NÁRODNÍ KONFERENCE PRO INTERNÍ AUDITORY



Český institut interních auditorů

AUDITNÍ DNA

11.–12. LISTOPAD 2026 BRNO

JSME SOUČÁSTÍ DNŮ AI 2026

GENERÁLNÍ PARTNER

HLAVNÍ PARTNEŘI

PARTNEŘI

PODPORUJEME

MEDIÁLNÍ PARTNEŘI

Hybridní hrozby a jejich dopady do fyzické a kybernetické bezpečnosti

Ing. Miroslav Fryšar

Soudní znalec v oblasti ochrany osob, majetku a informací

F.S.C. BEZPEČNOSTNÍ PORADENSTVÍ, a.s.

Bezpečnost není soubor opatření. Je to systém vazeb.



Osnova přednášky

1. Představení společnosti F.S.C. BEZPEČNOSTNÍ PORADENSTVÍ, a.s.
2. Hybridní hrozby – charakteristické rysy a aktuální případy v Evropě
3. Bezpečnost jako systém – propojení fyzické a kybernetické bezpečnosti
4. Slabá místa fyzické bezpečnosti a bezpečnostní rizika v praxi
5. Dopady hybridních hrozeb na bezpečnost a provoz organizace
6. Pohled interního auditu na bezpečnost organizace a možnosti spolupráce s auditory
7. Doporučení na závěr



Představení společnosti

- **Největší poradenská firma v ČR** v oblasti ochrany osob, majetku, informací a služeb bezpečnostního managementu
- **Pracujeme na principu externího bezpečnostního útvaru**
- **Dvacetipětiletá praxe** a bezpečnostní prověrka na stupeň Tajné
- **Vlastní analýzy mimořádných událostí** za posledních 25 let, včetně tzv. hybridních hrozeb
- **Tým špičkových odborníků a znalecká kancelář**
- **Spolupráce s širokým spektrem subjektů** – státní správa, státní firmy a společnosti kritické infrastruktury, velké investiční projekty a závody, střední a malé podniky a organizace
- **Zcela nezávislá** na dodavatelích bezpečnostních služeb a technologií
- **Princip rozumné dostatečnosti** uplatněný na základě analýzy rizik



Hybridní hrozby – aktuální případy v Evropě

Hybridní hrozby – žhářské útoky

- Česko, Polsko, Litva a Rumunsko – související žhářské útoky a pokusy o ně
- Německo, Polsko a Velká Británie – samozápalné zásilky v logistické dopravě

Hybridní hrozby – sabotáže

- Německo – vyšetřované pokusy o sabotáž německých vojenských lodí v přístavu Hamburg
- Polsko – koordinované destruktivní a kyberútoky na energetickou infrastrukturu

Hybridní hrozby – zneužití komerčních dronů

- Německo – nalezen dron s podezřelým výbušným zařízením na letišti Lipsko/Halle
- Dánsko – hlášení podezřelých dronů a omezení letištního provozu
- Evropa – opakovaná hlášení dronů v blízkosti kritické infrastruktury (letiště, energetika, vojenské objekty)

Kyberútoky a dezinformační kampaně

- Polsko – kyberútok na teplárenský provoz, odstavení turbíny a systému úpravy vody
- Evropa – zásah proti skupině KillSec, spojované s přibližně 1 000 podezřelými kyberútoky celosvětově
- ČR a Polsko – snaha rozeštvat obyvatelstvo obou států proti sobě na jaře 2026



Charakteristické rysy hybridních hrozeb

01 Vazba na válečné konflikty nebo teroristická hnutí

02 Často inspirace již provedenými útoky (i ve vzdálené historii)

03 Rozmanitost forem a způsobů provedení

04 Ve většině případů se připravují delší dobu

05 Snaha upoutat pozornost médií a zastrašovat

06 Většinou řetězec útoků

07 Použití kombinace útoků nebo zvyšování intenzity



Žhářské útoky

Charakteristika útoku

- Převažují útoky s využitím tzv. útočníka na jedno použití
- Před útokem pachatel obvykle místo navštíví nebo pozoruje více objektů, obvykle zvolí ten nejméně zabezpečený
- Útočník často improvizuje

Provedení a dopady

- Obvykle útočí se na nejzranitelnější část objektu (zařízení)
- Útok je odhalen často náhodně
- Hmotná škoda závidí na včasné detekci požáru



Útoky bezpilotními prostředky

Rizika a právní rámec

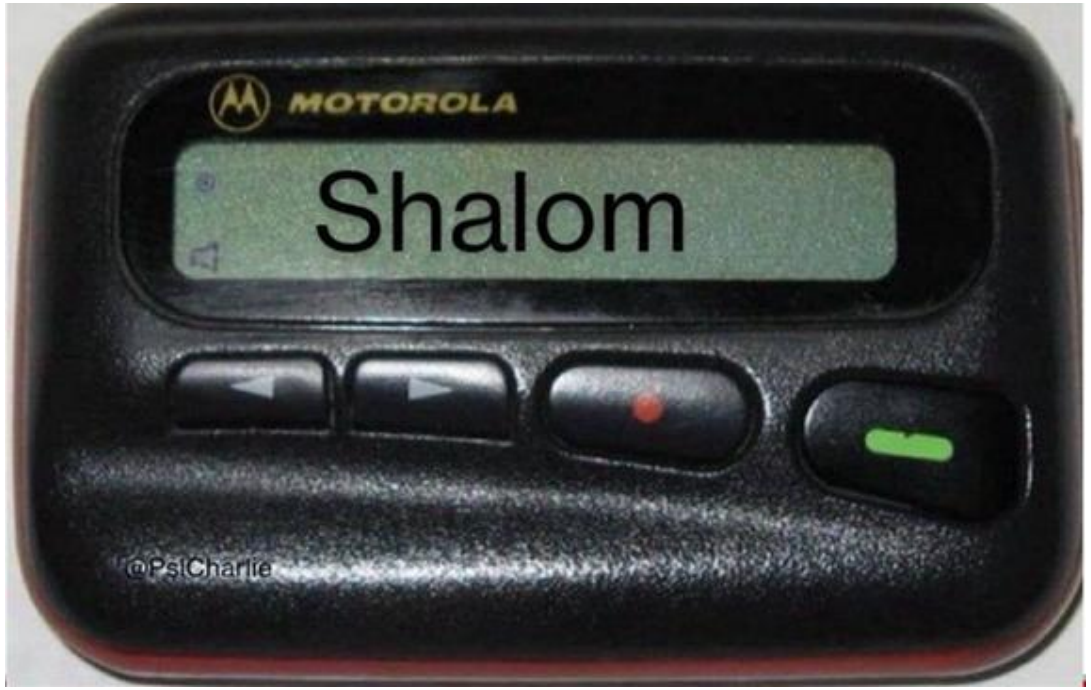
- Nutno odlišit komerční a vojenskou techniku
- Právní předpisy v ČR doposud ochranu proti bezpilotním prostředkům nevyřešily
- Legální je prozatím pouze detekce bezpilotních prostředků, eliminace může provádět pouze PČR

Ochrana a prevence

- Nejspolehlivější ochrana je stále zodolnění a instalace mechanických zábran
- Pozor na marketing dodavatelů

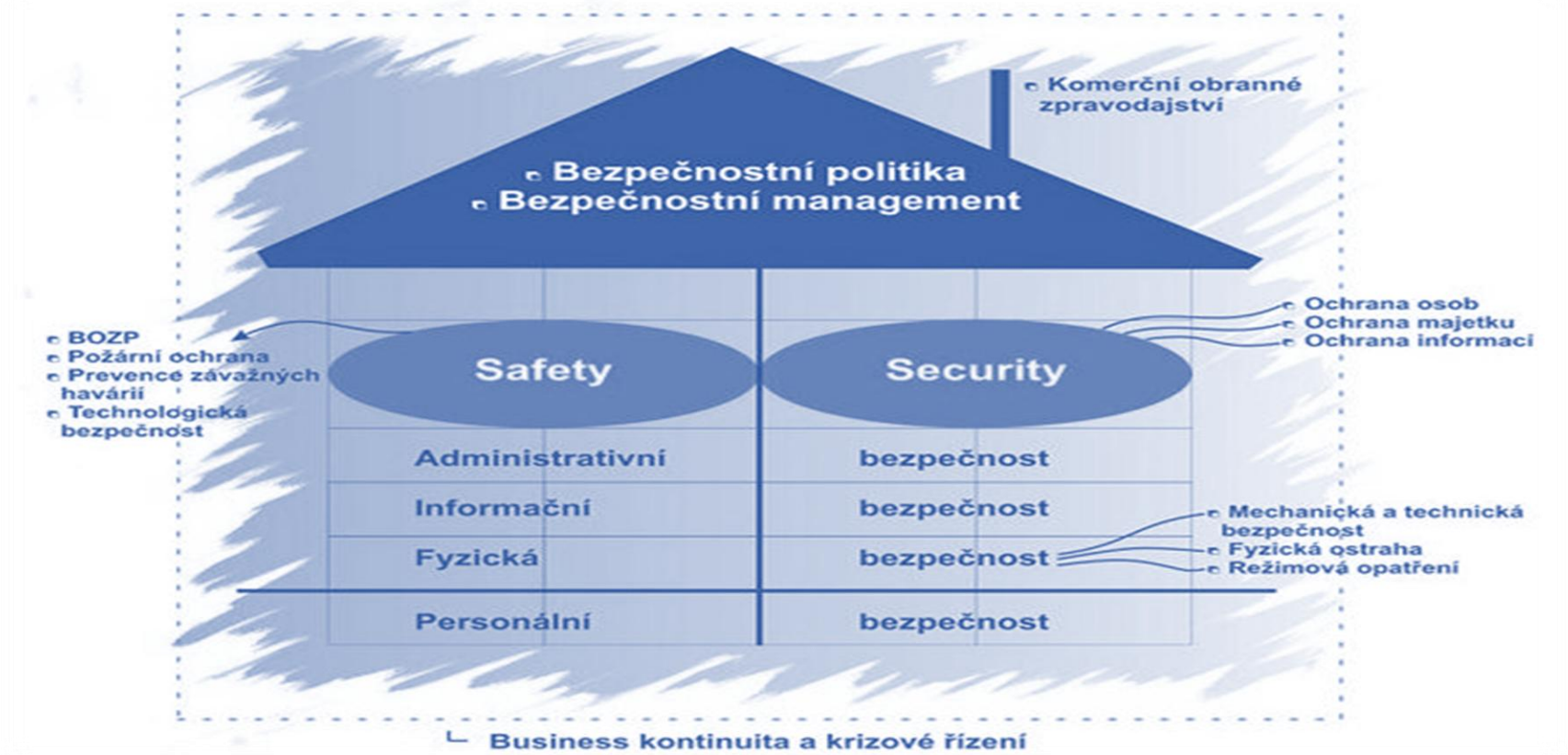


Útok prostřednictvím pagerů





Bezpečnost jako systém





Hybridní hrozba obvykle nekončí u jednoho typu útoku

Jak se na hybridní působení dívat v praxi

- Útočník může kombinovat několik způsobů působení a využít slabá místa organizace tak, aby zjistil její rozhodování nebo narušil provoz
- Vnitřní útočník, stále podceňovaná hrozba

Informační

manipulace, falešná identita

Digitální

phishing, kompromitace, výpadek

Fyzické

průnik, sabotáž, narušení dodávek

Ekonomické

tlak přes dodavatele či partnery



KLÍČOVÁ VAZBA

Fyzická a kybernetická bezpečnost se v praxi prolínají

FYZICKÁ

- objekt
- vstupy
- technologie
- klíčová pracoviště

LIDÉ A PROCESY

- oprávnění
- dodavatelé
- rozhodování
- eskalace

KYBERNETICKÁ

- účty
- sítě
- data
- řídící a dohledové systémy

Slabé místo v jedné oblasti může vytvořit problém úplně jinde.



Fyzická bezpečnost: kde se v praxi objevují slabá místa

01 fyzické osoby a jejich pohyb

ostraha, návštěvy, servis, externisté

02 Technické prostory

rozvaděče, serverovny, komunikační prvky, sklady, archívy, velíny, vrátnice

03 Přístupové prostředky

karty, klíče, identifikátory

04 Praxe vs. pravidla

co se skutečně děje mimo dokumentaci



AUDITNÍ POHLED

Audit by neměl končit kontrolou dokumentace

01 Vazby

kde se potkává fyzická, kybernetická a organizační ochrana

02 Odpovědnost

kde se předává mezi útvary a mizí vlastník

03 Realita

rozdíl mezi dokumentovaným postupem a praxí

04 Reakce

schopnost rozpoznat, eskalovat a koordinovat

05 Závislosti

co může způsobit řetězový dopad

06 Obnova

jak rychle se organizace vrátí k bezpečnému provozu



Otázky, na které bych se při auditu zaměřil

1. Kdo spojí několik zdánlivě nesouvisejících signálů?
2. Kdo rozhoduje, když incident zasáhne IT, bezpečnost i provoz?
3. Jsou fyzické vstupy a elektronické oprávnění přezkoumávány společně?
4. Vědí zaměstnanci, kam hlásit nestandartní nebo podezřelou situaci?
5. Jsou klíčoví dodavatelé zahrnuti do scénářů reakce a obnovy?



Otázky, na které bych se při auditu zaměřil

1. Kdy byla naposledy aktualizována analýza bezpečnostních rizik, obsahuje také hybridní hrozby?
2. Jsou definována, prováděna a kontrolována opatření personální bezpečnosti?
3. Jakým způsobem je ověřována znalost z postupů řešení bezpečnostních incidentů u jednotlivých kategorií zaměstnanců?
4. Byla klíčová bezpečnostní opatření podrobena penetračnímu testu?
5. Jaké nácviky řešení krizových situací byly od posledního auditu provedeny?



Některé možnosti spolupráce s auditory

01 **Účast externího specialisty v auditním týmu** (FO, KB, BCM, BDR, personální bezpečnost, krizové řízení, odolnost KI, …)

02 **Dodavatelské zjištění dílčí oblasti auditu**

03 **Dodavatelské ověření funkčnosti bezpečnostního opatření penetračním testováním nebo testem odolnosti**

04 **Zajištění vzdělávání auditorského týmu v oblasti security**

05 **Zasílání informací o hrozbách, novinkách a změnách předpisů a norem**



Doporučení na závěr

01 Aktualizace analýzy rizik

Pravidelně aktualizovat analýzu rizik a vyhodnocovat jejich možné dopady na organizaci.

02 Přijetí bezpečnostních opatření

Přijmout alespoň v nezbytné míře opatření vycházející ze zákonů č. 264/2025 Sb. a č. 266/2025 Sb., i pokud organizace není povinným subjektem.

03 Prověřování připravenosti organizace

Bezpečnostní opatření včetně fyzické a kybernetické bezpečnosti, odolnosti, kontinuity činnosti a bezpečnosti dodavatelského řetězce pravidelně školit a prověřovat testováním a nácviky.

04 Zapojení externích odborníků

Při interních auditech využívat také externí odborníky se zkušenostmi v příslušných oblastech bezpečnosti.



Děkuji za pozornost.

fsc-obchod@fsc-ov.cz

F.S.C.®
BEZPEČNOSTNÍ PORADENSTVÍ

+420 739 840 247

WWW.FSC-OV.CZ

