# “Cyberbezpieczeństwo w praktyce – jak chronić firmę przed realnymi zagrożeniami?”

## termin: 13 lutego 2026 r., godz. 09.00 – 12.00, online

***Prowadzący*** *–* ***Tomasz Sidor****,* ***Prezes Zarządu Instytut Antrotech Sp. z o.o.*** *- Zarządzenie instytucją wykonującą opinię i* ***ekspertyzy z zakresu informatyki śledczej****, cyberbezpieczeństwa oraz antropologii sądowej. Prowadzenie zajęć w Lubelskiej Akademii WSEI z zakresów: cyberbezpieczeństwo, informatyka śledcza (z elementami akademii AXIOM), informatyka kryminalistyczna,* ***bezpieczeństwo systemów informatycznych, praktyczne aspekty cyberbezpieczeństwa w organizacji****, zarządzanie bezpieczeństwem informacji, testy bezpieczeństwa.*

| **13.02.2026r., online** | |
|---|---|
| 9.00 – 9.10 | **Otwarcie spotkania**<br>***Marta Puczyk, Enterprise Europe Network, Lubelska Fundacja Rozwoju***<br>**Oferta sieci Enterprise Europe Network**<br>**Omówienie agendy**<br>*Krótka ankieta wstępna – badanie poziomu wiedzy uczestników*<br>*Ustalenie zasad komunikacji podczas webinaru* |
| 9.10 – 12.00 | **Krajobraz cyberzagrożeń w 2025 roku**<br>• Aktualne statystyki cyberataków na polskie firmy<br>• Ile kosztuje cyberatak? Realne straty finansowe i wizerunkowe<br>• Najczęstsze wektory ataku: e-mail, strony www, media społecznościowe<br>• Kto jest celem? Dlaczego MŚP są szczególnie narażone<br>**Przykład praktyczny:** Analiza głośnego incydentu z ostatnich miesięcy – co poszło nie tak i jak można było temu zapobiec<br>**Phishing i socjotechnika – największe zagrożenie**<br>• Rodzaje phishingu: e-mailowy, SMS (smishing), telefoniczny (vishing)<br>• Spear phishing i ataki ukierunkowane<br>• Jak rozpoznać fałszywy e-mail? Czerwone flagi<br>• Podejrzane załączniki i linki – na co zwracać uwagę<br>**Interakcja z uczestnikami – Scenariusze szkoleniowe**<br>**Hasła, uwierzytelnianie i ransomware**<br>Hasła i uwierzytelnianie:<br>• Dlaczego „Firma2024!" to złe hasło?<br>• Zasady tworzenia silnych haseł |

• Menedżery haseł – praktyczne wdrożenie (Bitwarden, 1Password, KeePass)
• MFA/2FA – uwierzytelnianie dwuskładnikowe jako standard

**Ransomware – szantaż cyfrowy:**
• Jak działa ransomware? Mechanizm ataku krok po kroku
• Co robić, gdy ekran pokazuje żądanie okupu?
• Strategia backupu 3-2-1
**Interakcja – Scenariusz szkoleniowy**

**Bezpieczeństwo pracy zdalnej i hybrydowej**
**Czy praca zdalna jest bezpieczna?**
• Zagrożenia: niezabezpieczone sieci Wi-Fi, prywatne urządzenia, współdzielone komputery
• VPN – co to jest i dlaczego jest niezbędny
• Polityka BYOD (Bring Your Own Device)
• Szyfrowanie dysków i komunikacji

**Jak przygotować bezpieczne stanowisko pracy zdalnej:**
• Lista kontrolna dla pracownika
• Separacja danych firmowych i prywatnych
• Aktualizacje systemu i oprogramowania
**Interakcja – Scenariusze szkoleniowe**

**Praca z AI, zgłaszanie incydentów i podsumowanie**
**Praca z AI – nowe wyzwania:**
• Ryzyko wycieku danych przy korzystaniu z ChatGPT i podobnych narzędzi
• Deepfake i syntetyczne media – nowe narzędzia oszustów
• Zasady bezpiecznego korzystania z AI w firmie

**Zgłaszanie incydentów:**
• Dlaczego szybkie zgłoszenie jest kluczowe?
• Komu zgłaszać? Procedura wewnętrzna
• CERT Polska – kiedy i jak zgłaszać
• Obowiązki wynikające z RODO i ustawy o KSC

**Audyt wewnętrzny – na co zwrócić uwagę:**
• Szybka lista kontrolna (10 punktów) do samodzielnej oceny
• Najczęstsze luki w zabezpieczeniach MŚP

**Zakończenie:**
• Podsumowanie kluczowych wniosków
• Sesja pytań i odpowiedzi (Q&A)