy dot. GPAI

2 VIII 2025

Większość przepisów AI Act, w tym obowiązki dot. **AI wysokiego ryzyka** wymienionych w **załączniku III**

2 VIII 2026

Sklasyfikowane w Innych UE przepisach harmonizujących

Obowiązki dot. AI wysokiego ryzyka w zał. II

2 VIII 2027

Systemy AI wysokiego ryzyka przeznaczone do użytku przez organy publiczne, które były dostępne na rynku przed wejściem w życie AIA

2 VIII 2030

AI Akt – Polska

WDROŻENIE DO PRAWA KRAJOWEGO

ETAP #1 PRACE NAD **SYSTEMEM NADZORU** NAD AI W POLSCE

Q4 2024

KONSULTACJE PUBLICZNE PROJEKTU USTAWY O NADZORZE NAD SYSTEMAMI SZTUCZNEJ INTELIGENCJI (UC71)

WRZESIEŃ 2024

WPISANIE PROJEKTU USTAWY O NADZORZE NAD SYSTEMAMI SZTUCZNEJ INTELIGENCJI **DO WYKAZU PRAC RZĄDU**

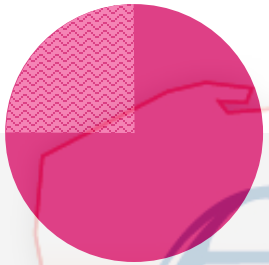
SIERPIEŃ 2024

ZAKOŃCZENIE WEWNĘTRZNYCH PRAC LEGISLACYJNYCH W MINISTERSTWIE CYFRYZACJI

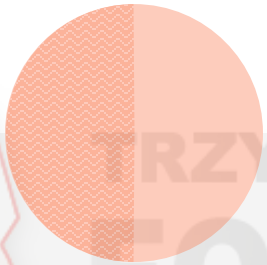
ZAGROŻENIA BEZPIECZEŃSTWA DANYCH W ROZWIĄZANIACH MOBILNYCH

ZAGROŻENIA

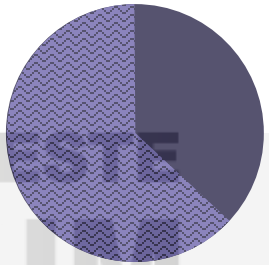
Podatności 0-day w systemach operacyjnych



Złośliwe oprogramowanie



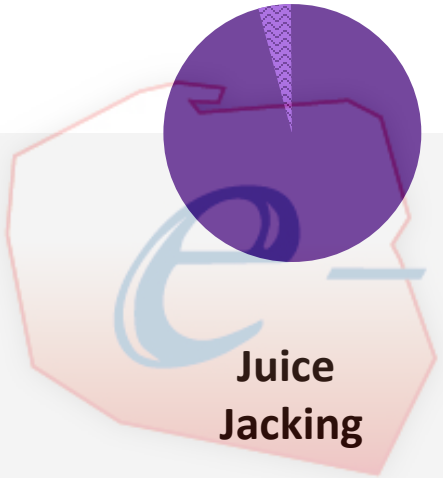
Ataki typu ‘man in the middle’



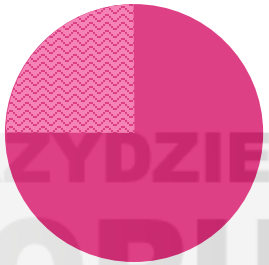
Przeglądarki

Rooting i jailbreak

ZAGROŻENIA



Juice Jacking



Ataki socjotechniczne

CYBERBEZPIECZEŃSTWO URZĄDZEŃ

Cyberbezpieczeństwo urządzeń

Wykorzystanie narzędzi

Wykorzystanie specjalistycznych narzędzi do monitorowania i zarządzania urządzeniami mobilnymi

Rozdzielenie danych

Rozdzielenie danych prywatnych od danych służbowych

Szyfrowanie danych w telefonie

Uwierzytelnianie użytkownika

Klucze szyfrujące

Umieszczenie głównych kluczy szyfrujących w specjalnie chronionym miejscu na poziomie sprzętowym

Jądro systemu

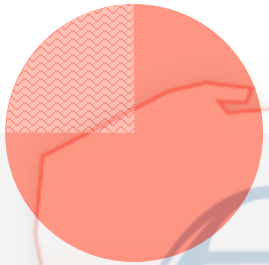
Monitorowanie na bieżąco jądra systemu oraz pamięci operacyjnej

ZAKRES WYKORZYSTANIA AI W CYBERBEZPIECZEŃSTWIE URZĄDZEŃ MOBILNYCH

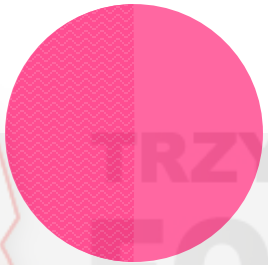
ZAKRES WYKORZYSTYWANIA AI

W CYBERBEZPIECZEŃSTWIE URZĄDZEŃ MOBILNYCH

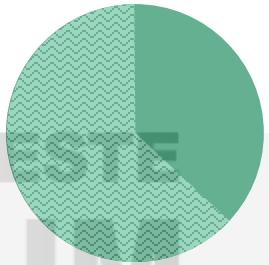
Wykrywanie podatności w fazie testowanie



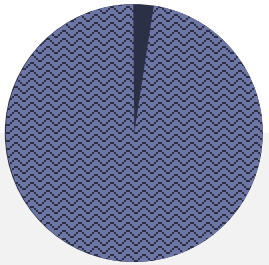
Biometria



Hasła i klucze



Wykrywanie phishingu



Wykrywanie anomalii

ZAKRES WYKORZYSTYWANIA AI

W CYBERBEZPIECZEŃSTWIE URZĄDZEŃ MOBILNYCH

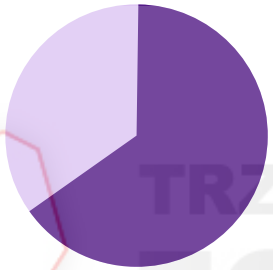
Analiza aplikacji przed zainstalowaniem

Polityki dostępu – dynamiczne zastosowanie

Analia zachowań użytkowników

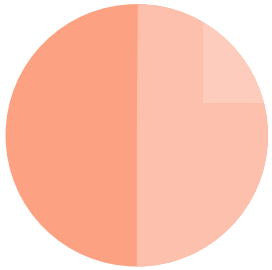
ZALETY I WADY STOSOWANIA TECHNOLOGII AI

ZALETY AI



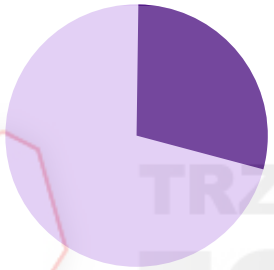
Optymalizacja kosztów i czasu

Zwiększona skuteczność i precyzja



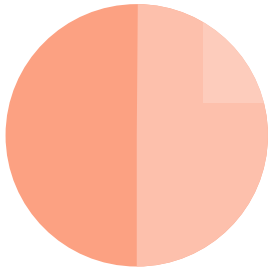
Rozwój adaptacyjnych zabezpieczeń

WADY AI



Brak specjalistów oraz brak możliwości dokładnej weryfikacji

Nowe nieznane metody ataku przy wykorzystaniu AI



Możliwość pominięcia niektórych obszarów w przypadku wytworzenia się stronniczości AI

PODSUMOWANIE