Duben 2026 - číslo 04

ZPRAVODAJ

Asociace škol kritické infrastruktury

Duben 2026

VZDĚLÁVEJTE BEZPEČNOST, CHRAŇTE BUDOUCNOST!
EDUCARE SECURITATEM, CUSTODIRE FUTURUM!

ASKI SOLUTIONS s.r.o.

ISSN 3029-6749

Vítejte v našem světě © ASKI ...

info@aski.cz ☎ +420 731 086 676 Revoluční 981, 66601 Tišnov www.aski.cz

Vydavatel:

Asociace škol kritické infrastruktury

Revoluční 981, 661 01 Tišnov

Číslo ročníku: 4 (duben)

Rok vydání: 2026

Počet stran: 46

E-mail: info@aski.cz

www.aski.cz

ISSN 3029-6749

OBSAH

Duben 2026 jako období posilování odbornosti a důležitých projektů

PhDr. Mgr. Dušan Kalášek, MBA

Vážení členové ASKI, kolegyně a kolegové, partneři,

čtvrté číslo letošního ročníku přichází v období, které na první pohled může působit méně viditelně. Ve skutečnosti ale šlo o jeden z nejdůležitějších měsíců z hlediska dalšího směřování ASKI.

Období od 25. března do 25. dubna 2026 bylo ve znamení prohlubování odbornosti, rozšiřování spolupráce, a především realizace projektů, které mají přímý dopad do praxe.

ASKI Solutions s.r.o. a první zásadní krok do praxe

Za zcela klíčový moment tohoto období považuji spuštění portálu a webové platformy naší dceřiné společnosti **ASKI Solutions s.r.o.** – www.askisolutions.cz

Tímto krokem jsme vytvořili samostatnou profesionální platformu pro realizaci vzdělávacích, poradenských a odborných aktivit v komerční sféře.

A hned první projekt, který tato platforma přináší, jasně ukazuje, jakým směrem se chceme ubírat.

Dne **27. května 2026** pořádá ASKI Solutions s.r.o. pod záštitou ministra zdravotnictví **Mgr. et Mgr. Adama Vojtěcha** odbornou konferenci:

Zdravotnictví pod tlakem legislativy

https://www.askisolutions.cz/zdravotnictvi-pod-tlakem-legislativy--konference/

Tato konference představuje **první komplexní odborné setkání svého druhu pro nemocnice a zdravotnická zařízení** po nabytí účinnosti nových právních předpisů:

- zákon č. 264/2025 Sb. o kybernetické bezpečnosti
- zákon č. 266/2025 Sb. o odolnosti subjektů kritické infrastruktury

Zdravotnictví se tímto dostává do zcela nové reality, kde se bezpečnost, IT infrastruktura, krizové řízení a legislativa propojují do jednoho funkčního celku.

Konference je koncipována jako **praktická odpověď na tyto změny** – nikoliv teoretická debata, ale konkrétní výklad dopadů do řízení nemocnic, bezpečnosti dat, odpovědnosti managementu a každodenního fungování zdravotnických zařízení.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Pokud jste z prostředí zdravotnictví, IT bezpečnosti, veřejné správy nebo krizového řízení, **tato konference je přesně pro vás**.

Ambicí je vytvořit prostor, kde se setkají:

- zástupci nemocnic a zdravotnických zařízení
- odborníci na kybernetickou bezpečnost
- legislativní experti
- zástupci státní správy

a společně budou hledat odpovědi na otázky, které dnes řeší prakticky každý subjekt v systému zdravotnictví.

Očekáváme, že půjde o jednu z našich nejdůležitějších odborných akcí v této oblasti zdravotnictví v roce 2026.

Odborná spolupráce a sdílení zkušeností

Dne 7. dubna 2026 proběhl odborný seminář Asociace pověřenců ČR zaměřený mimo jiné na problematiku kamerových systémů ve veřejné správě, školství a zdravotnictví a na otázky transparentnosti a ochrany osobních údajů.

ASKI zde zastupovala **Mgr. Bc. Marianna Kubušová, MBA**, které tímto děkuji za reprezentaci naší asociace.

Současně bych rád poděkoval předsedovi Asociace pověřenců **Ing. Jaroslavu Vítkovi, MBA** za pozvání a dlouhodobou spolupráci, které si velmi vážíme. Právě propojení odborných komunit je jedním ze základních pilířů našeho fungování.

Pokračování vzdělávání jako stabilní základ

Ve dnech 11. a 12. dubna 2026 pokračovala výuka programu **LL.M. Ochrana dat a správa informační bezpečnosti** na půdě Střední školy informatiky, poštovnictví a finančnictví v Brně.

Tento program dlouhodobě potvrzuje, že oblast ochrany dat a informační bezpečnosti je nedílnou součástí fungování organizací napříč sektory, a to od školství až po kritickou infrastrukturu.

Naše vzdělávací aktivity jsou zároveň podpořeny mezinárodní certifikací **International Education Society London (IES)** a **International Certification Institute (ICI)**, což garantuje jejich kvalitu i přesah do zahraničního prostředí.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Nová akreditace a důraz na lidskou infrastrukturu

V průběhu tohoto období jsme získali novou akreditaci pro **MBA studium zaměřené na leadership, koučink, komunikaci a vyjednávání**.

Tento krok považujeme za zásadní. Kritická infrastruktura není jen o technologiích a systémech. Stejně důležitá je i tzv. **lidská infrastruktura,** schopnost vést, rozhodovat, komunikovat a zvládat krizové situace.

Právě tyto kompetence dnes rozhodují o tom, jak organizace zvládají tlak, změny i mimořádné události.

Závěrem

Duben 2026 jasně ukázal, že ASKI i ASKI Solutions s.r.o. nezůstávají u teorie. Naopak systematicky překládáme odborné znalosti do praxe, vytváříme nové platformy, organizujeme důležité odborné akce a rozvíjíme vzdělávání v oblastech, které jsou pro fungování společnosti zásadní.

Bezpečnost a odolnost nejsou jednorázovým projektem. Jsou výsledkem dlouhodobé práce, spolupráce a schopnosti reagovat na nové výzvy.

Pokud máte jakékoliv dotazy, připomínky nebo návrhy, neváhejte nás kontaktovat na e-mailové adrese **info@aski.cz**. Těšíme se na vaše nápady a rady, které nám pomohou dále rozvíjet a zlepšovat naši práci.

S pozdravem a přáním všeho bezpečného,

PhDr. Mgr. Dušan Kalášek, MBA

prezident Asociace škol kritické infrastruktury

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Zdravotnictví pod tlakem legislativy

Odborná platforma, která přichází ve správný čas

Mgr. Andrea Babišová, MBA et MBA, LL.M
ambasadorka Asociace škol kritické infrastruktury, z.s.
ředitelka sekce zdravotnictví ASKI Solutions s.r.o.

Zdravotnictví v České republice se nachází v bodě, který lze bez nadsázky označit za zásadní přelom. Nejde o evoluci, ale o změnu prostředí, ve kterém budou zdravotnická zařízení fungovat v následujících letech.
Nové právní předpisy, a to zejména zákon č. 264/2025 Sb. o kybernetické bezpečnosti a zákon č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury, zásadně mění pravidla hry. A právě v této chvíli vzniká potřeba prostoru, kde se tyto změny nejen vysvětlí, ale především zasadí do praxe.

Právě na tuto potřebu reaguje odborná konference:
Zdravotnictví pod tlakem legislativy
📅 27. května 2026
📍 Praha
👉 https://www.askisolutions.cz/zdravotnictvi-pod-tlakem-legislativy--konference/

Nejde jenom o další konferenci, jde o reakci na realitu.
V posledních měsících se v odborné komunitě opakují stejné otázky:

- Co přesně pro nás znamená nová legislativa?
- Jaké povinnosti musíme splnit – a kdy?
- Jaké jsou reálné dopady na provoz nemocnic?
- Kdo za co odpovídá?
- Jak sladit IT, bezpečnost, management a právo?

Problém není v tom, že by odpovědi neexistovaly. Problém je v tom, že jsou roztříštěné.
Konference „Zdravotnictví pod tlakem legislativy“ vzniká jako **odborná platforma**, která tyto odpovědi spojuje, a to systematicky, srozumitelně a především prakticky.

Zdravotnictví jako kritická infrastruktura – konec teorie
Zdravotnická zařízení byla vždy klíčovou součástí fungování státu. Nová legislativa to ale poprvé jednoznačně překlápí do konkrétní odpovědnosti. Zdravotnictví už není jen

poskytovatelem péče. Stává se **plnohodnotnou součástí kritické infrastruktury**.

To znamená:

- vyšší nároky na kybernetickou bezpečnost
- nové povinnosti v oblasti řízení rizik
- důraz na kontinuitu provozu
- odpovědnost managementu za bezpečnostní procesy
- nutnost koordinace mezi IT, právem a vedením organizace

A právě tady vzniká největší problém: **tyto oblasti spolu často nemluví stejným jazykem.**

Konference jako místo, kde se propojí svět, který musí fungovat společně

Cílem této konference není přinést další teoretické prezentace.
Cílem je vytvořit prostředí, kde se setkají:

- ředitelé nemocnic a zdravotnických zařízení
- IT specialisté a bezpečnostní manažeři
- právníci a compliance odborníci
- zástupci státní správy
- odborníci na krizové řízení

a budou společně řešit jednu věc: **jak zvládnout novou legislativu v praxi.**

Co účastník skutečně získá

Tahle konference není o tom „být u toho“. Je o tom **odnést si konkrétní hodnotu**.
Účastník získá:

1. Jasný výklad legislativy

- Bez zbytečné složitosti.
  Bez právnických klišé.
  S důrazem na to, co je skutečně důležité.

2. Praktické dopady na řízení organizace

- Co se mění pro management?
  Kde vzniká odpovědnost?
  Jak nastavit procesy?

3. Reálné zkušenosti z praxe

- Jak k tomu přistupují jiné organizace?
  Co funguje – a co ne?

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

4. Propojení s odbornou komunitou

- Možnost diskutovat, ptát se a sdílet zkušenosti s lidmi, kteří řeší stejné problémy.

Pod záštitou, která dává smysl

Konference se koná pod záštitou ministra zdravotnictví
Mgr. et Mgr. Adama Vojtěcha
Záštitu také poskytl **MUDr. Martin Gebauer, MHA, LL.M.** náměstek hejtmana Moravskoslezského kraje.
Tato záštita není jen formální. Je signálem, že téma bezpečnosti, odolnosti a legislativy ve zdravotnictví je vnímáno jako **strategická priorita**.

ASKI Solutions s.r.o. – platforma pro praxi

Organizátorem konference je **ASKI Solutions s.r.o.**, dceřiná organizace Asociace škol kritické infrastruktury.
Zatímco ASKI dlouhodobě buduje odborné zázemí, vzdělávání a koncepci, ASKI Solutions přináší **realizaci do praxe**.
Tato konference je prvním velkým projektem této platformy a zároveň jasným signálem, že cílem není zůstat u teorie.

Proč je právě teď správný čas se přihlásit

Možná nejdůležitější otázka zní: Proč bych se měl zúčastnit právě teď?
Odpověď je jednoduchá:

- legislativa už platí
- požadavky se budou zpřesňovat
- tlak na organizace poroste
- a prostor pro chyby se bude zmenšovat

Ti, kteří se připraví včas, získají náskok. Ti, kteří budou čekat, budou reagovat pod tlakem.

Komu je konference určena

Konference je určena všem, kteří nesou odpovědnost za fungování zdravotnických zařízení:

- management nemocnic
- IT a bezpečnostní specialisté
- právníci a compliance pracovníci
- pracovníci veřejné správy
- odborníci na krizové řízení

Pokud se vás dotýká bezpečnost, legislativa nebo řízení organizace, pak se vás tato konference týká přímo.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Ambice, která přesahuje jednu akci
Ambicí této konference není jen jednodenní setkání.
Ambicí je vytvořit **dlouhodobou odbornou platformu**, která bude:

- propojovat odborníky
- přinášet aktuální informace
- pomáhat interpretovat legislativu
- a podporovat rozvoj bezpečnostního prostředí ve zdravotnictví

Závěrem
Zdravotnictví dnes stojí pod tlakem. Ale tlak nemusí znamenat problém. Může být impulsem ke změně. Konference „Zdravotnictví pod tlakem legislativy“ je příležitostí, jak tuto změnu uchopit správně.

👉 Přihlaste se zde:

https://www.askisolutions.cz/zdravotnictvi-pod-tlakem-legislativy--konference/
Těšíme se na setkání s vámi v prostoru, kde se z legislativy stává praxe.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Leadership v kritické infrastruktuře: přestaňte být „operativním rukojmím“ svého týmu

Mgr. Bc. Marianna Kubušová, MBA, lektor ASKI

Můžete mít nejmodernější technologie, nejpřísnější protokoly a nepropustné zabezpečení. Ale v okamžiku krize, strategického rozhodování nebo vyjednávání o klíčových zdrojích stojí v centru všeho jediný prvek: člověk. Otázkou není, zda vaše systémy fungují, ale zda lidé, které vedete, dokážou pod tlakem samostatně myslet a jednat.

V Asociaci škol kritické infrastruktury (ASKI) proto otevíráme nový postgraduální program **MBA Leadership koučink, komunikace a vyjednávání**. Nejde o další akademický titul do sbírky. Jde o hloubkovou přestavbu vašeho „operačního systému“ lídra.

Past jménem „univerzální opravář“

Většina manažerů v náročných odvětvích trpí stejným syndromem: stali se **operativními rukojmími** vlastní organizace. Každý problém končí na jejich stole, každé rozhodnutí čeká na jejich posvěcení. Jako „univerzální opraváři“ tráví dny lepením děr, místo aby budovali funkční celky.

Koučovací přístup je lékem na toto přehlcení. Podstata koučování v managementu není v „povídání si“, ale v precizním **přenosu odpovědnosti**. Výsledky se projevují ve třech rovinách:

- **Vztah 1 na 1:** Nejrychlejší cesta, jak z podřízeného udělat partnera, který místo čekání na příkazy přemýšlí o řešeních.
- **Vedení týmu:** Budování kultury, kde lidé aktivně přicházejí s hotovými návrhy.
- **Role lídra:** Přestáváte být „úzkým hrdlem“ organizace a získáváte prostor pro strategickou práci.

Tři pilíře vaší transformace

Program propojuje disciplíny, které v kombinaci vytvářejí neporazitelnou výbavu moderního lídra:

1. **Leadership koučink (standardy ICF):** Postoj, který odemyká potenciál jednotlivců skrze cílené otázky a aktivní naslouchání.
2. **Strategické vyjednávání (Harvardský model):** Jak dosáhnout dohody i v emočně vypjatých situacích a budovat dlouhodobou důvěru.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

3. **Cílená komunikace (typologie DISC):** Adaptace stylu tak, aby vám rozuměl i ten nejnáročnější partner.

Balíček elitního lídra: Co studiem získáte?

Uvědomujeme si, že pro vrcholového manažera je důležitý nejen obsah, ale i prestiž a oficiální uznání. Absolventi získávají unikátní kombinaci potvrzení:

- **Titul MBA:** Mezinárodně uznávaná známka manažerské kvality.
- **Certifikace IES a ICI:** Prestižní osvědčení od *International Education Society* a *International Certification Institute* potvrzující globální úroveň vzdělání.
- **Příprava na profesní zkoušku (NSK):** Kompletní příprava ke státní zkoušce pro profesi kouč, která má v českém prostředí nejvyšší možnou váhu.

Studium navržené pro vaši praxi

Víme, jak cenný je váš čas, proto je studium maximálně efektivní. Výuka probíhá **jeden víkend v měsíci** v Praze, Brně a Ostravě. Garantem programu je Mgr. Bc. Marianna Kubušová, MBA, ACC, certifikovaná koučka mezinárodní federace ICF, která do výuky vnáší etiku a světové standardy.

Nepřicházejte si jen pro titul. Přijďte se posunout do role architekta, který staví na schopnostech svých lidí, nikoliv na své vlastní operativě.

Staňte se součástí první vlny moderních lídrů. Kapacita je striktně omezena pro zajištění prostoru pro mentoring.

👉 **Zajistěte si své místo na startu zde:** https://mba.aski.cz/

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

LEGISLATIVNÍ A NORMATIVNÍ DIMENZE TECHNOLOGIE WAVETRAP V KYBERNETICKÉ BEZPEČNOSTI

Ing. Petr Stoklasa, MBA

Úvodem

V době, kdy bezdrátové technologie pronikají do všech oblastí lidské činnosti, od řízení průmyslových procesů přes zdravotnictví až po správu kritické infrastruktury, se otázka neúmyslného vyzařování elektromagnetického záření dostává do centra pozornosti odborníků na kybernetickou bezpečnost, ochranu osobních údajů i ochranu utajovaných skutečností.

Elektromagnetické vlnění je fyzikálním jevem, který nelze eliminovat, lze jej však selektivně potlačit. Právě tato schopnost tvoří základ moderních stínicích technologií určených pro ochranu prostor, v nichž jsou zpracovávány citlivé informace. Technologie WAVETRAP představuje řešení založené na speciálně konstruovaných sklech a filmech s vodivými vrstvami, integrovaných do stavebních konstrukcí. Na rozdíl od tradičních přístupů, jako jsou Faradayovy klece nebo plná kovová opláštění, jde o architektonicky nenápadné, esteticky přijatelné a funkčně selektivní řešení.

Selektivita zde znamená, že materiál účinně tlumí elektromagnetické signály v definovaných frekvenčních pásmech, zejména v pásmech využívaných technologiemi
WiFi, Bluetooth nebo dalšími bezdrátovými komunikačními systémy, aniž by zásadně bránil prostupu světla nebo narušoval architektonický charakter prostoru. Tato vlastnost z něj činí mimořádně zajímavý nástroj pro fyzickou a současně kybernetickou ochranu prostor, v nichž se pracuje s citlivými, důvěrnými nebo utajovanými informacemi.

Tato esej analyzuje principy technologie WAVETRAP, její technické vlastnosti, a především její nezastupitelnou roli v plnění povinností, které subjektům ukládají klíčové právní předpisy: zákon č. 264/2025 Sb., o kybernetické bezpečnosti, zákon č. 266/2025 Sb. o ochraně utajovaných informací, zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, nařízení DORA (EU) 2022/2554 a obecné nařízení GDPR (EU) 2016/679.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Fyzikální principy elektromagnetického stínění

Elektromagnetické vlnění je tvořeno oscilujícími elektrickými a magnetickými poli, která se prostorem šíří rychlostí světla. Z hlediska bezpečnosti jsou klíčové zejména frekvence používané pro rádiovou, mobilní a datovou komunikaci, tedy pásma, v nichž pracují technologie WiFi, Bluetooth, LTE či 5G. Každý bezdrátový systém vytváří elektromagnetické pole, které se šíří i za fyzické hranice budovy, pokud mu v tom nic účinně nebrání.

V běžných administrativních nebo technických budovách je významnou slabinou zejména sklo. Obyčejné skleněné výplně oken mají velmi nízký útlum elektromagnetického signálu, a proto se bezdrátové signály mohou dostávat mimo objekt, kde mohou být zachyceny útočníkem. To vytváří riziko pasivního odposlechu, mapování provozu bezdrátových sítí, identifikace zařízení nebo přípravy cílených útoků.

Popsaná technologie pracuje s principem vícevrstvého skla nebo systémem filmů, v němž je integrována vodivá vrstva tvořená například oxidy kovů, tenkou kovovou mřížkou nebo jiným průhledným vodivým materiálem. Tato vrstva část elektromagnetické energie odráží a část absorbuje. Výsledkem je významné oslabení intenzity signálu při jeho průchodu přes skleněnou plochu.

Fyzikálně tedy nejde o absolutní zablokování veškerého záření, ale o řízené a selektivní snížení intenzity elektromagnetického pole v určitém frekvenčním rozsahu. Právě selektivita je zásadní, protože materiál může být optimalizován tak, aby nejúčinněji působil proti pásmům, která z pohledu kybernetické bezpečnosti představují největší riziko.

Pro kybernetickou bezpečnost jsou klíčová frekvenční pásma bezdrátových technologií: pásmo UHF (300 MHz – 3 GHz) zahrnující WiFi 2,4 GHz, Bluetooth, GSM/LTE; pásmo SHF (3–30 GHz) zahrnující WiFi 5 GHz, WiFi 6E a 5G NR. V typické kancelářské budově s běžným sklem je WiFi signál 2,4 GHz detekovatelný až ve vzdálenosti 80–120 metrů od objektu.

Výhodou tohoto řešení je, že jde o pasivní technologii. Po správné instalaci není nutné aktivní napájení ani průběžné řízení. Ochranná funkce je přítomna trvale, což snižuje provozní náklady i pravděpodobnost lidské chyby. To je v prostředí bezpečnostního managementu významné, protože opatření, která nejsou závislá na každodenní disciplíně obsluhy, bývají z dlouhodobého hlediska účinnější.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Ochrana před digitálním odposlechem

Digitální odposlech v současnosti nemusí probíhat pouze formou průniku do sítě nebo kompromitace zařízení. Stále významnější je i možnost zachycení elektromagnetického vyzařování z prostoru, v němž jsou provozovány bezdrátové sítě, řídicí systémy nebo zařízení zpracovávající citlivé informace. Útočník vybavený směrovou anténou a spektrálním analyzátorem může zachytit provoz bezdrátové sítě, rekonstruovat obsah komunikace nebo provádět tzv. Van Eck phreaking, tedy odposlech elektromagnetického vyzařování monitorů, kabelů či klávesnic.

V prostředí kritické infrastruktury, datových center, státní správy, zdravotnických zařízení nebo finančního sektoru představuje tento typ úniku velmi závažnou hrozbu. Nejde jen o prostý odposlech. Únik elektromagnetického signálu může sloužit i jako podklad pro průmyslovou špionáž, přípravu cílených útoků na bezdrátovou infrastrukturu, zjišťování provozních režimů nebo plánování rušení komunikace.

Stínicí technologie takovou hrozbu snižuje tím, že omezuje průnik signálu skrze nejzranitelnější části budovy, tedy okenní a prosklené plochy. Pokud je bezdrátový signál významně utlumen ještě před tím, než opustí chráněný prostor, snižuje se možnost jeho zachycení ve veřejně přístupném prostoru nebo v sousedních budovách. Tím se zmenšuje útočná plocha organizace.

Nejde tedy pouze o ochranu před náhodným šířením signálu, ale i před cíleným digitálním průzkumem. V praxi se takové řešení stává součástí konceptu defense-in-depth, tedy vícevrstvé ochrany, kde fyzické omezení úniku elektromagnetického záření doplňuje šifrování komunikace, segmentaci sítí, dohled nad bezpečnostními událostmi a další technická i organizační opatření.

Význam pro kybernetickou bezpečnost bezdrátových technologií

Bezdrátové technologie přinášejí organizacím flexibilitu, nízké náklady na instalaci a vysokou provozní efektivitu. Současně však otevírají nové vektory útoku. WiFi sítě, Bluetooth zařízení, průmyslové IoT prvky, bezdrátové senzory nebo některé řídicí systémy komunikují prostřednictvím rádiových frekvencí, které překračují hranice fyzicky chráněného prostoru. To je z hlediska kybernetické bezpečnosti zásadní problém.

Klasické kybernetické zabezpečení bývá často orientováno především na logickou vrstvu, tedy na autentizaci, šifrování, monitoring a segmentaci. Pokud však organizace opomene fyzickou vrstvu šíření signálu, ponechává útočníkovi možnost sběru informací bez přímého kontaktu se systémy. Ochrana elektromagnetického perimetru je proto logickým rozšířením kybernetické bezpečnosti směrem k bezpečnosti fyzického prostoru.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Popsaný skleněný materiál v tomto směru funguje jako kontrola fyzického dosahu bezdrátové komunikace. Pomáhá vytvořit situaci, kdy bezdrátová síť zůstává funkční uvnitř definovaného prostoru, ale současně není snadno detekovatelná nebo zneužitelná zvenčí. Tím se zvyšuje důvěrnost provozu a snižuje pravděpodobnost incidentu.

Význam tohoto řešení je zvlášť vysoký tam, kde je potřeba chránit prostory s citlivými daty, zasedací místnosti pro strategická jednání, pracoviště SOC, NOC, serverovny, velíny, krizová centra nebo kanceláře orgánů veřejné moci. V takových prostorách může i zdánlivě drobný únik signálu představovat nepřijatelnou zranitelnost.

Hrozby, před nimiž technologie WAVETRAP chrání

Spektrum hrozeb spojených s nekontrolovaným šířením elektromagnetického záření z chráněných prostor zahrnuje několik zásadních kategorií. Jejich pochopení je nezbytnou podmínkou pro správné zařazení stínicí technologie do celkového bezpečnostního managementu.

Odposlech a únik dat představuje primární hrozbu. Útočník se směrovou anténou a spektrálním analyzátorem může zachytit provoz WiFi, Bluetooth nebo GSM sítí, rekonstruovat obsah komunikace, získat přístupové údaje nebo citlivá data. Kybernetické incidenty tohoto typu v minulosti reálně ohrozily provoz SCADA systémů energetické výroby odposlechem z blízkosti fyzického perimetru elektrárny.

Průmyslová špionáž a útoky na řídicí systémy jsou druhou kategorií. Únik elektromagnetického vyzařování (EMV) umožňuje získání know-how, plánů, technologických postupů nebo provozních dat. Útočník může analyzovat provozní režimy, identifikovat slabá místa a připravit cílený útok na řídicí prvky kritické infrastruktury.

Útoky typu rušení (jamming) představují třetí kategorii. Útočník může vysílat rušivé signály, které znemožní komunikaci v rámci chráněného objektu, způsobí výpadky nebo naruší provoz řídicích systémů. Jamming může být cílený na konkrétní pásmo nebo zařízení.

Laterální pohyb v síti (lateral movement): pokud útočník získá přístup do vnitřní sítě přes slabé místo, například nezabezpečený bezdrátový přístupový bod zachycený mimo objekt, může se dále pohybovat po infrastruktuře a získat vyšší oprávnění nebo přístup k dalším systémům.

Technologie WAVETRAP přímo adresuje první tři kategorie tím, že fyzicky brání přenosu elektromagnetického signálu za hranice chráněného prostoru, čímž eliminuje samu možnost vzdáleného odposlechu nebo rušení ze vzdálenosti.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Zákon o kybernetické bezpečnosti a jeho požadavky

Zákon č. 264/2025 Sb. o kybernetické bezpečnosti je stěžejním právním předpisem implementujícím požadavky evropské směrnice NIS2 (EU 2022/2555) do českého právního řádu. Zákon nabyl účinnosti k 1. lednu 2026 a nahradil předchozí zákon č. 181/2014 Sb. Zásadním způsobem rozšiřuje okruh povinných subjektů a zpřísňuje povinnosti v oblasti řízení kybernetické bezpečnosti.

Zákon ukládá povinným subjektům, správcům a provozovatelům kritické infrastruktury, poskytovatelům základních služeb a dalším regulovaným entitám, povinnost přijímat a udržovat bezpečnostní opatření k ochraně důvěrnosti, integrity a dostupnosti informací.

Konkrétně jde o provádění posouzení rizik včetně rizik spojených s elektromagnetickým vyzařováním, zavádění technických a organizačních opatření pro prevenci a detekci kybernetických incidentů, hlášení incidentů s významným dopadem do 24 hodin od jejich zjištění a zajišťování bezpečnosti dodavatelského řetězce a fyzické bezpečnosti prostor.

Technologie WAVETRAP přímo naplňuje požadavky zákona v části fyzické bezpečnosti a technických opatření. Stínicí sklo instalované na oknech a fasádách objektů, v nichž jsou zpracovávány citlivé informace, tvoří technické opatření zabraňující úniku elektromagnetického záření mimo fyzický perimetr. Tím je přerušen jeden z hlavních vektorů kybernetických útoků, vzdálený odposlech bezdrátové komunikace.

Zákon předpokládá přístup defense-in-depth, tedy vrstvené obrany, v níž fyzická vrstva (stínění EMV) spolupracuje se síťovou vrstvou (firewally, segmentace), aplikační vrstvou (šifrování, autentizace) a personální vrstvou (školení zaměstnanců). WAVETRAP posiluje fyzickou vrstvu způsobem, který je architektonicky integrovaný, provozně pasivní a dlouhodobě spolehlivý.

Očekávaná aktualizace prováděcí vyhlášky č. 316/2014 Sb. k zákonu č. 264/2025 Sb. směřuje k podrobnějšímu vymezení metodik pro posuzování rizik elektromagnetického vyzařování, včetně standardizovaných postupů měření úniku signálu z chráněných prostor. Současně má stanovit požadavky na certifikované stínicí materiály, kam lze zařadit i specializovaná stínicí skla typu WAVETRAP splňující minimální útlum 30 dB v pásmu 2,4–5 GHz. Tato skla umožňují regulovaným subjektům prokazatelně omezit šíření Wi-Fi, Bluetooth a dalších bezdrátových signálů mimo kontrolované prostředí a lépe tak sladit fyzickou vrstvu bezpečnosti s legislativními požadavky.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Typickým příkladem je jednací místnost, dispečerské pracoviště nebo operační centrum (SOC), kde je žádoucí minimalizovat riziko úniku kompromitujícího vyzařování, aniž by bylo nutné rezignovat na prosklené architektonické prvky. Předpokládaná povinnost pravidelného přezkumu a revize stínicích opatření pak zvýrazňuje potřebu, aby implementovaná řešení, jako je popisované sklo, byla dlouhodobě udržitelná, měřitelná a dobře zdokumentovaná z hlediska plnění požadavků zákona.

Stínicí technologie zde plní funkci technického opatření fyzické povahy. Pomáhá naplnit požadavky na ochranu komunikačních prostředků, ochranu prostor, v nichž dochází ke zpracování informací, a podporuje celkovou odolnost regulovaného subjektu. Zvláště v organizacích, které provozují bezdrátové technologie v kritických procesech, lze takové materiály chápat jako součást systému řízení kybernetické bezpečnosti.

Z pohledu compliance je podstatné, že zákon č. 264/2025 Sb. akcentuje systematický a prokazatelný přístup. Nejde tedy pouze o faktické provedení opatření, ale i o jeho zdokumentování, ověření a pravidelný přezkum. U tohoto typu řešení to znamená nutnost měření účinnosti, evidence technických parametrů, začlenění do bezpečnostní dokumentace a pravidelnou kontrolu při změnách provozu nebo stavebních úpravách.

Zákony o ochraně utajovaných informací o odolnosti kritické infrastruktury a stínění EMV

V oblasti ochrany utajovaných informací má elektromagnetické stínění dlouhodobě mimořádný význam. Zákon č. 412/2005 Sb. i navazující právní a bezpečnostní režim stanovují, že při ochraně utajovaných informací musí být zajištěna taková úroveň fyzické, personální, administrativní a technické bezpečnosti, která zabrání kompromitaci informací.

Jedním z tradičně sledovaných rizik je právě kompromitující vyzařování. Pokud z prostoru, v němž jsou zpracovávány utajované informace, uniká elektromagnetické záření nesoucí informační hodnotu, vzniká riziko, že oprávněně chráněné informace budou získány bez fyzického průniku do prostoru.

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, stanovuje přísné požadavky na fyzickou a technickou ochranu prostor, v nichž jsou zpracovávány informace stupně utajení „Vyhrazené", „Důvěrné", „Tajné" a „Přísně tajné".

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Zákon č. 412/2005 Sb. vyžaduje, aby přísně tajné a tajné informace byly zpracovávány v tzv. zabezpečených oblastech, které splňují specifické konstrukční a technické požadavky. Tyto požadavky zahrnují ochranu před únikem kompromitujícího vyzařování, tedy elektromagnetického záření, z nějž lze rekonstruovat zpracovávané informace. Tento aspekt je mezinárodně znám jako TEMPEST (Transient ElectroMagnetic Pulse Emanation Standard) a odpovídá standardům NATO SDIP-27 a SDIP-28.

Zákon č. 266/2025 Sb. tyto požadavky aktualizuje v kontextu moderních bezdrátových technologií a ukládá povinnosti hodnotit rizika kompromitujícího vyzařování při zpracování utajovaných informací, implementovat technická opatření k zamezení úniku elektromagnetických signálů mimo chráněné prostory, pravidelně ověřovat účinnost stínicích opatření certifikovanými měřeními a dokumentovat technická opatření pro potřeby bezpečnostních přezkumů Národního bezpečnostního úřadu (NBÚ).

Popisovaná technologie se v tomto kontextu jeví jako klíčové řešení pro objekty, v nichž jsou zpracovávány utajované informace, a to z několika důvodů. Za prvé, dosahovaný útlum 30–60 dB výrazně snižuje riziko vzdáleného odposlech kompromitujícího vyzařování. Za druhé, nenápadná integrace do okenních a fasádních prvků nevyžaduje rozsáhlé stavební úpravy, jež by byly nápadné z hlediska ochrany utajení. Za třetí, kombinace stínicího skla s dalšími prvky (stínicí fólie na zdech, správné uzemnění s odporem ≤ 1 Ω) umožňuje dosáhnout parametrů srovnatelných s náročnými TEMPEST standardy i v rekonstruovaných objektech.

Pro prostory stupně utajení „Přísně tajné" a „Tajné" je zpravidla vyžadována kombinace stínicích prvků dosahující celkového útlumu minimálně 60–80 dB, přičemž toto speciální sklo může tvořit výchozí vrstvu tohoto vícevrstvého řešení. Pro nižší stupně utajení a pro ochranu citlivých, nikoliv utajovaných informací, je dosažení útlumu 35–45 dB prostřednictvím samotné technologie WAVETRAP zpravidla dostačující.

Popsané řešení je v tomto ohledu mimořádně vhodné, protože umožňuje integrovat stínicí funkci přímo do transparentních stavebních konstrukcí, které by jinak představovaly významné místo úniku. Prostory určené pro práci s utajovanými informacemi, bezpečnostní jednání nebo zpracování citlivých bezpečnostních podkladů tak mohou být chráněny účinněji a současně bez nutnosti budovat plně neprůhledná nebo architektonicky nevyhovující řešení.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Nařízení o digitální provozní odolnosti finančního sektoru (DORA) a opatření řízení rizik

Nařízení DORA klade na finanční sektor vysoké požadavky v oblasti řízení ICT rizik, provozní odolnosti, kontinuity činností a bezpečnosti digitální infrastruktury. Jeho cílem je zajistit, aby finanční instituce dokázaly odolávat narušení, kybernetickým incidentům a provozním výpadkům, a to včetně incidentů vzniklých v důsledku zneužití komunikačních technologií.

Ačkoli DORA explicitně nepracuje s názvem konkrétní technologie nebo stínicího skla, vyžaduje přijetí takových technických a organizačních opatření, která odpovídají povaze rizik. Pokud finanční instituce využívá bezdrátové technologie v budovách, kde jsou zpracovávány transakční údaje, interní strategie, klientská data nebo bezpečnostní klíče, pak je riziko elektromagnetického odposlechu relevantní součástí ICT rizik.

Nařízení Evropského parlamentu a Rady (EU) 2022/2554 o digitální provozní odolnosti finančního sektoru (DORA) vstoupilo v účinnost v lednu 2025 a ukládá finančním institucím, bankám, pojišťovnám, investičním společnostem, správcům aktiv, poskytovatelům platebních služeb a dalším, komplexní požadavky na řízení ICT rizik a zajištění digitální provozní odolnosti.

DORA vyžaduje, aby finanční instituce implementovaly vícevrstvý přístup k ochraně svých ICT systémů, zahrnující fyzická bezpečnostní opatření jako klíčový element. Konkrétně čl. 9 DORA ukládá povinnost zajistit fyzická a logická kontrolní opatření pro přístup k ICT aktivům a datům. Čl. 10 DORA stanovuje povinnost provádět detekci anomálií a kybernetických hrozeb, přičemž neautorizovaný přístup k bezdrátové infrastruktuře přes zachycení elektromagnetického signálu mimo budovu přesně odpovídá typu hrozby, která musí být adresována.

Ve finančním sektoru jsou specifická rizika spojená s únikem EMV mimořádně závažná. Zpracování platebních transakcí, komunikace mezi obchodními systémy, přenos autentizačních údajů - toto vše probíhá prostřednictvím bezdrátových technologií v prostorách, které jsou zpravidla situovány v hustě zastavěných městských oblastech, kde je odposlech ze sousedních budov nebo z veřejného prostoru reálnou hrozbou.

WAVETRAP přispívá k plnění požadavků DORA jako prvek fyzické vrstvy ICT bezpečnosti, který omezuje oblast, z níž lze realizovat pasivní průzkum nebo aktivní útok na bezdrátovou infrastrukturu. Útočník, který nemůže zachytit WiFi signál mimo budovu, nemůže provádět pasivní analýzu komunikace, pokusit se o man-in-the-middle útoky na bezdrátové spojení ani identifikovat bezdrátová zařízení jako cíle pro následné útoky.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Z pohledu hodnocení ICT rizik dle DORA je klíčové, že zavedení stínicí technologie snižuje pravděpodobnost útoku přes vektor bezdrátové komunikace na úroveň akceptovatelného zbytkového rizika, čímž umožňuje regulovaným institucím prokázat proporcionalitu a úplnost přijatých bezpečnostních opatření při auditech prováděných příslušnými orgány dohledu (ČNB, ESA).

Obecné nařízení o ochraně osobních údajů (GDPR), opatření dle čl. 25 a 32

Obecné nařízení o ochraně osobních údajů (GDPR, EU 2016/679) ukládá správcům a zpracovatelům osobních údajů povinnost implementovat vhodná technická a organizační opatření k zajištění bezpečnosti zpracování (čl. 32 GDPR) a povinnost uplatňovat zásady záměrné ochrany soukromí a výchozího nastavení (čl. 25 GDPR, privacy by design and by default).

Čl. 32 GDPR výslovně uvádí, že bezpečnostní opatření mají zahrnovat zejména šifrování osobních údajů, ale také „schopnost zajistit trvalou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování". Únik elektromagnetického záření nesoucího nešifrované nebo slabě šifrované osobní údaje (například WiFi komunikace v prostorách nemocnic, ambulancí, call center nebo HR oddělení) může vést k porušení zabezpečení osobních údajů ve smyslu čl. 4 odst. 12 GDPR, přičemž správce je povinen takové porušení oznámit Úřadu pro ochranu osobních údajů (ÚOOÚ) do 72 hodin od zjištění.

Technologie WAVETRAP je relevantním technickým opatřením z hlediska čl. 25 GDPR, neboť zabezpečení fyzického perimetru prostoru, v němž jsou zpracovávána osobní data, přísluší k vrstvě ochrany soukromí „by design". Projektant systémů zpracování osobních údajů, který do návrhu prostoru zahrnuje stínicí technologie bránící úniku dat, prokazuje uplatnění principu záměrné ochrany soukromí v souladu s čl. 25 odst. 1 GDPR.

V kontextu zdravotnických zařízení zpracovávajících citlivé osobní údaje (čl. 9 GDPR, zvláštní kategorie osobních údajů) je fyzická ochrana prostoru před odposlechem prostřednictvím WAVETRAP zvláště relevantní, neboť zpracovávané informace požívají nejvyšší úrovně ochrany a jejich neoprávněné zpřístupnění by mohlo mít vážné důsledky pro práva a svobody fyzických osob. Stejný princip platí pro advokátní kanceláře, soudy, státní zastupitelství a orgány veřejné správy zpracovávající osobní údaje chráněné zákonnou mlčenlivostí.

Normativní rámec a technické standardy

Kromě právních předpisů je třeba zohlednit i technické normy a standardy, které konkretizují požadavky na elektromagnetické stínění, měření účinnosti a fyzickou bezpečnost prostor. Pro oblast stínění elektromagnetického vyzařování mají význam zejména normy související s elektromagnetickou kompatibilitou a se zkoušením stínicích vlastností.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Legislativní požadavky jsou v oblasti stínění EMV konkretizovány soustavou technických norem, jejichž splnění je nezbytnou podmínkou pro prokázání souladu s právními předpisy při auditech a certifikacích.

ČSN EN 50600 je norma pro datová centra stanovuje požadavky na fyzickou bezpečnost datových center, včetně stínění stěn a oken s útlumem minimálně 40 dB v pásmu 1–10 GHz, použití certifikovaných stínicích materiálů (sklo s vrstvou oxidu india a cínu) a uzemnění s odporem ≤ 1 Ω.

IEEE Std. 299.1-2013 je mezinárodním standardem pro měření účinnosti stínění elektromagnetického vlnění v budovách a zařízeních. Výrobci stínicích skel jako Pilkington, AGC Glass Europe (výrobce stínicího skla WAVETRAP) nebo Saint-Gobain dodávají svá skla s certifikáty odpovídajícími tomuto standardu, čímž garantují ověřenou kvalitu stínění.

ČSN EN 61000-4-3 stanovuje metodiku měření elektromagnetického stínění a imunitní testy. ČSN EN 55022/55024 jsou normy elektromagnetické kompatibility (EMC) stanovují limity pro vyzařování (emise ≤ 30 dBμV/m na 10 m vzdálenosti) a odolnost zařízení informační techniky.

ISO/IEC 27001 je norma pro systémy řízení bezpečnosti informací (ISMS) vyžaduje implementaci fyzických kontrol jako součásti komplexního bezpečnostního managementu. Stínicí technologie WAVETRAP je přirozenou součástí fyzické bezpečnostní domény dle přílohy A.11 ISO/IEC 27001 (fyzická a environmentální bezpečnost).

NATO SDIP-27 a SDIP-28 jsou standardy TEMPEST, které specifikují požadavky na stínění pro zpracování utajovaných informací NATO, jsou relevantní pro subjekty zpracovávající informace v mezinárodním bezpečnostním prostředí.

U takové technologie je proto nezbytné, aby její nasazení bylo doprovázeno technickou dokumentací, protokoly o měření, údaji o frekvenční charakteristice, způsobu instalace a pravidelných kontrolách. Teprve tehdy lze plně hovořit o jejím využití jako compliance nástroje.

Implementace WAVETRAP: od analýzy rizik k provozní validaci

Správná implementace stínicí technologie v prostředí regulovaného subjektu vyžaduje strukturovaný přístup zahrnující několik fází.

Analýza rizik je výchozím krokem. Identifikace zdrojů EMV a možných míst úniku prostřednictvím měření spektrálním analyzátorem (např. Rohde & Schwarz FSH). Měření musí být provedena v reálných podmínkách, v různých denních dobách a za různého provozního zatížení bezdrátových sítí, neboť intenzita signálu se dynamicky mění.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Návrh opatření zahrnuje výběr konkrétního stínicího řešení na základě požadovaného útlumu, estetických a architektonických omezení a finančních možností. Pro prostory zpracovávající utajované informace stupně „Přísně tajné" je zpravidla nutná kombinace stínicího skla s dalšími prvky (stínicí fólie na stěnách, speciálně konstruované dveře). Pro prostory zpracovávající citlivé, nikoliv utajované informace, může být WAVETRAP samotný dostačující.

Instalace a validace. Dosažení deklarovaného útlumu závisí nejen na kvalitě skla, ale zejména na preciznosti montáže: utěsnění rámů, správné propojení stínicích vrstev se stěnami objektu a uzemnění. Po instalaci je nezbytné provést verifikační měření dle IEEE 299.1, přičemž výsledky musejí být zdokumentovány.

Pravidelný přezkum je požadavkem jak technických norem (minimálně jednou ročně), tak právních předpisů. Poškozené stínicí vrstvy, například při výměně oken nebo stavebních úpravách, vedou ke vzniku slabých míst v ochraně.

Integrace s SIEM a BMS: moderní přístup propojuje stínicí systém s Building Management System (BMS) a Security Information and Event Management (SIEM). Importem dat o úniku EMV do SIEM platforem je dosaženo komplexnější korelace bezpečnostních událostí, což zvyšuje schopnost detekce anomálií a pokusů o průnik.

WAVETRAP v kontextu vícevrstvé ochrany a budoucích výzev

Technologie WAVETRAP není a nemůže být jedinou vrstvou ochrany. Její síla spočívá v tom, že fyzicky eliminuje nebo výrazně oslabuje jeden z hlavních vektorů kybernetických
útoků, čili vzdálený odposlech bezdrátové komunikace, a tím zvyšuje celkovou odolnost systému. V rámci přístupu defense-in-depth doplňuje síťovou vrstvu: segmentace sítě, firewally, IDS/IPS systémy, dále aplikační vrstvu: šifrování dat (end-to-end), silná autentizace, správa certifikátů, a v neposlední řadě také personální vrstvu, tedy školení zaměstnanců, awareness programy, správa přístupových práv.

Budoucí výzvy jsou spojeny s rozvojem nových technologií. Nástup sítí 6G přinese využití frekvenčních pásem nad 24 GHz (mmWave), kde jsou vlastnosti šíření a stínění EMV
odlišné, neboť vlny se šíří přímočaře s vyšším útlumem v materiálech, ale vyžadují nové přístupy ke stínění. Výzkum se zaměřuje na grafenové vrstvy, metamateriály a adaptivní stínicí sklo, které umožňuje dynamicky měnit útlum signálu podle aktuální potřeby. Proliferace IoT zařízení (typicky 868 MHz, LoRaWAN) rozšiřuje spektrum frekvenčních pásem, která musejí být adresována.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Evropská harmonizace v oblasti EMC stínění, probíhající v rámci aktualizace norem CEN/CENELEC, si klade za cíl sjednotit požadavky na elektromagnetické stínění napříč členskými státy EU. Tím bude usnadněna přeshraniční implementace certifikovaných
řešení a zvýší se předvídatelnost regulatorního prostředí pro výrobce i integrátory stínicích technologií.

Limity a podmínky účinnosti

Přestože je tato technologie velmi účinná, nelze ji absolutizovat. Sama o sobě nezaručuje úplnou ochranu před všemi formami elektromagnetického útoku. Její účinnost závisí na kvalitě materiálu, odborné montáži, návaznosti na další stavební prvky a na tom, zda nejsou v prostoru jiná místa úniku signálu, například netěsnosti, nechráněné dveře nebo kabelové prostupy.

Dalším limitem je potřeba sladit stínění s provozními požadavky. Organizace musí pečlivě zvážit, které signály chce omezit a které potřebuje zachovat. U některých objektů může být žádoucí úplné odstínění, jinde spíše řízené oslabení. To potvrzuje, že správné nasazení technologie musí vycházet z individuální analýzy prostředí.

Je rovněž třeba připomenout, že technologický vývoj bude přinášet nové frekvenční rozsahy a nové komunikační protokoly. Proto musí být stínicí řešení pravidelně přehodnocována z hlediska budoucí kompatibility. Skutečně bezpečná organizace nepovažuje jednorázovou instalaci za konečné řešení, ale za součást kontinuálního procesu řízení rizik.

Závěrem

Technologie WAVETRAP jako selektivně stínicí materiál představuje moderní, architektonicky integrované a legislativně relevantní opatření v oblasti kybernetické bezpečnosti, ochrany osobních údajů a ochrany utajovaných skutečností. Její schopnost dosáhnout útlumu 30–60 dB v klíčových frekvenčních pásmech bezdrátových technologií fyzicky eliminuje jednu z nejvážnějších, a přitom nejméně viditelných hrozeb, vzdálený odposlech elektromagnetického vyzařování mimo chráněný prostor.

Z legislativního hlediska tato technologie přispívá k plnění povinností podle zákona č. 264/2025 Sb. o kybernetické bezpečnosti (technická opatření fyzické bezpečnosti, posouzení rizik EMV), zákonů č. 412/2005 Sb. a č. 266/2025 Sb. o ochraně utajovaných informací (prevence kompromitujícího vyzařování, TEMPEST standardy), nařízení DORA (fyzická vrstva ochrany ICT aktiv, omezení vektoru bezdrátových útoků) a GDPR (technická opatření dle čl. 32, privacy by design dle čl. 25).

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Úspěšná implementace této technologie vyžaduje strukturovaný přístup zahrnující analýzu rizik spektrálním měřením, odbornou instalaci s verifikačním měřením dle IEEE 299.1, pravidelný přezkum a integraci s dalšími vrstvami bezpečnostní architektury. Jedině takto je dosaženo plného souladu s legislativními a normativními požadavky a skutečné eliminace rizika digitálního odposlechu a kybernetických útoků na bezdrátové technologie.

WAVETRAP představuje vysoce relevantní nástroj moderní kybernetické bezpečnosti, protože spojuje stavebně-technickou funkci se schopností chránit organizaci před únikem elektromagnetického vyzařování. Její význam spočívá zejména v tom, že omezuje možnost digitálního odposlechu, průzkumu bezdrátového prostředí a některých forem kybernetických útoků zaměřených na bezdrátové technologie.

Jako selektivně stínicí materiál je vhodná zejména pro prostory, v nichž jsou zpracovávány citlivé, důvěrné nebo utajované informace, a pro organizace, které musejí plnit vysoké nároky na řízení kybernetické bezpečnosti. Její nasazení je z právního i normativního hlediska dobře obhajitelné vůči požadavkům zákona č. 264/2025 Sb., zákona č. 266/2025 Sb., zákona č. 412/2005 Sb., nařízení DORA i GDPR.

Klíčové však je, aby nebyla chápána jako izolovaný stavební doplněk, nýbrž jako součást systému vícevrstvé ochrany. Teprve v kombinaci s analýzou rizik, měřením, dokumentací, kontrolou účinnosti a dalšími technickými a organizačními opatřeními naplňuje svůj plný potenciál. Právě v tomto komplexním pojetí lze spatřovat její největší přínos pro současné i budoucí požadavky kybernetického zabezpečení.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Závislost na infrastruktuře jako determinant přípravy obyvatelstva na mimořádné události

Ing. Josef Myslín, Ph.D., MSc., MPA, CEVRO Univerzita, Katedra bezpečnostních studií

Příprava obyvatelstva na mimořádné události je v současné době jedním z významných předpokladů společenské odolnosti. Přestože bývá tato problematika často spojována zejména s informovaností obyvatelstva, činností orgánů veřejné správy nebo schopností integrovaného záchranného systému reagovat na vzniklé situace, stále výrazněji vystupuje do popředí ještě jeden faktor, a to závislost jednotlivce i domácnosti na technické a obslužné infrastruktuře. Právě tato závislost významně ovlivňuje reálnou schopnost obyvatel překlenout první hodiny a dny narušení běžného života.

Moderní společnost je charakteristická vysokou mírou provázanosti. Dodávky elektrické energie, pitné vody, plynu, fungování dopravy, zásobovacích řetězců, elektronických komunikací i digitálních platebních systémů tvoří základní rámec každodenní existence. Tyto systémy jsou za běžných okolností vnímány jako samozřejmé, a proto bývá jejich význam plně doceněn až ve chvíli jejich omezení nebo úplného výpadku. Mimořádná událost pak nezasahuje pouze konkrétní území či objekt, ale prostřednictvím narušení infrastruktury rychle dopadá i na životní potřeby obyvatelstva. Kromě přímých obětí mimořádné události (např. lidé, kteří přišli o majetek při povodni) pak můžeme hovořit o těch, kteří jsou mimořádnou událostí dotčeni právě omezením poskytovaných služeb infrastruktury (výpadky elektřiny, vody, plynu, komunikačních sítí atd.)

Cílem tohoto textu je ukázat, že míra závislosti na infrastruktuře představuje významný determinant přípravy obyvatelstva na mimořádné události. Jinými slovy, čím vyšší je každodenní závislost obyvatel na externě zajišťovaných službách a technických systémech, tím vyšší jsou nároky na jejich přípravu pro případ narušení těchto systémů.

Infrastrukturní závislost jako znak moderní společnosti

Současný způsob života je postaven na trvalé dostupnosti služeb, které dříve buď vůbec neexistovaly, nebo nehrály tak zásadní roli. Elektrická energie dnes nezajišťuje pouze osvětlení, ale podmiňuje provoz vytápění, chlazení, přípravu stravy, uchovávání potravin, činnost domácích spotřebičů i dobíjení komunikačních zařízení. Mobilní sítě a internet již neslouží jen ke komunikaci, ale také k získávání informací, orientaci v prostoru, práci, vzdělávání, bankovním operacím či kontaktu s institucemi veřejné správy. Bez internetového připojení často nejsme schopni realizovat například ani některé úkony vůči orgánům státní správy. Obdobně doprava a logistika zabezpečují

plynulé zásobování obchodní sítě, která je v mnoha případech nastavena na rychlou obrátku zboží bez větších lokálních rezerv.

Tato situace vede k tomu, že domácnost sice může být materiálně vybavenější než v minulosti, avšak současně je funkčně zranitelnější. Vysoká životní úroveň totiž automaticky neznamená vysokou odolnost. Naopak lze konstatovat, že technicky komfortnější způsob života bývá často vykoupen nižší schopností fungovat při narušení základních systémů. Závislost na infrastruktuře se tak stává jedním z klíčových znaků současné společnosti a současně i jedním z jejích bezpečnostních limitů.

Proměna domácnosti a pokles každodenní soběstačnosti

Při srovnání minulosti a současnosti je třeba vycházet z toho, že dřívější domácnosti byly ve větší míře přizpůsobeny samostatnému fungování. Neznamená to, že by byly bezpečnější ve všech ohledech, ale jejich každodenní provoz nebyl do takové míry podmíněn nepřetržitou dostupností složité technické infrastruktury. Lidé byli více fixováni na bezprostřední okolí svého bydliště, častěji disponovali zásobami potravin a základních potřeb, byli zvyklí hospodařit s omezenými zdroji a v mnoha případech dokázali po určitou dobu fungovat i bez vnější podpory. Neexistence sítí a další infrastruktury znamenala výrazně nižší komfort (což ovšem nebylo nijak vnímáno, neboť tyto technologie vůbec nebyly známé), ale také menší závislost na okolí a na fungování externích systémů.

Současná domácnost naproti tomu často funguje v režimu průběžné spotřeby. Potraviny, hygienické potřeby i další základní zboží jsou nakupovány průběžně, mnohdy v množství odpovídajícím pouze velmi krátkému časovému horizontu. Ztrácí se dovednosti spojené s improvizací, náhradním řešením nebo úsporným hospodařením. Významná část obyvatel navíc každodenně dojíždí za prací, školou nebo službami, takže i krátkodobé omezení dopravy může narušit běžný chod domácnosti. K tomu se přidává vysoká závislost na digitálních technologiích, která zvyšuje citlivost populace na výpadky komunikace a informací.

Pokles každodenní soběstačnosti je přitom z hlediska krizové připravenosti zásadní. Domácnost, která není schopna zajistit si základní potřeby ani na omezené časové období, se stává velmi rychle závislou na vnější pomoci. V případě rozsáhlejší mimořádné události však nemusí být tato pomoc okamžitě dostupná, protože kapacity veřejných institucí a záchranných složek jsou vždy omezené. Dochází tak k tomu, že lidé, kterým se ve výsledku v podstatě nic nestalo, se stávají těmi, kteří vyžadují pomoc a kteří do určité míry zbytečně zahlcují síť snažící se pomoci postiženým.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Dopady výpadku infrastruktury na obyvatelstvo

Mimořádné události mají zpravidla vícevrstevnatý charakter. Přímý dopad události, například povodně, vichřice, technologické havárie nebo rozsáhlého výpadku elektrické energie, bývá často doprovázen sekundárními a terciárními efekty. Právě v těchto návazných dopadech se infrastruktura ukazuje jako rozhodující faktor.

Výpadek elektrické energie může vést k omezení vytápění, osvětlení, chlazení potravin, provozu vodáren či telekomunikačních zařízení. Omezení dodávek vody se promítá do hygieny, přípravy pokrmů i základního provozu domácnosti. Narušení mobilních sítí a internetu komplikuje nejen komunikaci mezi obyvateli, ale také šíření oficiálních informací a pokynů. Omezení dopravy a zásobování následně ztěžuje dostupnost potravin, léků a pohonných hmot. Pokud se tyto jevy spojí, vzniká situace, v níž ani relativně krátkodobé narušení infrastruktury nepůsobí pouze jako technický problém, ale jako faktor, který může zásadně destabilizovat každodenní život obyvatelstva.

Důležité je rovněž psychologické hledisko. Současný člověk je zvyklý na vysokou míru okamžité dostupnosti služeb a informací. Jejich náhlá absence proto nevyvolává jen objektivní omezení, ale také subjektivní pocit bezmoci, nejistoty a ztráty kontroly. Krizová připravenost obyvatelstva tedy nespočívá pouze v materiálním zabezpečení, ale také ve schopnosti mentálně přijmout, že některé standardní služby nemusí být v mimořádné situaci dostupné.

Infrastrukturní závislost jako determinant přípravy obyvatelstva

Pojem determinant zde označuje faktor, který zásadním způsobem ovlivňuje podobu i obsah přípravy obyvatelstva. Jestliže je současný člověk výrazně závislý na infrastruktuře, musí tomu odpovídat i struktura preventivních opatření, vzdělávání a doporučení pro obyvatelstvo. Nestačí obecně konstatovat, že občan má být připraven na mimořádnou událost. Je třeba přesně formulovat, na jaký typ omezení se má připravovat a jaké důsledky může výpadek konkrétní infrastruktury přinést. A následně pak definovat, jaké jsou možné cesty, jak výpadkům čelit a jak zajistit základní životní potřeby jednotlivých domácností – z filosofického, organizačního i materiálního hlediska.

Příprava obyvatelstva proto musí vycházet z realistického předpokladu, že při mimořádné události nemusí být po určitou dobu možné běžně nakupovat, telefonovat, používat internet, topit standardním způsobem, čerpat pohonné hmoty nebo využívat veřejnou dopravu. Taková situace přitom nemusí trvat dlouhé týdny, aby se projevila jako závažná. U mnoha domácností může být kritických již prvních 24 až 72 hodin.

Z tohoto pohledu se ukazuje, že závislost na infrastruktuře přímo určuje, jaké kompetence a jaké materiální zabezpečení by měly být u obyvatelstva rozvíjeny. Čím menší je každodenní soběstačnost, tím větší význam má cílená příprava zaměřená na krátkodobé autonomní fungování domácnosti.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Směry praktické přípravy domácností

Pokud má být příprava obyvatelstva efektivní, musí mít konkrétní a srozumitelnou podobu. Základním prvkem je vytváření přiměřených domácích zásob. Nejde přitom o hromadění nadměrného množství materiálu, ale o rozumnou rezervu potravin, pitné vody, léků, hygienických potřeb a dalších nezbytností pro překlenutí prvních dnů mimořádné situace. Významné je rovněž zajištění alternativních prostředků pro osvětlení, jednoduchou přípravu jídla, základní orientaci a příjem informací. Často přitom budeme narážet na nedůvěru obyvatelstva, které mnohdy podobné myšlenky vnímá jako „přípravu na válku“. Válečný konflikt samozřejmě (zejména v dnešní době) patří mezi potenciální rizika, nicméně zásadní omezení infrastruktury a zásobování může být způsobeno například povodněmi či například blackoutem způsobeným technickou poruchou vedení elektrické energie – tedy většinově hovoříme o ryze civilních, nevojenských hrozbách mající potenciál způsobit zásadní výpadky infrastruktury.

Neméně důležitá je znalost toho, jak se zachovat při dlouhodobějším výpadku elektřiny, při narušení dodávek vody nebo při omezení komunikačních sítí. Obyvatelstvo by mělo být vedeno k úvaze o tom, jak by jejich domácnost fungovala bez možnosti okamžitého nákupu a bez běžného technologického komfortu. Tato forma přípravy má význam nejen praktický, ale i pedagogický, protože posiluje uvědomění, že mimořádná událost není jen abstraktní krizový scénář, ale situace s velmi konkrétními dopady do každodenního života. Nutné je přitom, jak již bylo zmíněno, také filosofické a psychologické nastavení toho, že v případě mimořádné události může být nutné „přepnutí“ do bazálního módu, ve kterém budou řešeny pouze základní životní potřeby. Je zřejmé, že čím vyšší bude úroveň, na kterou jsme běžně zvyklí, tím náročnější bude návrat k bazálnímu fungování. Ostatně je nutné si uvědomit, že i kolektivní prostředky civilní ochrany budou řešit rovněž jen základní potřeby (společné ubytování, jednotné stravování, kolektivní přístup atd.) – pakliže vzhledem k rozsahu mimořádné události, počtu postižených a dalších faktorech bude vůbec možné postarat se o všechny. Každý člověk, který své „přežití“ zajistí sám, výrazně ulevuje státním složkám a zvyšuje kolektivní společenskou odolnost.

Příprava by měla zahrnovat také specifické potřeby zranitelných skupin, například seniorů, osob se zdravotním omezením, rodin s malými dětmi nebo osob závislých na pravidelném užívání léků či používání zdravotnických pomůcek. Právě u těchto skupin se může výpadek infrastruktury projevit rychleji a závažněji než u běžné populace.

Role veřejné správy a bezpečnostní komunikace

Příprava obyvatelstva nemůže být ponechána pouze na individuální iniciativě. Důležitou úlohu zde mají obce, školy, složky integrovaného záchranného systému i další veřejné instituce. Jejich úkolem není jen reagovat na již vzniklou událost, ale také systematicky rozvíjet preventivní působení vůči obyvatelstvu. Součástí tohoto

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

působení by měla být srozumitelná komunikace o tom, jaké infrastrukturní výpadky mohou nastat, jaké mají důsledky a jak se na ně mohou domácnosti připravit.

Bezpečnostní komunikace by přitom měla být praktická, věcná a zbavená zbytečné dramatizace. Obyvatelstvo je vhodné motivovat nikoli strachem, ale odpovědností a realistickým pohledem na fungování současné společnosti. Mimochodem, právě strašení je vnímáno společností velmi negativně. Důležitým cílem je vytvořit takové prostředí, v němž je základní domácí připravenost vnímána jako běžná součást odpovědného občanského chování, nikoli jako projev přehnaných obav.

Závěr

Závislost na infrastruktuře představuje v současné společnosti významný determinant přípravy obyvatelstva na mimořádné události. Zatímco v minulosti byly domácnosti ve větší míře schopny fungovat po určitou dobu samostatně, dnešní způsob života je úzce spojen s nepřetržitou dostupností energií, zásobování, dopravy a elektronických komunikací. Tato skutečnost zvyšuje zranitelnost obyvatelstva při narušení běžného provozu společnosti.

Příprava obyvatelstva proto musí reflektovat reálné podmínky moderního života. Její těžiště nespočívá pouze v obecné osvětě, ale především v rozvoji schopnosti domácností překlenout omezené období bez dostupnosti základních služeb. Posilování domácí soběstačnosti, vytváření přiměřených zásob, osvojení základních návyků pro krizové situace a cílená preventivní komunikace představují důležité předpoklady společenské odolnosti.

Lze uzavřít, že odolnost společnosti nezačíná až na úrovni státu nebo zásahu záchranných složek, ale na úrovni jednotlivce a domácnosti. Právě míra připravenosti obyvatel na dočasné selhání infrastruktury rozhoduje o tom, zda mimořádná událost zůstane zvládnutelným narušením, nebo se promění v hlubší společenský problém.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Írán mění taktiku: od náhodných útoků k trvalé kybernetické kampani proti kritické infrastruktuře

Kristian Pavlinec, student SŠIPF Brno

Abstrakt

Nová analýza amerického think-tanku Center for Strategic and International Studies (CSIS) dokumentuje zásadní proměnu íránské kybernetické strategie. Írán již neprovádí izolované, příležitostné kyberútoky ale buduje trvalou, strategicky řízenou přítomnost v sítích kritické infrastruktury svých protivníků. Energetika, vodohospodářství, doprava a zdravotnictví se stávají primárními cíli íránských státem sponzorovaných skupin i jejich hacktivistických proxy. Tento článek shrnuje klíčová zjištění CSIS, zasazuje je do širšího geopolitického kontextu a upozorňuje na dopady pro bezpečnostní komunitu.

Od epizodických útoků ke strategické kampani

Dlouhou dobu bylo íránské kybernetické působení vnímáno jako reaktivní, série útoků spouštěných jako odveta za politická nebo vojenská rozhodnutí protivníka. Analytici CSIS nyní upozorňují, že tato charakteristika přestává platit. Írán přešel na model trvalé strategické přítomnosti v sítích kritické infrastruktury, přičemž cílem není jen okamžité narušení služeb, ale především předpozicování pro budoucí eskalaci. Jinými slovy, íránské skupiny pronikají do systémů a čekají na vhodný geopolitický okamžik.

Analytici identifikují jako primární cíle energetický sektor, vodovodní a kanalizační systémy, dopravu a zdravotnictví – odvětví, která jsou z velké části závislá na průmyslových řídicích systémech (ICS/SCADA) s dlouhou dobou životnosti a obtížnou aktualizovatelností. Právě tyto systémy jsou pro íránské aktéry atraktivní: veřejně přístupné průmyslové řídicí prvky (PLC), slabá síťová segmentace a zastaralý software vytvářejí snadno zneužitelné vstupní body.

Írán a energetická infrastruktura USA

Data z Evropského úložiště kybernetických incidentů (EuRepoC) sledující politicky motivované útoky ukazují, že v období 2010–2024 byl energetický sektor druhým nejčastěji napadeným odvětvím v době geopolitických konfliktů, hned za telekomunikacemi. Z 62 připsaných útoků na energetiku připadá přibližně 39, tedy dvě třetiny, na trojici Čína, Rusko a Írán. Írán se přitom historicky zaměřoval na strategická

odvětví spojená se Spojenými státy a Izraelem: obranný průmysl, finanční služby, vodohospodářství a dopravu.

Americká agentura pro kybernetickou bezpečnost CISA ve svém poradenství z dubna 2026 potvrdila, že íránské APT skupiny aktivně narušují funkci průmyslových řídicích prvků (PLC) v americké kritické infrastruktuře přinejmenším od března 2026. Skupiny spjaté s Íránskou revoluční gardou (IRGC) přitom již dříve napadly nejméně 75 zařízení v sektoru vodohospodářství a komunálních služeb. Část obětí zaznamenala výpadky provozu i finanční ztráty.

Hacktivisté jako prodloužená ruka státu

Íránská kybernetická strategie je pozoruhodná svou vícevrstvostí. Stát provozuje sofistikované APT skupiny (APT33, APT34, APT35) pro cílenou špionáž a sabotáž, zároveň však využívá sítě hacktivistických proxy skupin pro operace s možností popření odpovědnosti a pro masový psychologický efekt. Analýza více než 250 000 zpráv ze 178 hacktivistických skupin na Telegramu odhalila koordinaci těchto skupin s vojenskými operacemi, načasování útoků, výběr cílů i sdílení nástrojů nesou znaky institucionálního řízení, nikoli spontánního aktivismu.

Tento model přináší Íránu asymetrickou výhodu: geograficky rozptýlené proxy skupiny mohou operovat i v situaci, kdy je samotný Írán izolován, ať už sankcemi nebo výpadkem internetu. Zároveň komplikuje atribuci útoků a tím i právní a diplomatické reakce postižených zemí.

Dopady a doporučení

CSIS upozorňuje, že více než 80 % americké energetické infrastruktury vlastní soukromý sektor, což zásadně ovlivňuje způsob řešení hrozeb: bez úzké spolupráce státu a firem nelze rizika účinně zmírňovat. Analytici identifikují jako přetrvávající slabiny nedostatečnou technickou pomoc malým provozovatelům, omezenou sdílení kybernetické intelligence v reálném čase a nízkou viditelnost dodavatelského řetězce softwaru a hardwaru pro řídicí systémy.

Pro provozovatele kritické infrastruktury, ať již v USA, nebo v Evropě, z těchto zjištění plyne několik konkrétních závěrů: nutnost síťové segmentace průmyslových řídicích systémů od zbytku IT infrastruktury, omezení přímé internetové dostupnosti PLC a HMI rozhraní, pravidelná aktualizace firmwaru a zavedení monitoringu anomálního chování v OT sítích.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Závěr

Íránská kybernetická strategie prošla kvalitativní proměnou: od reaktivních útoků jako nástroje politického tlaku k trvalé, strategicky řízené přítomnosti v sítích kritické infrastruktury. Tato změna vyžaduje odpovídající posun v obranném myšlení. Od reaktivního zvládání incidentů k proaktivní kybernetické odolnosti a průběžnému sledování hrozeb. Případ Íránu přitom ilustruje širší trend: kybernetický prostor se stává plnohodnotnou doménou státní moci, v níž se míra geopolitického napětí přímo promítá do intenzity kybernetických operací.

Zdroje

CSIS – Iran Conflict Heightens Cyber Threats to U.S. Energy Infrastructure: https://www.csis.org/analysis/iran-conflict-heightens-cyber-threats-us-energy-infrastructure

CSIS – Beyond Hacktivism: Iran's Coordinated Cyber Threat Landscape: https://www.csis.org/blogs/strategic-technologies-blog/beyond-hacktivism-irans-coordinated-cyber-threat-landscape

CISA – Iranian-Affiliated Cyber Actors Exploit PLCs Across US Critical Infrastructure: https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

CSIS – How Will Cyber Warfare Shape the U.S.-Israel Conflict with Iran?: https://www.csis.org/analysis/how-will-cyber-warfare-shape-us-israel-conflict-iran

EuRepoC – European Repository of Cyber Incidents: https://eurepoc.eu

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Důležitost interní a externí komunikace mezi složkami integrovaného záchranného systému

Barbora Jurenová, studentka vysoké školy AMBIS

Integrovaným záchranným systémem (IZS) se dle § 2 písmena a) zákona č. 239/2000 Sb., o IZS a o změně některých zákonů, ve znění pozdějších předpisů, rozumí koordinovaný postup jeho složek při přípravě na mimořádné události a při provádění záchranných a likvidačních prací. Jak z daného paragrafu vyplývá, samotný IZS se skládá ze čtyř základních složek, tedy z Hasičského záchranného sboru České republiky (HZS ČR), jednotky požární ochrany zařazené do plošného pokrytí kraje, Zdravotnické záchranné služby ČR (ZZS ČR) a Policie ČR. Dále jsou součástí i ostatní složky dle § 4 odst. 2 zákona č. 239/2000 Sb. Aby celkový systém mohl efektivně zajišťovat nepřetržitou pohotovost a poskytovat záchranné a likvidační práce, je potřeba, aby byly vždy k dispozici kvalitní komunikační procesy, systémy a střediska.

Za celkové fungování, výstavbu a provoz komunikačních sítí a služeb IZS je zodpovědné Ministerstvo vnitra. Zároveň koordinuje i tísňovou komunikaci pro občany skrze jednotné evropské tísňové číslo 112, na národní úrovni dále prostřednictvím čísel 150, 155 a 158. Společně s jinými ústředními správními úřady vytváří podmínky pro nouzovou komunikaci.

V důsledku množství aktérů zmíněných výše je nutné v kontextu IZS rozlišovat mezi **interní komunikací** probíhající uvnitř systému a **externí komunikací**, zaměřenou na styk s veřejností, médii a dalšími vnějšími subjekty krizového řízení. Oba typy komunikace jsou zásadní pro minimalizaci dopadů mimořádných událostí a krizových stavů na společnost.

INTERNÍ KOMUNIKACE V IZS

Vnitřní komunikace zahrnuje výměnu informací a pokynů mezi základními a ostatními složkami (např. Armáda ČR, Báňská záchranná služba, obecní policie, havarijní služby). Plní primární funkci zajištění **interoperability a společné součinnosti** všech zainteresovaných složek na místě zásahu pod vedením velitele. Jedná se tedy o základ dané **taktické účinnosti a bezpečnosti zasahujících příslušníků IZS** zajišťující jednotné velení a rychlé sdílení životně důležitých informací. Neustálé cvičení, rozvoj společných komunikačních protokolů a digitálních platforem je esenciální pro udržení vysoké úrovně interoperability.

TECHNOLOGICKÁ A LEGISLATIVNÍ PLATFORMA

Zásadním nástrojem pro interní komunikaci je **radiokomunikační neveřejná síť IZS PEGAS** disponující funkcemi pro PČR, HZS, ZZS, státní správu a mimo jiné je i plně odolná proti odposlouchávání. Vlastníkem je samotné Ministerstvo vnitra ČR.

PEGAS společně s navazujícími informačními systémy, jako je **Národní informační systém IZS,** umožňuje efektivní výměnu, sdílení dat a informací na úrovni operačních a informačních středisek OPIS (na krajské úrovni KOPIS) HZS, ZZS a PČR. Dále zajišťuje možnosti lepší koordinace, redukci následků mimořádných událostí v případě společných akcí více složek IZS díky rychlejším provázanějším zásahům. Navíc umožňuje přesnější určení místa zásahu, okamžité zahájení činnosti potřebných složek a rychlejší přepravu na místo (HZS ČR, 2016).

ROLE VELITELE ZÁSAHU A KOORDINAČNÍ MECHANISMY

Úspěšné zvládnutí jakéhokoliv zásahu je přímo závislé na **vertikální a horizontální komunikaci** v rámci řídící struktury. **Velitel zásahu** je ústřední řídící autoritou, jejíž efektivita je podmíněna přesným včasným tokem informací a znalostí taktických postupů.

Vertikální komunikací pro účely tohoto článku rozumíme komunikaci z vyšší organizační úrovně na úroveň nižší. Tedy předávání rozkazů, přidělování úkolů, provádění standardizovaných operačních postupů z OPIS na velitele zásahu a zasahující jednotky.

Horizontální komunikace naopak značí tok informací mezi sice funkčně odlišnými útvary, které se ale nacházejí na hierarchicky stejné úrovni. Zde se jedná o dialog mezi zástupci složek IZS na místě zásahu (např. styčný důstojník Policie a vedoucí ZZS), minimalizuje dobu trvání činnosti a podporuje týmovou práci při záchraně osob, třídění zraněných a následné likvidaci následků.

EXTERNÍ KOMUNIKACE V IZS

Vnější komunikaci v IZS lze definovat jako informační tok s externím prostředím zahrnující **veřejnost, média, orgány státní správy a samosprávy** a subjekty ovlivněné krizovou událostí, jak právnické, tak fyzické osoby. V krizovém řízení se jedná o nástroj pro snižování paniky, minimalizaci sekundárních škod, udržení důvěry mezi obyvateli a složkami IZS. Lze tedy říci, že se jedná o zásadní faktor **strategického zvládání krize** na úrovni celé společnosti. S vývojem technologií je nutná implementace pokročilých nástrojů, např. **Cell Broadcast** (geograficky hromadné rozesílání zpráv na mobilní telefony stěžejní pro varování a vyrozumění obyvatelstva při mimořádných událostech a krizových situacích), důsledné dodržování profesionální, proaktivní a etické komunikační strategie ze strany tiskových mluvčích IZS.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

KRIZOVÁ KOMUNIKACE

Dle krizového zákona se krizovou komunikací rozumí přenos informací mezi státními orgány, územními samosprávnými orgány a mezi složkami integrovaného záchranného systému za využití prostředků hlasového a datového přenosu informací veřejné telekomunikační sítě i vybrané části neveřejných telekomunikačních sítí. Jejímž cílem je informovat o nastalé situaci, ale také ovlivnit chování obyvatel a snížit psychologické dopady. Využívá k těmto činnostem jednotný systém varování a vyrozumění, jež rychle informuje občany např. pomocí systému sirén, Cell Broadcastu, navíc i poskytuje pokyny k ochraně obyvatelstva. Věcně, přesně a včasně sděluje informace veřejnosti a médiím, aby se zabránilo šíření paniky.

PSYCHOLOGICKÝ A SOCIÁLNÍ DOPAD

Úspěšná komunikace transformuje strach v akci, nejistotu v důvěru a chaos v koordinaci. Klade vysoké nároky na profesionalitu, etiku a morálku krizových mluvčích. Nezastupitelnou **roli zde má krizový intervent** komunikující specificky s osobami zasaženými mimořádnou událostí a poskytuje psychologickou první pomoc, vytváří důvěru a jistotu potřebnou pro další kooperaci v záchranných pracích.

Nutné jsou také jasné pokyny složek IZS ke koordinaci kolektivních akcí (např. evakuace), zároveň i řízení mediálního zájmu, jež se může stát dvojsečnou zbraní, buď může eskalovat krizi, nabourat soukromí poškozených osob, tvořit nepravdivé informace, anebo proaktivně sdílet ověřené informace pomáhající komunitám se vrátit k běžnému životu před událostí.

KOMUNIKAČNÍ BARIÉRY A RIZIKA

Faktory narušující efektivní komunikaci a přenos dat se mohou projevovat jak na úrovni interního, tak externí sdělení poškozující efektivitu, koordinaci, rychlost i bezpečnost nejen zasahujících složek, ale i samotné veřejnosti. Vše může vést až ke dlouhodobému poškození dobrého jména, důvěry a jistoty v IZS, tak i v stát sám.

INTERNÍ BARIÉRY

Vnitřními překážkami rozumíme, i přes snaha o sjednocení integrovaného záchranného systému, stále existující rozdíly zneschopňující snadnou součinnost HZS, PČR, ZZS a JPO, popř. se vyskytují i na úrovni OPIS, velitele zásahu a zasahujících jednotek.

Odchylky je možné vnímat jako rozdíly v odborné terminologii, nadále přítomné riziko výpadku energie v důsledku přetížení sítě. Ve členitém terénu pořád dochází ke ztrátě signálu vedoucí k nemožnosti zavolat na jakékoliv tísňové číslo. V důsledku časové tísně a psychického tlaku se objevuje zvýšený výskyt stresu, únavy, snížení kognitivních schopností přispívající až k chybnému pochopení instrukcí, komunikačnímu chaosu či syndromu tunelového vidění.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

EXTERNÍ BARIÉRY

Vnějšími komplikacemi nejčastěji dochází prostřednictvím narušení důvěry, způsobení sekundárních dopadů krize na obyvatelstvo. Nepostradatelným se zde stává mluvčí dané složky IZS, který v raných fázích zabraňuje potenciálnímu výskytu nekonzistentních rozporuplných sdělení a informačnímu šumu, zejména díky oznamování ověřených znalostí a informací z oficiálních zdrojů. Lze do této kategorie také zařadit jazykovou či kulturní bariéru, neboť v oblastech s vyšším výskytem cizinců nemusí být varování účinné (např. v turistických centrech, bydlištích s větší koncentrací cizojazyčných osob).

Zdroje

HZS ČR, 2016. Informační servis. *HZS ČR* [online]. [cit. 2025-10-20]. Dostupné z: https://hzscr.gov.cz/clanek/narodni-informacni-system-integrovaneho-zachranneho-systemu-byl-prezentovan-jako-uspesny-projekt-integrovaneho-operacniho-programu.aspx

MINISTERSTVO VNITRA ČR, leden 2014. Legislativa. *Ministerstvo vnitra ČR* [online]. [cit. 2025-10-20]. Dostupné z: https://mv.gov.cz/clanek/legislativni-ramec-site-pegas.aspx

MV GŘ HZS ČR, 2010. *Integrovaný záchranný systém a požární ochrana: Modul I* [online]. Praha: MV -GŘ HZS ČR [cit. 2025-10-20]. ISBN 978-80-86640-59-4. Dostupné z: https://hzscr.gov.cz/clanek/dokumenty-ke-stazeni.aspx

Vyhláška Ministerstva vnitra č. 328/2001 Sb.**:** o některých podrobnostech zabezpečení integrovaného záchranného systému. In: *Zákony pro lidi* [online]. AION CS, 2010–2025 [cit. 2025-10-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2001-328

Zákon č. 239/2000 Sb.: o integrovaném záchranném systému a o změně některých zákonů. In: *Zákony pro lidi* [online]. AION CS, 2010–2025 [cit. 2025-10-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-239/zneni-20250819

Zákon č. 240/2000 Sb.: o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Zákony pro lidi* [online]. AION CS, 2010–2025 [cit. 2025-10-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240?text=240%2F2000

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Sociálně-právní aspekty sextingu u českých dětí

Anna Budská, studentka vysoké školy Ambis

Sexting, v moderním pojetí definovaný jako zasílání, přijímání či další šíření vlastních fotografií nebo videí s intimním či sexuálně laděným obsahem (tzv. nudes), představuje jednu z nejvýznamnějších výzev současné kybernetické bezpečnosti dětí a dospívajících. Jak vyplývá z rozsáhlé studie Sexting u českých dětí 2020, realizované odborníky z Univerzity Palackého v Olomouci, nejde pouze o technologický fenomén, ale o komplexní sociální jev hluboce zakořeněný ve vztahových a vývojových procesech dospívání (Szotkowski, Kopecký & Dobešová, 2020).

Dospívající jedinci často vnímají pořízení a odeslání intimního materiálu jako přirozený projev důvěry v partnerském či potenciálně partnerském vztahu. Motivací může být také snaha získat pozornost, potvrzení vlastní atraktivity nebo udržení vztahu. V tomto kontextu sexting nebývá dětmi a mladistvými reflektován jako rizikové chování, ale spíše jako běžná součást digitální komunikace. Zásadním problémem však zůstává skutečnost, že v okamžiku odeslání digitálního obsahu jeho původce definitivně ztrácí kontrolu nad jeho dalším šířením. Virtuální prostředí totiž neumožňuje absolutní odstranění jednou sdíleného materiálu, což vytváří značný prostor pro zneužití důvěry a sekundární viktimizaci oběti (Szotkowski, Kopecký & Dobešová, 2020).

V praxi se často setkáváme s opakujícím se scénářem, kdy dívka v dobré víře zašle intimní fotografii chlapci, který ji následně – mnohdy bez původního úmyslu ublížit – přepošle dalším osobám ve svém vrstevnickém kolektivu. Motivací bývá snaha „pochlubit se“ atraktivní partnerkou, získat uznání či posílit vlastní sociální status ve skupině. Důsledky tohoto jednání jsou však pro oběť zpravidla devastující. Lavinovité šíření prostřednictvím sociálních sítí a soukromých skupin v komunikačních aplikacích, jako jsou WhatsApp či Messenger, může vést k tomu, že se k citlivému obsahu během velmi krátké doby dostane značná část školního kolektivu. Oběť se následně ocitá v sociální izolaci a čelí zesměšňování, ponižování a veřejným komentářům zaměřeným na její vzhled, tělo či sexualitu. Tato forma kyberšikany má prokazatelně negativní dopady na psychické zdraví, sebevědomí i školní fungování dítěte (Linka bezpečí, 2025).

Situace se výrazně vyhrocuje v okamžiku, kdy do procesu vstoupí úmyslné vydírání a manipulace. Pachatel, který získal přístup k intimním materiálům, začíná oběť systematicky zastrašovat požadavky na zaslání dalších fotografií či videí, případně na plnění jiných úkolů, a to pod hrozbou zveřejnění již existujícího obsahu rodině, pedagogům nebo jeho umístěním na veřejně přístupné weby. Tento typ tzv. sextortion

představuje pro nezletilé osoby extrémní psychickou zátěž a je často spojen s rozvojem úzkostných stavů, poruch spánku a výrazného stresu (Sexting.cz, 2024).

Z právního hlediska je nezbytné zdůraznit, že pokud je na intimním materiálu zachycena osoba mladší 18 let, je jakékoliv jeho další šíření klasifikováno jako šíření dětské pornografie. Trestní odpovědnost se přitom nevztahuje pouze na původního šiřitele, ale i na osoby, které materiál dále přeposílají, byť „jen ze zvědavosti“. Právní systém v tomto kontextu nerozlišuje mezi úmyslem „pochlubit se“ a záměrným poškozením oběti – klíčovým kritériem je samotná distribuce závadného obsahu a zásah do práva na soukromí a lidskou důstojnost dítěte (Sexting.cz, 2024).

Pokud dojde k úniku intimních materiálů nebo k vydírání, odborná metodika doporučuje jasně strukturovaný postup. Prvním krokem je uvědomění si, že oběť nenese vinu za zneužití důvěry; odpovědnost leží vždy na straně osoby, která obsah šíří nebo zneužívá. Zásadní je okamžité ukončení komunikace s pachatelem a systematické uchovávání důkazního materiálu. Snímky obrazovky zachycující komunikaci, výhrůžky či samotné sdílení obsahu jsou klíčové pro případné šetření Policií České republiky. Současně se doporučuje nahlásit závadný obsah provozovatelům daných platforem a v rámci možností požádat příjemce materiálu o jeho odstranění s jasným sdělením, že k šíření dochází bez souhlasu oběti (Linka bezpečí, 2025).

Nedílnou součástí krizové intervence je vyhledání podpory u důvěryhodné dospělé osoby, ideálně rodiče. Ačkoliv je tento krok pro dospívající často nejobtížnější, významně zvyšuje šanci na efektivní řešení situace. Pokud dítě nemá možnost nebo odvahu obrátit se na rodinu, jsou k dispozici anonymní poradenské služby, jako je Linka bezpečí nebo odborné online poradny projektu E-Bezpečí. Paralelně s psychologickou a právní pomocí je nezbytné přijmout technická bezpečnostní opatření, zejména změnu přístupových hesel, aktivaci dvoufaktorového ověřování a blokaci útočníka na všech komunikačních kanálech. Odborníci rovněž důrazně varují před osobními schůzkami s osobami z online prostředí, zejména pokud dochází k výhrůžkám či nátlaku (Sexting.cz, 2024).

Závěrem lze konstatovat, že efektivní prevence sextingu a jeho negativních dopadů musí být postavena na systematickém rozvoji digitální gramotnosti, právního povědomí a respektu k vlastní i cizí intimitě. Základní preventivní sdělení zůstává jednoduché, avšak zásadní: neposílej intimní materiály nikomu, ani osobě, které v daném okamžiku důvěřuješ. Digitální prostředí je ze své podstaty nestabilní a rizika spojená s budoucím zneužitím obsahu – ať už v důsledku rozpadu vztahu, tlaku vrstevníků nebo kybernetického útoku – jsou příliš vysoká. Sdílení intimity by proto mělo zůstat v offline prostoru, kde je ochrana soukromí lépe kontrolovatelná. Pouze kombinace preventivní osvěty, dostupné odborné pomoci a jasného právního rámce může dlouhodobě přispět ke snížení počtu dětí a dospívajících, kteří se v důsledku

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

sextingu ocitají v závažných životních situacích (Szotkowski, Kopecký & Dobešová, 2020).

Seznam použité literatury pro téma Sexting:

LINKA BEZPEČÍ. (2025). Online poradna: Nudes a sexting. [online]. [cit. 2025-12-31]. Dostupné z: https://www.linkabezpeci.cz/poradna/online

SEXTING.CZ. (2024). Průvodce riziky digitální intimity. [online]. [cit. 2025-12-31]. Dostupné z: https://www.sexting.cz/

SZOTKOWSKI, R., KOPECKÝ, K., & DOBEŠOVÁ, P. (2020). Sexting u českých dětí 2020. Olomouc: Univerzita Palackého, projekt E-Bezpečí. [online]. [cit. 2025-12-31]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/odborne-studie/144-sexting-u-ceskych-deti-2020-szotkowski-kopecky-dobesova/file

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Postpenitenciární péče

Filip Janda, student vysoké školy Ambis

Období, kdy se jedinec vrací z výkonu trestu odnětí svobody je velmi náročné. Postpenitenciární péče je termín, pod kterým je potřeba si představit jedince, o kterého je sociálně pečováno po výkonu trestu odnětí svobody, po tom, co prošel ochranným léčením nebo ochrannou výchovou. Tato péče spadá pod sekundární a terciární prevenci. (Raszková, Hoferková, 2014)

- **Sekundární prevence** – Prevence, která působí na osoby, u nichž se dá předpokládat riziko páchání trestných činů.
- **Terciární prevence** – Jedná se o snahu resocializovat osoby, které už problém mají na základě aktivit, které souvisejí se vzděláním, odbornou kvalifikací, zaměstnáním a zajištěním bydlení. (Zoubková a kol., 2011)

Tuto péči není jednoduché definovat. V užším smyslu je péče prováděna po propuštění z výkonu trestu odnětí svobody. Funguje na principu péče a pomoci. Je nutné zmínit, že je dobrovolná. V širším ohledu je dobrovolná, ale má formu povinného dohledu. Zaměřuje se na osoby, u nichž se očekává, že budou mít problém s adaptací. V nejširším pojetí je taková péče poskytována všem osobám, kterým skončil trest a tito jedinci o to mají zájem. Součástí je také raná pomoc, která je pachateli k dispozici již v přípravném trestním řízení. Základním cílem této péče je reintegrace člověka. Reintegraci lze dosáhnout pomocí a podporou s nalezením bydlení, zaměstnání a v neposlední řadě také upevněním vztahů s blízkými osobami. (Černíková, 2008)

Pokud se jedná o parametry úspěšné integrace, které vedou ke znovu začlenění, tak nejlépe to jde u osob, které:

- Jsou prvotrestaní
- Jsou mladí
- Jsou navyklí pracovat
- Mají dobré vztahy s rodinou
- Nejsou dlouho ve výkonu trestu odnětí svobody (Raszková, Hoferková, 2014)

Pokud mluvíme o postpenitenciární péči, tak jí lze rozdělit na **dobrovolnou** a **nedobrovolnou**. Pro dobrovolnou postpenitenciární péči je charakteristické, že se jedinec sám rozhodne tuto péči podstoupit. Kdykoliv může tuto péči ukončit a následně zase obnovit. S touto formou pomáhají například neziskové organizace, nebo kurátoři. Nedobrovolná péče je uskutečňována na základě zákona, kdy tato osoba je částečně omezována. Takovou formou postpenitenciární péče je parole. Parole je podmíněné

propuštění, kdy se jedinec vrací do společnosti dříve, než mu uplyne celý trest, ale pod dohledem a za jasně daných pravidel. (Raszková, Hoferková, 2014)

Sociální pracovník vězeňské služby

Sociální pracovník Vězeňské služby zajišťuje sociální a sociálně-právní pomoc a poradenství osobám, které jsou ve výkonu trestu odnětí svobody. Podstatou je snaha řádného života po propuštění, obnovení vztahů s nejbližšími a rozvoj jedince. Tento pracovník vypracovává sociální diagnostiku jedince již na nástupním oddělení, podle kterého je osobě ve výkonu trestu odnětí svobody vypracován program zacházení. Na výstupním oddělení se vyhodnocuje účinnost a rozhoduje se o dalších krocích pro dobré začlenění do běžného života. Poradenství může být skupinové, nebo individuální. Sociální pracovník také zajišťuje sociálně terapeutickou činnost a pomáhá při zařizování individuálních záležitostí. (Adamusová, 2022)

Podle Matouška můžeme rozdělit sociální pracovníky do čtyř kategorií. První z kategorií je **angažovaný sociální pracovník**. Je to člověk, který působí velmi přátelsky a je vůči vězňům velmi slušný. Takový jedinec vnímá sám sebe jako člověka a až poté jako sociálního pracovníka. **Radikální sociální pracovník** se vyjímá především ve faktu, že vkládá stejné úsilí jako angažovaný pracovník, ovšem nikoliv kvůli jedincům, ale především kvůli snaze změnit zákony, které jsou podle něj nespravedlivé. Třetím sociálním pracovníkem je **pracovník byrokratický**, který manipuluje s lidmi v zájmu jejich změny. U tohoto jedince jde o oddělení profesních a osobních hodnot. Poslední z pracovníků je **pracovník profesionální**, který má vystudovaný obor a jeho zájmem jsou práva a potřeby jedinců. Jedince ve věznici vnímá jako „kolegy“ a snaží se, aby se každý jedinec podílel na rozhodování určitých věcí, které se ho týkají.

Sociální práci rozdělil Matoušek do čtyř metod. První metodou je **případová studie**, kde je snaha podporovat jedince, aby se vyrovnal s problémy. Další metodou je **skupinová práce**, kde jde především o práci se skupinou. Jedná se například o víkendové programy, kurzy apod. Třetí metodou je **práce s rodinou**, která je zaměřena na rodinu jednotlivce, nebo skupinu rodin. Tato pomoc je nejčastěji podávána ve formě poradenství. Poslední z metod je **komunitní práce**, která spočívá v organizaci akcí místního společenství, jejichž cílem je naplnění místní potřeby nebo řešení místního problému. (Matoušek, 2013)

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Probační a mediační služba: druhá šance pro pachatele i větší jistota pro společnost

Zuzana Valtrová, studentka vysoké školy Ambis

Probační a mediační služba (PMS) je na první pohled nenápadná instituce. Na rozdíl od věznic není „vidět“, nemá mříže ani ostnaté dráty. Přesto zásadně ovlivňuje, jak vypadá spravedlnost v praxi – a jak bezpečně se ve společnosti cítíme. Stojí totiž mezi soudní síní a návratem člověka z trestu zpět do běžného života.

Co PMS dělá a proč je důležitá

PMS pomáhá řešit případy, kde už došlo k trestnému činu, ale ne všechno musí skončit jen zamčením člověka za mříže. Zajišťuje výkon alternativních trestů, jako jsou obecně prospěšné práce, domácí vězení, trest zákazu vstupu na sportovní či kulturní akce nebo dohled probačního úředníka. Současně klade důraz na ochranu společnosti a zájmy obětí – aby nezůstaly v celém procesu „neviditelné“.

Její práce stojí na dvou pilířích:

- **probaci**, tedy dohledu a podpoře pachatele při plnění uložených povinností,
- **mediaci**, tedy urovnávání konfliktu mezi pachatelem a obětí.

Mediace dává obětem možnost říct, jak trestný čin zasáhl jejich život, požadovat náhradu škody a získat odpovědi na otázky, které by v běžném trestním řízení často nezazněly. Pachatel naopak dostává šanci převzít odpovědnost, omluvit se a aktivně se podílet na nápravě škody.

Probace se více zaměřuje na každodenní život pachatele. Probační úředník s ním vytváří plán – řeší bydlení, práci, dluhy, léčbu závislosti, vztahy s rodinou. Zároveň ale kontroluje, jestli dodržuje podmínky stanovené soudem. Probační dohled tak není „měkká varianta“ trestu, ale náročná cesta, která kombinuje kontrolu a pomoc. Cílem je, aby se člověk po trestu dokázal obejít bez trestné činnosti – a společnost byla bezpečnější.

Z věznice zpět domů: jak probace vypadá v praxi

Během praxe na středisku PMS v Jablonci nad Nisou a ve Věznici Rýnovice jsem měla možnost vidět, jak tato práce vypadá mimo učebnice.

Pracovnice PMS zde pravidelně dochází na besedy s odsouzenými i na individuální pohovory. Na jedné z besed, které jsem se účastnila, vysvětlovala vězňům, co všechno musí splnit, pokud chtějí žádat o podmíněné propuštění. Nejde jen o papírové podmínky, ale i o to, jak přemýšlejí o své trestné činnosti, jak pracují se závislostí, jak řeší dluhy a kde budou po propuštění bydlet. Odsouzení se aktivně ptali – zajímalo je,

jestli má smysl spolupracovat, jak soud nahlíží na doporučení PMS a co všechno se bude prověřovat u rodiny nebo budoucího zaměstnavatele.

Ještě výrazněji se význam PMS ukazuje v individuálních příbězích. Jeden z odsouzených, se kterým probační pracovnice vedla rozhovor, byl ve výkonu trestu kvůli výrobě a distribuci pervitinu. Sám byl závislý, ve vězení začal spolupracovat s odborníky na léčbu závislosti, pravidelně absolvoval testy a připravoval se na návrat domů – do domu své rodiny, kde má zajištěné bydlení i možnost práce. Rodina mu pomáhá zvládat dluhy, má rozjednanou insolvenci a dlouhodobě ho podporuje. PMS u něj ověřuje nejen formální podmínky, ale především to, jestli je změna opravdu reálná a udržitelná.

Jiný příběh byl mnohem těžší. Mladý muž, který vyrůstal v prostředí domácího násilí a dlouhodobého chaosu, se dopustil závažného násilného trestného činu na partnerovi své matky. Ve věznici pracuje, udržuje vztahy se sourozenci a připravuje se na propuštění, přesto je zřejmé, že jeho návrat na svobodu bude velmi náročný. PMS v jeho případě hodnotí nejen to, zda má kam jít a z čeho žít, ale i to, jak pracuje se svou minulostí, jak zvládá emoce a co dělá pro to, aby se situace neopakovala.

V obou případech je probační pracovnice jakýmsi „filtračním“ bodem mezi věznicí a svobodou. Její úkolem není otevírat dveře každému, kdo si podá žádost o podmíněné propuštění, ale zodpovědně zhodnotit, zda má konkrétní člověk šanci obstát na svobodě bez další kriminality.

Ideály vs. realita

Jako příslušnice Vězeňské služby vnímám celou problematiku možná realističtěji – a někdy i skeptičtěji – než bych si přála. Z praxe vím, že mnoho odsouzených dokáže být velmi přesvědčivé, ale motivace bývají často spíše účelové. Spolupráce s PMS je pro ně někdy hlavně prostředkem, jak zvýšit své šance na dřívější propuštění. Ve věznici navíc vznikají nové vztahy a „spojenectví“, která spíše posilují kriminální identitu než podporují změnu.

Na druhou stranu právě tohle ukazuje, proč je role PMS tak důležitá. V systému, kde jsou možnosti individuální práce omezené, představuje PMS jeden z mála nástrojů, který dokáže propojit kontrolu, podporu a dlouhodobou práci s člověkem i po propuštění. Neexistuje žádná záruka stoprocentního úspěchu – ale i když se podaří změnit jen část příběhů, má to velký smysl. Každý člověk, který se po výkonu trestu nevrátí k trestné činnosti, znamená menší počet obětí, stabilnější rodiny a bezpečnější komunitu.

Praxe na PMS pro mě byla důležitou zkušeností. Ukázala mi, jak složitá je realita nápravy odsouzených, jak se ideální představy střetávají s tvrdými životními příběhy a limity systému. Zároveň mi ale potvrdila, že investovat energii do podpory změny – byť nejisté a postupné – má smysl.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Zdroje

ALMANACH PMS, 2021. Praha: Dům tisku s.r.o.

DRÁPAL, Jakub a JIŘIČKA, Michal a RASZKOVÁ, Tereza, 2021. České vězeňství. Praha:

Wolters Kluwer. ISBN 978-80-7676-066-0.

CHMELÍK, Jan, 2014. Trestní řízení. Monografie. Plzeň: Vydavatelství a nakladatelství Aleš

Čeněk. ISBN 978-80-7380-488-6.

ŠTERN, Pavel a OUŘEDNÍČKOVÁ, Lenka a DOUBRAVOVÁ, Dagmar (ed.), 2010. Probace

a mediace: možnosti řešení trestných činů. Praha: Portál. ISBN 978-80-7367-757-2.

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz

Našim aktivitám jsou příznivě nakloněny tyto fyzické a právnické osoby a organizace:

info@aski.cz +420 731086676 Revoluční 981, 666 01 Tišnov www.aski.cz