Fundusze Europejskie

Cyberpułapki w zamówieniach publicznych

Bartosz Polak

7 września 2026

Fundusze Europejskie

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

Dlaczego urzędy są celem?

- Dane przetargowe, oferty, ceny - wysoka wartość dla cyberprzestępców
- Kontakty do setek wykonawców i tajemnica przedsiębiorstwa oferentów
- Presja terminów przetargowych - atakujący wykorzystują pośpiech
- Widoczność publiczna urzędu (BIP, rejestry) ułatwia profilowanie pod ataki
- Jedna przejęta skrzynka mailowa może dać dostęp do całego urzędu

Najczęstsze wektory ataków

- Phishing i spear phishing — najtańszy i najskuteczniejszy wektor
- Ransomware — paraliż urzędu i możliwy wyciek danych
- BEC — podmiana numeru konta przy płatnościach przetargowych
- Vishing i deepfake — weryfikacja głosem staje się trudniejsza
- Wycieki przez publiczne narzędzia AI — rosnące zagrożenie 2024–2026

Socjotechnika — jak sprawcy hackują ludzi

- Manipulacja emocjami: strach, presja czasu, autorytet przełożonego
- Urzędnik państwowy reaguje szybciej na „pilne polecenie” niż na spam
- Spear phishing — spersonalizowany atak na konkretną osobę
- Dane z BIP, LinkedIn i komunikatów prasowych budują wiarygodność
- To nie głupota ofiary — to profesjonalnie przygotowany scenariusz

Przykład ataku na urzędników

Zaawansowany Spear-Phishing

Urzędnicy otrzymują sfabrykowane wiadomości e-mail. Często wykorzystuje się motyw "pilnych dokumentów przetargowych", "odwołania " lub komunikatów od rzekomego działu IT. Link w wiadomości prowadził do fałszywego panelu logowania, który wiernie odwzorowuje interfejs używany przez urząd.

Powiecie Państwo, że mamy uwierzytelnianie dwuskładnikowe i jesteśmy bezpieczni na takie ataki...

Atak AiTM (Adversary-in-the-Middle)

Fałszywa strona logowania działa w tym modelu jako serwer proxy – przekazuje wpisywane dane w czasie rzeczywistym do prawdziwego serwera, wyzwala u użytkownika prośbę o kod SMS lub akceptację w aplikacji autentykującej, a następnie przechwytuje token sesyjny (cookie) autoryzujący dostęp.

Urzędnik jest przekonany, że zalogował się poprawnie, podczas gdy przestępca uzyskuje pełny dostęp do jego skrzynki pocztowej.

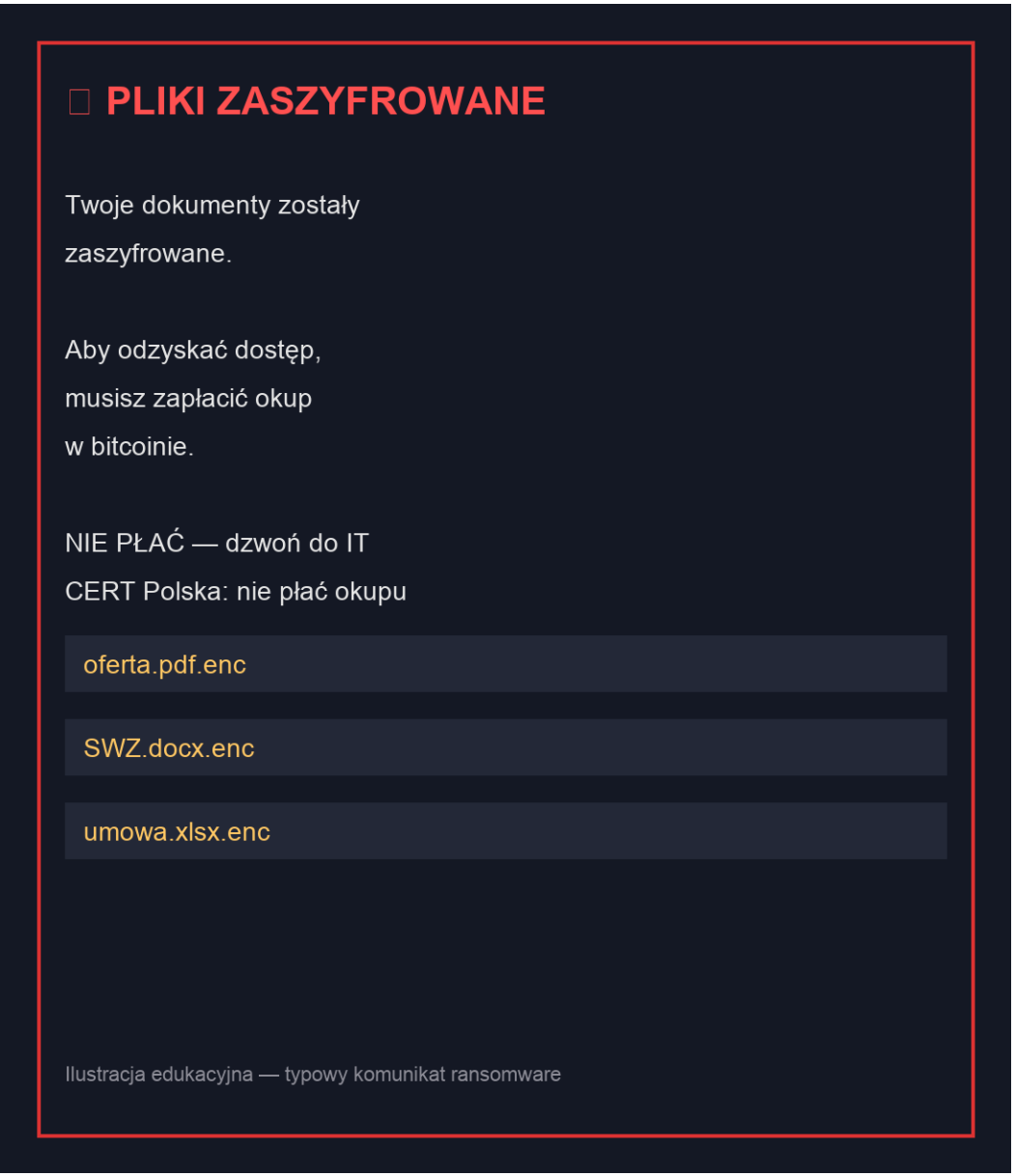
Co dalej robią sprawcy?

- **Eksfiltrację danych:** Poczta w urzędach tego typu to kopalnia wiedzy – zawiera tajemnice przedsiębiorstw biorących udział w przetargach, wyceny, strategie odwoławcze i korespondencję z wykonawcami. Pobierają całą pocztę i załączniki.
- **Persystencję i ukrywanie śladów:** Standardową procedurą po przejęciu skrzynki jest zakładanie przez przestępców złośliwych reguł pocztowych (Forwarding Rules). Reguły te automatycznie przesyłają kopie przychodzących wiadomości na zewnętrzne serwery kontrolowane przez atakujących lub przenoszą je do rzadko sprawdzanych folderów (jak *RSS Feeds* czy *Archiwum*), aby urzędnik nie zorientował się, że ktoś manipuluje jego pocztą.

Jak chronić konta?

Stosuj silniejszy wektor uwierzytelniania, odporny na 99,9% ataków

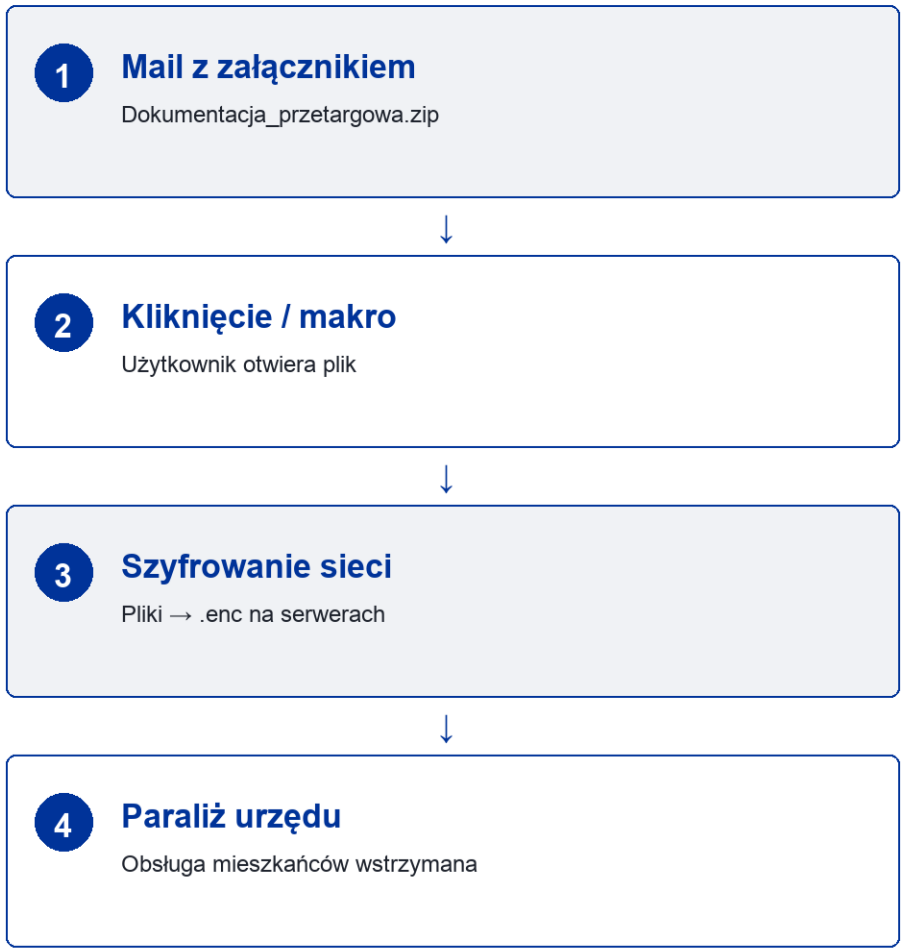
sprzętowych kluczy zabezpieczeń



Ransomware - cyfrowy szantaż

- Malware szyfruje pliki i żąda okupu (np. w bitcoinie)
- Ransom note na ekranie — po lewej przykład
- Paraliż urzędu, wyciek danych, odpowiedzialność prawna
- nie płać okupu — brak gwarancji odzyskania danych

Zapobiegaj kopiami zapasowymi i reaguj szybko gdy coś się dzieje.



Urzędy zaatakowane ransomware

Głównym wektorem ataków są maile z załącznikami.

Urzędnik otwiera zainfekowany plik.

Sprawcy dostają dostęp przez ten komputer do sieci wewnętrznej i starają się przeskanować ją całą.

Następnie przygotowują payload ransomware, który odpala się na wszystkich komputerach i serwerach w tym samym monecie szyfrując dane całego urzędu.

Skutek:

Paraliż systemów, zatrzymanie obsługi mieszkańców

Niebezpieczne rozszerzenia plików, które przesyłane są przez sprawców

Ryzykowne rozszerzenia: .exe, .scr, .bat, .js, .vbs, .iso, .lnk

Makra w odebranych dokumentach .docm, .xlsm — nie włączaj

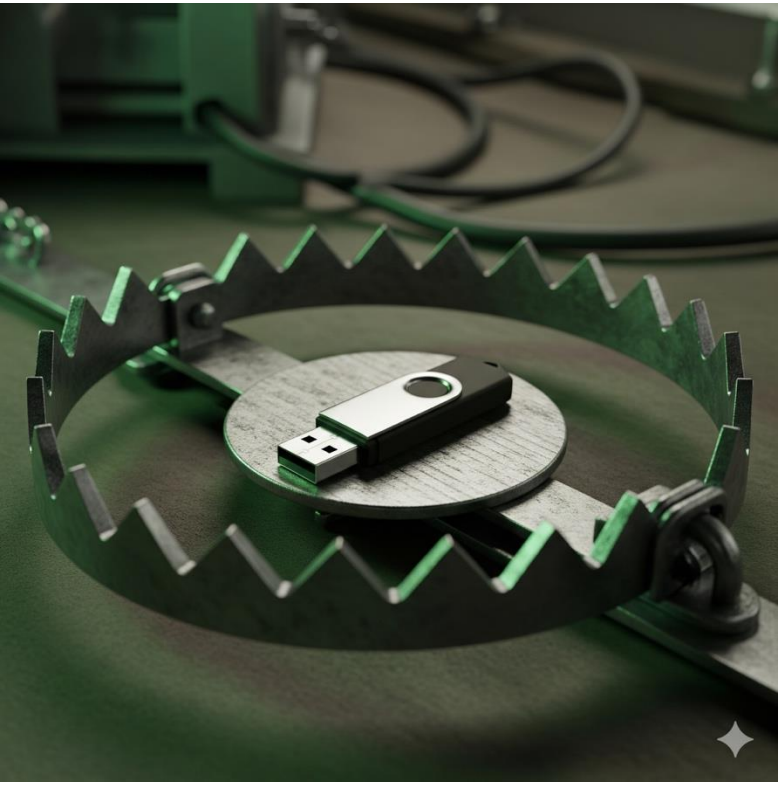
Pliki archiwum .zip / .rar z hasłem w mailu — to typowy wektor ransomware

Widzisz nieznane rozszerzenie załącznika albo archiwum z hasłem w tym samym mailu?

NIE OTWIERAJ

Przekaż do IT

Zagrożenia podrzuconych nośników USB



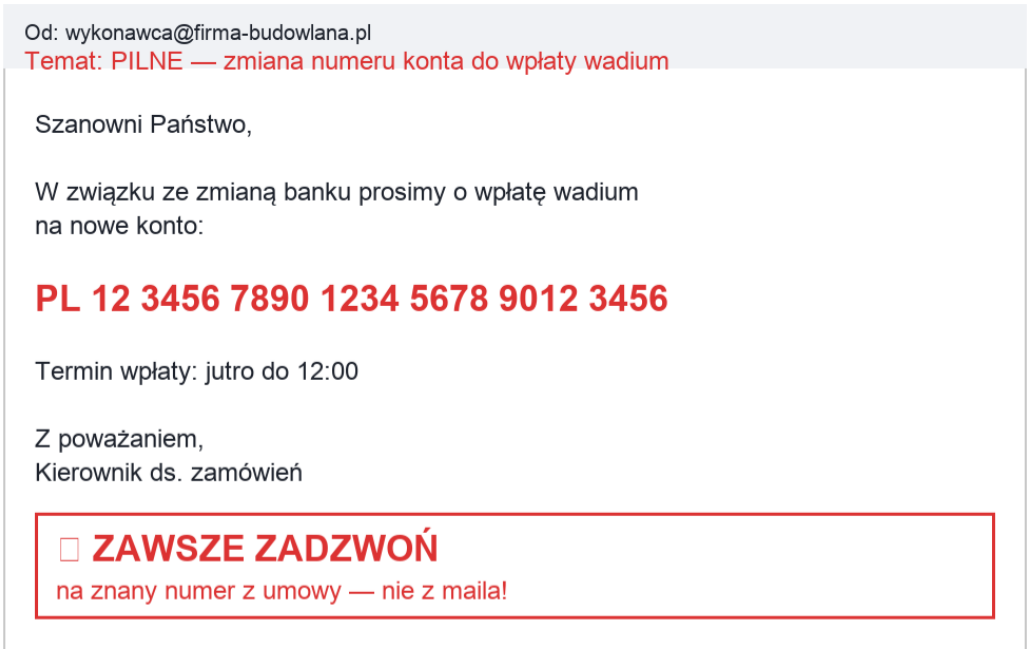
- Pendrive w dokumentacji przetargowej - potencjalny wektor
- Malware, keylogger, urządzenia typu Rubber Ducky
- Zasada urzędu: nie podłączaj nieznanego nośnika
- Otrzymany pendrive przekaż do IT w oryginalnym opakowaniu
- Akcja „Zobaczę tylko , co tam jest” - może być najdroższa.

Systemy powinny wykrywać czy nośnik jest autoryzowany przez Urząd i nie dopuszczać tych nieautoryzowanych.

POKAZ LIVE

nieznane urządzenie

Business Email Compromise (BEC)


Od: wykonawca@firma-budowlana.pl
Temat: PILNE — zmiana numeru konta do wpłaty wadium

Szanowni Państwo,

W związku ze zmianą banku prosimy o wpłatę wadium na nowe konto:

PL 12 3456 7890 1234 5678 9012 3456

Termin wpłaty: jutro do 12:00

Z poważaniem,
Kierownik ds. zamówień

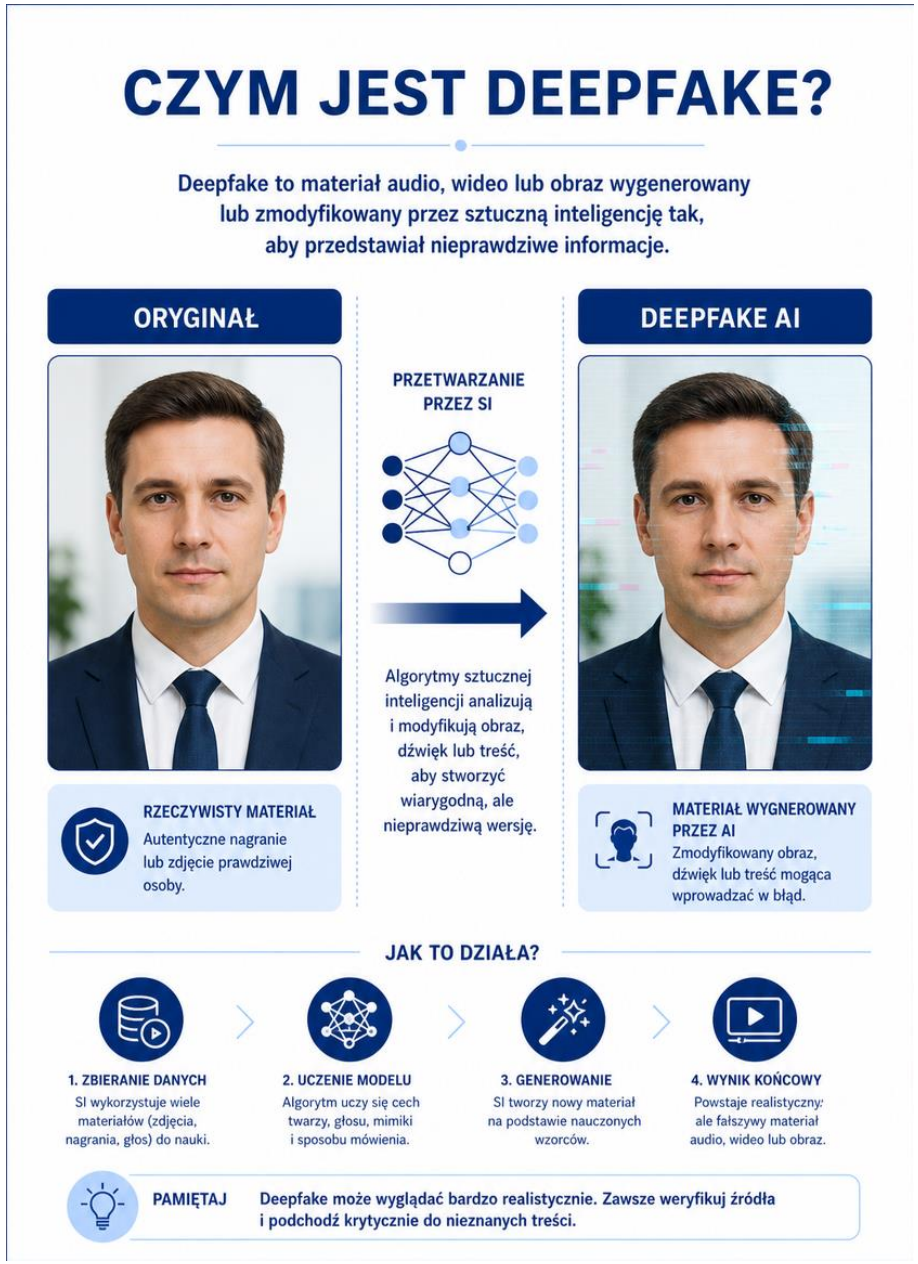
ZAWSZE ZADZWOŃ
na znany numer z umowy — nie z maila!

- Przejęcie / naśladownictwo skrzynki wykonawcy lub urzędu
- Fałszywy mail z nowym numerem konta
- Monitoring korespondencji → wstrzyknięcie w kluczowym momencie
- Kwoty w zamówieniach publicznych są wysokie

Obrona:
weryfikacja telefoniczna każdej zmiany konta

Deepfake


15:13
WhatsApp
LTE
Gospodarka Polski
3 dni
Rejestracja dostępna od 01.06
DOWIEDZ SIĘ WIĘCEJ
Dowiedz się więcej
Zarejestruj się
Lubię to!
Skomentuj
Zapisz
Udostępnij
8
Komentujesz jako Bartosz PK
GIF



Czym jest Deepfake?

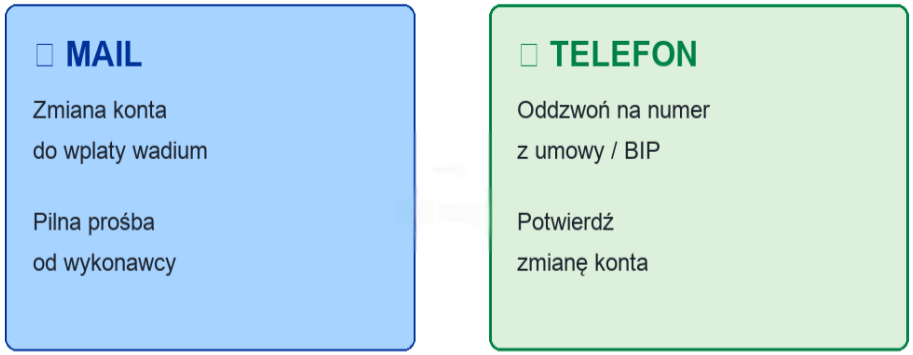
- Syntetyczny obraz lub dźwięk generowany przez AI
- jak powstaje deepfake? (nagranie → model → fałszywe wideo/głos)
- Ktoś „mówi” coś, czego nigdy nie powiedział
- Narzędzia dostępne publicznie — nie wymaga studia filmowego

Deepfake w urzędzie — ryzyka

- Fałszywe polecenia finansowe „od przełożonego”
- Manipulacja decyzjami w postępowaniach przetargowych
- Dezinformacja wobec mieszkańców (fałszywe komunikaty urzędu)

Obrona:
weryfikacja innym kanałem, hasła ustalane w urzędzie

Zasada ograniczonego zaufania



- Każde nietypowe polecenie finansowe - weryfikuj innym kanałem
- Mail → telefon na znany numer; telefon → mail potwierdzający
- MFA wszędzie, gdzie to możliwe
- Zmiana konta wykonawcy, prośba o dane oferentów - zawsze drugi kanał
- Standard w bankach - czas wprowadzić go w urzędach

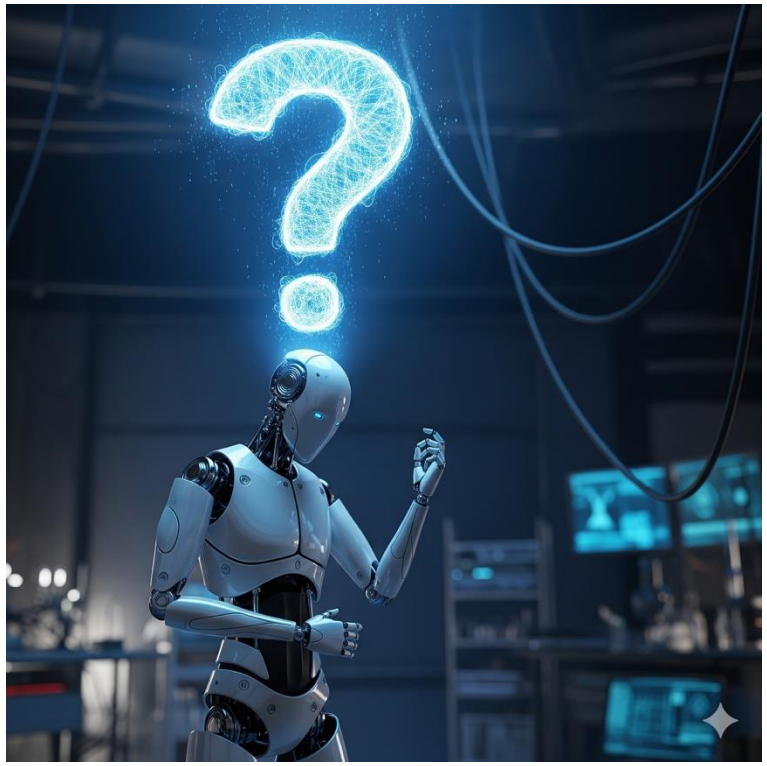
Sztuczna inteligencja w codziennej pracy

- ChatGPT, Copilot, Gemini — coraz częściej używane w administracji. Pracownicy sami zaopatrują się w narzędzia jeśli posiadają komputery z dostępem do internetu.
- Urzędnicy używają AI do: streszczania dokumentów, szkiców pism, tłumaczeń z innych języków, a nawet pełnej pracy na danych!

O czym pamiętać?

- Publiczne modele uczą się na danych, które wpisujemy
- Oferty przetargowe mogą zawierać wyodrębnione informacje prawnie chronione jako **tajemnica przedsiębiorstwa** (art. 11 ust. 2 *Ustawy o zwalczaniu nieuczciwej konkurencji* oraz art. 18 ust. 3 *Ustawy Prawo zamówień publicznych*). Wklejenie oferty do ChatGPT = potencjalny wyciek

AI potrafi zmyślać



- Halucynacje: nieistniejące artykuły prawne, zmyślone sygnatury
- Błędna interpretacja - ryzyko procesowe
- AI może być tylko szkicem, nie jest źródłem prawdy - zweryfikuj dane
- Zawsze sprawdzaj dane w pewnych źródłach
- Nie polegaj na „pewności” modelu - potrafią być przekonujące

Higiena cyfrowa w urzędzie

- Blokuj ekran (Win+L) przy każdym odejściu od stanowiska
- Nie podłączaj obcych nośników USB do komputera służbowego
- Unikalne hasła + wszędzie uwierzytelnianie dwuskładnikowe
- Aktualizuj urządzenia
- Nie wrzucaj danych do AI

Co robić, gdy coś pójdzie nie tak?

- Nie panikuj i nie ukrywaj incydentu — zgłoś natychmiast do działu IT urzędu
- Zapisz: nadawcę, treść, godzinę, co kliknąłeś
- Podejrzenie ransomware: odłącz sieć, nie wyłączaj komputera
- Phishing: przekaż mail do IT, zgłoś na incydent.cert.pl
- Znaj numer kontaktowy do IT i osobę ds. bezpieczeństwa informacji

Co wdrożyć w urzędzie? — perspektywa decydenta

- Polityka: weryfikacja dwukanałowa każdej zmiany konta i płatności przetargowej
- Procedura incydentu: kto decyduje, kto informuje, całodobowy kontakt do IT
- Szkolenia z cyberbezpieczeństwa co roku — nie tylko IT, także wszyscy pracownicy administracji, zamówień publicznych i księgowość.
- Backup i test odtwarzania — raz w roku, z raportem dla kierownictwa
- Polityka AI: tylko zatwierdzone narzędzia, zakaz wklejania danych bez anonimizacji czy ofert przetargowych
- Współpraca z CERT: zgłaszaj phishing, śledź alerty branżowe

mgr Bartosz POLAK, MBA

www.szkoleniacyberbezpieczenstwo.pl

szkolenia
cyberbezpieczeństwo

Fundusze Europejskie

Dziękuje za uwagę

Fundusze Europejskie

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską