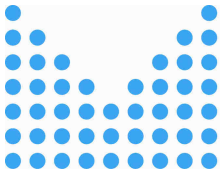


MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ZÁKLADY OCHRANY MĚKKÝCH CÍLŮ

METODIKA

Základy ochrany měkkých cílů - metodika (1. verze)

Zpracoval tým Soft Targets Protection Institute, z.ú. (STPI) pod vedením Ing. Zdeňka Kalvacha.

Praha

Červen 2016

OBSAH

Úvod

Čtenáři se zde předkládá metodika ochrany tzv. **měkkých cílů** (viz níže), zaměřující se nikoliv na běžnou ochranu majetku osob a organizací, ale na ochranu před **závažnými násilnými útoky**, tedy primárně na ochranu **fyzických osob** samotných.

Metodika je proto dobře využitelná pro útoky jak ze strany teroristů, tak násilných extrémistů či osob s čistě kriminální motivací, anebo i osob útočících z čistě osobních důvodů (např. bývalý zaměstnanec) či ze strany osob duševně nemocných. Je v principu aplikovatelná na jakoukoliv organizaci (formální či neformální, tedy např. firma, škola, nevládní organizace, veřejná organizace, ale i rodina) a na jakoukoliv budovu (komerční, veřejnou, soukromou).

Vzhledem k trvalému nedostatku kapacit měkkých cílů zasahovat přímo proti takovým útokům, se metodika primárně zaměřuje na **prevenci těchto útoků a omezování jejich dopadů,** zásah proti útočníkovi je ponechávána většinou na profesionálních státních, obecních, výjimečně soukromých složkách.

Vztah ochrany měkkých cílů a systému ochrany veřejného pořádku a bezpečnosti a systému krizového řízení v ČR

Bezpečnostní opatření měkkých cílů jsou opatřeními přijímanými primárně **dobrovolně** samotnými správci/vlastníky měkkých cílů. Smyslem těchto opatření není jakkoliv nahrazovat, ale synergicky doplnit systém ochrany veřejného pořádku a bezpečnosti nastavených státem prostřednictvím právních předpisů.

Potřeba měkkých cílů vytvářet vlastní postupy pro závažné bezpečnostní incidenty vychází zejména ze dvou skutečností:

1. Některé incidenty svou závažností a rozsahem nesplňují parametry pro přijetí opatření ze strany systému ochrany veřejného pořádku a bezpečnosti, avšak pro samotný měkký cíl představují natolik závažný zásah do rutinního chodu, že je vhodné aplikovat postupy pro závažné bezpečnostní incidenty. Příkladem může být havárie školního autobusu se zraněním dětí nebo zvýšení bezpečnostní hrozby lokálního charakteru.

2. Bezpečnostní (krizové) plány měkkého cíle mají svou zásadní funkci v rámci prevence (zejména zvýšení bezpečnostního povědomí a přípravy personálu) a při vzniku bezpečnostního incidentu do převzetí kontroly nad situací složkami Integrovaného záchranného systému. Jak prokazují teroristické útoky a další případy aktivních střelců, první minuty a připravenost na ně hraje zásadní roli pro zmírnění dopadu incidentu.

Zodpovědnost za bezpečnost na této mikro úrovni jednotlivých podniků ležela dosud na samotných podnicích. V soukromém sektoru soběstačných a poučenějších organizací, zejména firem, vznikají pro tento účel tzv. Business Continuity Plans

(BCP), které se v rámci ohroženosti činnosti podniku zabývají i postupy při závažných bezpečnostních incidentech.

MĚKKÉ CÍLE A JEJICH OHROŽENOST

Bezpečnostní situace se z pohledu terorismu a extremismu v Evropě zhoršuje a přibývá i terorismu podobných, nikoliv ideologicky motivovaných, násilných útoků vedených stejně jako ty teroristické právě na měkké cíle s cílem zranit náhodně přítomné osoby. Byť se České republice doposud teroristické útoky ve smyslu práva vyhýbaly[1], již má neblahé zkušenosti s rasisticky, tedy extrémisticky motivovaným žhářským útokem na dům obývaný romskou rodinou ve Vítkově (2009), ale i s druhou skupinou „neideologických" útoků. Zde je příkladem střelba v restauraci v Uherském Brodě (2015) a útok nožem a braní rukojmí ve škole ve Žďáru nad Sázavou (2014). Kromě těchto uskutečněných útoků bylo v České republice několika obdobným útokům zabráněno, případně byly zastaveny v přípravné fázi.

Tyto útoky přesahují standardní možnosti samotných napadených subjektů se zabezpečit a bránit útokům na úrovni běžné kriminality. Jejich následky současně bývají fatální. Důsledky takových útoků kromě toho často dopadají na širší lokalitu nebo vyžadují koordinaci při nastavování protiopatření. Zároveň je zřejmé, že teroristé mají čím dál tím více tendenci útočit na nechráněná místa s vysokým počtem lidí, a to bez ohledu na to, zda jde o místa politicky či nábožensky symbolická či nikoliv (**tzv. měkké cíle**).

Pro stát je navíc významný fakt, že měkkých cílů je velké množství. To silně limituje praktické možnosti jejich zabezpečení pouze ze strany státu, resp. veřejné správy a zvyšuje význam bezpečnostních opatření přijímaných samotnými měkkými cíli. Řada měkkých cílů navíc dokáže svoji bezpečnost zajistit i lépe (např. má k tomu více prostředků – znalost prostředí, kontakt s ním, přítomnost lidí na místě, ale i finanční prostředky atd.), než stát.

Měkké cíle a jejich členění

Přestože termín „měkké cíle" (soft targets) není nikde přesně definován, v zásadě je toto označení bezpečnostní komunitou používáno pro označení **míst s vysokou koncentrací osob a nízkou úrovní zabezpečení proti násilným útokům**, která jsou pro tuto svou charakteristiku vybírány jako cíl takovýchto útoků, typicky útoků teroristických. Tím se liší měkké cíle od tzv. hard targets, tvrdých cílů, kterými jsou

[1] Jediný pachatel odsouzený v novodobé historii ČR za teroristický útok dle § 311 trestního zákoníku byla osoba, která vyhrožovala tehdejšímu ministrovi financí prostřednictvím dopisu.

dobře chráněné a střežené objekty útoků (např. některé státní objekty, vojenské objekty, objekty dalších bezpečnostních složek, ale i některé dobře chráněné či střežené nestátní či komerční objekty).

Členění objektů na soft targets a hard targets je významné i z hlediska samotného přístupu k problematice zabezpečení. Vychází z optiky útočníků a jejich cíle, je zaměřené na pravděpodobnost útoku, nezkoumá jeho dopad a význam pro společnost. Tento přístup je tedy v mnohém přínosný, neboť se zabývá ochranou subjektů, které by z hlediska tradičního pojetí nebyly zahrnuty – komerční, komunitní, soukromé osoby apod.

Mezi soft targets lze podle tohoto klíče zařadit:

- školská zařízení, koleje, menzy, knihovny,
- církevní památky a místa určená k uctívání,
- nákupní centra, tržiště a obchodní komplexy,
- kina, divadla, koncertní sály, zábavní centra,
- shromáždění, průvody, demonstrace,
- bary, kluby, diskotéky, restaurace a hotely,
- parky a náměstí, turistické památky a zajímavosti, muzea, galerie,
- sportovní haly a stadióny,
- významné dopravní uzly, vlaková a autobusová nádraží, letištní terminály,
- nemocnice, polikliniky a další zdravotnická zařízení.
- veřejná shromáždění, průvody, poutě
- kulturní, sportovní, náboženské a další akce
- komunitní centra

K některým typům měkkých cílů:

Školská zařízení

Vzhledem k přítomnosti dětí a jejich mimořádné zranitelnosti a současně vzhledem k hodnotě, jakou představují děti pro celou společnost, jsou útoky ve školách vnímány jako jedny z nejhorších. Incidenty z minulosti poukazují jak na možné teroristické útoky, tak i na útoky organizované samotnými žáky. Proto je u nich třeba i specifický bezpečnostní přístup.

Obchodní centra

Jde o jeden z typických představitelů měkkých cílů, zejména vzhledem k mimořádně vysoké návštěvnosti obchodních center a jejich nízkému zabezpečení. V minulosti došlo v obchodních centrech k řadě tragických incidentů. Mezi nejznámější patří teroristické útoky s použitím výbušnin, braní rukojmí apod. Např. od roku 1998 do roku 2005 bylo na obchodní centra uskutečněno přes 60 teroristických útoků[2].

[2] Podle studie RAND Corporation: Reducing Terrorism Risk at Shopping Centers, 2006. Počet se týká všech evidovaných útoků celosvětově v letech 1998 až 2005.

Hotely
Sami o sobě koncentrují značné množství osob. V kombinaci s bezpečnostně rizikovou konferencí či jinou akcí hrozba útoku stoupá. Významné bývá pro útočníky i vlastnictví hotelu nebo národnostní skladba hostů.

Sportovní a kulturní akce
Organizace bezpečnostních opatření při větších společenských či sportovních akcí pro veřejnost bývá samozřejmou součástí příprav akce, avšak mnohdy zůstává u základní pořadatelské služby s důrazem na oddělení vyhrazených zón a dodržování organizačních pravidel. Některé akce však vzhledem ke svému charakteru vyžadují důslednější bezpečnostní přípravu. Jde zejména o akce s větším počtem účastníků, akce mediálně atraktivní, pořádané na rizikových místech, v rizikový čas.

Náboženské (v ČR v současnosti zejména židovské) objekty a místa bohoslužeb
Specifickou kategorií měkkých cílů jsou náboženské (v ČR typicky židovské) objekty a místa bohoslužeb, které jsou notoricky cílem islamistického teroru a extrémně pravicových skupin.

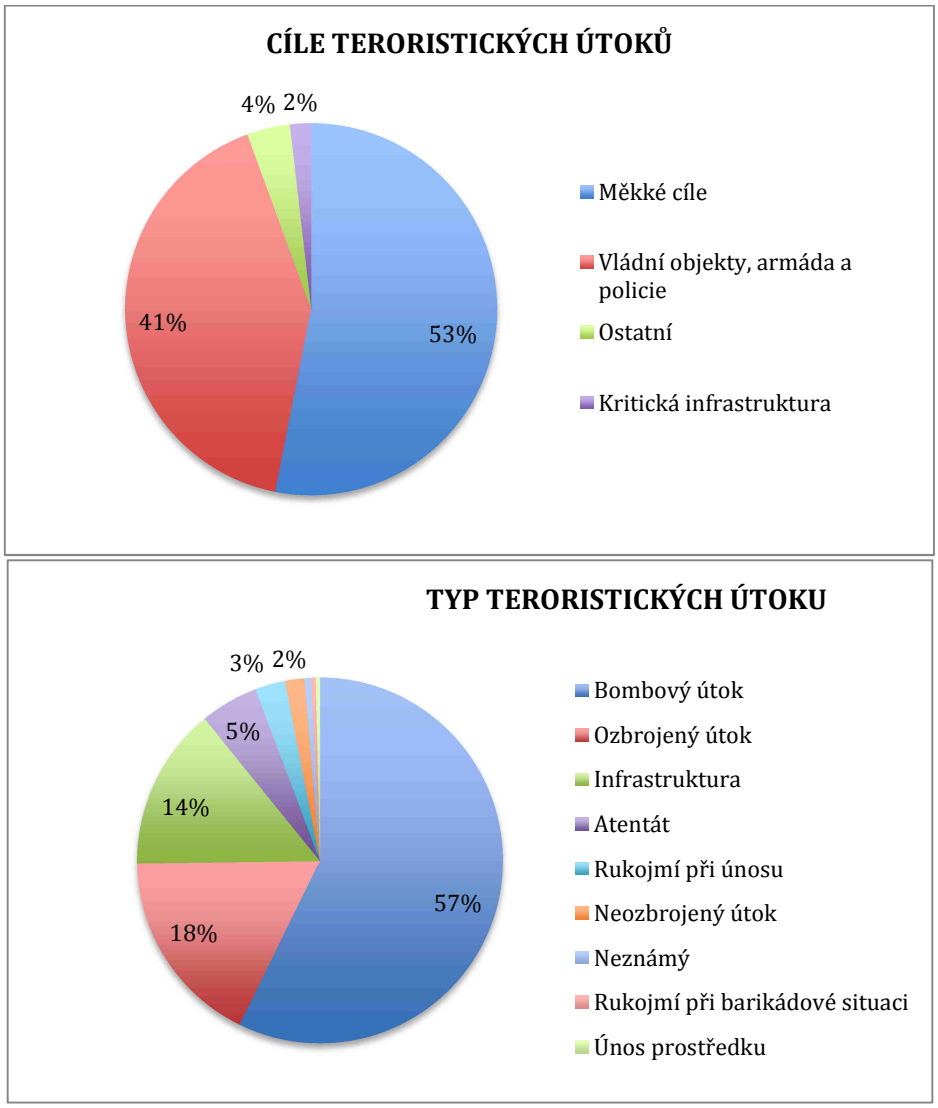
Dopravní prostředky
Útoky na dopravní sítě a prostředky mohou nejen zasáhnout značné množství lidí, ale mohou ochromit i dopravní infrastrukturu. Dopady na společnost jsou tak znásobeny.

Ohrožení měkkých cílů hrozbou terorismu

Měkké cíle čelí široké škále hrozeb různého typu ze strany jednotlivců i skupin s různou motivací. Aby bylo možné vytvořit efektivní metodiku zabezpečení, je nutné s hrozbami pracovat systematicky a bezpečnostní opatření vystavět na základě znalosti postupu útočníků. Pro vytvoření univerzální, přesto však ještě efektivní metodiky zabezpečení měkkých cílů, budeme metodiku stavět na základě protiteroristického přístupu, který je dlouhodobě ověřený a zohledňuje faktory relevantní i pro drtivou většinu ostatních typů útoků na měkké cíle, včetně těch nejzávažnějších. Současný trend teroristických útoků je cílit na veřejná místa se slabým zabezpečením, kde symbolická vazba na specifické náboženství či národnost hraje stále menší roli[3]. Tím se dostala do popředí i otázka zabezpečení měkkých cílů jako bezpečnostní disciplína. Hrozby, které by se vymykaly principům systému funkčnímu pro ochranu před teroristickými útoky, budou upřesněny.

[3] Viz. na příklad studie Europolu k měnícím se trendům modu operandi tzv. Islámského státu: Changes in modus operandi of Islamic State terrorist attacks: Review held by experts from Member States and Europol on 29 November and 1 December 2015. In: Europol [online]. The Hague: Europol Public Information, 2016 [cit. 2016-01-10]. Dostupné z: https://www.europol.europa.eu/content/changes-modus-operandi-islamic-state-terrorist-attacks.

Pro účely tohoto dokumentu byly vyhodnoceny teroristické útoky provedené v letech 1998 – 2014 v Evropě, kterých bylo celkem 5297[4]. Následující grafy ukazují jejích zacílení a způsob provedení:



Z analýz teroristických útoků vyplývají následující prioritní způsoby provedení útoku, které je nezbytné při tvorbě bezpečnostního systému měkkých cílů zaměřeného na teroristické hrozby zohlednit:

1. Útok výbušninou (vyjma za použití vozidla)
2. Sebevražedný útok výbušninou
3. Výbušnina v poštovní zásilce
4. Výbušnina v zaparkovaném vozidle
5. Nájezd vozidla s výbušninou se sebevražedným útočníkem

[4] Statistika vychází z dat Global Terrorism Database Marylandské univerzity. Zahrnuje evidované útoky provedené i nedokončené.

6. Žhářský útok
7. Útok střelnou zbraní (pistole, samopal apod. – aktivní střelec)
8. Braní rukojmí a barikádová situace
9. Napadení chladnou zbraní (nůž)
10. Napadení měkkého cíle davem
11. Útok nájezdem vozidla

Z analýz provedených teroristických útoků na měkké cíle vyplývají i další důležité poznatky, které je při jejich zabezpečování nutné zohlednit:

1. Je nutné počítat s tím, že **přítomným osobám nebude hned jasné, že jde o násilný útok**. Často dochází k záměně střelby se zvukem zábavní pyrotechniky (Charlie Hebdo 2015, Bombaj 2008).

2. Situace při útoku a těsně po něm je typická nedostatkem informací a **vyžaduje reakci bez ohledu na nejasnost situace**. Časová prodleva spojená s delším zjišťováním, co se stalo, vede k fatálním důsledkům. Z toho důvodu je okamžitou reakci nutné modelovat nejen na specifické teroristické útoky (car bomb, střelba, výbuch…), ale na zjevné projevy, které člověk pocítí – zvuk pyrotechniky, zvuk výbuchu, panika davu apod. Tento fakt je zásadní při nácviku reakcí.

3. **Útoky bývají koordinované nebo simultánní**. Dochází k útoku na několik cílů během krátké časové frekvence. Z toho důvodu je nutné podniknout bezpečnostní opatření i v případě útoku na jiný cíl, a to minimálně v rozsahu daného města, kde k útoku došlo.

4. **Teroristické útoky bývají především bombové**. Místní personál je proto vhodné školit na rozpoznání podezřelé předmětu a správném postupu při jeho nalezení.

5. **Útočníci jdou cestou nejmenšího odporu** – tzv. do prvních zavřených dveří. Ty nemusí být zavřené tak, aby nutně splňovaly bezpečnostní třídu, neboť na rozdíl od zlodějů, útočník postupuje dál. Bezpečnostní strategie by tedy měly důsledně řídit touto logikou.

6. **Útočníci mívají změněné vnímání reality**. Bývají nabuzení drogami, prošli silnými sugestivními manipulacemi mysli (tzv. brainwashingem), jsou na své sebevražedné misi, případně jde o psychicky nemocné osoby. To stěžuje předvídatelnost jejich reakcí a možnost komunikace, včetně vyjednávání.

PRINCIPY ZABEZPEČENÍ MĚKKÝCH CÍLŮ

Metoda stanovení vhodného opatření

Měkké cíle jsou rozsáhlá a velmi různorodá skupina subjektů. V kapitolách výše byly uvedeny jejich bezpečnostně relevantní charakteristiky, kterými se odlišují od ostatních cílů a i sami mezi sebou. Dále byly identifikovány charakteristické způsoby provedení teroristických útoků, které představují největší množinu útoků a zastřešují většinu z opatřeních relevantních i pro ostatní typy útků. Díky těmto znalostem je možné přesněji cílit obranné prvky, formulovat principy zabezpečení a doporučit specifická opatření.

Bezpečnostní teorie definuje následující kroky, které je třeba podniknout (resp. otázky, které je třeba si odpovědět ve správném pořadí) pro nastavení funkčního bezpečnostního systému:

Při vytváření bezpečnostního systému měkkého cíle (objektu nebo akce) je třeba začít **ujasněním si chráněných zájmů**. V první fázi je tedy potřebné definovat, čeho si ceníme, o co nechceme přijít, co by nás poškodilo. Základně jde o zdraví a životy lidí, majetek, informace, hodnoty nebo dobré jméno. **Tato metodika se věnuje primárně ochraně před násilnými útoky, tedy zejména ochraně životů a zdraví. Nicméně zde probíraná opatření poslouží dobře též jako opatření proti narušování veřejného pořádku, proti některým útokům na majetek nebo jako prevence nebezpečných situací způsobených technickými haváriemi.**

V druhé fázi jsou definovány **možné zdroje nebezpečí/hrozby** vůči chráněným zájmům. Identifikujeme konkrétní nepřátelské skupiny či kategorie osob s potenciální motivací útočit. K tomu se používá analýza dosavadních obdobných útoků a úvaha nad potenciálními zdroji ohrožení. Vždy je třeba také zohlednit specifika daného objektu / akce, a tedy i specifické hrozby (přítomnost VIP, mediální zájem, riziková data konání, pyrotechnika, odolnost staveb apod.).

Dobře definované zdroje ohrožení a pak podle nich konkretizované **hrozící způsoby útoku** jsou základním stavebním kamenem bezpečnostního systému měkkého cíle. Pokud nejsou připraveny na základě důsledné analýzy zájmů a potenciálních nebezpečí, je výsledný bezpečnostní systém ohrožen neefektivitou a plýtváním zdroji. Tento přístup je charakteristický systematickým analyzováním hrozeb konkrétnímu měkkému cíli, a teprve pak následným nastavováním příslušných opatření. Jde tedy o postup důsledně vycházející z možných hrozeb.

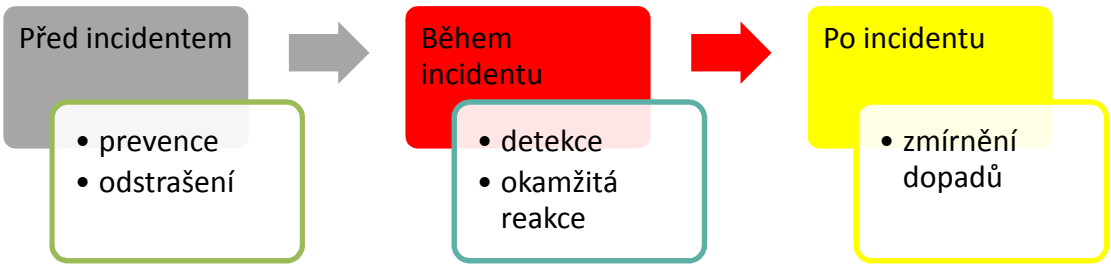
Specifikované hrozby se následně analyzují jednou z **metod analýzy hrozeb a rizik** s cílem **určit prioritní hrozby**, kterým se bude bezpečnostní systém prioritně věnovat a na které se budou prioritně alokovat zdroje. Metod zpracování analýzy hrozeb a rizik je několik. Základní princip spočívá v porovnání pravděpodobnosti realizace hrozby a míře dopadu (následků) u jednotlivých hrozeb. Maticí je pak generován přehled míry ohrožení, díky čemuž je možné efektivněji alokovat zdroje na řešení prioritních hrozby. Postup bude upřesněn níže (viz příloha č. 8).

Na základě ujasnění si prioritních hrozeb a ujasnění si vhodných **bezpečnostních opatření**, jsou tato opatření aplikována na daný objekt. Jsou instalované technické prvky a vypracovány specifické bezpečnostní plány, které se zabývají jak preventivními opatřeními a rutinními postupy, tak reakcí v případech, kdy se krizové situaci nepodařilo zabránit a je nezbytné zabránit jejímu rozvinutí či pokračování a minimalizovat její následky.

Tato metodika **se explicitně zaměřujeme na násilné útoky**, tedy úmyslná jednání fyzických osob, tedy ohrožením života, zdraví, respektive svobody či lidské důstojnosti. Je třeba si nicméně uvědomit, že tyto útoky obvykle vedou zprostředkovaně i ke ztrátám materiálním, resp. finančním.

Časová osa incidentů a bezpečnostních opatření

Se všemi zvažovanými incidenty je nutné pracovat ve všech třech časových fázích. Co lze udělat ještě před výskytem incidentu tak, aby se pravděpodobnost jeho výskytu a rozsah následků snížily, případně se incident odklonil od daného cíle. Co lze udělat v momentu, kdy incident probíhá, a co lze udělat k zmírnění dopadů, když již incident proběhl.



Před incidentem

- Preventivní opatření, která vedou k snížení pravděpodobnosti výskytu útoku, zvýšení rychlosti a intenzity reakce a omezení rozsahu následků a jejich rychlejší zmírnění
- Nástroje odstrašení, které vedou útočníky k rozhodnutí nezvolit daný cíl
- Asertivní komunikace vedoucí ke zklidnění situace a deeskalace konfliktu

Během incidentu

- Co nejrychlejší detekce nežádoucí činnosti či narušení chráněných zón pokud možno ještě dříve, než k útoku dojde
- Okamžitá reakce bezpečnostních pracovníků nebo jiných členů bezpečnostního systému optimálně podle připraveného plánu

Po incidentu

- Postup podle připraveného koordinačního plánu pro management a jím definovaných priorit pro každou z fází po incidentu
- Včasná obnova činnosti organizace

Autoři tohoto dokumentu chtějí zvláště upozornit na dobrou zkušenost s metodou tzv. OORZ (Odstrašit – Odhalit – Reagovat – Zmírnit dopad). Jde o metodický nástroj, který ověřuje účelnost bezpečnostních opatření a řešení hrozeb, jejichž dopad chceme opatřením snížit. S metodou pracujeme tak, že k výčtu možných incidentů, které byly pro daný objekt vyhodnoceny jako relevantní a chceme je minimalizovat, přiřadíme opatření pro odstrašení, včasné odhalení, reakci a snížení dopadu po incidentu. Po vytvoření finální podoby bezpečnostního systému zpětně ověřujeme, zda opatření poskytují řešení u stanovených hrozeb ve fázi před, při i po incidentu.

Teroristické a obdobné extrémní hrozby patří do kategorie hrozeb, se kterými mají měkké cíle možnost pracovat zejména ve fázi před a po útoku. Preventivními opatřeními zaměřenými na včasné odhalení a na zmírnění dopadu.

Okamžitá reakce, která by zastavila útočníka (fyzická obrana), je totiž většinou v silách pouze profesionálních týmů, které umí takticky a technicky správně eliminovat útočníky a současně pracovat s nevinnými osobami okolo. Tyto týmy u

většiny měkkých cílů nejsou k dispozici. Poučený personál měkkého cíle (popř. i ostatní veřejnost přítomná incidentu) však může sehrát ve fázi okamžité reakce důležitou roli. Přivolat pomoc, odklonit kolemjdoucí osoby od místa útoku, oddělit osoby od útočníka uzamčením, varovat ostatní, ale i eliminovat útočníka vlastními silami v rámci nutné obrany. V této souvislosti doporučujeme postup „utíkej – schovej se – braň se“ podle amerického *run-hide-fight*[5].

Bezpečnostní opatření měkkých cílů musí být vzhledem k jejich charakteristice:

- **důsledně účelné** kvůli vysokým rizikům, zejména ztrátám životů
- **kreativní** kvůli mnohdy omezeným prostředkům, kterými měkké cíle disponují,
- **flexibilní** kvůli proměnlivosti prostředí, změnám nepřátelských skupin, jejich taktiky útoků a používaným zbraním.

[5] Instruktážní video je dostupné např. na webu FBI: www.fbi.gov/about-us/office-of-partner-engagement/active-shooter-incidents/run-hide-fight-video

BEZPEČNOSTNÍ PRVKY A JEJICH VYUŽITÍ

Následující kapitola obsahuje přehled různých bezpečnostních opatření roztříděných do základních kategorií bezpečnostního systému:

1. fyzická bezpečnost,
2. elektronické prvky,
3. mechanické prvky.

Detailním členěním těchto prvků a způsoby jejich využití se zabývá řada odborných publikací. Z pohledu zabezpečení měkkých cílů je však zásadní vhodně dané prvky kombinovat. Zejména elektronické prvky vyžadují ujasnění jejich realistického využití a provázanost s obsluhou. Například sebelepší otočná kamera bude mít minimální efekt, pokud nebude ujasněno, kdo ji bude ovládat, co bude na monitorech hledat a jak bude na nežádoucí situace reagovat. Obdobné je to s mechanickými prvky, například když jsou v objektu instalovány bezpečnostní dveře, ale kontrola osob probíhá u těchto dveří, zatímco je otevírají odcházející osoby. U režimových opatření jsou obdobným problémem neaktuální procedury, které pak ostrahu vedou k vytváření vlastních postupů.

Proto tím podstatným při výběru bezpečnostního prvku není jeho kvalita (poslední model, nejmodernější verze apod.), ale jeho účelnost, kompatibilita a vazba na ostatní prvky systému. A dále určení, kdo bude daný prvek řídit, jak v tom bude vyškolen a kontrolován.

Fyzická bezpečnost

Bezpečnostní pracovníci mohou provádět kontrolu vstupu, pochůzkovou činnost nebo obsluhovat velín a bezpečnostních technologie v něm umístěné. Kvalitně vyškolená fyzická ostraha je nejefektivnějším bezpečnostním nástrojem, neboť působí při odstrašení, včasné detekci, okamžité reakci i při mírnění dopadů. Bezpečnostní pracovníci můžou být buď zaměstnanci ohrožené instituce, nebo zaměstnanci soukromé bezpečnostní služby, se kterou má daná instituce kontrakt. Bezpečnostní personál by měl pracovat na základě standardizovaných procedur, které je nutné vypracovat vždy pro daný objekt a pravidelně revidovat. Pro rutinní činnosti bývají detailně rozepsané a obsahují i postupy pro méně běžné situace. Postupy pro bezpečnostní incidenty bývají naopak velice stručné a musí být doplněny o taktické nácviky. Základním nástrojem ostrahy je komunikace. Proto by výcvikový plán ostrahy měl zahrnovat i školení na asertivitu a krizovou komunikaci.

Ostatní personál. Ostatním personálem rozumíme pracovníky organizace, do jejichž pracovní agendy nespadá primárně bezpečnost, avšak jsou zařazeni do organizační struktury a mohou se na bezpečnosti podílet. Takovými pracovníky mohou být například vrátní, školníci, pořadatelé akce, učitelé, pedagogický dozor, uvaděči, dobrovolníci nebo pracovníci úklidu. Zvláštní funkci má management organizace, který je možné vycvičit zejména pro koordinaci potřebných úkonů po bezpečnostním

incidentu.

Elektronické prvky

Kamerový systém používaný k monitorování vnitřních a vnějších prostor a osob a dění v nich. Kamerový systém může být neustále obsluhován bezpečnostním personálem, popř. vrátným, nebo sloužit pouze jako záznamové zařízení pro pozdější použití. Pokud nemůžete instalovat kamery do všech prostor, upřednostněte kamery monitorující vstup.

Důležité je zvážit množství instalovaných kamer vzhledem k počtu obsluhy. Doporučuje se na 17 palcový monitor umístit maximálně 4 kamerové pohledy. Dále je vhodné kamery přepnout do režimu sepnutí v případě pohybu, tak aby rozsvícení monitoru upoutalo pozornost dispečerů. Pohybové kamery je vhodné instalovat jen doplňkově, neboť snaha vidět všechno může vést k tomu, že neuvidíte nakonec nic.

Řada kamerových systémů má užitečné analytické funkce. Vyhodnocení podoby (tzv. face detection), rozpoznání podezřelé aktivity apod. Užití těchto analytických funkcí je však vždy nutné doplnit o způsob jejich kvalifikovaného vyhodnocení obsluhou.

Poplachové zabezpečovací a tísňové systémy (PZTS), dříve nazývané elektronický zabezpečovací systém (EZS) slouží primárně k detekci neautorizovaného, popřípadě násilného narušení perimetru nebo vstupu do objektu. Systémy se dělí na perimetrické, plášťové, prostorové, předmětové a nabízejí širokou škálu možností využití. Například detektory pohybu, otevření dveří a oken, detekce tříštění skla, přelezení plotu atd. Poplachy z těchto čidel je možné svést do ústředny přímo na objektu, poslat pomocí SMS na mobilní telefon nebo odeslat přímo na tzv. dohledové a poplachové přijímací centrum (DPPC).

Dohledové a poplachové přijímací centrum (DPPC) dříve označované jako pult centralizované ochrany (PCO) poskytuje služby centrálního dispečera s možností sběru různých dat ze střežených objektů a jejich dálkový dohled i dálkovou kontrolu.

Vnitřní rozhlas je mimořádně funkčním nástrojem pro komunikaci v případě nebezpečných situací. Vhodným je nastavení dvou poplachových hlášení – pro evakuaci ven (požární evakuaci) a pro povel k uzamčení se v místnostech (lock down).

Rentgen (dále jen RTG) slouží k detekci zbraní, bomb a výbušnin v zavazadlech při vstupní kontrole. Kontrola pomocí RTG se provádí v součinnosti s kontrolou detektorem kovů. Kontrola může být prováděna i namátkově. K efektivnímu využití rentgenu je zapotřebí proškolené a pravidelně kontrolované (testované) obsluhy.

Detektory kovů se standardně objevují ve dvou provedení - ruční a rámové. Slouží ke kontrole vstupujících osob a detekci kovových zbraní a kovových částí bomb. Limitací detektoru kovu jsou pak nekovové zbraně a nekovové části bomb, především pak samotné výbušniny. Kontrola může být prováděna i namátkově. K efektivnímu využití detektoru kovů je zapotřebí proškolené obsluhy.

Detektory výbušnin (tzv. sniffery) patří k novějším a sofistikovanějším přístrojům v oboru bezpečnosti. Jsou náročné na údržbu, ale relativně uživatelsky jednoduché. Oproti služebním psům vycvičeným k vyhledávání výbušnin mají sniffery výhodu větší škály výbušnin, které jsou schopny detekovat. Sniffery mají využití především při vstupní kontrole, např. formou namátkových kontrol zavazadel a při detekci podezřelého předmětu nebo vozidla.

Přístupové a docházkové systémy slouží kromě evidenčních účelů ke ztížení vstupu neautorizované osoby, případně k omezení jejího dalšího pohybu po objektu. Nicméně vstupy a průchody na čipy, karty, případně biometrická detekční zařízení jsou efektivní při boji proti běžné kriminalitě či vandalství, nikoliv však pro situace typu aktivní útočník.

Čtečky dokladů slouží především k ověření pravosti dokladů totožnosti při vstupní kontrole. K efektivnímu využití čtečky dokladů je zapotřebí dobře proškolené obsluhy.

Systémy šíření varování (mobilní aplikace, SMS brány) jsou velmi důležitým prvkem včasného varování osob dané lokality či organizace. Adresná zpráva a možnost komunikace s dispečerem může významně zklidnit napětí, zabránit vstupu osob do nebezpečných zón apod.

Osvětlení (na fotočidla) je podceňovaný prvek zabezpečení. S minimálními náklady slouží jako jeden z nejefektivnějších prvků odstrašení. Zvláště, pokud je světlo sepnuto pohybovým čidlem.

Mechanické prvky

Bezpečnostní dveře v různých certifikovaných třídách slouží ke snížení moznosti násilného vstupu a k celkovému posíleni plášťové ochrany objektu. Bezpečnostní dveře můžou například odolat i výbuchu, střelbě nebo mimořádně násilnému pokusu o vstup. Především v kombinaci s přístupovými a docházkovými systémy jsou efektivním nástrojem pro kontrolu vstupu. Pokud nejsou rámy bezpečnostních dveří zapuštěny do stěn, ztrácejí celé dveře na odolnosti proti výbuchům. Ideální je, když jsou proto bezpečnostní dveře zahrnuty již do projektu stavby, neboť jejich dodatečná instalace, především do historických objektů, je velice komplikovaná.

Bezpečnostní okna, odolná proti střelbě, výbuchu nebo prohození předmětů v různých certifikačních třídách, jsou efektivním prvkem plášťové ochrany objektu. Stejně jako u dveří i u oken platí, že pokud nejsou jejich rámy kvalitně ukotveny do pevných stěn, ztrácejí okna na efektivitě. Alternativním způsobem, jak chránit okno proti různým druhům útoku, včetně výbuchům, jsou těžké závěsy.

Ploty jsou prostředkem pro zamezení vstupu neautorizovaným osobám na pozemek. Především v kombinaci s prvky PZTS a CCTV jde o efektivní nástroj pro zabezpečení perimetru zúžením přístupových cest.

Turnikety jsou užitečné pro uspořádání a autorizaci vstupu a východu. Účelné jsou zejména, pokud je pod kontrolou i zbylá délka perimetru či pláště objektu. Proti násilným útokům je důležité, aby nebylo možné turniket překonat, aniž by byl varován obslužný personál. Turnikety jsou vhodné zejména pro kontrolu při odchodu osob z rozsáhlých areálů, kde je tím eliminována možnost průchodu neautorizované osoby dveřmi otevřenými odcházející osobou (přidržení dveří cizí osobě). Často jsou instalovány v kombinaci se čtečkou pro osobní identifikaci.

Sloupky, betonové bloky a jiné mechanické zábrany jsou používány proti neoprávněnému parkování (režimové opatření) nebo proti nájezdu vozidel s výbušninami (bezpečnostní opatření). Důležitý je jejich materiál, ukotvení a vzájemná vzdálenost, tak aby nedocházelo k jejich objetí, případně je nebylo možné snadno urazit. Sloupky, které jsou instalovány aby zabránily nájezdu vozidel musí odpovídat specifickým parametrům daných kombinací rychlosti a váhy vozidla.

BEZPEČNOSTNÍ DIAGNOSTIKA MĚKKÉHO CÍLE

V úvodu byly měkké cíle roztříděny do skupin podle své funkce – školy, společenské akce, obchodní centra, apod. Pro volbu vhodných bezpečnostních opatření je však účelnější posuzovat každý cíl individuálně, se zohledněním jeho funkce, ale zejména s ujasněním si bezpečnostně relevantních faktorů, které mají vliv **na dvě zásadní kritéria: atraktivitu cíle z pohledu útočníka** a reálné **možnosti jeho zabezpečení**.

Za tyto diagnostické faktory považujeme:

- **Otevřenost pro veřejnost**
- **Bezpečnostní personál**
- **Množství a koncentrace osob**
- **Přítomnost policie**
- **Přítomnost médií**
- **Symboličnost cíle**

1. **Otevřenost pro veřejnost.** Zda jde o venkovní akci, uzavřený objekt, nebo veřejně přístupný objekt. Větší otevřenost atraktivitu cíle zvyšuje. Pro měkký cíl má tato charakteristika vliv na koncept zabezpečení – zda může realizovat opatření na vstupech nebo v otevřeném prostoru. Čím je subjekt otevřenější veřejnosti bez možnosti uzavřít perimetr a autorizovat vstup, tím se atraktivita zvyšuje.

2. **Vlastní bezpečnostní personál.** Možnost využít vlastní personál pro bezpečnostní úkoly možnosti bezpečnostního systému zásadně rozšiřuje. Přítomnost bezpečnostních pracovníků nebo pořadatelské služby atraktivitu cíle snižuje.

3. **Množství a koncentrace osob**. Tato jedna ze dvou definičních charakteristik měkkých cílů má bezpochyby vliv na atraktivitu cíle. Více koncentrovaných osob riziko zvyšuje, přestože trend posledních útoků ukazuje, že pro provedení útoku stačí určitý počet přítomných osob a jejich další navyšování již atraktivitu nenavyšuje v takové míře. Pro měkký cíl je množství a koncentrace osob na určitém místě v určitý čas především faktor ovlivňující zaměření bezpečnostního systému a přípravu bezpečnostních procedur.

4. **Přítomnost policie**. Policie je významným odstrašujícím prvkem a její přítomnost atraktivitu cíle snižuje. Pokud je u objektu trvale přítomná policie, nejde již o měkký objekt. Mnohdy je však policie zastoupena jen krátkodobě, lokálně či k udržování veřejného pořádku bez zásahových dovedností.

5. **Přítomnost médií**. Pro teroristické útočníky a mnohdy i pro jinak motivované násilníky je mediální přítomnost velmi přitažlivá. Zejména, pokud jde o významné akce s televizním přenosem v reálném čase.

6. **Symboličnost.** Pokud je subjekt pro teroristy či jiné násilné skupiny symbolickým cílem, ohroženost subjektu se významně zvyšuje. Typicky se jedná o židovskou, americkou či romskou symboliku. Pro měkký cíl to znamená zohlednit v bezpečnostním plánu způsoby provedení útoků specifických násilných skupin a přizpůsobit svou bezpečnostní strategii i extrémním hrozbám.

Z hlediska schopnosti sebe-ochrany jsou důležité následující faktory:

- **Organizační struktura**
- **Zdroje a prostředky na bezpečnost**
- **Schopnost identifikace vlastních rizikových situací**

7. **Organizační struktura.** Pro útočníka nemusí být tato vlastnost určující, ale pro měkký cíl jde o zásadní charakteristiku, která má vliv na schopnost formulovat a realizovat bezpečnostní politiku, zpracovat realistický bezpečnostní plán a řídit provádění bezpečnostních opatření ohroženého cíle. Typickým příkladem takové více-vlastnické struktury jsou obchodní centra nebo lokality Židovského města v Praze. Více subjektů v jedné ohrožené lokalitě vytváří potřebu koordinace. S tím souvisí i mnohdy nejasná zodpovědnost za bezpečnost daného prostoru a nutnost dobrovolného zapojení pro společný bezpečnostní zájem a sdílení případných nákladů.

8. **Zdroje a prostředky na bezpečnost.** Dalším prvkem, který zásadně ovlivňuje možnosti měkkého cíle přijmout vhodná opatření, je rozpočet na bezpečnost a určení funkce bezpečnostního manažera, tedy osoby v organizační struktuře organizace zodpovědnou za bezpečnostní agendu organizace.

9. **Schopnost identifikace vlastních rizikových situací**. Tento faktor zkoumá, zda je subjekt schopný vyhodnotit, které aktivity a situace jsou rizikové, na co se bezpečnostně zaměřit, co považovat za významné a řešit dle vlastních možností. Většinou jde o to, zda je přítomný bezpečnostní manažer nebo jiný pracovník zodpovědný za bezpečnost a komunikaci s policií.

Každý měkký cíl si může na základě výše uvedených faktorů ujasnit, co patří mezi jeho silné a slabé stránky a co jsou jeho příležitosti či rizika. Pomocí takové SWOT analýzy lze stanovit, na co je vhodné se pro rozvoj vlastní bezpečnosti zaměřit.

DESET PRINCIPIÁLNÍCH DOPORUČENÍ PRO ZODOLNĚNÍ MĚKKÝCH CÍLŮ

1. **Poznejte svá bezpečnostní specifika**. Začněte tím, že si ujasníte, co chcete chránit, jaké činnosti a osoby, se kterými jste ve styku, jsou rizikové. Kdy jste

nejvíce ohroženi během dne, měsíce, roku? Koho je možné využít pro bezpečnostní úkoly? Co již funguje. Specifikujte, na co se chcete zaměřit, jaké jsou vaše silné a slabé stránky.

2. **Bezpečnost řešte metodicky.** Vaším cílem je účelnost. Té dosáhnete, když si nejprve ujasníte, jaké incidenty potřebujete řešit a až pak budete volit opatření, která budete aplikovat. Vaším cílem není nakupovat, ale eliminovat hrozby ve všech třech fázích. Každému bezpečnostnímu opatření, které již máte nebo zvažujete, ujasněte jeho účel – k čemu konkrétně slouží? Kdo bude opatření spravovat? Kdo ho to naučí a bude kontrolovat?

3. **Zapojte místní personál**. Místní pracovníci se mohou významně zapojit do prevence, včasné identifikace ohrožujících situací a zmírnění dopadů bezpečnostních incidentů. I když nemáte bezpečnostní pracovníky, ujasněte si, kde, co potřebujete a úkoly vhodně rozložte mezi stávající pracovníky, dobrovolníky, pořadatele apod.

4. **Zaměřte se primárně na prevenci a zmírnění dopadu.** Vaší rolí není eliminovat útočníky, ale udělat vše pro prevenci útoku, jeho včasné rozpoznání a zmírnění jeho dopadu. Eliminaci útočníka spíše nechte na policii, popř. ozbrojenou ostrahu.

5. **Standardizujte postup.** Připravte si vlastní plán postupů pro bezpečnostně relevantní situace – ověření návštěv, kontrola dokladů, reakce na podezřelou situaci apod. **Připravte se na evakuaci ven i dovnitř**. Ne vždy je vhodné evakuovat se ven, jako při požáru. Pokud má nebezpečí charakter útoku (střelba před objektem, u vstupní recepce, rvačka v objektu, loupežné přepadení apod.), je bezpečnější zůstat uvnitř objektu a uzamknout se do příjezdu policie. Připravte si proceduru „lock down“ (uzamčení se) a máte li možnost, připravte si pro tyto účely uzamykatelnou místnost - úkryt, tzv. „safe haven“.

6. **Připravte si vlastní koordinační plán pro management**. Situace po výskytu bezpečnostního incidentu je mimořádně stresová. Situace vyžaduje řadu rozhodnutí, která je vhodné stanovit dopředu. Zodpovědnosti za jednotlivé oblasti je nutné rozdělit mezi několik osob a jejich postup koordinovat.

7. **Zvyšujte bezpečnostní povědomí** svých pracovníků a přítomných osob. Pravidelně připomínejte pravděpodobné incidenty a proberte postup reakce. Občas postupy procvičujte.

8. **Spolupracujte s místním oddělením Policie ČR a obecní policie**, případně dalšími složkami Integrovaného záchranného systému (zejména hasiči a zdravotnickou záchrannou službou). Nabídněte prohlídku a zhodnocení Vašeho objektu, zapojte je do příprav akcí a vyhodnocení ohroženosti, informujte o mimořádných událostech a konzultujte postupy v případě stavu nebezpečí.

9. **Pokud provádíte autorizaci vstupu a kontrolu osob, zaměřte se na detekci násilného úmyslu, nikoli pouze na nalezení zbraně**. Bezpečnostní rámy, ani rentgeny zbraně nedokáží odhalit bez dobře připravené a často testované obsluhy. Jako zbraň může posloužit mnoho předmětů za kontrolním bodem. Využijte metod detekce podezřelého chování a bezpečnostních pohovorů k tomu, abyste věděli, koho, s jakým záměrem pouštíte a zda osoba nevykazuje podezřelé znaky.

10. **Zabývejte se i prostorem v okolí měkkého cíle.** Při ochraně měkkých cílů jde mnohdy o ochranu lokalit, ne jen jednotlivých objektů nebo organizací. To platí zejména v případě měkkých cílů, které jsou blízko u sebe nebo tvoří jeden celek (např. obchodní pasáž s přilehlým hotelem).

DOPORUČENÝ POSTUP

1. Poznejte svá bezpečnostní specifika

Začněte tím, že si ujasníte vlastní ohroženost a nebezpečí, kterým čelíte. Optimálním nástrojem je jednoduchá tzv. SWOT analýza, pomocí které si ujasněte své silné a slabé stránky a své příležitosti a slabiny. Zásadní faktory, které doporučujeme do analýzy zařadit, jsou uvedeny v kapitole výše.

Velmi důležité je porozumět tomu, jak se vyvíjí v denní rutině míra ohrožení – když by si útočník mohl vybrat (a on si vybrat může), kdy by měl jeho útok na Váš cíl největší efekt? Kdy je pohromadě nejvíc lidí během dne ? Kdy se pořádá atraktivní akce s ještě více lidmi, případně novináři? Kdy je objekt navštěvován nejvíce? Kdy se před objektem pohybuje nejvíc lidí? Apod.

Ujasněte si též, jaké máte finanční a personální zdroje, s kým spolupracujete a kolik času můžete v rámci své organizaci bezpečnosti věnovat.

2. Metodické nastavení bezpečnostního rozvoje

Vzhledem k tomu, že většina měkkých cílů nemá bezpečnostního manažera, považujeme za vhodné, aby alespoň v rámci svého stávajícího týmu zaměstnanců:

1. byl určen jeden pracovník, který bude zodpovídat za bezpečnostní agendu.
2. byla zpracována bezpečnostní analýza měkkého cíle, která bude obsahovat:
    a. identifikaci hrozeb (druh možných incidentů) a jejich specifikace z hlediska místa a času v daném objektu / pro danou akci,
    b. posouzení pravděpodobnosti a dopadu jednotlivých incidentů (analýza hrozeb a rizik – viz příloha),
    c. rozhodnutí, které hrozby budou akceptovány, které delegovány a které řešeny.
3. Na základě bezpečnostní analýzy by pak měla být vybrána vhodná bezpečnostní opatření z kategorie technických a mechanických prostředků, fyzické ostrahy a režimových opatření tak, aby byly nástrojem odstrašení, detekce, reakce anebo zmírnění dopadu pro jednotlivé, analýzou určené, hrozby.
4. Následně by měl být vytvořen plán postupné realizace navržených opatření (plán bezpečnostního rozvoje) s doporučeným výhledem, např. na 2 roky.

3. Zapojení neodborného personálu

Vlastní bezpečnostní službu využívá velmi málo měkkých cílů. Zároveň pouhá přítomnost bezpečnostního personálu nezaručuje plnění potřebných bezpečnostních úkolů. Některá režimová opatření však nevyžadují speciální znalosti či dovednosti a mohou být prováděna jakýmkoli poučeným, byť neodborným personálem.

Všichni zaměstnanci by měli být poučeni v následujících oblastech:

- jaká jsou specifická rizika na daném objektu / akci,
- jak identifikovat podezřelý předmět, vozidlo, osobu či zásilku
- jak se zachovat v případě útoku, nebo jiného závažného incidentu, zejména:

- jak a koho informovat při podezření nebo incidentu,
- jak se rozhodnout, kam je lepší se evakuovat,
- jak rozpoznat podezřelou zásilku,
- jak reagovat na výhružný telefonát.

Např. ve školách je vhodné zapojit pedagogický dozor a školníka do zajištění autorizace vstupu osob. Tyto zaměstnance je třeba poučit o tom, jak postupovat v různých standardních situacích jako např.:

- kdo mě na pozici u vchodu nahradí, když „musím" jít řešit něco jiného v rámci svých povinností,
- jak reagovat na neznámou osobu, která čeká před školou,
- jak reagovat na cizí osobu, která se snaží bez povšimnutí projít se skupinou dětí,
- jak reagovat na osobu, která na dotaz tvrdí, že je návštěva za ředitelem/kolegou učitelem/jiným pracovníkem,
- jak reagovat na rodiče, který se domáhá doprovodit své dítě do šatny / třídy,
- jak reagovat, když mě žáci upozorní na podezřelou osobu / předmět / vozidlo,
- jak reagovat na osobu, která tvrdí, že je oprávněna dítě vyzvednout, ale není na seznamu oprávněných osob, případně personálu není známa.

Výše uvedené platí obdobně i pro ostatní druhy měkkých cílů.

Při pořádání společenských akcích bývají využíváni dobrovolníci, které je velmi vhodné zapojit i do bezpečnostního systému.

Neodborný personál při prevenci

Hlavní předností místního personálu je jejich znalost místního prostředí. Díky tomu mohou lépe, než kdo jiný, detekovat osoby nebo předměty, které se vymykají rutině a mohou být nebezpečné. Právě schopnost detekce podezřelých osob či předmětů bývá slabina jednorázově zapojených bezpečnostních profesionálů, kteří sice mají znalosti postupů, je pro ně ale velkou překážkou porozumět danému prostředí.

Neodborný personál bude díky své přítomnosti na místě incidentu většinou první, kdo může informovat o vznikajícím nebezpečí nebo výskytu bezpečnostního incidentu.

Pro jejich zapojení je nutné personálu tuto roli vysvětlit a instruovat jej v tom, co má hledat a jak na to reagovat (zejména koho informovat). Doporučeným postupem je pravidelné bezpečnostní zaškolení, respektive briefing před akcí.

Neodborný personál při okamžité reakci

Reagovat na bezpečnostní incidenty typu násilný útok je velice obtížné, neboť jde o extrémní, nadlimitní stresovou zátěž, která vyžaduje reagovat bez pokynů, mnohdy proti přirozenému intuitivnímu schématu útěk – zmrznutí – útok.

Přesto je vhodné laickému personálu vštěpovat alespoň první reakci, základní směr, jakým se mají při bezpečnostním incidentu vydat. Pro každý objekt, případně pořádanou akci, je vhodné uvést výčet možných bezpečnostních incidentů a k nim přiřadit jednu z následujících uvedených reakcí:

1. Naslouchej a zmírni konflikt!
2. Varuj ostatní a zabraň přístupu k incidentu
3. Utíkej!
4. Schovej se a zamkni se!
5. Bojuj!

Orientační schéma okamžitých reakcí zaměstnance do příchodu profesionála, vedoucího, policie apod.:

SITUACE	REAKCE
Panika nebo neujasněný incident	**1.** Neřeš, co se přesně stalo, ale JEDNEJ! **2.** Kde je bezpečněji? Venku nebo vevnitř? **3.** Naviguj ostatní přítomné do bezpečného prostoru **4.** Dej o sobě vědět, kontaktuj nadřízeného
Verbální konflikt	**1.** Uklidňuj! Projev zájem situaci řešit **2.** Informuj bezpečnostní personál
Fyzický konflikt nízké intenzity (např. rvačka)	**1.** Informuj ostrahu nebo policii 158 **2.** Snaž se izolovat ostatní, aby nebylo ohroženo více osob **3.** Velmi zvažuj vlastní zapojení s ohledem na poměr sil a své schopnosti na obranu sebe i druhého **4.** Pokud jsi sám ohrožen a nemůžeš utéct ani se schovat, bojuj!
Technická havárie (zborcení nosných konstrukcí apod.)	**1.** Dbej na vlastní bezpečnost, situace se může dále zhoršit **2.** Informuj bezpečnostní personál **3.** Varuj a naviguj ostatní do bezpečného prostoru
Fyzický konflikt ozbrojený	**1.** Utíkej pryč a varuj ostatní! **2.** Pokud nemůžeš utíkat, schovej se, lehni si a zamkni se! **3.** Pokud není jiná možnost, bojuj!
Hrozící výbuch	**1.** Kryj se! Drž se pravidla – zeď je dobrá, sklo špatné. **2.** Varuj ostatní

Je známým rčením u bezpečnostních týmů, že nejtěžší rozhodnutí je rozhodnout se. I zkušené profesionální týmy mají problém spustit krizovou proceduru, která má vážné důsledky. Útoky jsou mimořádně stresové situace a nelze očekávat standardní postup od osob, které neprošli speciální přípravou, která zahrnuje taktické drily ve stresu. Přesto, základní ujasnění postupů upravených tak, aby odpovídaly specifickým potřebám dané akce, může snížit riziko neočekávaných reakcí.

Zapojení neodborného personálu při zmírňování dopadu proběhlého incidentu

Pokud dojde k mimořádné situaci typu útok, budou do okamžité reakce i následných opatření zapojeny s nejvyšší pravděpodobnosti základní složky Integrovaného záchranného systému (IZS). tj. policie, hasiči a rychlá záchranná služba.

Majitel/správce měkkého cíle, případně organizátor akce však bude muset řešit

1) Opatření do příjezdu složek IZS (může být i 15 minut vzhledem k místu akce)
2) Interní komunikaci uvnitř organizace a další úkoly, které složky IZS řešit nebudou.

Do příjezdu složek IZS může přítomný personál pomoci tím, že:

1. Izoluje místo incidentu a zabrání přístupu dalších osob do nebezpečného prostoru.
2. Poskytne laickou první pomoc.
3. Bude navigovat lidi do bezpečí – podle situace uvnitř nebo vně objektu.
4. Pokud se jedná o akci na větším území, kde nemusí být hned zjevné, že někde došlo k bezpečnostnímu incidentu vyžadující mimořádný postup (např. maraton), mohou být pořadatelé využiti k odklonu trasy do předem ujasněných bezpečných prostor a k informování účastníků akce.

Čím více lidé vnímají, že má nějaká autorita situaci pod kontrolou, tím jsou klidnější a klesá riziko paniky. Autoritu lze efektivně posílit např. reflexní vestou, kterou nemusí personál nosit stále u sebe, ale může být pro účely evakuace umístěna na k tomu určených místech (na každém patře budovy, v jednacím sále, úseku trasy apod.).

Po příjezdu složek IZS se situace zpravidla uklidňuje a místní personál může pomoci tím, že bude:

5. navigovat složky IZS díky své místní znalosti
5. pomáhat udržet uzavřený / vyhrazený přístup do postižené oblasti
5. přesměrovávat dotazy médií, účastníků a jejich příbuzných na štáb a tiskového mluvčího
5. pomáhat s evidencí zraněných
5. pomáhat s evidencí a organizací uložení opuštěných osobních věcí, věcí z opuštěných šaten apod.

Pro majitele objektu nebo organizátora akce je též důležité vědět, jaký je po incidentu stav vlastního personálu, zda jsou všichni v pořádku, případně kdo byl kam převezen záchrannou službou. Z toho důvodu je nutné:

1. Mít k dispozici neustále seznam personálu a jejich kontaktů a předem určeného zaměstnance, jehož úkolem bude zjistit jejich stav a ten průběžně aktualizovat.
2. Personál musí být v rámci bezpečnostního školení / briefingu poučen, koho v případě bezpečnostního incidentu kontaktovat, mít uložené kontaktní číslo, případně mít smluvené místo setkání pro případ, že by kontaktování po telefonu nebylo možné.

Školení neodborného personálu

Struktura školení musí být přizpůsobena konkrétní organizaci či akci. Obecně je možné doporučit následující sdělení, která by si měl personál uvědomit:

1. Které bezpečnostní incidenty mohou nastat:
    a. Tyto situace je potřeba vyjmenovat tak, aby si je účastníci uvědomili a dokázali představit.
    b. Je třeba vysvětlit, že ačkoli se organizátor snaží dělat pro bezpečnost maximum, řada situací se může stát i přes tuto snahu a nepředvídaně.
2. Význam role personálu v bezpečnostním systému:
    a. Každý může pomoci, bez ohledu na to, že je laik.
    b. Zdůraznit, že personál bude vnímán jako autorita a ostatní k němu budou mít důvěru i očekávání.
    c. Upozornit na oprávnění a místní znalosti, které personál má a může jimi pomoci.
3. Uvést příklady, kde může personál pomoci při prevenci, okamžité reakci, návazných opatření:
    a. Prevence: regulování vstupu osob, detekce konfliktních situací, technických závad, odložených zavazadel, podezřelých osob, tlačenic apod.
    b. Okamžitá reakce: navigace, informování, uklidňování, útěk, schování se, přivolání pomoci apod.
    c. Návazná opatření: poskytnutí první pomoci, pomoc složkám IZS, navigace ostatních osob do bezpečí, poskytnutí informací managementu
4. Instruovat, koho a jak informovat při bezpečnostním incidentu.
5. Zopakování postupů při nejpravděpodobnějších bezpečnostních incidentech.

4. Opatření pro prevenci a zmírnění dopadů

Závažným útokům je těžké čelit, když již nastanou. Útočníky je však možné odradit a jejich útok odklonit viditelnými bezpečnostními prvky, případně mediálním zvyšováním obrazu o bezpečnosti daného subjektu. Pokud se nepodaří odradit od úmyslu zaútočit , je možné zachytit průvodní jevy přípravy útoků během fáze sběru informací. Nejúčinnějším aktivním způsobem, jak zabránit připravovanému útoku, je včasná identifikace podezřelých osob, předmětů, vozidel nebo zásilek.

V současnosti jsou již i v ČR dostupná školení **metody detekce podezřelého chování**, která se z letištních kontrol přesunula do veřejného prostředí a je úspěšně aplikována.

Metoda detekce podezřelého chování

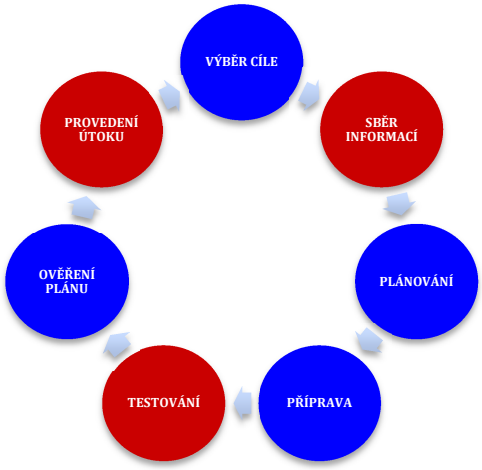
Metoda detekce podezřelého chování je součástí tzv. proaktivních bezpečnostních přístupu. Ten je charakteristický tím, že bezpečnostní systém nečeká na útok, ale snaží se co nejdříve identifikovat podezřelou aktivitu předcházející útoku, tak aby se

útoku buď zabránilo, nebo se útočníkům provedení útoku zkomplikovalo včasnou reakcí bezpečnostního systému.

Cílem detekce je aktivní vyhledávání podezřelých znaků v prostředí, které chráním a pokud je to možné i jeho okolí. Metoda je založena na dobré znalosti místní rutiny a osob, které se v prostředí pohybují - jejich chování, vzezření, dokumentace, komunikace, případně další charakteristiky. Znaky je nutné generovat pro každé prostředí samostatně, neboť každé prostředí má svá specifika. Předně je tedy nutné si ujasnit, co je pro dané prostředí „normální“, a to pomocí tzv. kontextuální analýzy. V případě ochrany před teroristickými útoky se ke kontextuální analýze doplňuje analýza chování útočníků pomocí modelování různých typů incidentů v daném prostředí. Analýza útočníků tedy popisuje, co musí útočník udělat, aby dosáhl svého cíle (např. umístit výbušninu na atraktivní místo, pobodat ředitele cestou z práce, sesbírat potřebné informace, apod.). Pomocí ujasnění normy a chování útočníků je možné identifikovat podezřelé znaky, které se vymykají rutině a odpovídají alespoň fragmentu chování útočníka.

Detekce podezřelého chování je možné aplikovat v různě podobě. Nejjednodušší verze mohou být zpracovány formou úvahy nad typy osob v daném prostředí a jejich charakteristickým chováním a vzezřením. Ve školním prostředí je například možné stanovit tyto typy osob: zaměstnanci školy, žáci, rodiče žáků, dodavatelské servisní firmy, odpolední basketbalisté (soukromý pronájem), apod. Pro obchodní centra to mohou být tyto kategorie: prodejci nájemních jednotek, zaměstnanci centra, úklid a ostraha, bezdomovci, dopolední důchodci a maminky s kočárky polední pracovníci okolních firem, odpolední školáci, večerní návštěvníci kina, apod. Pro tyto typy je dále identifikováno jejich normální chování - kdy chodí a odchází, kudy chodí, zda prostor znají nebo v něm bloudí, jaké toalety používají, zda nosí zavazadla a jaká jsou pro ně typická, kde se autorizuje jejich vstup, zda a jak se identifikují apod. Smyslem je, aby si bezpečnostní personál ujasnil, co je pro dané místo normální a byl schopný identifikovat odchylky. Kvalifikovaný personál je pak schopný identifikovat odchylky od normy a identifikovat ty z nich, které mohou být znakem (symptomem) nežádoucí aktivity. Základně je však možné a v praxi velmi prospěšné proškolit místní laický personál, který se dlouhodobě v prostředí pohybuje a velmi dobře ho zná. Znalost místní rutiny je nejcennější součást této bezpečnostní metody.

Sofistikované bezpečnostní systémy, zejména ty, které jsou ohroženy terorismem, se zabývají tříděním podezřelých osob i podle fáze přípravy útoku. Z analýz provedených útoků vyplývá, že útoku předchází i několikaměsíční aktivita. V rámci tohoto období mimo jiné útočníci sbírají informace o potenciálních cílech s cílem vyhodnotit, který z nich je pro útok nejvhodnější. Sběr informací je stále více prováděn pomocí internetu, ale některé informace je nutné získat pozorováním, případně provokacemi bezpečnostního systému přímo u objektu.



Detekce podezřelého chování v prostředí ohrožených terorismem je tedy zaměřena na včasnou identifikaci sběru informací, testování bezpečnostního systému a přítomnosti útočníků ještě před zahájením útoku. Měkké cíle, pro které není hrozba teroristických útoků relevantní, může svou pozornost věnovat znakům spojených s aktivitou těsně před provedením útoku a přípravě reakce.

Detekce podezřelých znaků je však jen první ze dvou činností, které je potřeba udělat. Pro účinnou ochranu nemůže zůstat jen u odhalení podezřelých znaků, vždy musí následovat i vhodná reakce. Reakce se výrazně liší podle schopností a možností daného bezpečnostního systému a také podle toho, jaké fázi útoku znaky odpovídají. Schematicky lze postup detekce podezřelého chování znázornit takto:

Jiná reakce je vhodná při podezření na sběr informací a jiná při podezření na útočníka se zbraní. Obecně však lze říci, že reakcí na identifikovanou podezřelou osobu je ověření podezřelých znaků, a to většinou komunikací s osobou s cílem podezřelý znak potvrdit nebo vyvrátit. Zde je vhodné zdůraznit, že osob, které se vymykají rutině daného místa může být mnoho. Proto samotná identifikace podezřelého znaku neznamená, že je osoba útočníkem nebo teroristou. Znamená to však, že je vhodné se na osobu zaměřit a znaky ozřejmit.

Pohovory profesionálních bezpečnostních týmů mají přesně danou strukturu. Pokud se podezřelé znaky nepodaří ozřejmit, případně pokud jde o podezřelé znaky útočníka ve fázi těsně před útokem, následuje okamžitá preventivní reakce vedoucí k zmírnění dopadu útoku, který může nastat každým okamžikem. Takovou reakcí

může být uzavření vstupních dveří, pozdržení odchodu osob z chráněného objektu apod.

5. Standardizace bezpečnostních postupů

Je běžné, že vlastníci měkkých cílů nemají zpracované postupy pro standardní bezpečnostní situace a nechávají postup na svém personálu a jeho „selském rozumu“, což mnohdy přinese nepříjemné překvapení při prvním výskytu, byť drobného incidentu.

Velmi doporučujeme ujasnit a sepsat následující procedury písemně (pokud je to pro daný subjekt relevantní):

- režim vstupu osob do objektu, způsob jejich autorizace a kontroly
- režim vjezdu vozidel, způsob jejich autorizace a kontroly
- reakce v případě výhružného / obtěžujícího telefonátu
- reakce v případě nálezu podezřelého předmětu
- reakce v případě verbálního konfliktu/napadení
- reakce v případě agresivního incidentu (napadení či vyhrožování beze zbraně, bez smrtícího úmyslu)
- reakce v případě smrtícího útoku či vyhrožování
- procedura „lock down“ (uzavření se v místnosti)
- vytvoření tematického plánu zaškolení personálu v bezpečnostních postupech
- vytvoření vlastního koordinačního plánu pro management pro zmírnění dopadu po výskytu incidentu

Tyto procedury mohou být s místní znalostí kvalitně připraveny i ne-bezpečnostním personálem. Již samotné jejich zpracování vede k ujasnění řady skutečností, které by nebylo vhodné řešit až při výskytu bezpečnostního incidentu.

Připravte se na evakuaci ven i dovnitř. Ne vždy je vhodné evakuovat podle požárních směrnic, tedy ven z objektu. Pokud je nebezpečí jiného charakteru (střelba před objektem, u vstupní recepce apod.), je často bezpečnější zůstat uvnitř objektu. Připravte si pro tyto situace proceduru „lock down“ a zvažte vzhledem ke svým možnostem i proceduru „safe haven“[6].

[6] Procedura „**safe haven**“ (bezpečný přístav) se využívá především při bombových a raketových hrozbách a tehdy, kdy je možné opustit místnost a běžet do připravené, zpevněné a vybavené místnosti, která je pro úkryt v daném prostředí nejvýhodnější. Nehodí se tedy v případě aktivních střelců, kde by vybíhání do úkrytu přes chodby vystavilo osoby riziku při setkání s útočníky. Příprava safe havenu také vyžaduje další úroveň výcviku a přípravy, což bývá pro řadu subjektů zásadní limit. Pro tyto situace proto spíše doporučujeme mnohem univerzálnější proceduru lock down.

Úkryt „safe haven“ je možné připravit improvizovaně téměř v každém objektu. Měla by to být místnost pokud možno bez oken, se silnými zdmi a uzamykatelnými dveřmi. V místnosti budou čekat lidé na zásahový policejní tým, což může trvat vzhledem k rozsahu objektu a charakteru útoku i několik hodin. Místnost by proto měla být vždy vybavena adekvátním množstvím vody, dekami,

„Lock down“ (zamkni se) je procedura, která se využívá ve školách nebo administrativních budovách. Využívá se tehdy, když není možné utéci z ohroženého prostoru / objektu a je bezpečnější se schovat uvnitř. Typicky je využívána při ozbrojených útocích. Součástí procedury je i způsob varování – rozhlasem, křikem, zprávou do mobilu, na displej telefonu.

Spuštění procedury „**lock down**“:

1. Cílem je dostat se z veřejně dostupných prostor a najít úkryt v nejbližší uzamykatelné místnosti
2. V místnosti se zamknout, případně improvizovaně zablokovat dveře
    a. pokud možno, zakrýt vhled do místnosti, nebýt u okna
    b. schovat se za zeď, pod stůl apod. (tzv. „duck and cover“)
    c. být tiše, ztlumit zvonění telefonu
3. Čekat na pokyny policie nebo pracovníků ostrahy – do té doby nevycházet

6. Koordinační plán pro management

Koordinační plán pro management je dokument, ve kterém jsou definovány prioritní úkoly pro jednotlivé fáze bezpečnostního incidentu a osoby, které jsou za dílčí úkoly zodpovědné. Smyslem je ulehčit ve stresové situaci rozhodování odpovědných osob, vymezit odpovědnosti jednotlivých osob, minimalizovat zmatky a připravit materiály a dokumenty, které jsou během bezpečnostního incidentu zapotřebí.

Také každá akce vyžaduje svůj koordinační plán. Typ hrozeb určuje, na co se musí organizátor připravit, kdo musí být ve štábu a jaké priority bude štáb mít v jaké fázi. Záleží též na profesionalitě organizátorů a jejich dosavadních zkušenostech s takovýmto plánováním. V mnoha případech platí pravidlo „méně je více“ s cílem ujasnit si alespoň několik pravidel, která budou spolehlivě platit, namísto nefunkčních, byť profesionálně připravených sofistikovaných plánů.

Koordinační štáb je složen primárně z vedení organizace, avšak tak, aby byli jeho členové reálně schopni při bezpečnostních incidentech pracovat na úkolech ve štábu a nebyla jejich přítomnost nutná jinde.

Následně by měl být plán systematicky rozčleněn tak, aby byly zodpovězeny otázky:

1. Jaká událost vyžaduje aktivaci bezpečnostního plánu?
2. Kdo je ve koordinačním štábu?
3. Za co je který člen koordinačního štábu konkrétně zodpovědný?
4. Kde bude koordinační štáb pracovat?
5. Kam má který člen štábu jít, jakmile se dozví o bezpečnostním incidentu?

---

lékárnou, hroznovým cukrem, baterkou, případně vysílačkou spojenou s ostrahou objektu. Pokud má místnost okna nebo jiné skleněné vitríny, je vhodné místnost zatemnit a ochránit proti střepům např. těžkými závěsy.

6. Jsou v ohrožení další aktivity? Kdo z managementu se o ně postará?
7. Jak zjistím, kdo byl zraněn, kam byl odvezen?
8. Kdo bude v kontaktu se složkami IZS?
9. Kdo zjistí stav vlastních zaměstnanců?
10. Kdo může komunikovat s médii / klíčovými partnery apod.?
11. Kdo bude reagovat na dotazy rodin, přátel apod.?
12. Ad.

Úkoly managementu při bezpečnostním incidentu je vhodné rozdělit do chronologicky řazených fází. Každá fáze má své prioritní úkoly a každý člen štábu by měl být seznámen s tím, kde by měl být a co zajišťovat. Základní rozdělení fází je uvedeno v tabulce níže:

ČASOVÁ PRIORITIZACE ÚKOLŮ				
	FÁZE 1	**FÁZE 2**	**FÁZE 3**	**FÁZE 4**
ČAS	**0-15min**	**15min – 3hod**	**3 – 6hod**	**Dále**
PRIORITY	1. Reakce v místě incidentu 2. Informování IZS 3. První pomoc	1. Koordinace se složkami IZS na místě 2. Ochrana ostatních aktivit 3. Zahájení řízení podle koordinačního plánu	1. Stabilizace činnosti KŠ (logistika, zázemí) 2. Stav zraněných 3. Aktualizace informací o situaci	1. Co zítra? 2. Obnova týmu KŠ 3. Širší interní komunikace
ÚKOLY	- Izolování incidentu a prevence dalšího šíření - Pomoc zasaženým na místě - Aktivace štábu	- Kooperace s IZS - Zjišťování informací o situaci - Info dovnitř organizace (interní) - Zabezpečení pozdějších a vzdálenějších aktivit	- Pravidelné briefy štábu - Info externí i interní je přesnější a po více kanálech	- Psychologická podpora - Střídání členů KŠ

Postup při přípravě koordinačního plánu pro management

1. **Definování koordinačního štábu a koordinačního centra**

   Prvním krokem při přípravě koordinačního plánu je definování týmu (**koordinačního štábu**), který bude zodpovědný za řízení organizace bezprostředně po výskytu bezpečnostního incidentu. Koordinační štáb je definován na základě stanovení zodpovědností a ujasnění všech důsledků, které bezpečnostní incident může v dané organizaci vyvolat, a ujasnění specifických možností a prostředků organizace. Plán též definuje **koordinační centrum**, místo, kde bude štáb zasedat, jeho pravomoci a procedury k jeho otevření. Dále ujasňuje jeho vybavení, zejména co se týče dokumentů, které budou při bezpečnostním incidentu potřebné. Centrum by mělo být uzavřené a s dostatečným soukromí pro práci, s omezeným přístupem ostatních zaměstnanců a v případě teroristických útoků i mimo zasaženou lokalitu.

2. **Definování fází incidentu a priorit managementu**

Čas je jeden z hlavních faktorů při metodickém zpracování koordinačního plánu. S časem se dramaticky mění situace a potřeby zasažených. Plán ujasňuje managementu tyto priority tak, aby mohl účelně cílit své limitované prostředky a zdroje.

3. **Specifikace úkolů pro jednotlivé členy krizového štábu v jednotlivých fázích**
   Definované prioritní úkoly jsou přiděleny jednotlivým členům koordinačního štábu (komunikace s rodiči, navázání vztahu s nemocnicí, příprava tiskové zprávy apod.). Pro jednotlivé členy tak plán definuje úkoly a nástroje. Definování úkolů je nastaveno prakticky, maximálně srozumitelně a konkrétně, tak aby mohly být provedeny i poučeným laikem.

4. **Modelové nácviky a ověření funkčnosti**
   Koordinační plán je vždy individualizovaný. Pro zasazení kontextu dané organizace a její specifické situace do celého přípravného procesu je doporučená **metoda zážitkové simulace a otestování připravenosti cvičeními**.

7. Zvýšení bezpečnostního povědomí

Obecně je vhodné minimálně jednou ročně **seznámit pracovníky s hrozbami**, kterým je možné v daném objektu / akci čelit a **zopakovat základní bezpečnostní postupy**.

Začněte také důsledně evidovat konfliktní a podezřelé situace, bezpečnostní incidenty, bezpečnostně relevantní závady apod. Veďte si přehled a statistiku o těchto událostech, které se zdají být mnohdy banální a rutinní.

Kromě toho poučte a podpořte vlastní personál, případně své spolupracovníky, sousedy apod. v tom, aby informovali, pokud si všimnou podezřelé aktivity, vyzvídání apod. Pokud vidíte něco divného, nahlaste to ostraze nebo policii na 158.

Doporučujeme:

1) Jednou ročně uskutečnit **bezpečnostní školení věnované prevenci a postupům při bezpečnostních incidentech**. Program může zahrnovat nácviky bezpečnostních postupů, krizové komunikace, sebeobrany apod.
2) Jednou ročně uskutečnit **cvičení pro vedení organizace** zaměřené na koordinaci postupu bezprostředně po bezpečnostním incidentu. Toto cvičení je vhodné kombinovat s povinným požárním cvičení a zvýšit tak jeho efektivitu.
3) Téma bezpečnosti **zahrnout do vlastních periodik, mobilních aplikací apod.** s cílem udržovat povědomí o bezpečnostních rizicích a prevenci u zaměstnanců a návštěvníků.

V případě velkých kulturních a sportovních akcí doporučujeme zařadit **bezpečnostní briefing pro dobrovolníky a pořadatele**.

8. Spolupráce se složkami Integrovaného záchranného systému (IZS)

Spolupráce s Policií ČR, obecní policií, hasiči, zdravotnickou záchrannou službou a dalšími složkami IZS Vám může pomoci při rozvoji vaší bezpečnosti, přípravě plánů a následně při řešení bezpečnostních incidentů.

Je vhodné složkám IZS nabídnout prohlídku a zhodnocení Vašeho objektu, zapojit složky IZS do příprav pořádaných akcí a do vyhodnocení ohroženosti objektu. Dále je vhodné informovat Policii ČR o mimořádných událostech a konzultovat nastavené postupy pro případy bezpečnostních incidentů. Vhodné je kontaktovat zejména místně příslušné místní/obvodní oddělení, popř. územní odbor Policie ČR, dále preventivně informační oddělení, vhodné je také sdílet některé informace (např. plány budov) s operačním odborem krajského ředitelství .

9. Důsledná autorizace a kontrola vstupu s důrazem i na detekci nežádoucího úmyslu

Bezpečnostní kontroly u vstupu do objektů jsou běžným bezpečnostním opatřením, avšak v mnoha případech nejsou důsledné a neplní požadovanou funkci. V případě ochrany měkkých cílů je často kontrola nemožná vzhledem k charakteru cíle, jeho lokalizace v otevřeném prostoru, případně jeho veřejné přístupnosti.

Pokud to však možné je, měl by být perimetru objektu pod kontrolou. Ta může mít tři stupně:

1. dochází k autorizaci osob
2. dochází k autorizaci osob i ke kontrole zaměřené na nežádoucí předměty
3. dochází k autorizaci osob, nežádoucích předmětů a nebezpečný úmysl

Pro smysluplnost těchto opatření je nezbytné, aby byl pod kontrolou celý perimetr po celou dobu provozu. Důsledná autorizace znamená, že každá vstupující osoba prochází schválením vstupu podle předem daného klíče. K autorizaci může dojít pomocí technologií (např. pomocí čtečky, kamer, videotelefonu apod.) nebo fyzickou identifikací pověřeným pracovníkem.

Osobní kontroly představují další stupeň kontroly. Bezpečnostní rámy ani rentgeny nedokáží odhalit zbraně bez dobře připravené a často testované obsluhy. Jako zbraň může posloužit mnoho předmětů i za kontrolním bodem. Optimální je proto využití kombinace kontrol zaměřených na nežádoucí předměty a detekce podezřelého chování při preventivní kontrole doplněné o **bezpečnostní pohovor. Pohovor kvalifikovaným pracovníkem.**

10. Zabývejte se Vaší lokalitou a spolupracujte s dalšími měkkými cíli

Tento princip je zásadní pro účelné nastavení bezpečnostního systému. Útoky na měkké cíle jsou často koordinované, simultánní a útočníci pokračují v útoku na více subjektů. Útočníci často do objektů ani nevstupují a zaútočí před ním.[7] Na tyto místa „za perimetrem“ je třeba myslet při vytváření analýzy ohroženosti a při aplikaci bezpečnostních opatření.

Bezpečnostní management by si měl uvědomit, zda chrání primárně budovu, nebo osoby (to je typické pro měkké cíle) a do jaké vzdálenosti by provedený útok byl spojován s danou organizací, resp. by mohl ovlivnit její chod.

Lokalita může mít ještě širší pojetí, než je bezprostřední sousedství objektu. Může jím být dané město nebo region. Z toho důvodu je vhodné rozvíjet spolupráci mezi měkkými cíli (zejména v lokalitě) a kooperovat při nastavování těch opatření, která jsou pro všechny zapojené strany výhodná. Příkladem může být výměna informací, vzájemné varování při bezpečnostních incidentech, sdílení jednoho koordinačního centra (viz výše), společná koordinovaná cvičení bezpečnostní procedur, sdílení nákladů na zabezpečení apod.

[7] Z tohoto pohledu je na příklad **velice problematické vytváření front před bezpečnostní kontrolou do objektu**, které mohou být snadným cílem. V rámci analýzy ohroženosti je nutné zvážit, o kolik je pro útočníka atraktivnější útočit skutečně uvnitř objektu a na kolik se tedy frontou jen nevytváří další měkký cíl.

PŘÍLOHY

Příloha 1 - Obecná doporučení postupu při bezpečnostních incidentech

1. Přivolejte pomoc (tel. 158) – co nejdříve! Nezůstávejte v situaci sami.
2. Pokud máte podezření, že jde o vážný útok či jiný incident, musíte jednat okamžitě a dlouze stav neověřovat.
3. Pokud dostanete od policie, případně ostrahy varování s doporučením evakuovat, musíte reagovat okamžitě.
4. Počítejte s nedostatkem času. Pokud si to situace bude vyžadovat, buďte připraveni přijmout krajní a kreativní opatření - zejména při evakuaci. Nesvazujte se pravidly.
5. Pro každý bezpečnostní incident platí stejné pravidlo: **musíte dostat lidi z dosahu problému.**
6. K ochraně před explozí si zapamatujte: „zeď je dobrá, sklo je špatné“[8].
7. Nepřekombinovávejte, nefantazírujte o dalších možných nástrahách – to vás jen paralyzuje. Reagujte na to, co vidíte na 100%![9]
8. Místo, kam se evakuuje, musí být bezpečnější než místo, odkud se evakuuje. Zodpovězte si otázku: Je bezpečněji vevnitř nebo venku?
9. Komunikujte, mluvte nahlas, říkejte, co děláte.
10. Kdykoli budete evakuovat, musíte dostat evakuované minimálně z dohledu od problému.

[8] Při výbuchu dochází k nejvíce zraněním vlivem sekundárních fragmentů, nejčastěji roztříštěného skla. V bezpečí nejsou ani výlohy na opačné straně objektu.

[9] Pravidlo „nepřekombinovávat“ reakci na útok reaguje na (zejména teoretické) otázky, jak řešit vícečetný útok, zejména různého typu, na různých místech současně apod. Ze zkušeností se jako nejefektivnější ukazuje jednoduše co nejrychlejší reakce na zjevný útok, nikoliv nadbytečné zvažování, jaká různá úskalí by reakce mohla mít či jaká další nebezpečí mohou současně hrozit.

Příloha 2 – Doporučená reakce na výhružný telefonát

V případě, že obdržíte výhružný telefonát:

1. Zapište si ihned detaily rozhovoru.
2. Pokud se Vám zobrazuje číslo volajícího, zapište je.
3. Nikdy nezavěšujte! Snažte se volající/volajícího udržet na telefonu, ptejte se na detaily a sdělení si zapisujte.
4. Po dokončení hovoru informujte místní ostrahu.
5. Zvažte, zda byl volající důvěryhodný, zda obsahoval konkrétní informace či zda měl volající znalost místa. Pokud ano, iniciujte evakuaci podle svých procedur.
6. Informujte policii na tel.: 158.
7. Policii a jednotkám IZS asistujte. Pomoci můžete např. s vhodným informováním přítomných osob, zabráněním vstupu do objektu pracovními vchody apod.

Příloha 3 – Doporučená reakce na nález podezřelého předmětu

Pokud předmět:

- nezapadá do rutiny místa,
- nemá zjevného majitele a
- vzhledem ke své velikosti a umístění by mohl v případě výbuchu ohrozit osoby v okolí.

Postupujte následovně:

1. Informujte bezpečnostní personál.
2. Dohlédněte, aby nikdo s předmětem nehýbal ani se k němu nepřibližoval.
3. Pokuste se zjistit majitele. Ověřte, zda nepatří někomu v okolí. Využijte vnitřní rozhlas.
4. Pokud neznáte majitele, zajistěte, aby se v dostatečné vzdálenosti k předmětu nikdo nepřibližoval. Evakuujte (směrem od předmětu).
5. Informujte policii.
6. Pořiďte záznam.

Příloha 4 – Doporučená reakce na podezřelé vozidlo

Pokud je zjevné, že se jedná o „car bomb“:

1. Okamžitě evakuujte pryč od vozidla, přitom se snažte, abyste měli co nejvíce zdí mezi vozidlem a lidmi.
2. Zapojte do evakuace bezpečnostní personál.
3. Informujte policii.

Pokud jde o podezřelé vozidlo:

1. Na vozidlo nesahejte, neotvírejte ho a nepohybujte s ním.
2. Informujte bezpečnostní personál
3. Nesoustřeďte se na řidiče, ale na vozidlo!
4. Zjistěte, zda neznáte majitele. Ověřte, zda nepatří někomu v okolí. Využijte vnitřní rozhlas.
5. Informujte policii.
6. Pořiďte záznam. (pokud možno s viditelnou RZ).

Příloha 5 – Doporučená reakce při obdržení podezřelé zásilky

Podezřelá zásilka může být identifikována podle následujícího:

- odesilatele neznáte, případně není vůbec uveden
- Vaše adresa je uvedena nepřesně
- příchod zásilky je neočekávaný
- zásilka je nerovnoměrně zatížená, hrbolatá
- zásilka je neobvykle objemná či vyztužená
- obal je místy promaštěný, podivně páchne
- zásilka je nadbytečně známkována

1. Podezřelý dopis / balíček nikdy NEOTEVÍREJTE!
2. Opatrně jej uložte do malé, uzavřené místnosti. Riziko aktivování výbušniny přenosem předmětu je menší, než jistá škoda způsobená výbuchem v prostorách, kde se zdržují lidé.
3. Nepoužívejte v jeho blízkosti radiové přístroje (mobilní telefony, vysílačky).
4. Informujte bezpečnostní personál.
5. Informujte policii.
6. Pořiďte záznam.

Příloha 6 - Telefonování s integrovaným záchranným systémem při nebezpečných situacích

Při komunikaci s IZS dodržujte následující postup:

1. Představte se celým jménem.
2. Sdělte svoje organizační zařazení.
3. Sdělte, odkud voláte
4. Popište, co se stalo.
5. Popište, jaká je situace teď
6. Sdělte zda jsou na místě zranění.
7. Řekněte, co potřebujete.
8. Nezavěšujte jako první.
9. V následujících minutách z telefonu netelefonujte, aby se Vám bylo možné dovolat.

Příloha 7 - Příklady útoků na jednotlivé typy měkkých cílů:

Školy

- Žďár nad Sázavou, ČR, 2014. 1 mrtvý, MO: rukojmí, útok nožem
- Brindisi, Itálie, 2012. 1 mrtvý, 7 zraněných. MO: Bomba před školou
- Toulouse, Francie, 2012. 4 mrtví. MO: Střelba
- Winnenden, Německo, 2009. 15 mrtvých. MO: Střelba
- Beslan, Rusko, 2004. 385 mrtvých, 1100 rukojmí. MO: Rukojmí, střelba
- Dunblane, Skotsko, 1996. 15 mrtvých, 18 zraněných. MO: Střelba
- Vukovar, Chorvatsko, 1991. 41 mrtvých, 0 raněných. MO: Střelba

Náboženské (v ČR zejména židovské) objekty a místa bohoslužeb

- Kodaň, Dánsko, 2015: 1 mrtvý, MO: Střelba u synagogy
- Paříž, Francie, 2015, 4 mrtví, MO: Rukojmí a střelba v košer obchodě
- Brusel, Belgie, 2014. 4 mrtvý, MO: Střelba v židovském muzeu
- Dijon, Francie, 2014. 11 zraněných, MO: Najíždění autem do lidí
- Toulouse, Francie, 2012. 4 mrtvý, 1 zraněný, MO: Střelba v židovské škole

Dopravní prostředky

- Bologoye, Rusko, vlak, 2009. 26 mrtvých, 100 raněných. MO: Bombový útok
- Moskva, Rusko, metro, 2010. 44 mrtvých, 88 raněných. MO: Bombový útok
- Londýn, Anglie, metro, 2005. 56 mrtvých, 784 raněných. MO: Bombový útok
- Madrid, Španělsko, vlak, 2004. 191 mrtvých, 1800 raněných. MO: Bombový útok

Sportovní a kulturní akce

- Paříž, Francie, 2015. 1 mrtví při fotbalovém zápase. MO: Sebevražedné útoky
- Kodaň, Dánsko, 2015. 1 mrtvý, 3 ranění při přednášce o svobodě slova. MO: Střelba
- Boston, USA, 2013. 2 mrtvý, 132 raněných. MO: Bombový útok

Obchodní centra a restaurace

- Paříž, Francie, 2015. 15 mrtvých a 10 zraněných. MO: Střelba z auta na restaurace
- Uherský Brod, ČR, 2015. 8 mrtvých. MO: Střelba
- Kodaň, Dánsko, 2015. 1 mrtvý. MO: Střelba
- Bombaj, Indie, 2008. 10 mrtvých. MO: Střelba, granát, Leopold Cafe
- Tel Aviv, Izrael, 2003. 3 mrtví. MO: Sebevražedný útok, Mike's place

Hotely

- Islamabad, Pakistan, 2008, 61 mrtvých, 200 zraněných. MO: sebevražedný útok
- Sharm el-Sheikh, Egypt, 2005, 91 mrtvých, 110 zraněných. MO: sebevražedný útok
- Taba, Egypt, 2004, 34 mrtvých, 159 zraněných. MO: car bomb
- Bombaj, Indie, 2008, 68 mrtvých, 76 zraněných. MO: Střelba, bombový útok

Příloha 8 - Tabulka vyhodnocení míry ohrožení pomocí analýzy rizika

MODUS OPERANDI	LOKALIZACE ÚTOKU	DOBA ÚTOKU	PRAVDĚPODOBNOST				DOPAD				MÍRA OHROŽENÍ
			Dostupnost	Složitost	Atraktivita	**Celkem hrozba**	Poškození budovy	Ohrožení životů	Dopady na komunitu	Ekonomické důsledky	
Útok nožem	před objektem	denní provoz									
Útok nožem	před objektem	akce pro pozvané									
Střelba	před objektem	denní provoz									
Bomba	uvnitř	akce pro pozvané									
...											