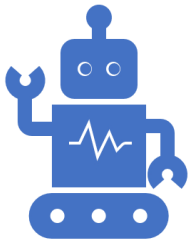
Bezpečnostní audit ve škole

Tomáš Matějíček, CEH

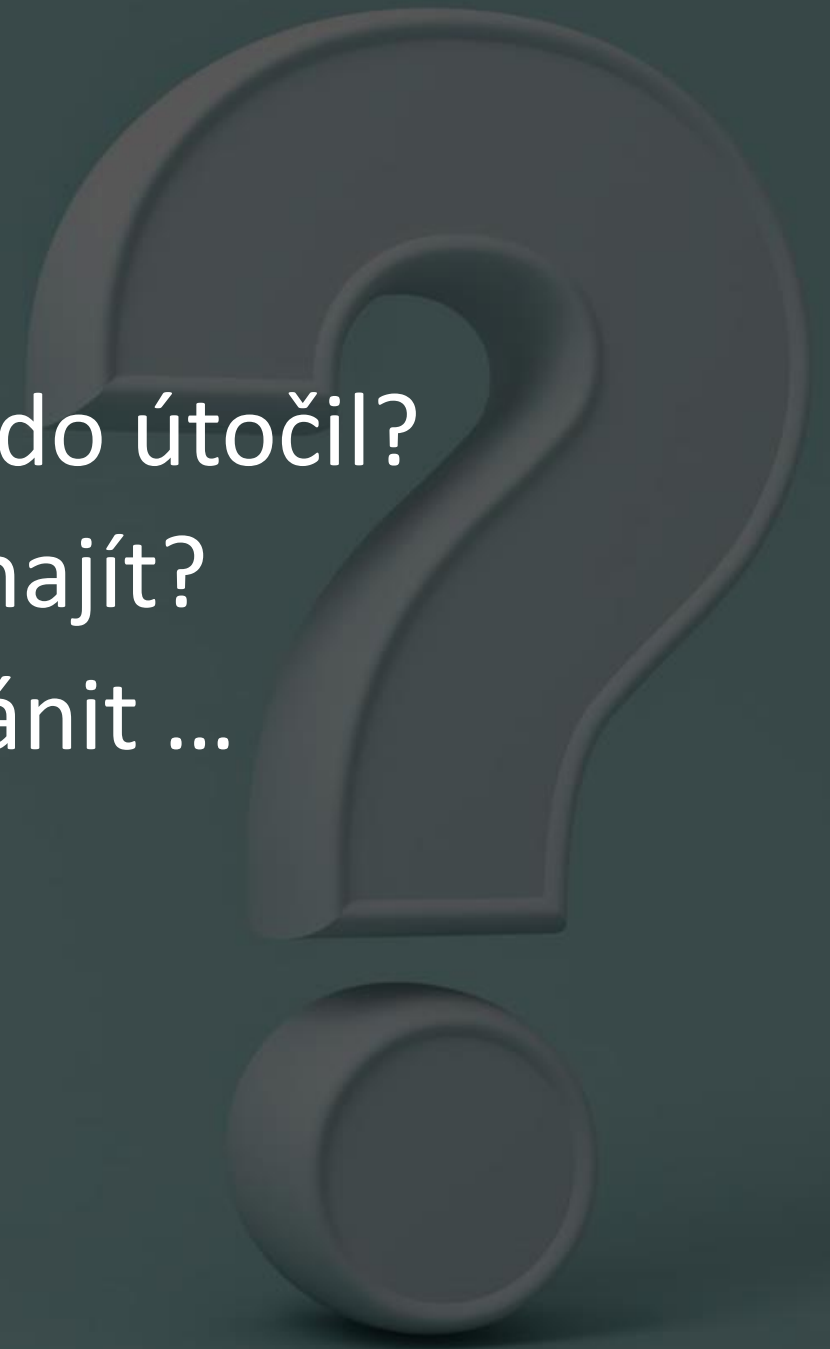


Proč řešit kyber-bezpečnost?

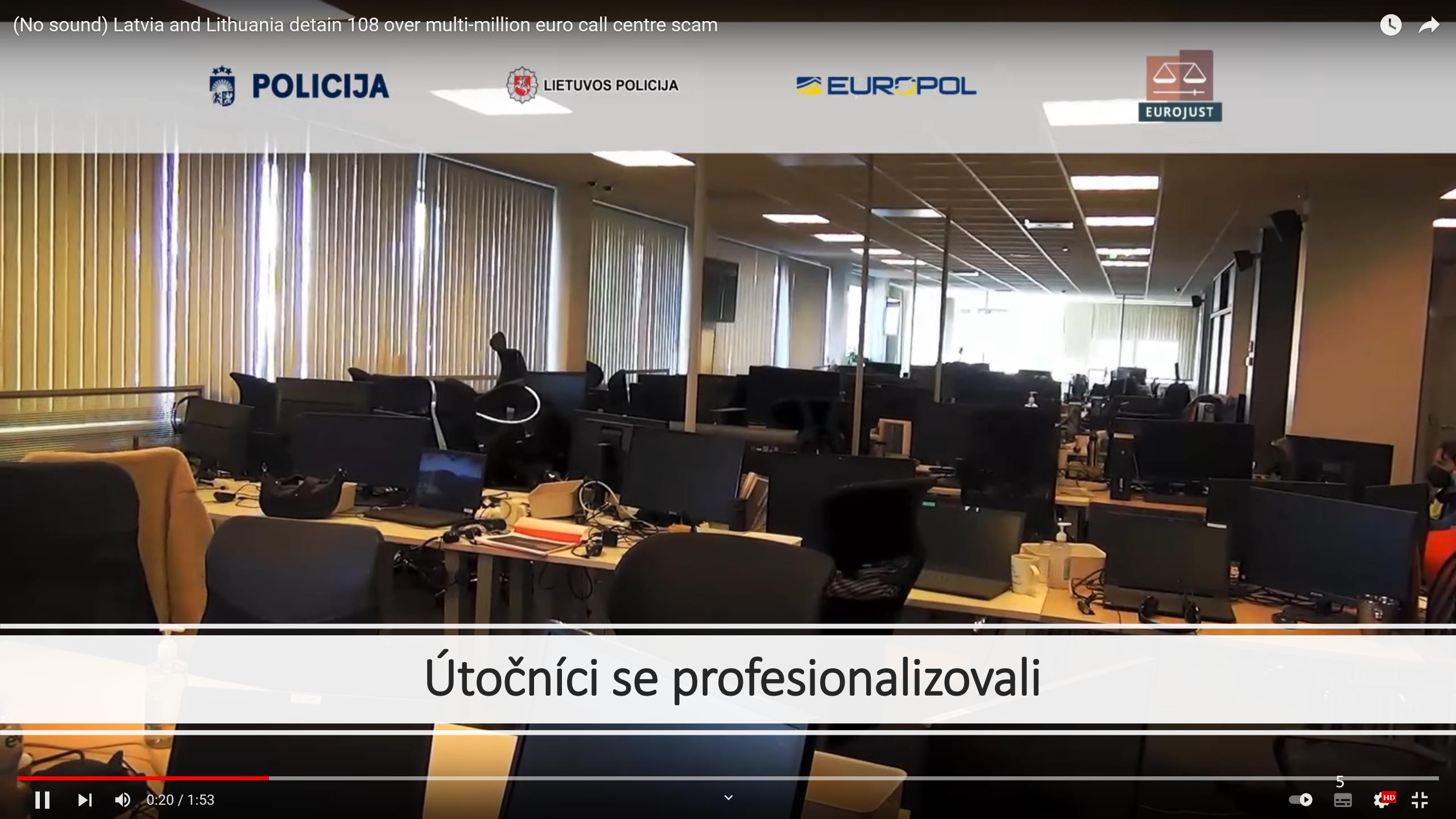
Jaké jsou možnosti řešení?

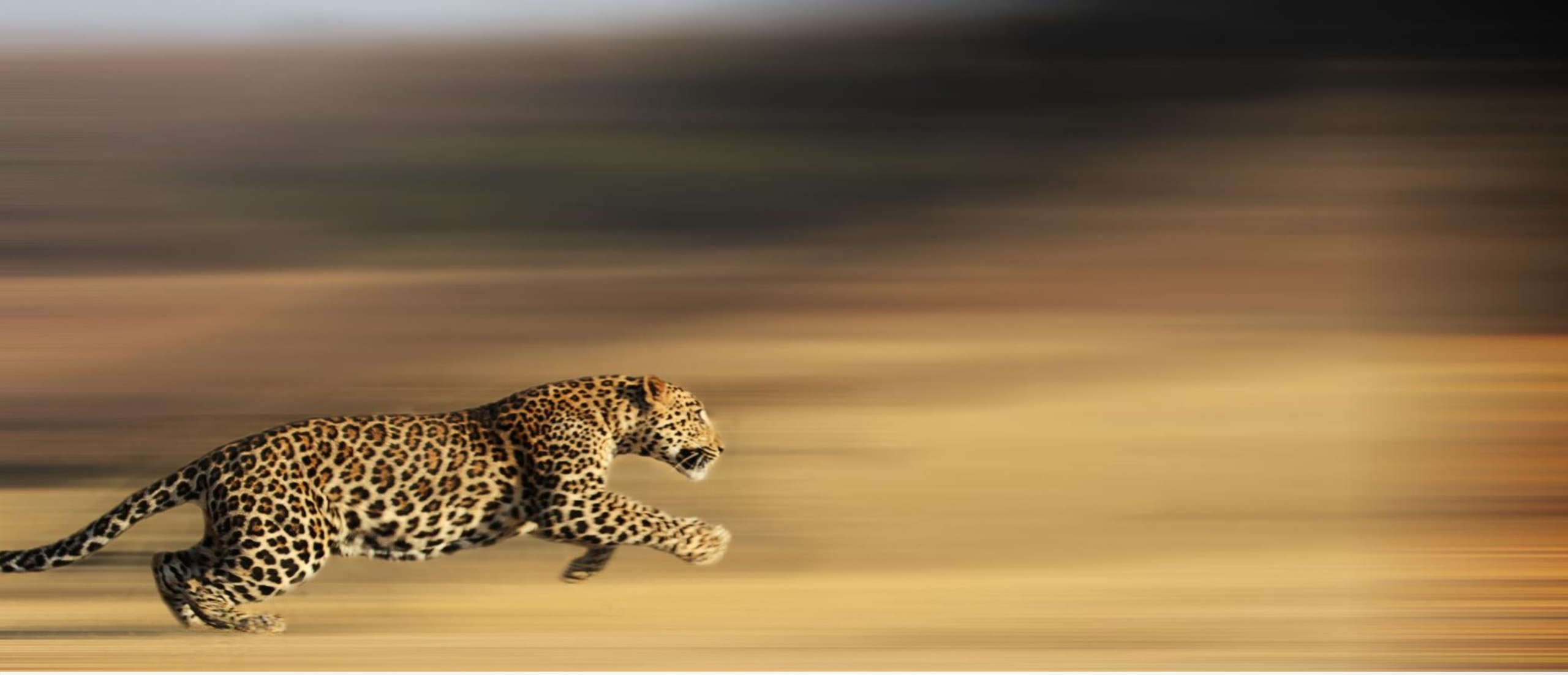
Co dělám?

- Proč by zrovna na nás někdo útočil?
- Co by u nás asi tak mohli najít?
- Stejně se tomu nedá zabránit …



Kriminalita se přesouvá z „ulice“ na „internet“


(No sound) Latvia and Lithuania detain 108 over multi-million euro call centre scam
POLICIJA
LIETUVOS POLICIJA
EUROPOL
EUROJUST
Útočníci se profesionalizovali
0:20 / 1:53
5



Predátoři útočí na slabé kusy

Predátoři útočí na slabé kusy

- Bytová družstva
- Energetika
- Facility
- IT
- Obchod
- Právo
- Reality
- Státní správa
- Školství
- Účetní
- Výroba
- Zdravotnictví
- a další …

Data mají cenu zlata

НАЦІОНАЛЬНА ПОЛІЦІЯ

Dopady napadení

GDPR
Krádež a zveřejnění dat
Náklady na řešení
Náklady na výkupné
Odpovědnost statutárního orgánu
Poškození dobrého jména
Přerušení provozu
Vydírání (Ransomware)
a další ...

Tři příběhy na motivy skutečných událostí

- Podvodná zpráva (phishing)
- Slabé heslo
- Napadení poskytovatele IT služeb

Jak se můžeme bránit kyber-útokům?

Jak se můžeme bránit kyber-útokům?

- Směrnice - Digitální hygiena aneb bezpečné informační chování
- Nástroje - Antivir, Firewall, VPN, MFA, SPF, …
- Kurz – uživatelé, správci
- Trénink rozpoznávání podvodných e-mailů
- Dokumentace zavedených opatření
- Pravidelné kontroly účinnosti zavedených opatření
- ZoKB, ISO 27000, Minimální bezpečnostní standard
- Konzultant – Know-how, Metodické vedení

Co dělám?

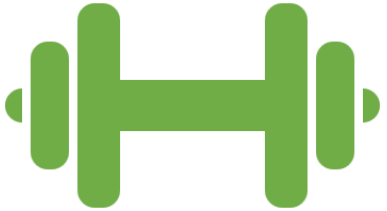
1. Audit dle Minimálního bezpečnostního standardu

Neprobíhá pravidelný audit kyberbezpečnosti	🔴
Chybí plán zavádění bezpečnostních opatření	🔴
Plán obnovy po havárii existuje, ale není k dispozici v písemné formě	🟡
Všechna koncová zařízení jsou zařazena do centrální správy (AD)	🟢
Někteří uživatelé používají privilegované účty i pro běžnou práci	🟡
Politika hesel neodpovídá standardu (počet znaků: 17 privilegované účty, 10 uživatelské účty)	🔴
Neprobíhá pravidelné testování kvality hesel	🔴
Chybí vícefaktorové ověřování	🔴
Síť organizace je segmentována	🟢
Chybí centrální úložiště logů	🔴
Chybí šifrování disků	🔴
Chybí definice požadavků na dostupnost informačních systémů	🔴

2. Řízení zavedení Minimálního bezpečnostního standardu

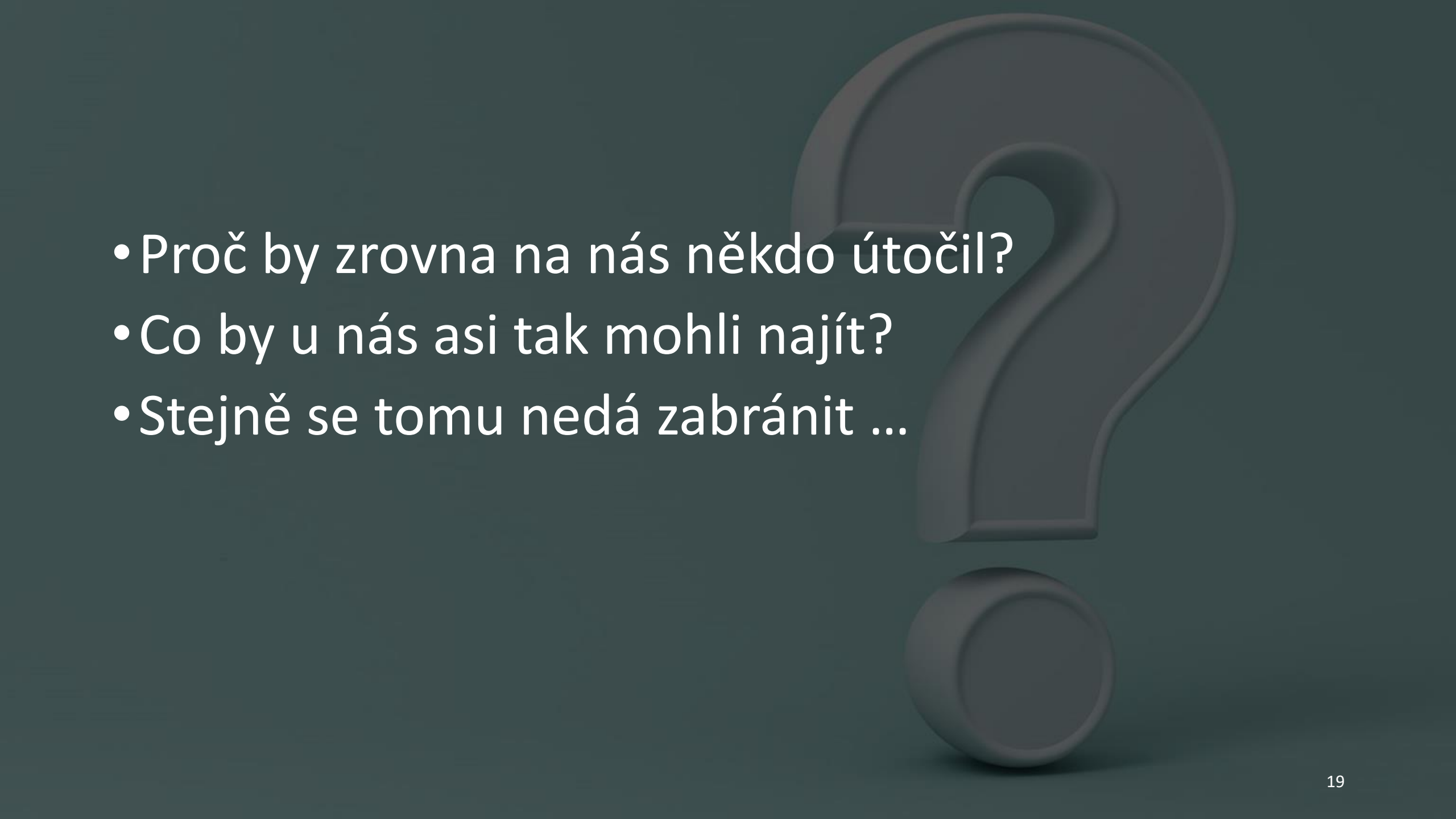
3. Trénink a testování

Minimální bezpečnostní standard – audit a zavedení



Trénink a testování

- Proč by zrovna na nás někdo útočil?
- Co by u nás asi tak mohli najít?
- Stejně se tomu nedá zabránit …



Dotazy, komentáře

Děkuji za pozornost ☺

Kontakty

Tomáš Matějíček

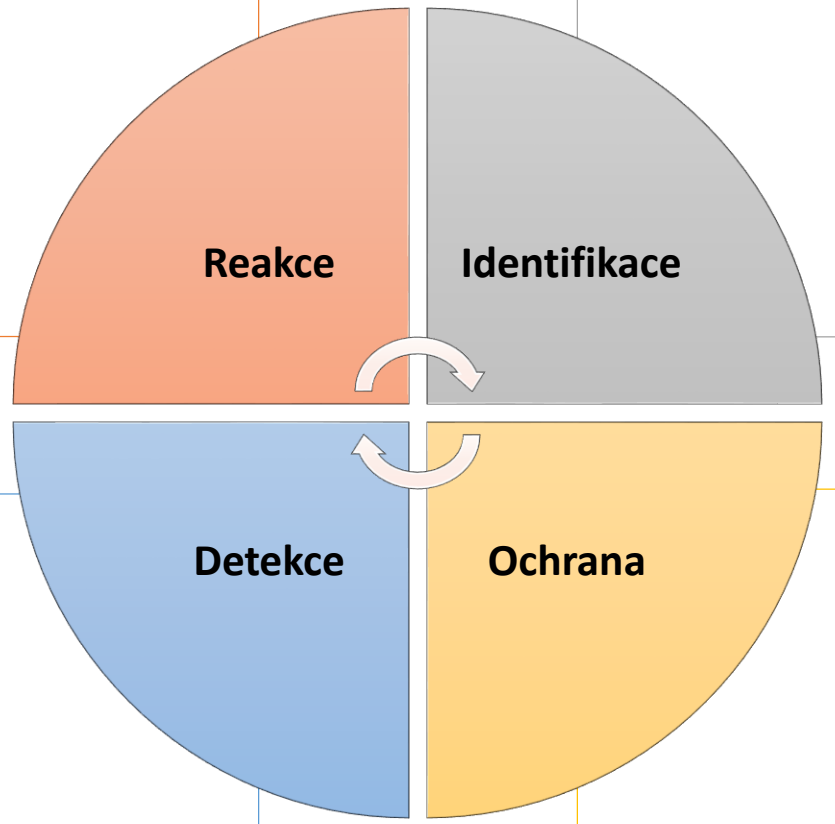
t@te23.cz

https://www.linkedin.com/in/tmatejicek/

https://www.facebook.com/tmatejicek/

Služby pro posílení kyberbezpečnosti

- Vyšetřování incidentů
- Mitigace slabin



- Skeny zranitelností
- Kontrola bezpečnostních opatření
- Phishing kampaně na uživatele
- Penetrační testy
- OSINT Monitoring

- Monitoring bezpečnostních událostí

- Kurzy kyberbezpečnosti pro uživatele
- Strategie kyberbezpečnosti
- Podpora při zavádění opatření
- Zpracování plánů obnovy
- Next Generation Firewall
- eXtended Detection and Response