REGULATOR, HAKER I BACKUP WCHODZĄ DO BARU…

CZYLI O CYBERBEZPIECZEŃSTWIE W KSIĘGOWOŚCI

BARTOSZ PRAUZNER-BECHCICKI
SYSTEMY INFORMATYCZNE ITXON SP. Z O.O.

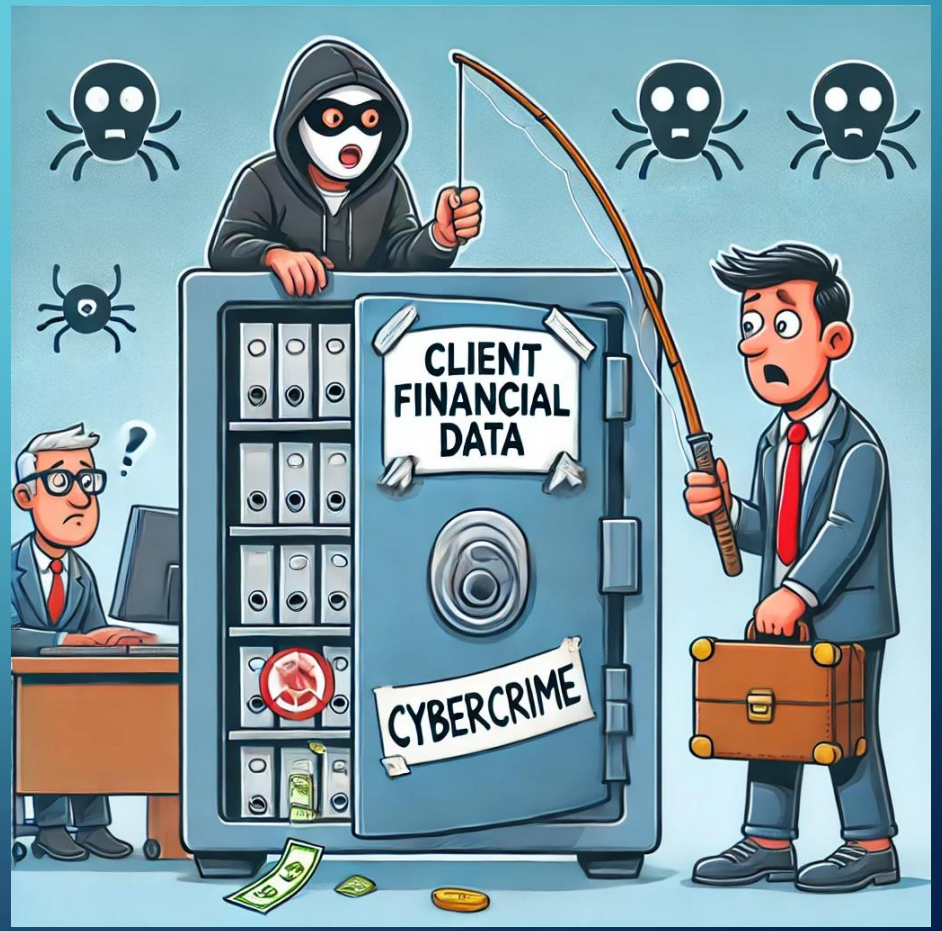
Cyfrowy Księgowy 2.0
Arche Hotel, Warszawa, 8-9 października 2025

REGULATOR, HAKER I BACKUP WCHODZĄ DO BARU…

- Prezentacja z przymrużeniem oka, ale na bardzo poważny temat
- 3 bohaterów: Regulator, Haker i Backup
- Kto wygra to starcie?

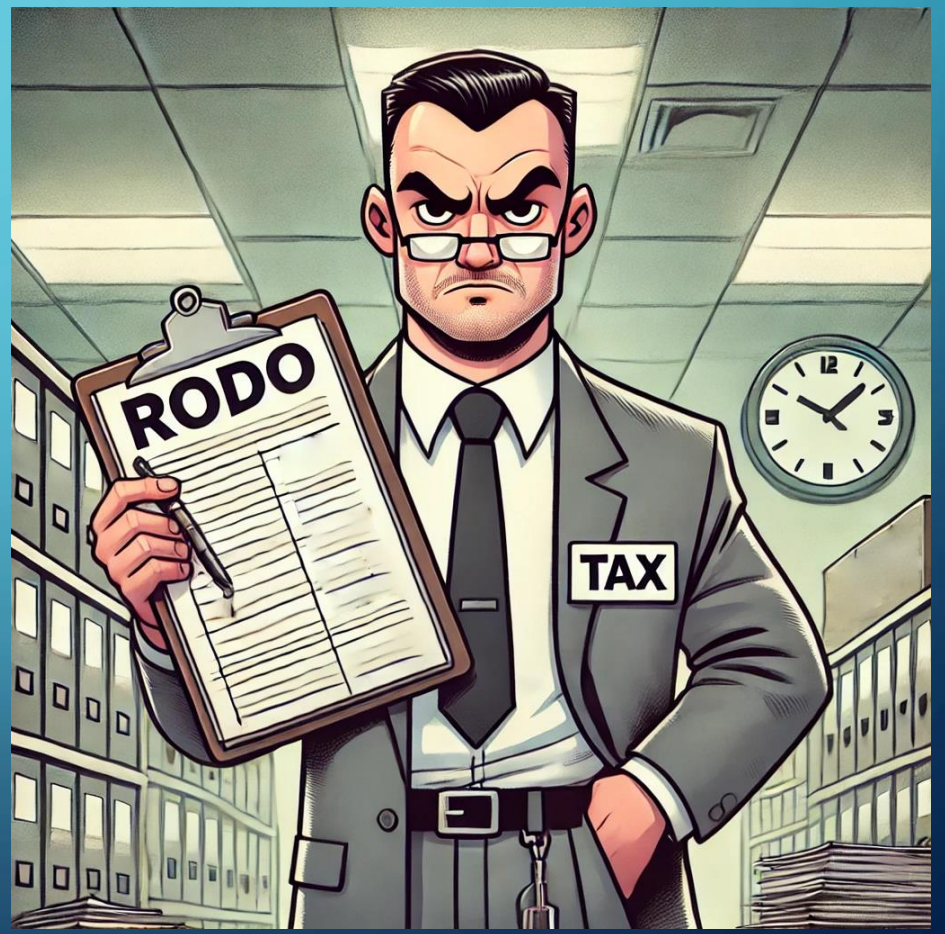
DLACZEGO KSIĘGOWOŚĆ JEST CELEM?

- Duże ilości danych finansowych i osobowych
- Często słabe zabezpieczenia IT
- Wysoka odpowiedzialność prawna
- Hakerzy dobrze wiedzą, gdzie uderzyć



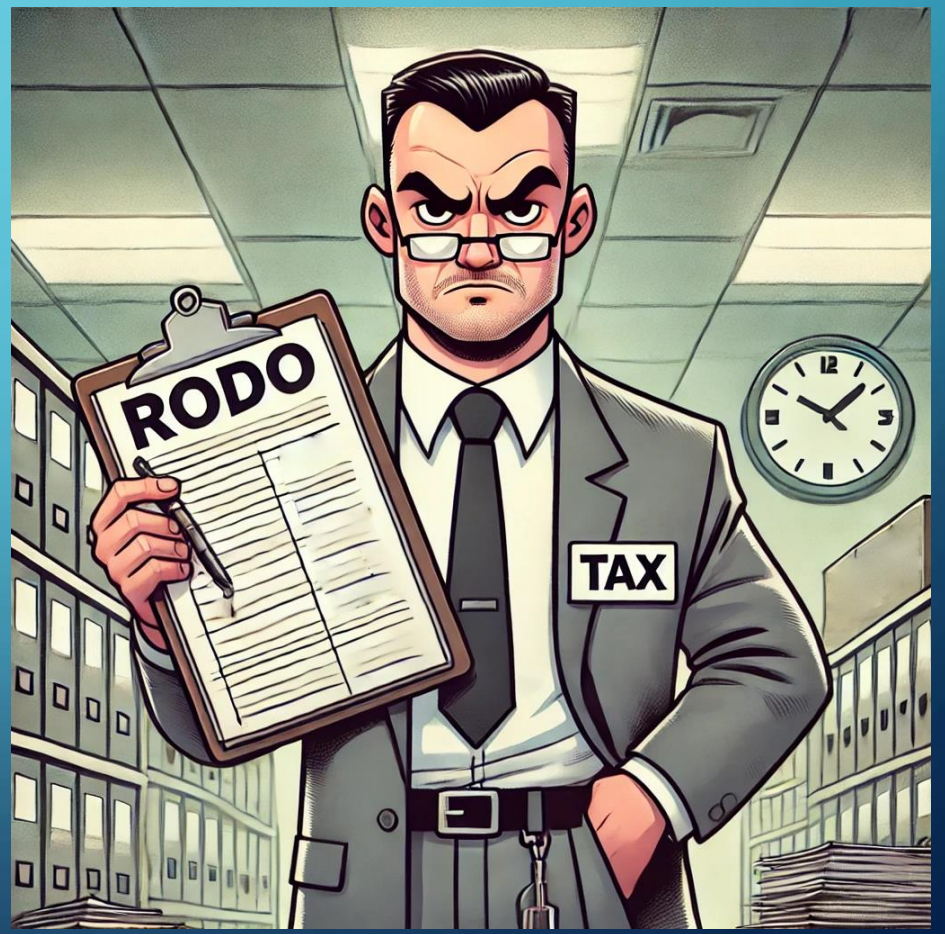
REGULATOR – SUROWY STRAŻNIK PORZĄDKU

- RODO – ochrona danych osobowych
- NIS2 – nowe obowiązki: raportowanie incydentów, audyty, polityki bezpieczeństwa IT
- KSeF – nowa era e-fakturowania: automatyzacja, weryfikacja, bezpieczeństwo danych
- KAS – kontrola skarbowa i bezpieczeństwo danych podatkowych
- Ryzyko kar finansowych i reputacyjnych



REGULATOR – NIE MA ZMIŁUJ!

- Hakerzy wydają się być groźni, dopóki regulator nie zapyta o procedury bezpieczeństwa
- Audyty, dokumentacja, polityki bezpieczeństwa
- Każde niedociągnięcie może kosztować



HAKER – MISTRZ CHAOSU

- Ransomware – blokada danych, żądanie okupu
- Phishing – wyłudzanie danych przez e-maile i fałszywe strony
- Kradzież loginów do systemów (ePUAP, bankowość)
- Ludzkie błędy jako główny wektor ataku
- AI utrudnia zadanie - realistyczne wiadomości phishingowe i fałszywe strony bez błędów i z personalizacją

HAKER – NIE POTRZEBUJE ŁOMU

- **Haker nie musi się włamywać przez drzwi, jeśli ktoś mu poda klucz**
- Ten klucz to często nieświadomy pracownik
- Dziś cyberprzestępcą może zostać każdy – wystarczy dostęp do narzędzi (często z pomocą AI)
- **Szkolenia i procedury** to kluczowa zapora
- AI działa także po stronie obrony – wykrywa anomalie i automatyczna reakcja

PRZYKŁADY CYBERATAKÓW Z POLSKI I NIE TYLKO

- 2025 – Jaguar Land Rover, ransomware: 4 tygodnie przestoju, 50 mln funtów strat tygodniowo
- 2024 – biuro rachunkowe, ransomware, zgłoszenie do UODO
- 2023 – firma produkcyjna ze śląska, ransowmare, kilkaset tys. kosztów, kilka tygodni przestoju
- 2025 – firma budowlana, podmienione numer konta na fakturze, brak MFA w poczcie email

BACKUP – CICHY BOHATER

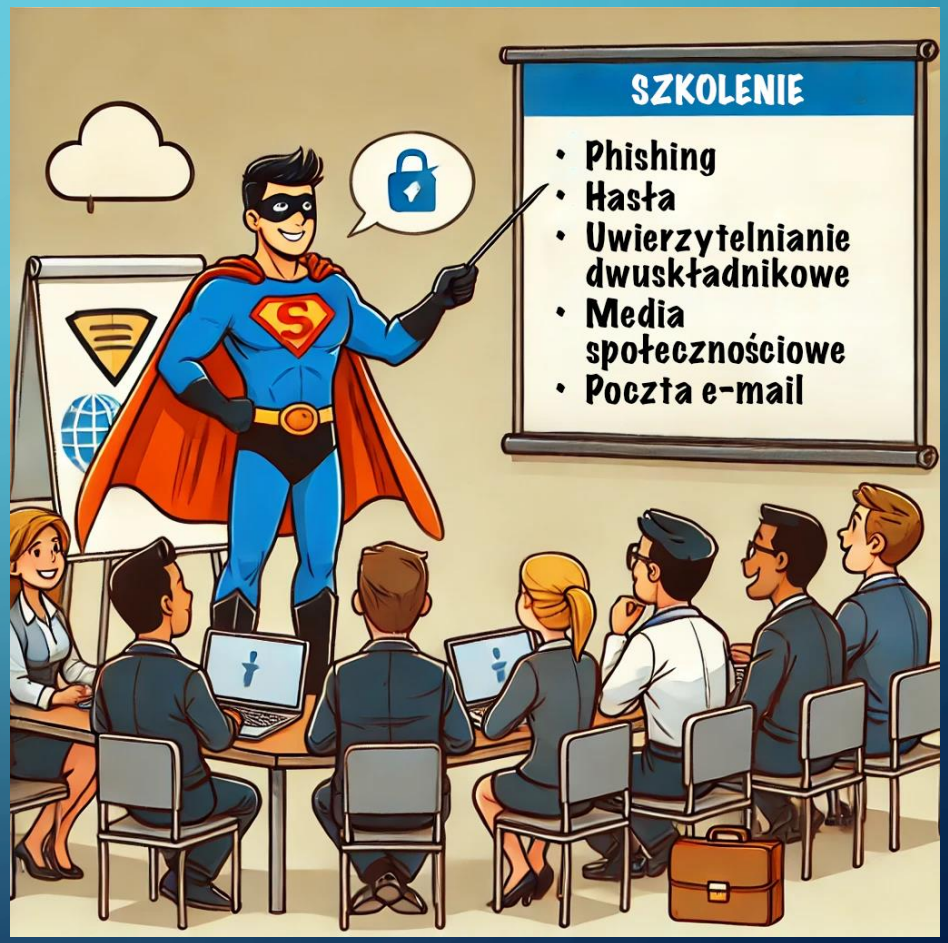
- **Backup to ostatnia linia obrony**
- Musi być: **automatyczny, regularny, testowany**
- Warto stosować zasadę 3-2-1-1-0: 3 kopie, 2 różne nośniki, 1 kopia poza firmą, 1 kopia niezmienialna, 0 błędów po weryfikacji
- **Disaster Recovery (DR)** – zapewnia **ciągłość działania** w razie awarii lub ataku

BACKUP – DZIAŁA CZY TYLKO ISTNIEJE?

- Bez dobrego backupu po ataku ransomware jedyny dokument, jaki wystawi firma to… faktura za okup
- Backup musi działać, nie tylko „być”
- Najlepszy backup to taki, który można szybko odtworzyć
- Testuj Backup i plan Disaster Recovery – sprawdź, jak szybko możesz wznowić pracę po awarii

BACKUP MOŻE WIELE, ALE TO NIE WSZYSTKO…

- Dobre rozwiązanie cyberbezpieczeństwa pozwala zapobiegać zanim dojdzie do ataku - może być zintegrowane z backupem
- Szkolenia personelu w zakresie cyberbezpieczeństwa to nie tylko obowiązek regulacyjny - to rzeczywiście działa!



KTO WYGRAŁ NASZE STARCIE Z BARU?

- Regulator wymaga zgodności
- Haker szuka dziury
- Backup ratuje sytuację

Wygrywa ten, kto jest przygotowany!

WNIOSKI

- **Regulacje** to obowiązek – nie wybór
- **Ataki są realne** – nawet na małe firmy
- **Backup** ratuje dane – **Disaster Recovery** ratuje ciągłość
- **Cyberbezpieczeństwo** to nie koszt – to inwestycja
- **Świadomość i szkolenia** to najlepszy antywirus
- **Bezpieczeństwo to proces** – warto zacząć już dziś

DZIĘKUJĘ ZA UWAGĘ!

Zachęcam do kontaktu:

bartosz.prauzner@itxon.pl