Linke Kulicki

Czy cyberbezpieczeństwo jest możliwe w dobie sztucznej inteligencji?

Łódź, 07.12.2023 r.

r. pr. Marek Porzeżyński

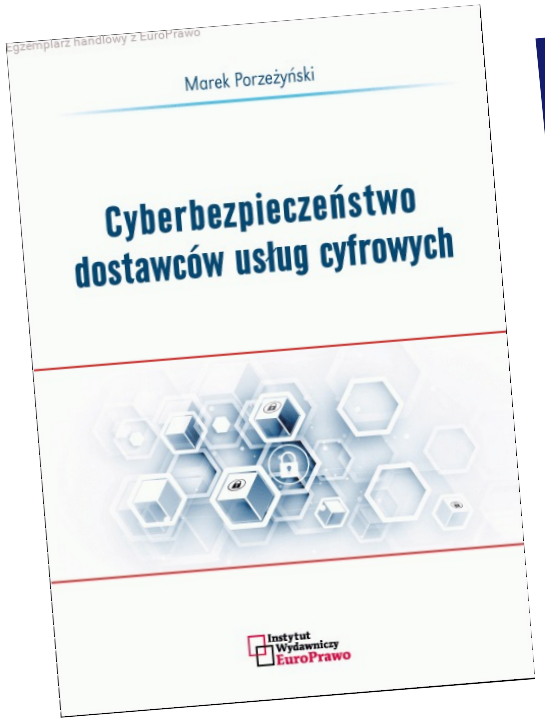
Linke
Kulicki

Agenda

1. Wprowadzenie
2. Sztuczna inteligencja i AI Act
3. Cyberbezpieczeństwo i NIS
4. NIS 2 - przyczyny
5. Możliwości wykorzystania sztucznej inteligencji w służbie cyberbezpieczeństwa
6. Wyzwania dla Cyberbezpieczeństwa
7. Q&A

Linke Kulicki // Politechnika Warszawska

Marek Porzeżyński



- **Doktor nauk prawnych, MBA, CIPP/E,**
- **Radca prawny, członek OIRP w Warszawie,**
- Wykładowca, badacz na Politechnice Warszawskiej, Wydział Administracji i Nauk Społecznych,
- Specjalizuje się w zagadnieniach związanych z **ochroną własności intelektualnej i prawem nowych technologii** ze szczególnym uwzględnieniem ochrony danych osobowych i cyberbezpieczeństwa,
- Od ponad dekady doradza Klientom w zakresie swojej specjalizacji oraz uczestniczy w transakcjach na rynku nowych technologii. Doświadczenie zdobywał w największych międzynarodowych i polskich kancelariach prawnych,
- Autor ponad 50 publikacji naukowych, w tym książek **„Zdolność patentowa programów komputerowych”** i **”Cyberbezpieczeństwo dostawców usług cyfrowych”.**

Linke
Kulicki

Nowa definicja systemów sztucznej inteligencji

Artificial intelligence system (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments.

-

System sztucznej inteligencji oznacza system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii i który może do wyraźnych lub dorozumianych celów generować wyniki, takie jak przewidywania, zalecenia lub decyzje wpływające na środowiska fizyczne **lub wirtualne.**

Linke
Kulicki

Implementacja

Czekamy...

Linke
Kulicki

Cyberbezpieczeństwo

Zachowanie poufności, integralności i dostępności informacji w cyberprzestrzeni, co obejmuje zapobieganie oraz minimalizowanie wpływu cyberataków i w przypadku ich wystąpienia, przywrócenie usług cyfrowych.

Linke
Kulicki

Implementacja dyrektywy NIS w Polsce

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560) - weszła w życie 28 sierpnia 2018 r. i obowiązuje obecnie

Linke
Kulicki

Implementacja dyrektywy NIS w Polsce – akty wykonawcze

1. Rozporządzenie Rady Ministrów w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.
2. Rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za poważny.
3. Rozporządzenie Rady Ministrów w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.
4. Rozporządzenie Ministra Cyfryzacji w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
5. Rozporządzenie Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.
6. Rozporządzenie Rady Ministrów w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa.
7. Rozporządzenie Ministra Cyfryzacji w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług.
8. Rozporządzenie Ministra Cyfryzacji w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług.

Linke
Kulicki

Czym jest dyrektywa NIS 2 ?

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.

Linke Kulicki

Powody wprowadzenia dyrektywy NIS 2

1. Wybuch pandemii COVID-19 i przyspieszenie cyfryzacji.
2. Nieegzekwowanie przez Państwa Członkowskie kar nałożonych na podstawie dyrektywy NIS.
3. Konieczność odzwierciedlenia znaczenia danych sektorów lub usług dla działalności społecznej i gospodarczej Unii Europejskiej.
4. Chęć unifikacji przepisów implementacyjnych w Państwach Członkowskich.
5. **Odpowiedź na zmiany w zakresie cyfryzacji i zaawansowane ataki cybernetyczne.**
6. Konieczność zapewnienia spójności z przepisami sektorowymi.

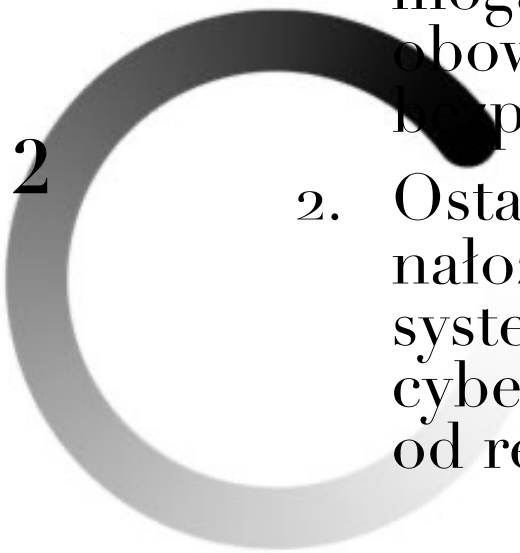
Linke
Kulicki

Implementacja NIS 2

1. NIS 2 zakłada harmonizację minimalną – państwa członkowskie mogą wprowadzić dodatkowe obowiązki, które nie wynikają bezpośrednio z dyrektywy.
2. Ostateczny kształt obowiązków nałożonych na podmioty krajowego systemu w zakresie cyberbezpieczeństwa będzie zależał od regulacji państw członkowskich.

Linke
Kulicki

Implementacja NIS 2



1. NIS 2 zakłada harmonizację minimalną – państwa członkowskie mogą wprowadzić dodatkowe obowiązki, które nie wynikają bezpośrednio z dyrektywy.
2. Ostateczny kształt obowiązków nałożonych na podmioty krajowego systemu w zakresie cyberbezpieczeństwa będzie zależał od regulacji państw członkowskich.

Linke
Kulicki

AI jako narzędzie „obronne”

1. **Automatyzacja wykrywania i reagowania** - AI może szybko identyfikować i reagować na zagrożenia ceybernetyczne, znacznie szybciej niż ludzkie zespoły bezpieczeństwa.
2. **Analiza behawioralna -** Systemy AI mogą uczyć się wzorców zachowań użytkowników i sieci, co umożliwia wykrywanie anomalii i potencjalnych zagrożeń.
3. **Prognozowanie i prewencja -** Algorytmy predykcyjne mogą przewidywać przyszłe ataki na podstawie trendów i danych historycznych, pozwalając organizacjom przygotować się na nie.

Linke
Kulicki

AI jako narzędzie „obronne”

4. **Weryfikacja istniejących zabezpieczeń** – sztuczna inteligencja znacznie precyzyjniej od człowieka sprawdzi zabezpieczenia i wychwyci ich luki.
5. **Weryfikacja tożsamości** – AI może przeprowadzać weryfikację znacznie szybciej niż człowiek oraz może weryfikować tożsamość kilku lub kilkunastu osób jednocześnie.
6. **Ochrona przed phishingiem** – AI ma możliwość rozpoznawania prób phishingu, dzięki czemu może informować użytkownika o takim zagrożeniu.

Linke
Kulicki

AI jako narzędzie stanowiące zagrożenie dla cyberbezpieczeństwa

1. **Automatyzacja ataków** możliwość wykorzystania AI do przeprowadzania skomplikowanych ataków na wielką skalę, które są trudne do wykrycia i zatrzymania.
2. **Dynamiczne dostosowywanie złośliwego oprogramowania** - AI może adaptować złośliwe oprogramowanie do zmieniających się warunków sieciowych, unikając wykrycia przez tradycyjne antywirusy.
3. **Rozbudowa technik phishingowych** AI ma możliwość generowania bardzo wiarygodnych fałszywych wiadomości e-mail/sms/komunikatów, które są trudne do odróżnienia od autentycznych z uwagi na możliwość uczenia się, w jaki sposób ludzie reagują na daną próbę wyłudzenia informacji.

Linke
Kulicki

AI jako narzędzie stanowiące zagrożenie dla cyberbezpieczeństwa

4. **Wykrywanie luk w oprogramowaniu ochronnym** sztuczna inteligencja może nie tylko szukać luk w oprogramowaniu, by je naprawiać ale również w celu przeprowadzenia skuteczniejszego ataku.

5. **Dynamiczne dostosowywanie złośliwego oprogramowania** - AI może adaptować złośliwe oprogramowanie do zmieniających się warunków sieciowych, unikając wykrycia przez tradycyjne antywirusy.

6. **Potencjalne wywoływanie fałszywych alarmów** - AI może wywoływać fałszywe alarmy bezpieczeństwa ze względu na czułość w wykrywaniu niedoskonałości zabezpieczeń.

7. **Zagrożenie dla prywatności i danych osobowych** niekontrolowane gromadzenie danych przez systemy AI, wycieki danych, profilowanie, spoofing tożsamości, scrapping, scoring społeczny, deepfake

8. **Zatruwanie AI danymi w prowadzającymi w błąd** wprowadzenie błędnych lub fałszywych danych do modeli AI, które są używane do analizy zagrożeń lub podejmowanych decyzji.

Linke Kulicki

Wyzwania związane z AI w cyberbezpieczeństwie

1. **Wykorzystanie AI w przestępczości**
2. **Złożoność decyzji i algorytmów** – trudności w interpretacji decyzji podejmowanych przez AI oraz weryfikacji ich neutralności
3. **Stronniczość w algorytmach AI** – AI może dyskryminować pewne grupy lub wykazywać uprzedzenia, co prowadzi do nierównego traktowania i może wpływać na decyzje dotyczące cyberbezpieczeństwa.

Linke
Kulicki

Konieczne obszary działania

1. **Regulacje prawne, ustanowienie standardów etycznych i standardów bezpieczeństwa, jak i zakazanych praktyk w zakresie sztucznej inteligencji** np. AI Act, NIS 2, działanie ENISA, Strategia Sztucznej Inteligencji dla NATO, Biała księga w sprawie sztucznej inteligencji
2. **Edukacja** szkolenia, programy edukacyjne mające na celu nauczenie identyfikacji i reagowania na cyberzagrożenia, jak również korzystanie z nowych technik wykorzystujących AI, zwiększenie świadomości w zakresie cyberbezpieczeństwa
3. **Współpraca międzynarodowa** wymiana wiedzy i najlepszych praktyk, ułatwienie współpracy pomiędzy państwami i organizacjami w zakresie rozwoju i wdrażania skutecznych strategii cyberbezpieczeństwa

Linke
Kulicki

Konieczne obszary działania cd.

4. **Innowacje technologiczne:**

1) **rozwój narzędzi zabezpieczających** tworzenie zaawansowanych technologii wykorzystujących AI do lepszego wykrywania i zwalczania cyberzagrożeń

2) **inwestycje w badania i rozwój** finansowanie projektów badawczych skupionych na innowacyjnych rozwiązaniach w dziedzinie cyberbezpieczeństwa

5. **Wzmocnienie infrastruktury krytycznej** - zabezpieczenie kluczowych zasobów infrastruktury krytycznej takiej jak sieci energetyczne, systemy finansowe, usługi publiczne przed cyberatakami

Linke Kulicki

Dziękuję za uwagę

- dr Marek Porzeżyński, r. pr., MBA, CIPP/E
- www.linkekulicki.pl / www.marekporzezynski.pl
- + 48 606 433 023
- m.porzezynski@linkekulicki.pl