10.10.2025

Fundusze Europejskie

KONFERENCJA

Cyberbezpieczeństwo w zamówieniach publicznych

Warszawa, 12 września 2025 r.

Fundusze Europejskie

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

10.10.2025

Fundusze Europejskie

Cyberbezpieczeństwo w zamówieniach publicznych – blaski i cienie

Tomasz Chomicki

Dr hab. prof. UŚ Dariusz Szostek

Fundusze Europejskie

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

10.10.2025

Fundusze Europejskie

Tomasz Chomicki, PIIT

Dr hab. prof. UŚ Dariusz Szostek, Cyber Science, Związek Polska Cyfrowa

10.10.2025

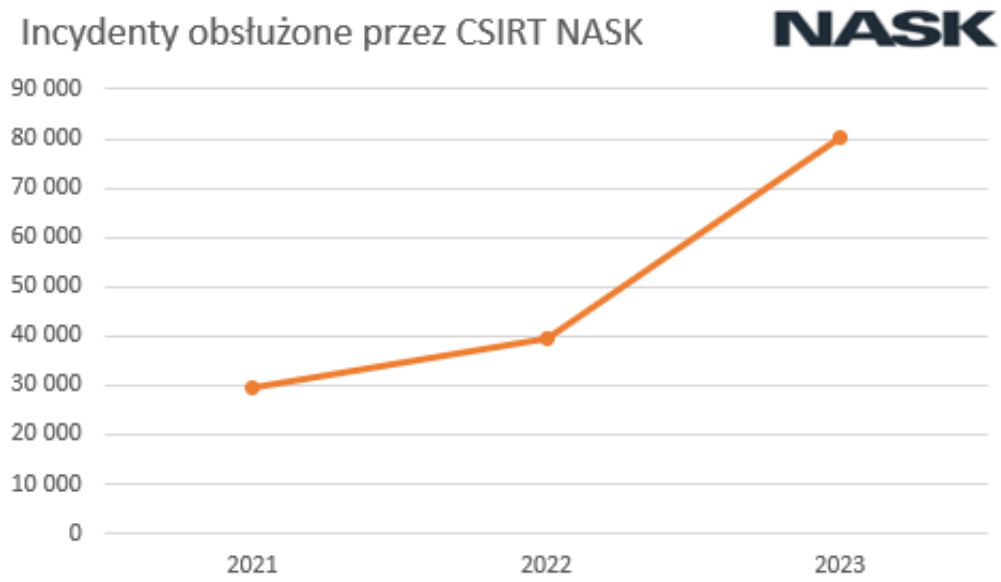
Fundusze Europejskie

Gdzie jesteśmy ?

I dokąd zmierzamy ?

Ilość cyberataków Polska 2024r.

Ponad 114 tys.



10.10.2025

Cyberbezpieczeństwo w AI a zamówienia publiczne

- **W 2024 roku odnotowano 442% wzrost liczby ataków wykorzystujących techniki inżynierii społecznej wspomagane przez generatywną AI**

- **W I półroczu 2025 wzrost ataków ransomware**
  - **Polska** **6 proc. globalnych incydentów**
  - **USA** **5,74 proc.**
  - **Słowacja** **5,45 proc.**
  - **Ukraina** **4,68 proc.**

Pożar Centrum Marywilska 44, Warszawa 12 maja 2024r.

10.10.2025

Zagadnienia w zakresie pzp

- Cyberbezpieczeństwo w komunikacji w ramach przygotowań zamówień publicznych.
- AI a zamówienia publiczne
- Cyberbezpieczeństwo jako jedno z ważniejszych kryteriów zamówień publicznych
- Certyfikacja jako element procesu zamówień publicznych
- Weryfikacja dostawców (łańcuch dostaw) w ramach zamówień publicznych (audyt oferentów ?)
- Terminy i czas w ramach zamówień publicznych
- Czy nie czas na wyłączenie zamówień publicznych z zakresu cyberbezpieczeństwa ?
- Bezpieczeństwo w sektorze infastruktury krytyczne

  oraz kluczowych instytucji państwowych.

Blaski – pozytywne aspekty

1. **Rosnąca świadomość administracji**
   Zamawiający coraz częściej zdają sobie sprawę z konieczności ochrony danych i systemów. W specyfikacjach pojawiają się zapisy dotyczące szyfrowania, kopii zapasowych, czy audytów bezpieczeństwa.

2. **Implementacja prawa unijnego (NIS2)**
   Dyrektywa NIS2, implementowana w polskim systemie prawnym, nakłada na podmioty publiczne i ich dostawców konkretne obowiązki. To przyspiesza proces harmonizacji i podnoszenia standardów.

3. **Rozwój certyfikacji i norm**
   Coraz większe znaczenie mają międzynarodowe standardy, takie jak ISO/IEC 27001 czy Common Criteria. Certyfikaty te w naturalny sposób podnoszą poprzeczkę w przetargach publicznych.

4. **Profesjonalizacja kadr**
   Administracja sukcesywnie rozwija swoje zespoły ds. IT i bezpieczeństwa, co

5. **Wykorzystanie rekomendacji branżowych**

Cienie – problemy i zagrożenia

1. **Cena jako dominujące kryterium** – wciąż często decyduje najniższa cena, co ogranicza bezpieczeństwo zamawianych systemów – obawa przed karą.
2. **Fragmentaryczne regulacje** – brak jednolitych wymogów bezpieczeństwa; każdy zamawiający ustala je indywidualnie.
3. **Brak kompetencji** – niedostatek specjalistów powoduje, że zapisy w specyfikacji bywają zbyt ogólne lub łatwe do obejścia.
4. **Problemy z weryfikacją wykonawców** – zamawiający nie mają narzędzi do sprawdzenia faktycznego poziomu bezpieczeństwa oferentów.
5. **Vendor lock-in** – uzależnienie od jednego dostawcy powoduje podatność i brak elastyczności.
6. **Praktyczne incydenty** – np. ataki ransomware na szpitale i urzędy, niedoszacowane wymagania bezpieczeństwa w systemach e-zdrowia, błędy przy wdrażaniu systemów administracyjnych.
7. **Rola polskich dostawców cyberbezpieczeństwa**– selekcja na bazie kompetencji i wybranych referencji

Fundusze Europejskie

Kluczowe obszary cyberbezpieczeństwa i pzp

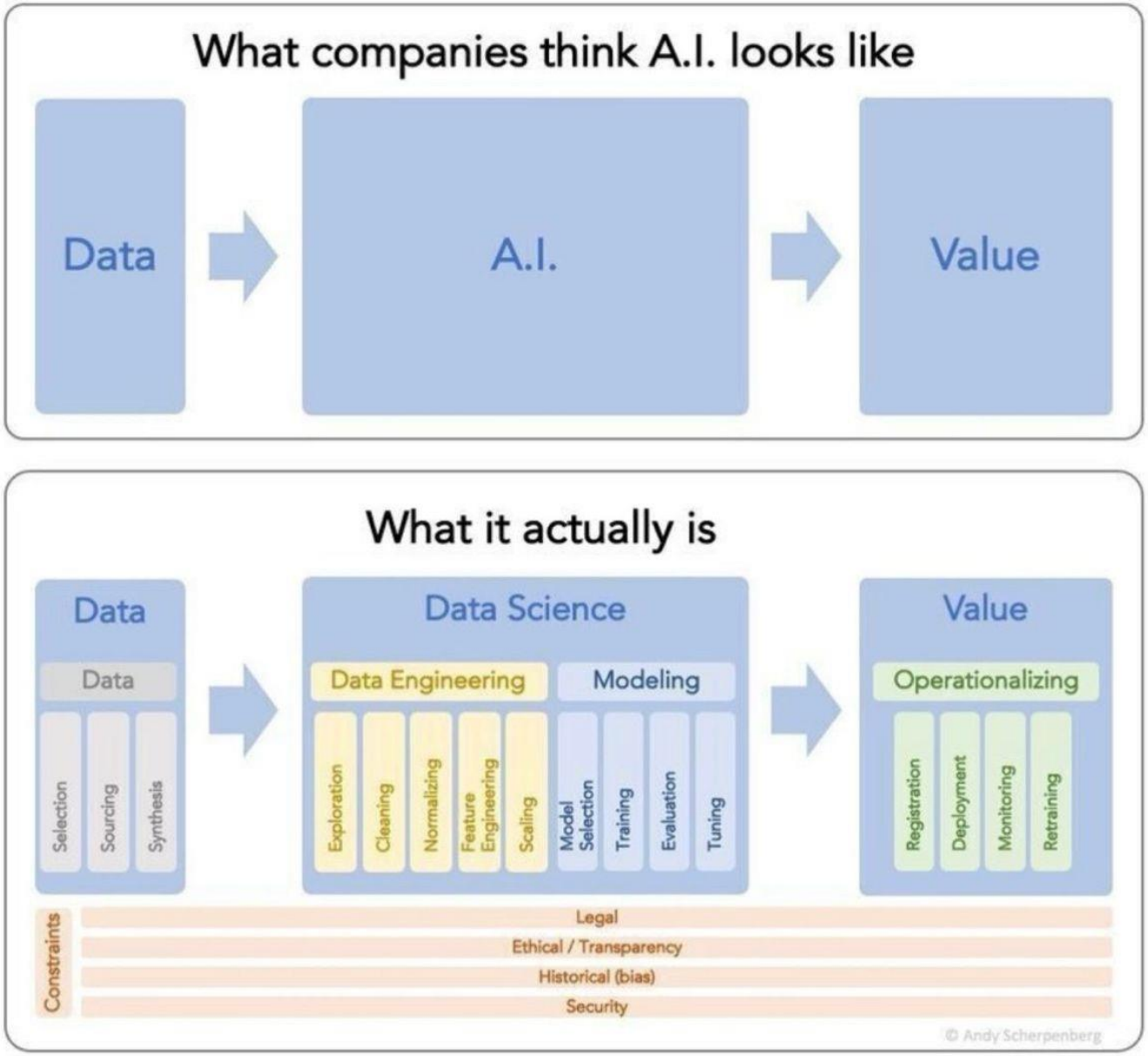
Cyberbezpieczeństwo w komunikacji w ramach przygotowań zamówień publicznych

- **Znaczenie:** proces przetargowy zaczyna się od przygotowania dokumentów. Niewłaściwa komunikacja (np. używanie prywatnych maili) otwiera drzwi do wycieku danych i manipulacji SIWZ.

- **Rekomendacje:**
  - Korzystanie wyłącznie z bezpiecznych, szyfrowanych kanałów komunikacji
  - Klasyfikacja informacji jako „zastrzeżone” do momentu publikacji.
  - Szkolenia cyberbezpieczeństwa dla zespołów przetargowych.
  - Zakaz korzystania z otwartych narzędzi AI/chmury do przechowywania i analizy wrażliwych projektów dokumentów.
  - Przy dużych przetargach tarcza ochronna

AI w procesie przetargowym

- Używanie AI w procesie przygotowania siws zgodnie z z zasadami cyberbezpieczeństwa
- Używanie AI w procesie analizy dokumentów przetargowych (ofert) zgodnie z zasadami cyberbezpieczeństwa
- Wdrażanie AI w pzp wyłącznie po analizie ryzyka i zgodnie z normami cyberbezpieczeństwa


What companies think A.I. looks like
Data
A.I.
Value
What it actually is
Data
Data
Selection
Sourcing
Synthesis
Data Science
Data Engineering
Exploration
Cleaning
Normalizing
Feature Engineering
Scaling
Modeling
Model Selection
Training
Evaluation
Tuning
Value
Operationalizing
Registration
Deployment
Monitoring
Retraining
Constraints
Legal
Ethical / Transparency
Historical (bias)
Security
© Andy Scherpenberg

CyberPOLICY NASK

Cyberbezpieczeństwo AI

- Środki specyficzne dla algorytmów modeli AI/ML
- Standardowe środki techniczne i organizacyjne stosowane w cyberbezpieczeństwie

Kategorie obszarów zagrożeń:

- skierowanych na same algorytmy czy modele sztucznej inteligencji,
- w procesie zarządzania i przetwarzania danych, którymi posługują się algorytmy,
- dla procesu trenowania algorytmów zbiorami danymi,
- dla implementacji programowej modeli oraz systemu sztucznej inteligencji,
- wynikających z istniejących podatności infrastruktury teleinformatycznej (zwirtualizowanej, chmurowej lub fizycznej), na której działa system AI.

Analiza zagrożeń wykorzystania AI w organach publicznych

Metodyki modelowania zagrożeń dla AI w organach publicznych:

1. Tradycyjne dotyczące zagrożeń : poufność, integralność, dostępność, autentyczność, niezaprzeczalność

2. Dotyczące AI:
   - Odporność na ataki i niepożądane zmiany
   - Wyjaśnialność sposobu uzyskania wyniku
   - Skuteczność działania w odniesieniu do spodziewanych efektów
   - Audytowalność (możliwość badania cyberbezpieczeństwa systemu AI w każdej fazie jego cyklu życia)

Cyberbezpieczeństwo jako jedno z ważniejszych kryteriów zamówień publicznych

- **Dlaczego:** bezpieczeństwo musi być mierzalnym kryterium, a nie ogólnym hasłem.

- **Przykładowy model punktacji (waga 30%):**
  - **Warunek brzegowy:** spełnienie minimalnych wymagań (MFA, szyfrowanie, backupy).
  - **Metryki usługowe:** SLA bezpieczeństwa (np. czas reakcji na incydent, czas aktualizacji krytycznych podatności).
  - **Dojrzałość procesów:** istnienie ISMS, testy penetracyjne, polityka zarządzania podatnościami.
  - **Dowody:** certyfikaty, raporty audytowe, raporty z testów.

Certyfikacja jako element procesu zamówień publicznych

- **Cel:** uwiarygodnienie deklaracji wykonawcy i produktów.

- **Akceptowane certyfikaty lub równoważne (przykład):**
  - Organizacyjne: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2, ISO 22301.
  - Produktowe: Common Criteria, certyfikaty w schematach UE (EUCC), raporty SBOM/VEX.
- **Dobre praktyki:**
  - Żądanie zakresu certyfikatu zgodnego z przedmiotem zamówienia.
  - Weryfikacja aktualności audytów (≤12 miesięcy).
  - Akceptowanie równoważnych dowodów (np. audyty zewnętrzne).

Weryfikacja dostawców (łańcuch dostaw)

- **Znaczenie:** bezpieczeństwo systemu = bezpieczeństwo całego łańcucha dostaw.

- **Model weryfikacji (przykład):**
  - **Krok 1 – desk review:** ankieta due-diligence, polityki bezpieczeństwa, SBOM.
  - **Krok 2 – audyt:** przegląd u zwycięzcy przetargu (on-site/remote), testy techniczne, przegląd logów i procesów.
- **Zakres audytu:**
  - Personel i procesy: szkolenia, podział ról, procedury weryfikacji.
  - Technologia: segmentacja, EDR/SIEM, zarządzanie podatnościami.
  - Łańcuch dostaw: lista podwykonawców, jurysdykcja, zgodność z prawem.
  - Oprogramowanie: SBOM, praktyki secure-by-design, reagowanie na CVE.

Co należy zmienić w prawie polskim

- **Zastanowić się nad nowelizacją pzp:** obowiązek stosowania minimalnych wymogów cyberbezpieczeństwa w każdym przetargu IT; wprowadzenie kryteriów jakościowych; obowiązek oceny ryzyka.
- **Wyłączenie części pilnych zakupów** cyber z pzp
- **Zmiany w ustawie o krajowym systemie cyberbezpieczeństwa:** rozszerzenie obowiązków na wykonawców zamówień publicznych; utworzenie centralnej bazy certyfikowanych dostawców.
- **Wyspecjalizowane zespoły doradcze:** obowiązek konsultacji ekspertów ds. cyberbezpieczeństwa przy dużych zamówieniach IT.
- **Kontrole i audyty:** obowiązkowe testy penetracyjne i audyty bezpieczeństwa; weryfikacja historii incydentów (na etapie ofertowym, przed zawarciem umowy)
- **Edukacja:** obowiązkowe szkolenia z cyberbezpieczeństwa dla pracowników przygotowujących postępowania.

Projekt uchwały Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025-2029

Kancelaria Prezesa Rady Ministrów

- Wymogi cyberbezpieczeństwa w pzp
- Wyłączenie części pilnych zakupów w cyber z pzp
- Stworzenie chmury niejawnej i wyłączenie jej z pzp
- Rozwój rodzinnych technologii i zwiększenie suwerenności technologicznej

Fundusze Europejskie

Dziękujemy

Tomasz.Chomicki@piit.org.pl

Dariusz.szostek@szostek-digital.eu