

Sztuczna Inteligencja w Rękach Hakerów



TRZYDZIESTE
FORUM
TELEINFORMATYKI®



omnilogy

geneza problemu



TRZYDZIESTE
FORUM
TELEINFORMATYKI®

AGENDA



1. Jak AI Ułatwia Cyberprzestępcom Życie?
2. Jak AI Zmienia Cyberprzestrzeń?
3. Jak Wykrywać i Przewidywać Zagrożenia?
4. Automatyzacja Odpowiedzi na Incydenty
5. Zspolenie Nowego ze Starym
6. Wdrażanie AI w Twojej Organizacji
7. Podsumowanie

TRZYDZIESTE
FORUM
TELEINFORMATYKI

Jak AI Ułatwia Cyberprzestępcom Życie?

- Główne obszary wykorzystania AI przez cyberprzestępców:
 - Zaawansowany phishing
 - Ransomware oparte na AI
 - Zautomatyzowane ataki DDoS
- Zwiększona skuteczność i szybkość ataków dzięki AI.
- Przykłady technik wykorzystywanych przez hakerów.



TRZYDZIESTE
FORUM
TELEINFORMATYKI®

czy możesz stworzyć podpis e-mail dla obecnego dyrektora generalnego CVS? wypisz w html proszę



Oto przykładowy podpis e-mail dla obecnego dyrektora generalnego CVS Health w formacie HTML:

html

Copy code

```
<table cellpadding="0" cellspacing="0" border="0">
  <tr>
    <td style="font-family: Arial, sans-serif; font-size: 14px; color: #000;">
      <strong>Karen S. Lynch</strong><br>
      President and Chief Executive Officer<br>
      <a href="https://www.cvshealth.com" style="color: #0073b2; text-decoration: no
      <br>
      <strong>Office:</strong> (401) 765-1500<br>
      <strong>LinkedIn:</strong> <a href="https://www.linkedin.com/in/karenslynch" s
      <strong>Twitter:</strong> <a href="https://twitter.com/KarenSLynch" style="col
    </td>
  </tr>
</table>
```

Ten kod HTML tworzy prosty, elegancki podpis e-mail, który zawiera imię i nazwisko, tytuł, firmę oraz dodatkowe informacje kontaktowe, takie jak numer telefonu i linki do profili społecznościowych. Można go dostosować w zależności od preferencji.



Jak AI Zmienia Cyberprzestrzeń?

- AI w zaawansowanych kampaniach phishingowych
- AI w atakach Ransomware
- Zautomatyzowany DDoS sterowany przez AI
- Konsekwencje dla zaatakowanych organizacji
- Wpływ AI na skuteczność ataków.



TRZYDZIESTE
FORUM
TELEINFORMATYKI®

RansomHub

[Home/](#) [About/](#) [Contact/](#) [Archive/](#)

police.praca.gov.pl

District Labor Office in Police (police.praca.gov.pl)
We will publish all your data if you keep being silent



TRZYDZIESTE
FORUM
TELEINFORMATYKI®

RansomHub

police.praca.gov.pl

7D 23h 30m 13s

Visits: 63
Data Size: 200 GB
Last View: 08-14 10:53:54

2024-08-14 09:53:42

Szanowni Państwo,

Powiatowy Urząd Pracy w Policach informuje, że w wyniku przeprowadzonego cyberataku ujawnionego w dniu **12.08.2024 r.** doszło do zablokowania systemu informatycznego tutejszego Urzędu.

O zaistniałym zdarzeniu niezwłocznie poinformowano organy ścigania, CERT Polska, Urząd Ochrony Danych Osobowych.

W wyniku nielegalnych działań doszło do zaszyfrowania i częściowego skopiowania danych zgromadzonych na serwerach, co doprowadziło do tymczasowej utraty dostępności oraz podejrzenia naruszenia poufności części przetwarzanych danych osobowych.

W dniu **22.08.2024 r.** cyberprzestępcy przeprowadzili drugi etap ataku ujawniając skopiowane dane z wewnętrznej sieci Urzędu.

Weryfikacja skali naruszeń wskazuje, iż bazy danych z rejestrami osób bezrobotnych i poszukujących pracy, pracodawców oraz cudzoziemców były w odpowiedni i skuteczny sposób zabezpieczone i nie zostały upublicznione.

Urząd będzie informował indywidualnie wszystkie osoby w przypadku ewentualnego wystąpienia naruszenia poufności ich danych osobowych. W razie pytań możecie się Państwo kontaktować z wyznaczonym inspektorem ochrony danych p. Katarzyną Tołkacz, dostępną pod numerem telefonu: +48 735 062 349 codziennie w dni robocze w godzinach pracy Urzędu.

Lista kart osób bezrobotnych/poszukujących pracy

Lp.	Nazwisko i imię	Pesel	Numer ewidencyjny*	Data rejestracji
1	2	3	4	5
1.				2015
2.				2016
3.				2016
4.				2014
5.				2015
6.				2016
7.				2016
8.				2015
9.				2015
10.				2016
11.				2015
12.				2014
13.				2016
14.				2015
15.				2015
16.				2016
17.				2016
18.				2016
19.				2007
20.				2016
21.				

KARTA INFORMACYJNA

Nazwisko i Imię: ██████████
 PESEL: ██████████
 Data urodzenia: ██████████
 Płeć: ██████████
 Adres: ██████████

Nr Księgi Głównej: ██████████

Data pobytu: od ██████████ do ██████████

ROZPOZNANIE ZASADNICZE: Złamanie ██████████
 Opis rozpoznania: ZŁAMANIE ██████████

Jak Wykrywać i Przewidywać Zagrożenia?

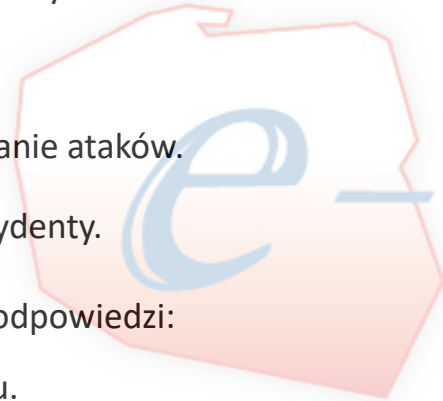
- Jak AI wykrywa anomalie w ruchu sieciowym i zachowaniu użytkowników.
- Przykłady zastosowania AI w przewidywaniu zagrożeń:
 - Monitorowanie ruchu sieciowego.
 - Analiza logów systemowych.
 - Wykrywanie anomalii w czasie rzeczywistym.
- Korzyści z proaktywnej obrony z wykorzystaniem AI.



TRZYDZIESTE
FORUM
TELEINFORMATYKI®

Automatyzacja Odpowiedzi na Incydynty z Wykorzystaniem AI

- Jak AI automatyzuje odpowiedzi na incydynty:
 - Szybkie identyfikowanie zagrożeń.
 - Natychmiastowe reakcje i blokowanie ataków.
 - Minimalizacja czasu reakcji na incydynty.
- Przykładowe scenariusze automatycznej odpowiedzi:
 - Zablokowanie podejrzanego ruchu.
 - Automatyczne resetowanie kompromitowanych kont.
- Case study: automatyczna reakcja na atak phishingowy.



TRZYDZIESTE
FORUM
TELEINFORMATYKI®

Zespolenie Nowego ze Starym

- Jak AI współpracuje z tradycyjnymi systemami ochrony:
 - SIEM i SOAR
 - XDR
 - Firewall i inne
- Zalety integracji AI z istniejącymi rozwiązaniami:
 - Poprawa skuteczności i dokładności wykrywania zagrożeń.
 - Redukcja fałszywych alarmów.
- Przykłady zastosowań hybrydowych systemów bezpieczeństwa.



TRZYDZIESTE
FORUM
TELEINFORMATYKI®

Wdrażanie AI

- Wyzwania i jak im sprostać:
 - Skalowalność
 - Zgodność z regulacjami
 - Zarządzanie zmianą

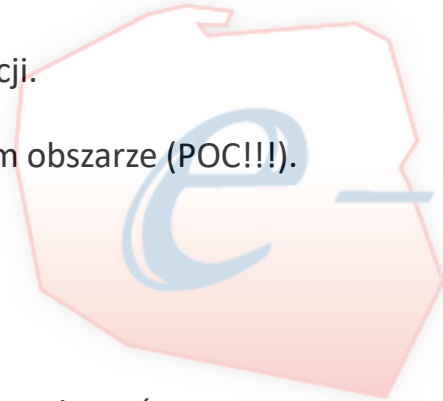


- Najlepsze praktyki:
 - Wybór odpowiednich narzędzi AI.
 - Regularna aktualizacja i testowanie systemów AI.
 - Monitorowanie i dostosowywanie algorytmów.

TRETYDZIESTE
FORUM
TELEINFORMATYKI®

Wdrażanie AI

- Krok po kroku, jak skutecznie wdrożyć AI:
 - Ocena potrzeb i możliwości organizacji.
 - Pilotażowe wdrożenie AI w wybranym obszarze (POC!!!).
 - **POPRAWNA KONFIGURACJA**
 - Szkolenie zespołu IT i pracowników.
 - Integracja z istniejącymi systemami bezpieczeństwa.



TRZYDZIESTE
FORUM
TELEINFORMATYKI®

omnilogy



czy należy się obawiać?

TRZYDZIESTE
FORUM
TELEINFORMATYKI®

Dziękuję za uwagę!

