CESTOVNÍ MAPA PROJEKTU

(AKTUALIZOVANÁ FORESIGHTOVA STUDIE ZA OBDOBÍ OD 27.2.2022)

OBSAH

ÚVOD

V rámci poslední etapy řešení tohoto projektu je zpracován tento materiál, který do jisté míry reflektuje poslední trendy v oblasti ochrany a bezpečnosti kritické infrastruktury a současně popisuje budoucí vývoj problematiky resilience zvolené oblasti infrastrukturních systémů. Materiál je členěn na 2 hlavní kapitoly, jimiž jsou Ochrana a odolnost kritické infrastruktury s využitím přístupů ku konvergenci druhů bezpečnosti a dopadová studie Směrnice Evropského parlamentu a rady o posílení odolnosti kritických subjektů. Na konci každé kapitoly je celkové shrnutí a návrhy na možná zlepšení v kontextu možného výzkumu a možného odborného rozvoje.

1 OCHRANA A ODOLNOST KRITICKÉ INFRASTRUKTURY S VYUŽITÍM PŘÍSTUPŮ KU KONVERGENCI DRUHŮ BEZPEČNOSTI

S technologickým rozvojem proniká problematika bezpečnosti do čím dále tím většího počtu oblastí lidské společnosti. Ještě donedávna se bezpečnost týkala především státu, života a zdraví osob a majetku. Postupně, s rozvojem technologií, nárůstem množství aktiv, počtu typů bezpečnostních problémů se začaly etablovat nové ucelené soubory bezpečnostních opatření. Tyto samostatné soubory opatření představují, tím pádem se

i nazývají druhy bezpečnosti. Mezi hlavní druhy bezpečnosti v současnosti patří mezinárodní bezpečnost, fyzická bezpečnost, administrativní bezpečnost, požární ochrana, informační bezpečnost, kybernetická bezpečnost, bezpečnost a ochrana zdraví při práci, osobní bezpečnost, bezpečnost výrobků, surovinová bezpečnost, energetická bezpečnost, potravinová bezpečnost, environmentální bezpečnost, provozní bezpečnost atd. V současnosti existuje více jak 50 druhů bezpečnosti. Řada druhů bezpečnosti se řeší na úrovni státu, avšak nezanedbatelný počet se jich uplatňuje na úrovni organizace.

Na jednu stranu je dobře, že jsou celky, referenční objekty a jejich aktiva chráněna tolika soubory opatření, na druhou stranu však tato situace způsobuje řadu problémů. Mezi hlavní problémy patří oddělená existence samostatných druhů bezpečnosti, vyšší personální i finanční náklady na zajištění bezpečnosti, či absence souvztažnosti mezi jednotlivými událostmi v bezpečnostním prostředí. Zejména v organizacích typu podnik nebo úřad tato situace způsobuje řadu problémů. Jedním ze způsobů, jak uvedený soubor problémů řešit, je koncept konvergované bezpečnosti. Obecně konvergence znamená přibližování až splynutí dříve samostatných prvků. Koncept konvergované bezpečnosti znamená sloučení vybraných druhů bezpečnosti do jednoho celku.

1.1 Druhy bezpečnosti a jejich konvergence

Zajišťování bezpečnosti a rozšiřování její agendy se děje zaváděním jednotlivých druhů bezpečnosti. Za druh bezpečnosti se považuje ucelený soubor opatření, který řeší specifickou skupinu bezpečnostních problémů. V bezpečnostní komunitě se používá obdobný pojem sektor bezpečnosti. Za sektor bezpečnosti se považuje určitá část bezpečnostního prostředí,

v níž vznikají specifické bezpečnostní problémy. Autoři Kodaňské bezpečnostní školy specifikovali pět sektorů bezpečnosti: vojenský, politický, ekonomický, societární a environmentální. K nim lze v současnosti přidat další samostatné sektory, například informační sektor. Druhy bezpečnosti pak v jednotlivých sektorech bezpečnosti řeší specifické bezpečnostní problémy. Příkladem může být informační sektor, v němž jsou bezpečnostní problémy (např. únik utajované informace, neoprávněná modifikace dat, neoprávněné zamezení přístupu k informacím, záměrné přerušení funkce informačního systému) aktivně řešeny prostřednictvím informační bezpečnosti, kybernetické bezpečnosti, administrativní bezpečnosti nebo datové bezpečnosti. V současnosti je zavedeno více jak 50 druhů bezpečnosti.

1.1.1 Vymezení druhu bezpečnosti

Druhy bezpečnosti vznikají na základě potřeb praxe jejich institucionalizací. Zajištění bezpečnosti je prosazováno řadou nástrojů: legislativa, strategie, orgány, řízení, technologie, způsob zajištění a vynucení. Legislativa vymezuje řešené bezpečnostní problémy, kdo a jak je bude řešit a případně stanovuje i sankce jejich původcům. Významným prvkem legislativního vymezení druhu bezpečnosti je specifikace orgánů, které budou druh bezpečnosti zajišťovat. Základem tohoto vymezení je specifikace struktury orgánů, jejich role a působnosti v zajištění bezpečnosti. Zavedení druhu bezpečnosti do praxe pak znamená vytvoření orgánů, jejich vybavení potřebnými nástroji a technologiemi a realizace úkonů bránících vzniku narušení bezpečnosti (bezpečnostních problémů), případně jejich řešení v případě jejich vzniku.

Původně vznikaly druhy bezpečnosti především na základě vlastní potřeby společnosti (státu) řešit nově vzniklé kategorie bezpečnostních problémů. Jednalo se například o pracovní úrazy za průmyslové revoluce v 19. století. Další příčinou vzniku druhu bezpečnosti je záměrná politizace a sekuritizace tématu, umělé vytvoření problému z politických důvodů (např. z důvodu zbavení se protivníka). Příkladem budiž zavedení státních policií. V současnosti se druhy bezpečnosti zavádí rovněž z důvodu jejich doporučení / vynucení nadřazenou autoritou (z důvodu harmonizace bezpečnostního prostředí). Příkladem budiž Evropská unie, která v tomto sehrává významnou roli. V poslední době se jednalo zejména o problematiku ochrany osobních údajů a kybernetické bezpečnosti.

1.1.2 Konvergence druhů bezpečnosti

Když budeme mluvit o jakémkoliv objektu nebo třeba prostoru, kde se nachází lidé a vykonávají určitou činnost/aktivitu, budeme také mluvit o druzích bezpečnosti, které se na tyto objekty, prostory, lidi a činnosti vztahují. V dnešní době je každý druh bezpečnosti řešen samostatně, bez návaznosti na jiné druhy bezpečnosti týkající se stejného subjektu (osoby, objektu apod.). Pro každý druh bezpečnosti existují samostatné nástroje, kterými lze sledovat požadované parametry a zhodnotit stav vybraného druhu bezpečnosti.

Jako příklad můžeme uvést jakýkoliv úřad, kde je samostatně sledováno, jestli se ve vyhrazených prostorech nepohybuje cizí osoba, samostatně je sledován systém požární ochrany, přístup do serverovny a nakládání s elektronickými daty, nebo i manipulace s různými tiskopisy. Dnes, když je zaznamenána cizí osoba ve vyhrazených prostorech (např. v kanceláři bez přítomnosti pracovníka), je řešen problém jenom s narušením vyhrazených prostor, tzn. bezpečnostní služba/policie narušitele zajistí a až posléze je vyšetřováno, proč se tato osoba v daném prostoru nacházela, jestli např. neodcizila nějaký majetek nebo data z počítačů, případně do počítačů pracovníků nenainstalovala vir apod. Chybí okamžité propojení mezi jednotlivými druhy bezpečnosti, kde by souběžně se zaznamenáním nepovolané osoby v kanceláři, došlo ke kontrole činností na počítačích z dané kanceláře (pokus o zadání hesla, přihlášení se do systému, připojení USB, spuštění programu, vyhledávání dat v síti apod.) a k okamžitému zablokování těchto pracovních počítačů, jejich oddělení od vnitřní sítě, aby případný narušitel nemohl získat hledaná data, případně šířit prostřednictvím těchto počítačů vir.

Správné propojení různých druhů bezpečnosti, tzv. konvergence, by zpřehlednila a ulehčila řešení mnohých situací, kdy by se v rámci jednoho podnětu z jednoho druhu bezpečnosti dokázala předvídat možná rizika i pro jiný druh bezpečnosti a na základě tohoto podnětu by se aktivovala opatření, která by mohla zamezit vzniku případných dalších škod.

Je však potřeba si uvědomit, kolik různých druhů bezpečnosti se týká každého subjektu, které druhy bezpečnosti jsou v tomto subjektu pro nás nejdůležitější a také si nutno uvědomit, že ne všechny druhy bezpečnosti lze vzájemně propojovat. Ne vždy je jasné spojení mezi jednotlivými druhy bezpečnosti a jejich vzájemná konvergence musí být vhodně nastavena, jinak by mohla znepřehlednit situaci a konvergence by uživateli přinesla víc problémů než užitku.

Bezpečnost objektů strategického významu zahrnuje ochranu objektů obranné infrastruktury. Objekty obranné infrastruktury se rozdělují na kategorii objektů důležitých pro obranu státu (ODOS) a kategorii objektů, které mohou být za stavu ohrožení státu nebo za válečného stavu napadeny (OMN – objekty možného napadení). Jedná se např. o objekty mající velký význam pro obranu státu, mající vliv na chod hospodářství státu. Dále objekty, které řídí obranu státu, velí ozbrojeným silám, zajišťují leteckou dopravu, výrobu energií, přepravu strategických surovin a přenos dat potřebných k zajištění obrany státu, zajišťují výrobu, skladování a odběr životně důležitých produktů nebo životně důležitého zboží potřebného k zajištění obrany státu apod.

Bezpečnost kritické infrastruktury je chápaná jako souhrn činností, mechanismů, sil, prostředků a opatření na:

- prevenci před rizikovými faktory,
- odvrácení útoku na prvek kritické infrastruktury,
- zabránění negativním venkovním nebo vnitřním vlivům ohrožujícím existenci, stabilitu a fungování prvků kritické infrastruktury,
- odstranění následků.

Ochranu jednotlivých prvků kritické infrastruktury organizuje v plném rozsahu právnická osoba, vlastník nebo správce jako součást vlastních opatření na ochranu majetku.

Odvětví kritické infrastruktury:

- energetika,
- vodní hospodářství,
- potravinářství a zemědělství,
- zdravotnictví,
- doprava,
- komunikační a informační systémy,
- finanční trh a měna,
- nouzové služby,
- veřejná správa.

Kapitola Druhy bezpečnosti a jejich konvergence v úvodu uvádí, co jsou to druhy bezpečnosti a jak vznikají.

1.2 Konvergovaná bezpečnost a její význam

Cílem této podkapitoly je seznámit s významem a obsahem pojmu „konvergovaná bezpečnost (KnB)“, který se začíná rozšiřovat z hlediska potřeby zajištění komplexní bezpečnosti objektů, firem nebo organizací jako celku, nikoliv jako dříve z pohledu jednotlivých oddělených druhů bezpečností, jako jsou fyzická, informační, kybernetická, provozní, personální atd. KnB je multifunkční obor s novou přidanou hodnotou, jehož vznik byl podpořen vývojem nových sofistikovaných systémů informačního managementu, jako jsou CSIM (Converged Security Information Management) nebo SIEM (Security Information and Event Management). Tyto systémy pracují v oblastech fyzické a kybernetické bezpečnosti, přičemž využívají prostředků situační analýzy a zpracování hromadných dat.

1.2.1 Uvažované druhy bezpečnosti

Pojem „druh bezpečnosti“ představuje soubor opatření předurčených k zajištění bezpečnosti jakožto stavu bezpečnostní situace ve vymezené části bezpečnostního prostředí. Jedná se o soustavné a opakované řešení nežádoucích jevů narušení bezpečnosti určitého typu. Zejména vlivem technologického rozvoje narůstá počet druhů bezpečnosti, které musí sledovaný objekt v rámci své ochrany zajišťovat. Např. pro objekt typu výrobní podnik mohou patřit mezi tyto druhy bezpečnosti fyzická bezpečnost (FB), kybernetická bezpečnost (KB), informační bezpečnost (IB), provozní bezpečnost (PB) a bezpečnost a ochrana zdraví při práci (BOZP). V případě požadavku či potřeby se pro jiné typy podniků a institucí mohou k těmto nejběžnějším bezpečnostem dále přidat i další druhy bezpečností, jako jsou např. administrativní bezpečnost, personální bezpečnost, ekologická bezpečnost, radiační bezpečnost aj. V různé literatuře lze najít definice cca 50 druhů bezpečnosti, i když ne všechny jsou všeobecně uznávány jako samostatné druhy. Některé druhy bezpečností jsou řešeny i na úrovni státu a jiné lze najít aplikované v segmentech a organizacích, kde jsou začleněny přímo do podnikových procesů. Většina organizací nepovažuje za potřebné sledovat samostatně méně běžné druhy bezpečností. Například personální bezpečnost se řeší v rámci personálního úseku organizace, jehož je nezbytnou součástí. Málokdy se setkáme se samotným pojmem personální bezpečnosti v podnikové bezpečnostní strategii.

Z důvodu potřeby zajištění celkové bezpečnosti organizace je nutné přistupovat k výběru pouze takových parciálních bezpečností (tj. druhů bezpečnosti), které budou pro danou organizaci nebo dané odvětví podstatné a bude dávat smysl je sledovat. Principem dále definované konvergované bezpečnosti je právě slučovat za určitých podmínek tyto vybrané parciální bezpečnosti tak, aby vznikla kvalitativně vyšší úroveň zabezpečení celé organizace nebo odvětví.

1.2.2 Požadavky na slučování bezpečností

Konvergovaná bezpečnost (KnB) představuje specifický druh bezpečnosti, vzniklý sloučením několika slučitelných druhů bezpečnosti do jednoho celku. Takovýto druh bezpečnosti umožňuje díky analýze souvztažnosti projevů narušení bezpečnosti dříve (pokud možno ještě ve stádiu příznaků), rychleji a přesněji odhalit vznikající narušení celkové bezpečnosti a cíleněji zajistit reakci na toto narušení. Konvergovaná bezpečnost KnB v nejběžnější formě obvykle zahrnuje fyzickou (FB), kybernetickou (KB), informační (IB) a provozní bezpečnost (PB). Struktura slučovaných druhů bezpečnosti může ovšem být i jiná, což záleží na potřebách sledovaného objektu i na nezbytnosti požadavku slučitelnosti jednotlivých druhů bezpečnosti.

Požadavek slučitelnosti vychází zejména z potřeb identifikace provázaných rizik plynoucích z hrozeb takového charakteru, která by se v případě jednotlivých dílčích bezpečností nedala vůbec identifikovat a ani efektivně řídit. Při procesu slučování různých druhů bezpečnosti by se mělo vycházet především z potřeby ochrany stejných aktiv sledovaného objektu, u kterých jsou také časové charakteristiky projevů narušení bezpečnosti přibližně ve stejných intencích (vteřin – minut – hodin). Pokud by došlo k sloučení z hlediska následků podobných druhů bezpečnosti, kdy u jednoho dochází ke změnám v minutách a v dalším v hodinách, pak by sloučení do konvergované bezpečnosti postrádalo smysl, protože dominantní roli by sehrával druh bezpečnosti s časově krátkými změnami.

1.3 Fyzická bezpečnost kritické infrastruktury

Mezi nejstarší druhy bezpečnosti a ochranných opatření patří ochrana prostřednictvím klasických stavebních opatření, často také nazývaná ochrana majetku nebo rovněž fyzická[1] bezpečnost. Mechanické zábranné systémy a prostředky a fyzická ostraha (strážní) byly z pragmatických důvodů dlouhodobě jedněmi z prvních a často jediných opatření k zajištění fyzické bezpečnosti. Teprve až s rozvojem technologií došlo k rozšíření spektra opatření fyzické bezpečnosti o další možnosti, zejména o bezpečnostní technologie na bázi elektronických systémů.

Pojem „fyzická bezpečnost" je obvykle chápán dvojím způsobem a ve dvojím významu. Jako stav i jako soubor opatření. Jako „stav" pojem fyzická bezpečnost vyjadřuje „stav bezpečnostní situace" (bezpečí, nebezpečí, ohrožení, újma). Častěji však pojem fyzická bezpečnost[2] označuje soubor opatření vůči škodícímu účinku, hrozeb působících fyzickou cestou. Jedná se o zabezpečení referenčního objektu ochrannými opatřeními fyzického charakteru, zejména mechanickými zábrannými systémy a prostředky, poplachovými systémy, fyzickou ostrahou a režimovými opatřeními.

Má-li se zajistit požadovaná úroveň bezpečnosti, je potřebné v rámci referenčního objektu identifikovat chráněný zájem nebo aktiva. Aktivy jsou v rámci fyzické bezpečnosti peníze, starožitnosti, umělecké předměty, utajované informace, aktiva charakteru duševního vlastnictví, ale také omamné látky, zbraně, jedovaté látky atd. Je to cokoliv, co je důležité chránit proti zcizení fyzickou cestou.

Úroveň bezpečnosti vyjadřuje vztah hrozeb (velikosti škodícího účinku) a rizik vůči opatřením k minimalizaci vlivu škodícího účinku. Obvykle je kvalita opatření odvozena od ceny aktiv nebo jiným způsobem vyjádřené potřebnosti ochrany (jed nemusí být drahý, ale je nebezpečný z pohledu jeho zneužití, a proto musí být chráněn). Podle pravidla

---

[1] V 90. letech minulého století se v některých případech označovala jako objektová bezpečnost.

[2] Např. dle § 5, písm. d) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů je *„systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat"*.

ALARP/ALARA[3] by měly náklady na bezpečnostní opatření představovat asi 10–15 % ceny aktiv. Bezpečnostní posouzení umožňuje zhodnocení stupně bezpečnosti a také míry zabezpečení aktiv proti předpokládaným rizikům. Základem posouzení je identifikace hrozeb, které aktiva nebo chráněný zájem ohrožují.

1.3.1 Systém fyzické bezpečnosti

Systém fyzické bezpečnosti představuje soubor ochranných opatření, jejichž cílem je zamezit nebo ztížit přístup narušiteli k chráněným aktivům fyzickou cestou. Jedná se o personálně technický systém, realizující vymezené bezpečnostní metody. Základem realizace ochranných opatření, zajišťovaných systémem fyzické bezpečnosti, je:

- komplexnost,
- vícestupňovost,
- automatizace,
- průlomová odolnost,
- reakceschopnost.

Komplexnost představuje šíři a vzájemnou návaznost ochranného, detekčního a reaktivního účinku přijatých opatření.

Vícestupňovost představuje rozdělení opatření do více oddělených vrstev. Každá vrstva plní samostatnou funkci.

Automatizace vyjadřuje využití systémů k automatické identifikaci narušení zastřežené zóny a předání této informace na dohledové poplachové a přijímací centrum a následně zásahové jednotce.

Průlomová odolnost představuje dobu potřebnou k překonání opatření na bázi mechanických zábranných systémů. Respektují se při tom schopnosti i vybavení předpokládaného narušitele. Je vhodné volit takovou průlomovou odolnost, aby doba pro překonání opatření převyšovala dobu pro pachatele únosnou (zejména z obavy jeho odhalení).

---

[3] ALARA – As Low As Reasonable Achievable (tak nízké, jak lze rozumně dosáhnout při respektování ekonomických [a dalších] hledisek).

Reakceschopnost představuje schopnost bezpečnostního orgánu (sil a prostředků, fyzické ostrahy, policie atd.) včas a správně reagovat na narušení bezpečnosti a minimalizovat vznikající újmu. Jedná se o represivní opatření ve formě zadržení pachatele, hašení požáru atd.

Systém fyzické bezpečnosti zajišťuje bezpečnost prostřednictvím režimového modelu, bariérového modelu a reaktivního modelu zajištění bezpečnosti. Systém fyzické bezpečnosti referenčního objektu zpravidla zahrnuje:

- režimová opatření,
- fyzickou ochranu (činnost fyzické ostrahy),
- technickou ochranu (technické prostředky systému fyzické bezpečnosti).

Jedním z klíčových požadavků na systém fyzické bezpečnosti je vícestupňovost a průlomová odolnost. Tyto požadavky se promítají do bariérového modelu zajištění bezpečnosti. V systému fyzické bezpečnosti se bariérový model používá ve formě vícevrstvé bariéry. Každá vrstva bariéry má svá specifika, která vychází z určení, pořadí a prostorových dispozic dané ochrany. Technické prostředky, použité k zajištění dané ochrany, musí respektovat její požadavky. Z hlediska detektorů narušení se jedná především o typ monitorovaných demaskujících příznaků narušitele, tvar a dosah detekční charakteristiky, citlivost a odolnost vůči planým poplachům. Prostorově se systém fyzické bezpečnosti dělí na:

- perimetrickou ochranu,
- plášťovou ochranu,
- prostorovou ochranu,
- předmětovou ochranu.

Zobecníme-li pohled na fyzickou bezpečnost, pak se jedná o zajištění požadovaného stavu (stupně) bezpečnosti cestou zabezpečovacích opatření fyzického charakteru (omezení nebo znemožnění pohybu, identifikace narušení zastřežené zóny, zadržení narušitele). Díky opatřením je zajištěn definovaný stav bezpečnosti (bezpečí), jehož překonání vyžaduje určitého stupně schopností. Důležité je, aby bezpečnostní opatření

měla větší ochranné schopnosti, než jsou předpokládané schopnosti narušitele k jejich překonání. Při tomto poměru bude bezpečnost zajištěna. Teoreticky vzato však absolutní bezpečnost zajistit nejde.

1.4 Kybernetická bezpečnost

Kybernetická bezpečnost je termín, kterým se obecně označují technologie sloužící k ochraně počítačových systémů a uživatelských dat před nedovolenou manipulací[4]. Jejím hlavním cílem je snižovat riziko kybernetických útoků a zajištění ochrany před vyvíjejícími se bezpečnostními hrozbami. V dnešním světě informačních technologií se jedná o obzvlášť důležitou oblast, protože se týká všech uživatelů, kteří již běžně používají internet.

Bezpečností informačních systémů se rozumí kolektivní postupy a mechanismy, jejichž citlivé a cenné informace a služby jsou chráněny před zveřejněním, poškozením nebo kolapsem, neoprávněnou činností nebo činností nedůvěryhodné osoby a neplánované události. Strategie a metody informační bezpečnosti se často liší od většiny jiných výpočetních technologií, protože jejich výhradním cílem je zabránit nežádoucímu chování počítačů.

Kybernetická bezpečnost je bezpochyby jedním z nejvíce specifických odvětví bezpečnosti. Je to dáno tempem rozvoje nových informačních technologií a s nimi souvisejícími službami. Ovšem tím hlavním faktorem je její působnost. Kybernetická bezpečnost je realizována jak v reálném – fyzickém světě, tak ve světě abstraktním – kyberprostor. Specifika kybernetické bezpečnosti tedy úzce souvisí s kyberprostorem a anonymitou, kterou nabízí. Obecně lze vymezit tyto základní vlastnosti:

- Ohraničenost – případný útok může přijít naprosto z kteréhokoliv místa, které je připojeno k internetu. Hranice ani vzdálenost zde nehrají žádnou roli.
- Čas – v kyberprostoru se jedná skutečně o velmi relativní pojem, jedná se opět jen o interpretaci digitálních dat a ty lze měnit. Příkladem mohou být zkušební

[4] Nedovolenou manipulací je myšleno odcizení, poškození, modifikace nebo znepřístupnění dat.

licence, které jsou omezeny dobou používání (zpravidla 30 dní). V dřívějších dobách pak po vypršení takové licence stačilo změnit systémové datum a uživatel mohl produkt užívat dále.

- Motivovanost útočníka – motivy, které stojí za útoky v kyberprostoru, se příliš neliší od motivů v reálném světě, i když jsou zde dva poměrně specifické. Prvním z nich je nuda, internet je plný různých návodů a průvodců, takže proč to nezkusit? Druhým poměrně specifickým motivem je potřeba dokazovat si své vlastní kvality, překonávání překážek. Typickým příkladem jsou počítačové programy, respektive hry. Vydavatel nového herního titulu se pyšní novou a dokonalou ochranou před cracknutím jejich produktu. Tohle prohlášení vede vždy k jedinému, soutěži o to, komu se to podaří jako prvnímu.
- Anonymita – v kyberprostoru je relativně jednoduché skrýt svou pravou identitu a vydávat se za někoho jiného, a především je možné se zcela vyhnout osobnímu kontaktu.

1.4.1 Hrozby v kybernetickém prostoru

Kybernetické útoky představují obrovský problém, protože mohou mít za následek například krádež velkého objemu citlivých údajů. Stávají se stále vážnějšími a je žádoucí jim věnovat velkou pozornost. V dnešní době informačních technologií, které stále více zasahují do běžného života, se neustálé objevují nové kybernetické hrozby, kterým je třeba se vyvarovat a stejně tak se bránit proti možným škodám. Útoky se oproti minulosti změnily v jejich komplexnosti a nyní se objevují v nejrůznějších formách. Počítačová kriminalita pak představuje závažný problém, protože může přesahovat i národní měřítko. Níže jsou uvedeny a popsány některé z nejčastějších typů hrozeb, které mají v úmyslu například získat přístup do počítačové sítě bez souhlasu vlastníka.

Kybernetické hrozby mají většinou za cíl získat finanční prostředky, způsobit uživateli škodu nebo provádět špionážní činnost. Postupně se zdokonalují a každý rok jsou vytvářeny nové podoby útoků.

Nástrojů a technologií, které mohou dopomoci snížit riziko expozice kybernetického aktiva hrozbou, je celá řada. Ve stručnosti lze rozdělit tyto technologie a postupy do následujících skupin:

1. Firewall
2. Antivirus a Anti-Malware software
3. AntiSpam
4. Technologie pro monitoring, prevenci a detekci
5. Virtual Private Network
6. Penetrační testy
    a. Interní penetrační test a externí penetrační test
    b. Penetrační test webových aplikací
    c. Penetrační test sociálního inženýrství

Kybernetická bezpečnost je vzhledem k dnešnímu využívání a rozšířenosti informačních technologií velmi důležitá. Přesto se velmi často můžeme setkat s tvrzením „*já nejsem zajímavý, co by se mi asi tak mohlo stát. Investovat do kybernetické bezpečnosti je zcela zbytečné*“. Realita je ovšem mnohdy jiná a terčem útoků se pak velmi často stávají právě takoví uživatelé. V lepším případě dojde k poškození systému, v horším případě se může jednat o vydírání, krádež dat a s nimi spojené přihlašovací údaje k důležitým službám na sociálních sítích, internetovému bankovnictví, e-mailu atd. U běžného uživatele začíná prevence „inteligentním“ chováním, tedy uživatel by měl znát hrozby a případná rizika spojená s jeho chováním a rozhodováním v kybernetickém světě. S cenou chráněných aktiv pak logicky rostou i náklady na zabezpečení a nelze se už jen spoléhat na „inteligentní“ chování. Je tedy vždy potřeba nalézt kompromis mezi případnou ztrátou a tím, kolik jsme ochotní do bezpečnosti investovat. Jak je možné pozorovat na níže uvedeném grafu, v určitý okamžik jsou náklady na zabezpečení zbytečně vysoké. Tohle ovšem neplatí pouze pro kybernetickou bezpečnost, ale je možné toto rozhodování aplikovat všude tam, kde potřebujeme zajistit bezpečnost.

1.5 Provozní bezpečnost

Na začátek je důležité si definovat, co provozní bezpečnost je. Můžeme tedy říct, že provozní bezpečností se rozumí nepřetržitý provoz firmy, podniku nebo systému za předvídatelných provozních podmínek.

Provozní bezpečnost je jedním z druhů bezpečnosti, které nejsou zatím v České republice podrobně rozebrány. V porovnání s ostatními druhy bezpečnosti (fyzická a kybernetická

bezpečnost) není ale o nic méně důležitá. Všechny tři musí spolu velmi úzce spolupracovat, protože stačí, aby jedna z nich byla narušena, a systém přestává plnit svou funkci.

Chod firmy musí být neustále zajištěn a majitel nebo bezpečnostní manažer musí proto vyspecifikovat klíčové procesy a systémy, které jsou pro provoz nezbytné. Prvním krokem, jako u každého druhu bezpečnosti, je nastavení systému řízení rizik. Aby firma pochopila a poznala své klíčové prvky a stav jejich současného zabezpečení.

Cílem provozní bezpečnosti je zajistit chod firmy či podniku z pohledu jejich provozu. Zabezpečují se tedy ty činnosti, které by mohly tento chod výrazně narušit nebo dokonce úplně zastavit. Každá oblast, každá firma má jiná aktiva, která tvoří provoz a jsou nezbytná pro jeho plynulost. Prvním krokem je tedy detailní seznámení s konkrétním podnikem nebo systémem, poznání všech procesů a následné definování aktiv. Dále se postupuje podle fází řízení rizik.

Hrozby provozní bezpečnosti je možné chápat jako hrozby, které mohou ohrozit provoz vybraného objektu, případně mohou tento provoz úplně vyřadit z funkčnosti. Na provozní bezpečnosti objektu[5] mají přímý vliv následující faktory:

- provozní technologie,
- řídicí systémy zajišťující provozuschopnost organizace,
- provozní informace,
- provozní události,
- procesy organizace.

S uvedenými faktory úzce souvisí právě hrozby, které mohou uvedené faktory ovlivnit. Mezi hlavní hrozby provozní bezpečnosti patří:

- krátkodobá až dlouhodobá ztráta anebo výpadek provozní technologie,
- krátkodobá až dlouhodobá ztráta funkčnosti řídicího systému zajištujícího provozuschopnost organizace,
- úplná ztráta funkčnosti provozní technologie anebo řídicího systému organizace,
- ztráta anebo změna provozní informace, která má přímý vliv na bezpečnost objektu,
- provozní událost (specifické pro konkrétní druhy objektů),

[5] V bezpečnostní terminologii se označuje také jako referenční objekt.

- změna procesů řídících provoz organizace (procesy popisují funkčnost daného systému).

Je nutno podotknout, že jednotlivé hrozby provozní bezpečnosti se liší vzhledem k povaze a druhu objektu. Každý referenční objekt může mít různé hrozby, které ohrožují jeho provoz. Hrozby referenčního objektu jsou přímo ovlivňovány druhem objektu, vnějšími faktory objektu, které na něj přímo působí a nastavením procesů objektu.

Z hlediska bezpečnosti budeme vycházet ze zásad nově vzniklé platformy managementu provozní bezpečnosti (SMS), která se osvědčila pro provozní bezpečnost v odvětvích letectví, železnice, lodní dopravy aj. Jedná se o zajištění procesů provozní bezpečnosti z hlediska ochrany osob ve smyslu pojmu „safety“ (opatření pro zabránění nehodám). Jedná se především o:

- Důsledný přístup k řízení rizik pro proaktivní identifikaci nebezpečí a posouzení rizik s přihlédnutím k jejich pravděpodobnosti a důsledkům.
- Proces zavádění opatření ke zmírnění, omezování a snížení rizik na přijatelnou úroveň v celém životním cyklu všech aktiv nutných pro přenos elektrické energie.
- Proces plánování robustní přenosové sítě, který zahrnuje požadavky zákazníků, trhu, jurisdikce a jiných zúčastněných stran, čímž se minimalizuje přerušení nebo omezení dodávek zákazníkům.
- Správa aktiv pomocí dobře specifikovaných a zdokumentovaných zásad a postupů musí být navržena tak, aby byla vyvážena rizika, náklady a výkonnost přenosové sítě při zajištění požadované úrovně bezpečnosti.
- Dále musí být zajištěny realizace následujících plánů a postupů:
    - Směrnice a plány pro zajištění požadované úrovně bezpečnosti pro různá pracoviště již na úrovni projektu.
    - Procesy pro řízení bezpečného provozu elektrické sítě.
    - Směrnice a procesy pro řízení prací na elektrických zdrojích, vedeních a rozvodnách přenosové soustavy.
    - Směrnice a postupy pro řízení bezpečnosti a zdraví pracovníků BOZP a ochrany životního prostředí.

- Procesy pro zajištění efektivní správy bezpečnosti elektrické sítě využívající monitorování funkčnosti, průběžné zlepšování vlastností elektrické sítě, průběžné bezpečnostní audity a realizaci následných nápravných opatření.

Sledování procesů provozní bezpečnosti na základě dodržování příslušných předpisů, zajištění potřebné komunikace mezi jejich účastníky, zvýšení jejich povědomí o reálné situaci, nabízení vhodných pracovních postupů při nestandardních situacích a jiné podobné činnosti budou jedním z hlavních přínosů systémů Converged Security Information Management (CSIM) z hlediska provozní bezpečnosti.

1.6 Odolnost referenčního objektu

Odolnost je obecně vnímána jako vlastnost systému překonat (absorbovat) narušení, snášet negativní změny systému, a přitom zajistit základní (esenciální) funkce, strukturu, identitu a zpětnou vazbu systému. Odolnost lze také vnímat jako schopnost zajistit funkci systému, v podmínkách působení negativních vnitřních a vnějších faktorů.

V následujícím textu jsou vymezeny a definovány základní oblasti, kterými je odolnost infrastrukturních systémů determinována. Jedná se o připravenost, absorpci, reakceschopnost, obnovitelnost a adaptabilitu.

1.6.1 Připravenost

Připravenost (preparedness) infrastrukturních systémů představuje schopnost odolávat očekávaným krizovým situacím, plánovat a mít reálně připravená opatření, síly a prostředky k jejímu překonání a zajištění obnovy funkce. Připravenost se zajišťuje prostřednictvím manažerských nástrojů, zejména s využitím analýzy rizik a přípravy na jejich minimalizaci (či eliminaci). V rámci ochrany se zajišťuje zpracováním bezpečnostního plánu (např. plánu krizové připravenosti subjektu kritické infrastruktury) a implementací přijatých opatření k zajištění ochrany a obnovy funkce.

1.6.2 Absorpce

Absorpce (Absorption) je endogenní vlastnost systému, která charakterizuje jeho schopnost automaticky absorbovat dopady systémových poruch a minimalizovat následky s co nejnižším úsilím. Jiní autoři mohou používat i jiné označení pro vlastnosti, které mohou mít stejný

nebo podobný význam. Často se používá pojem absorpční kapacita či stálost (Absorptive capacity or perzistence). Jedná se o vlastnost, která zachovává stabilitu a strukturu systému. Absorbovatelnost je tedy schopnost subsystému nést působení negativních faktorů bez významné odchylky od požadovaného fungování.

1.6.3 Redundance

Redundance (Redundancy) je definována jako schopnost systému přizpůsobit se. Princip spočívá v nahraditelnosti, kdy v případě poruchy části systému jedna složka selže a druhá složka je stále schopna plnit svou funkci, resp. funkci složky nahradit.

1.6.4 Robustnost

Robustnost (Robustness) lze definovat jako schopnost udržet provoz, nebo schopnost systému zajistit požadovanou funkci v případě, že selže redundance systému. V některých případech se to promítá do návrhu konstrukce nebo systémů, které musí být dostatečně silné (robustní), aby vydržely předvídatelný dopad mimořádné události. V jiných případech robustnost vyžaduje náhradní nebo redundantní systém, který lze využít v situacích, kdy něco důležitého přestane pracovat.

1.6.5 Rezistence

Cílem rezistence (Resistence) je vytvořit takové změny, které mohou zabránit poškození nebo narušení, popř. snížit vliv a dopady hrozeb. Výchozím aspektem pro tento cíl jsou skutečnosti, které byly dříve zažity, nebo také skutečnosti, které lze předpovědět na základě historických záznamů.

1.6.6 Reakce-schopnost

Reakce-schopnost (Responsiveness) je oblast, která představuje způsobilost systému k aktivaci sil a prostředků směřujících k obnově funkce infrastrukturního systému. Vyjadřuje se dobou mezi vznikem mimořádné události a zahájením eliminace degradace funkce a následně i její obnovou.

1.6.7 Obnovitelnost

Obnovitelnost (Recoverability) jako rychlá obnova (Rapid recovery) neboli rychlé zotavení je schopnost získat věci zpět k normálu tak rychle, jak je to jen možné. Obnovitelnost je v

některých publikacích definována také jako rychlost zotavení, kdy zotavení může trvat v řádech několika hodin až týdnů.

1.6.8 Adaptabilita

Adaptabilita (adaptability) je soubor vlastností, které charakterizují schopnost systému přijmout změnu, resp. vyhledávat strategie, jak se vypořádat s neznámem. Jedná se o důležitou vlastnost, resp. složku odolnosti, která umožňuje systému reagovat na změny.

Navzdory měnícím se potřebám moderní společnosti jsou základní potřeby obyvatelstva stejné, bez geografického omezení. Těmito potřebami jsou zejména pitná voda, dýchatelný vzduch, strava, teplo, bezpečnost apod. Tyto základní potřeby plní infrastrukturní systémy, které jsou pro člověka z pohledu přežití kritické. Na naplňování základních, a tedy životních potřeb se podílejí určené sektory infrastrukturních systémů, primární energetika, ICT a doprava. Další potřeby člověka (odpočinek, vyprazdňování, čistota, jistota, bezpečí aj.) mohou plnit další sektory. potravinářství a zemědělství, zdravotnictví, finanční trh a měna nebo nouzové služby a veřejná správa. Každá moderní společnost se primárně zabývá infrastrukturou, která plní potřeby jejího obyvatelstva, a to podle jejich vyspělosti a požadavků.

Z toho vyplývá, že každý společensky významný infrastrukturní systém by měl být odolný a měl by mít dostatečnou kapacitu zabránit vzniku nebo rozšíření krize, absorbovat dopady a zkrátit dobu obnovy.

Odolnost a nároky na ni se v čase mění a mění se i různé cíle. Definice a vnímání odolnosti by mělo zahrnovat zmínku o dynamice procesů jejího utváření a zvyšování. Tato kapitola měla proto ambici vytvořit obecný exkurz do širšího spektra vnímání odolnosti a popsat oblasti a jejich vazby které předmětnou problematiku utvářejí.

1.7 Konvergovaná bezpečnost

V současnosti fungují jednotlivé druhy bezpečnosti samostatně a nezávisle na ostatních druzích bezpečnosti. Tento způsob zajištění bezpečnosti má řadu negativ. Mezi základní negativa uvedené situace patří nemožnost propojit demaskující příznaky vznikajícího narušení bezpečnosti, detekované senzory v jednotlivých druzích bezpečnosti, v jeden celek. Dalším negativem výše uvedené situace jsou zvyšující se náklady na zajištění bezpečnosti, plynoucí z nezávislého zajištění jednotlivých druhů bezpečnosti. To se projevuje jak v technologické

stránce, tak zejména v personální stránce. Každý druh bezpečnosti je obvykle zajišťován samostatnou skupinou odborníků, má vlastní bezpečnostní technologie a vlastní ochranné procesy, vlastní finanční rozpočet.

V současnosti se z praktických důvodů ukazuje, že je potřeba hledat cesty pro slučování jednotlivých druhů bezpečnosti do jednoho celku. Tento trend vyústil v koncept konvergované bezpečnosti. ***Konvergovaná bezpečnost představuje specifický druh bezpečnosti, vzniklý sloučením více slučitelných druhů bezpečnosti do jednoho celku.*** Takovýto druh bezpečnosti umožňuje díky analýze souvztažnosti projevů narušení bezpečnosti dříve (ještě ve stádiu příznaků), rychleji a lépe odhalit vznikající narušení bezpečnosti a cíleněji zajistit jeho řešení. Konvergovaná bezpečnost obvykle zahrnuje fyzickou bezpečnost, kybernetickou bezpečnost a provozní bezpečnost. Struktura slučovaných druhů bezpečnosti může být i jiná. Vše záleží na potřebách referenčního objektu i nezbytnosti slučitelnosti jednotlivých druhů bezpečnosti. Zmíněná slučitelnost vychází především z potřeby ochrany stejných aktiv referenčního objektu. Další podmínkou slučitelnosti jsou časové charakteristiky projevů narušení bezpečnosti, které by měly být v přibližně stejných intencích. V rámci výše uvedeného příkladu konvergované bezpečnosti budou projevy v časovém rozmezí vteřin – minut – hodin. Pokud by došlo k sloučení druhů bezpečnosti, kdy u jednoho dochází ke změnám v minutách a v dalším v letech, pak by sloučení do konvergované bezpečnosti postrádalo smysl, protože dominantní roli by sehrával druh bezpečnosti s časově krátkými změnami.

Základní principy, na nichž je konvergovaná bezpečnost postavena:

- konvergovaná bezpečnost se zajišťuje pro určitý (společný) referenční objekt,
- do konvergované bezpečnosti lze zahrnout pouze slučitelné druhy bezpečnosti,
- je žádoucí, aby zahrnuté druhy bezpečnosti chránily shodná nebo alespoň částečně shodná aktiva,
- dopady působení hrozeb nesmí být protichůdné a projevují se na aktivech referenčního objektu negativně,
- všechny hrozby můžou mít pro referenční objekt existenciální dopady.

Z výše uvedených principů plyne, že konvergovaná bezpečnost se zajišťuje u společného referenčního objektu. Tento referenční objekt má jedno nebo několik aktiv a všechny zahrnuté druhy bezpečnosti se podílí na zajištění jejich bezpečnosti. Konvergovaná bezpečnost

slučuje tyto druhy bezpečnosti v jeden celek. To umožňuje vyhodnocovat stav bezpečnostní situace jako jeden obraz, v němž se promítají všechny dílčí bezpečnostní situace jednotlivých druhů bezpečnosti. Přidanou hodnotou sloučení dříve nezávislých druhů bezpečnosti je možnost vnímání souvztažnosti jednotlivých projevů narušení bezpečnosti v jeden celek, rychlejší odhalení narušení bezpečnosti, jeho způsobu, rozsahu a predikce možného scénáře dalšího průběhu. Mezi další významné přínosy konvergované bezpečnosti patří komplexní a aktuální hodnocení bezpečnostní situace. Toto hodnocení umožňuje bezpečnostní situaci adekvátně řešit a tím minimalizovat negativní dopady narušení bezpečnosti. Z pohledu referenčního objektu se stav bezpečnostní situace hodnotí nejčastěji pomocí stavu odolnosti jeho systému ochrany (bezpečnostního systému), případně odolnosti referenčního objektu jako takového. Pro konvergovanou bezpečnost platí, že se u ní hodnotí odolnost systému ochrany. Neposuzuje se stav naplňování cílové funkce referenčního objektu, ale stav ochrany aktiv referenčního objektu prostřednictvím systému ochrany referenčního objektu. Systém ochrany je tvořen opatřeními, přijatými v jednotlivých druzích bezpečnosti.

1.7.1 Podstata hodnocení odolnosti z pohledu konvergované bezpečnosti

Konvergovaná bezpečnost představuje specifický druh bezpečnosti, jehož cílem je ochránit aktiva referenčního objektu vůči bezpečnostním hrozbám, zahrnutým pro více druhů bezpečnosti. V popisované metodice zahrnuje konvergovaná bezpečnost fyzickou bezpečnost, kybernetickou bezpečnost a provozní bezpečnost. Fyzická bezpečnost ochraňuje vůči hrozbám fyzického charakteru. Mezi hlavní bezpečnostní hrozby, spadající do kategorie fyzického charakteru, patří krádež vloupáním, sabotáž, vandalismus, teroristický útok, požár atd. Kybernetická bezpečnost zajišťuje ochranu aktiv vůči hrozbám kybernetického prostoru. Jedná se především o zajištění důvěrnosti, integrity a dostupnosti aktiv (dat, služeb, prostředků atd.). Mezi hlavní hrozby patří kyberkriminalita, hacktivismus, kybernetická válka nebo kybernetická špionáž. Tyto hrozby lze také charakterizovat jako záměrné a nežádoucí aktivity, které jsou z pohledu referenčního objektu spojeny s nedostupností, mazáním, modifikací či kopírováním jeho dat, přetěžováním systémů, šířením škodlivého kódu atd.

Provozní bezpečnost je spojena se zajišťováním naplňování cílové funkce organizace. Cílem je vytvořit při zajišťování cílové funkce organizace / podniku takové podmínky, aby nedocházelo k omezování či zastavení provozu. Zajištění provozní bezpečnosti závisí na konkrétnostech realizace cílové funkce. Jiná opatření budou v dopravě či energetice a jiná ve veřejné

správě. Na rozdíl od výše uvedených druhů bezpečnosti je problematika provozní bezpečnosti nová a postupně se utváří.

Odolnost systému ochrany referenčního objektu z pohledu konvergované bezpečnosti představuje schopnost opatření, realizovaných v jednotlivých druzích bezpečnosti (zahrnutých do konvergované bezpečnosti) ochránit jeho aktiva a zajistit tak naplňování cílové funkce referenčního objektu. Hodnocení odolnosti by mělo odrážet její aktuální stav. Stav odolnosti jako vlastnosti referenčního objektu lze sledovat prostřednictvím snímání projevů či změn vnějších a vnitřních faktorů (činitelů).

Obecně platí, že každá změna se může do odolnosti promítnout kvalitativně nebo kvantitativně, a proto může být ohodnocena vlivy a dopady na odolnost referenčního objektu. Hodnocení odolnosti může být založeno na snímání těch změn stavu faktorů (činitelů), které se do změn odolnosti promítají podstatně. Míra vlivu na odolnost může být při tom odstupňována kvantitativně. Může být vyjádřena jako penalizace čili snížení odolnosti. Podstata hodnocení odolnosti z pohledu konvergované bezpečnosti s využitím penalizace je založena na následujících principech:

- odolnost z pohledu konvergované bezpečnosti závisí na ochranných vlastnostech systému ochrany referenčního objektu, jejich stavu a současně na stavu, intenzitě a podmínkách působení škodícího účinku na referenční objekt,
- změny odolnosti systému ochrany i působení škodícího účinku mají statický nebo dynamický charakter,
- změny odolnosti lze vymezit událostmi (s časem vzniku / zániku),
- odolnost systému ochrany lze hodnotit semikvantitativně společným ekvivalentem, který se nazývá penalizace,
- penalizace se vztahuje k jednotlivým faktorům (vnějším a vnitřním činitelům),
- penalizace představuje číslo, v jehož velikosti se odráží míra závažnosti vlivu faktoru (úrovni působení škodícího účinku) na referenční objekt a jeho aktiva,
- penalizace se určuje pro jednotlivé druhy bezpečnosti,
- penalizace může být vztažena jak k jednotlivým aktivům, tak centrálně na celý referenční objekt,
- vliv jednotlivých penalizací na jednom aktivu (vyvolaný stejnou událostí) by se neměl překrývat,

- velikost odolnosti by měla být vyjádřena v určitém rozmezí hodnot (např. 100–0), případně omezená alespoň z jedné strany maximální hodnotou (100).

V rámci výpočtu indexů odolnosti referenčního objektu I_{ro} se pracuje s penalizačními faktory, které jsou uvedeny v katalozích penalizačních faktorů. Vychází se při tom z obecných katalogů penalizačních faktorů. V další části této podkapitoly je uveden postup práce s katalogy penalizačních faktorů a penalizacemi při výpočtu indexů odolnosti aktiv pro jednotlivé druhy bezpečnosti. Klíčové je především provedení prioritizace obecné hodnoty penalizace daného penalizačního faktoru na podmínky hodnoceného aktiva. Tato prioritizace se provádí z důvodu posouzení vlivu faktoru na skutečné podmínky aktiva v konkrétním referenčním objektu.

V obecném katalogu penalizačních faktorů je velikost penalizace stanovena obecně. Pomocí váhy bude možné v katalogu penalizačních faktorů aktiva zvýšit nebo snížit velikost penalizace v závislosti na tom, jaké dopady ve skutečnosti faktor na aktivum má. Váha se stanovuje v rozmezí 1–5, přičemž hodnota 3 předpokládá normální dopad. Hodnota 1 znamená, že faktor má na aktivum menší vliv a dopad, hodnota 5 znamená maximální dopad.

Postup:

a) specifikace referenčního objektu,
b) specifikace aktiv, které referenční objekt zahrnuje,
c) vytvoření výchozího katalogu penalizačních faktorů zahrnujícího všechny druhy bezpečnosti,
d) zpřesnění katalogu penalizačních faktorů pro jednotlivá aktiva zahrnujícího všechny druhy bezpečnosti,
e) výpočet indexu odolnosti aktiva pro jednotlivé druhy bezpečnosti,
f) výpočet indexu odolnosti pro druh bezpečnosti,
g) výpočet indexu odolnosti pro celý referenční objekt.

1.8 Penalizační faktory

Konvergovaná bezpečnost představuje specifický přístup k řešení problémů zajištění bezpečnosti v referenčních objektech, přičemž jsou integrovány, analyzovány a vyhodnocovány slučitelné druhy bezpečnosti v jeden celek (zpravidla se integruje fyzická, kybernetická a

provozní bezpečnost). Schopnost referenčního objektu chránit aktiva a zvládat narušení bezpečnosti je vyjádřena jeho odolností, která vyjadřuje, jak je objekt schopen vzdorovat působení škodícího účinku a jak ochraňuje svoje aktiva.

V této souvislosti je možno definovat metodu penalizace jako postup pro hodnocení odolnosti objektů z hlediska druhů bezpečnosti a tím i bezpečnosti konvergované. Metoda penalizace tedy představuje nástroj pro sledování stavu opatření a tím i stupně ochrany aktiv.

V rámci hodnocení odolnosti fyzické bezpečnosti referenčního objektu je využíván katalog penalizačních faktorů, který zahrnuje statické faktory a dynamické faktory.

Účelem obecného katalogu penalizačních faktorů je vytvoření přehledu všech potencionálních vnějších a vnitřních činitelů (faktorů), který je využit v rámci vyhodnocování odolnosti konkrétního referenčního objektu v následujících etapách:

h) vytvoření výchozího katalogu penalizačních faktorů pro vybraný konkrétní referenční objekt, zahrnujícího všechny druhy bezpečnosti (výběrem faktorů z obecného katalogu – na základě znalosti referenčního objektu, aktiv, vnějších a vnitřních konfiguračních a ochranných činitelů bude vytvořen přehled penalizačních faktorů, odrážejících stav odolnosti a stupeň ohrožení referenčního objektu),
i) zpřesnění katalogu penalizačních faktorů pro jednotlivá aktiva v objektu, zahrnujícího všechny druhy bezpečnosti,
j) výpočet indexu odolnosti aktiva pro jednotlivé druhy bezpečnosti,
k) výpočet indexu odolnosti pro celý referenční objekt.

Stěžejním cílem procesu určování penalizačních faktorů je vytvoření obecného katalogu penalizačních faktorů z pohledu konvergované bezpečnosti, která zahrnuje penalizační faktory pro provozní bezpečnost, fyzickou bezpečnost a kybernetickou bezpečnost. Vytvořený obecný katalog penalizačních faktorů bude obsahovat maximum statických a dynamických faktorů, využitelných pro hodnocení odolnosti referenčních objektů a jejich aktiv. V rámci hodnocení vybraného referenčního objektu a jeho jednotlivých aktiv budou z obecného katalogu vybrány ty penalizační faktory, které skutečně mají vliv na ochranu těchto aktiv a pro něž bude rozumné odolnost hodnotit (katalog bude obsahovat pouze faktory, jež bude potřebné snímat a brát do úvahy pro hodnocení odolnosti konkrétního aktiva) [6].

K jednotlivým faktorům budou ještě přiřazeny váhy (1–5) k penalizacím pro každé aktivum zvlášť, aby byl zohledněn dopad jednotlivých faktorů na odolnost aktiva. Bude vytvořeno tolik katalogů penalizačních faktorů, kolik je aktiv (při větším počtu aktiv budou vybrána jenom klíčová aktiva).

Obecný katalog penalizačních faktorů se skládá ze tří částí:

- fyzická bezpečnost,
- kybernetická bezpečnost,
- provozní bezpečnost.

Každá část katalogu je dále rozdělena na:

- statické faktory,
- dynamické faktory.

Vhodným zdrojem pro zpracování výčtu penalizačních faktorů jsou různé seznamy hrozeb a popisy systémů ochrany. K tvorbě takových seznamů může být použita projektová dokumentace poplachových systémů, počítačových sítí a systémů jejich ochrany atd. Lze rovněž využít výsledky bezpečnostních posouzení a bezpečnostních auditů.

1.9 Závěr kapitoly

Oblast bezpečnosti patří mezi významné priority lidské společnosti. Ve své podstatě se dotýká téměř všech jejích oborů i úrovní. Díky rozvoji technologií a institucionalizaci bezpečnosti existuje v současnosti více jak padesát druhů bezpečnosti. To způsobuje v organizacích řadu problémů, zejména v oblasti vyhodnocování souvztažnosti bezpečnostních incidentů, rozsáhlosti bezpečnostního managementu a nákladů na zajištění bezpečnosti. Bezpečnostní komunita hledá způsoby, jak vzniklý problém řešit. Jedním ze způsobů řešení uvedeného problému je konvergence vybraných druhů bezpečnosti v jeden celek. Mezi nejdůležitější poznatky a závěry patří specifikace konceptu konvergované bezpečnosti, algoritmus pro hodnocení odolnosti z pohledu konvergované bezpečnosti a definice „penalizace“. Právě penalizace, v níž se odráží míra významu jednotlivých událostí na snižování odolnosti, patří mezi slibná témata pro budoucí výzkum.

1.10 Hodnocení

Ochrana a odolnost kritické infrastruktury s využitím přístupů ku konvergenci druhů bezpečnosti je relativně novodobým přístupem k objektivizaci procesu hodnocení bezpečnosti/odolnosti a optimalizaci systému řízení rizik v těchto infrastrukturních systémech. Prezentované skutečnosti jsou ve své podstatě využitelné pro pozici Security liaison officer subjektu kritické infrastruktury.

1.11 Možný vývoj

Možný vývoj:

- Tvorba informační podpory pro predikci vývoje bezpečnostního problému,
- Zjednodušení a objektivizace nasazení relevantních opatření,
- Automatizace konvergované bezpečnosti.

2 SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY O POSÍLENÍ ODOLNOSTI KRITICKÝCH SUBJEKTŮ

Druhá kapitola této aktualizované verze cestovní mapy projektu bude analyzovat a do jisté míry i syntetizovat skutečnosti související a předcházející procesu tvorby a implementace připravované Směrnice Evropského parlamentu a rady o posílení odolnosti kritických subjektů.

Lze obecně konstatovat, že předmětná Směrnice bude mít zásadní vliv na bezpečnost a odolnosti kritických infrastruktury s jistou paralelou na již přijatou směrnici 2008/114/ES.

2.1 Odůvodnění a cíle návrhu

Obecně se dá konstatovat, že tvorba Směrnice byla podmíněna faktem, že životní podmínky evropských občanů a dobré fungování vnitřního trhu závisí na různých infrastrukturách, které musí spolehlivě poskytovat služby potřebné k zachování kritických společenských a hospodářských činností. Tyto služby, které jsou za normálních okolností životně důležité, jsou o to důležitější v době, kdy se Evropa snaží zvládnout dopady pandemie COVID-19 a kdy usiluje o to, aby se z této pandemie zotavila. Z toho vyplývá, že subjekty poskytující základní služby musí být odolné, tj. schopné odolat incidentům, které mohou vést k vážným narušením napříč odvětvími a hranicemi, dále musí být schopné tyto incidenty absorbovat, přizpůsobit se jim a zotavit se z nich.

Cílem tohoto návrhu je posílit poskytování služeb nezbytných pro zachování nejdůležitějších společenských funkcí nebo hospodářských činností na vnitřním trhu, a to prostřednictvím posílení odolnosti kritických subjektů poskytujících tyto služby.

Návrh dále zohledňuje vnitrostátní přístupy objevující se ve stále větším počtu členských států, které mají tendenci klást důraz na vzájemnou propojenost napříč odvětvími a hranicemi a které stále více uvažují o posílení odolnosti, kde je jedním z prvků ochrana, vedle prevence a zmírňování rizik, kontinuity činnosti a obnovy.

K dnešnímu dni bylo určeno 94 EKI, z nichž dvě třetiny se nacházejí ve třech členských státech ve střední a východní Evropě. Rozsah opatření EU v oblasti posilování odolnosti kritické infrastruktury však přesahuje tato opatření a zahrnuje opatření v rámci odvětví i napříč odvětvími týkající se mimo jiné posilování odolnosti vůči klimatickým změnám,

civilní ochrany, přímých zahraničních investic a kybernetické bezpečnosti[6]. Samotné členské státy mezitím přijaly v této oblasti vlastní opatření, která se od sebe navzájem liší.

Je proto zřejmé, že současný rámec ochrany kritické infrastruktury nestačí k řešení aktuálních výzev kritických infrastruktur a subjektů, které je provozují. Vzhledem k narůstajícímu propojení infrastruktur, sítí a provozovatelů poskytujících základní služby na vnitřním trhu je nutné zásadně změnit současný přístup od ochrany konkrétního majetku k posílení odolnosti kritických subjektů, které je provozují.

Jak dokazuje hodnocení směrnice o EKI[7] z roku 2019, stávající evropská a vnitrostátní opatření jsou omezená, pokud jde o pomoc provozovatelům postavit se provozním výzvám, kterým v současné době čelí, a zranitelnostem, které s sebou nese jejich vzájemně závislá povaha.

Existuje pro to několik důvodů, které jsou uvedeny v posouzení dopadů, které podpořilo vývoj tohoto návrhu. Zaprvé si provozovatelé plně neuvědomují dopady prostředí dynamického rizika, ve kterém působí, nebo jim plně nerozumí. Zadruhé se úsilí v oblasti odolnosti mezi členskými státy a odvětvími významně liší. Zatřetí jsou podobné typy subjektů některými členskými státy uznávány jako kritické, jinými však nikoli, což znamená, že srovnatelné subjekty dostávají různé stupně oficiální podpory budování kapacit (v podobě např. pokynů, organizace školení a výcviku) podle toho, kde v Unii působí, a podléhají různým požadavkům. Skutečnost, že se požadavky a vládní podpora provozovatelům v jednotlivých členských státech liší, vytváří pro provozovatele překážky v rámci přeshraničního působení, zejména u klíčových subjektů působících v členských státech s přísnějšími požadavky. Vzhledem k narůstající propojenosti poskytování služeb a odvětví v členských státech a v celé EU představuje nedostatečná úroveň odolnosti jednoho provozovatele vážné riziko pro subjekty v jiné části vnitřního trhu.

---

[6] Sdělení Komise o strategii EU pro přizpůsobení se změně klimatu COM(2013) 216, rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU ze dne 17. prosince 2013 o mechanismu civilní ochrany Unie, nařízení Evropského parlamentu a Rady (EU) 2019/452, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie, směrnice 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

[7] SWD(2019) 308.

2.2 Vybrané aspekty stavu řešení otázek bezpečnosti

Táto podkapitola v odrážkách formuluje vybrané aspekty současného stavu pragmatického řešení otázek bezpečnosti a odolnosti v systému kritické infrastruktury. Mezi nejvýznamnější poznatky lze zařadit:

- Navzdory stávajícím opatřením na úrovni Unie[8] a na vnitrostátní úrovni zaměřeným na podporu ochrany kritických infrastruktur v Unii nejsou subjekty provozující tyto infrastruktury dostatečně vybavené k řešení stávajících a předpokládaných budoucích rizik pro jejich provoz, které mohou vést k narušení poskytování služeb, které jsou zásadní pro výkon nejdůležitějších společenských funkcí nebo hospodářských činností.
- Narůstající vzájemná závislost je výsledkem stále častější přeshraniční a vzájemně závislé sítě poskytování služeb využívající klíčové infrastruktury v celé Unii. Tyto vzájemné závislosti znamenají, že jakékoli narušení, dokonce i když se původně omezilo na jeden subjekt nebo jedno odvětví, může mít v širším měřítku kaskádové účinky, což může mít za následek dalekosáhlé a dlouhodobé nepříznivé dopady na poskytování služeb na vnitřním trhu.
- Na subjekty zapojené do poskytování základních služeb se stále více vztahují odlišné požadavky stanovené právními předpisy členských států. Skutečnost, že některé členské státy mají na tyto subjekty méně přísné bezpečnostní požadavky, nejen že může mít nepříznivý dopad na zachování nejdůležitějších společenských funkcí nebo hospodářských činností v celé Unii, ale také vede k překážkám řádného fungování vnitřního trhu.
- Je proto nezbytné stanovit minimální harmonizovaná pravidla, která zajistí poskytování základních služeb na vnitřním trhu a posílí odolnost kritických subjektů.
- S cílem zajistit komplexní přístup k posílení odolnosti kritických subjektů by každý členský stát měl mít strategii stanovující cíle a politická opatření, která mají být provedena.

---

[8] Evropský program na ochranu kritické infrastruktury (Evropský program OKI).

- Opatření členských států zaměřená na určení a pomoc při zajišťování odolnosti kritických subjektů by se měla řídit přístupem založeným na analýze rizik, který je zaměřen na úsilí subjektů, která jsou pro výkon nejdůležitějších společenských funkcí nebo hospodářských činností nejpodstatnější. V zájmu zajištění takového cíleného přístupu by měl každý členský stát v harmonizovaném rámci provést posouzení všech příslušných přírodních rizik a rizik způsobených člověkem, která mohou poskytování základních služeb ovlivnit, včetně havárií, přírodních katastrof, mimořádných událostí v oblasti veřejného zdraví, jako je pandemie, a nepřátelských hrozeb, včetně teroristických trestných činů.
- Členské státy by měly určit orgány příslušné k dohledu nad uplatňováním této směrnice a v případě nutnosti k prosazování jejích pravidel a zajistit, aby tyto orgány měly odpovídající zmocnění a zdroje.
- Aby se usnadnila přeshraniční spolupráce a komunikace a umožnilo se účinné provádění této směrnice, měl by každý členský stát, aniž by byly dotčeny právní požadavky Unie v rámci odvětví, určit v rámci jednoho z orgánů, které určil jako příslušný orgán podle této směrnice, jednotné kontaktní místo odpovědné za koordinaci záležitostí souvisejících s odolností kritických subjektů a přeshraniční spoluprací v tomto ohledu na úrovni Unie.
- Aby se usnadnila přeshraniční spolupráce a komunikace a umožnilo se účinné provádění této směrnice, měl by každý členský stát, aniž by byly dotčeny právní požadavky Unie v rámci odvětví, určit v rámci jednoho z orgánů, které určil jako příslušný orgán podle této směrnice, jednotné kontaktní místo odpovědné za koordinaci záležitostí souvisejících s odolností kritických subjektů a přeshraniční spoluprací v tomto ohledu na úrovni Unie.
- Kritické subjekty by měly za účelem zajištění své odolnosti mít komplexní povědomí o všech příslušných rizicích, jimž jsou vystavovány, a tato rizika analyzovat. Za tímto účelem by měly provádět posouzení rizik, kdykoli je to nutné s ohledem na jejich konkrétní situaci a vývoj těchto rizik, avšak v každopádně každé čtyři roky. Posouzení rizik kritickými subjekty by mělo vycházet z posouzení rizik provedeného členskými státy.

- Kritické subjekty by měly přijmout organizační a technická opatření, která jsou vhodná a přiměřená rizikům, jimž čelí, aby zamezily incidentům, odolávaly jim, zmírňovaly je, absorbovaly je, přizpůsobily se jim a zotavily se z nich.
- Umožnit kritickým subjektům požadovat ověření spolehlivosti u osob spadajících do konkrétních kategorií jejich zaměstnanců a zajistit, aby tyto žádosti byly rychle posouzeny příslušnými orgány v souladu s platnými pravidly unijního a vnitrostátního práva, včetně práva na ochranu osobních údajů.
- Kritické subjekty by měly co nejdříve za daných okolností hlásit příslušným orgánům členských států incidenty, které významně narušují nebo mohou významně narušit jejich provoz. Hlášení by mělo příslušným orgánům umožnit rychle a adekvátně reagovat na incidenty a mít komplexní přehled o celkových rizicích, kterým kritické subjekty čelí.
- Členské státy by měly zajistit, aby jejich příslušné orgány měly ve vztahu ke kritickým subjektům určité zvláštní pravomoci pro řádné uplatňování a prosazování této směrnice, pokud tyto subjekty spadají do jejich působnosti stanovené v této směrnici. Mezi tyto pravomoci by měla patřit zejména pravomoc provádět inspekce, dohled a audity, vyžadovat, aby kritické subjekty poskytly informace a důkazy o opatřeních, která přijaly za účelem splnění svých povinností, a v případě potřeby vydávat příkazy k nápravě zjištěných porušení těchto povinností.

2.3 Strategie pro posílení odolnosti kritických subjektů

Každý členský stát přijme do [tří let po vstupu této směrnice v platnost] strategii pro posílení odolnosti kritických subjektů.

Tato strategie bude obsahovat alespoň tyto prvky:

a) strategické cíle a priority za účelem posílení celkové odolnosti kritických subjektů s přihlédnutím k přeshraniční vzájemné přeshraniční a meziodvětvové závislosti;
b) správní rámec pro naplnění cílů a priorit, včetně popisu úlohy a povinností různých orgánů, kritických subjektů a dalších stran zapojených do provádění této strategie;
c) popis opatření nezbytných k posílení celkové odolnosti kritických subjektů, včetně vnitrostátního posouzení rizik, určení kritických subjektů a subjektů rovnocenných kritickým subjektům, a opatření na podporu kritických subjektů přijatá v souladu s touto kapitolou;

d) politický rámec pro posílenou koordinaci mezi příslušnými orgány určenými podle článku 8 této směrnice a podle [směrnice o bezpečnosti sítí a informací 2] pro účely sdílení informací o incidentech a kybernetických hrozbách a výkonu úkolů v oblasti dohledu.

Strategie se podle potřeby aktualizuje, nejméně však každé čtyři roky.

2.4 Posouzení rizik členskými státy

Do [tří let po vstupu této směrnice v platnost], v případě potřeby a nejméně každé čtyři roky provedou posouzení všech příslušných rizik, která mohou mít dopad na poskytování těchto základních služeb, s cílem určit kritické subjekty.

Posouzení rizik zohlední všechna příslušná přírodní a člověkem způsobená rizika, včetně havárií, přírodních katastrof, mimořádných událostí v oblasti veřejného zdraví, nepřátelských hrozeb, včetně teroristických trestných činů.

Při provádění posouzení rizik vezmou členské státy v úvahu alespoň:

a) obecné posouzení rizik provedené podle čl. 6 odst. 1 rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU9;
b) další příslušná posouzení rizik prováděná v souladu s požadavky příslušných odvětvových právních aktů Unie, včetně nařízení Evropského parlamentu a Rady (EU) 2019/94110 a nařízení Evropského parlamentu a Rady (EU) 2017/1938 Parlamentu a Rady11;
c) veškerá rizika vyplývající z meziodvětvových závislostí uvedených v příloze, včetně rizik pocházejících z jiných členských států a třetích zemí, a dopad, který může narušení v jednom odvětví mít na ostatní odvětví;
d) veškeré informace o incidentech ohlášených v souladu s článkem 13.

---

[9] Rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU ze dne 17. prosince 2013 o mechanismu civilní ochrany Unie (Úř. věst. L 347, 20.12.2013, s. 924).

[10] Nařízení Evropského parlamentu a Rady (EU) 2019/941 ze dne středa 5. června 2019 o rizikové připravenosti v odvětví elektroenergetiky a o zrušení směrnice 2005/89/ES (Úř. věst. L 158, 14.6.2019, s. 1).

[11] Nařízení Evropského parlamentu a Rady (EU) 2017/1938 ze dne 25. října 2017 o opatřeních na zajištění bezpečnosti dodávek zemního plynu a o zrušení nařízení (EU) č. 994/2010 (Úř. věst. L 280, 28.10.2017, s. 1).

2.5 Určení kritických subjektů

Do [tří let a tří měsíců po vstupu této směrnice v platnost] členské státy určí kritické subjekty pro každé odvětví a pododvětví uvedené v příloze Směrnice. Bude se převažne jednat o formulaci kritérií:

a) subjekt poskytuje jednu nebo více základních služeb;
b) poskytování této služby závisí na infrastruktuře umístěné v členském státě; a
c) incident by významně narušil poskytování služby nebo jiných základních služeb v odvětvích uvedených v příloze, která na službě závisí.

Každý členský stát vytvoří seznam určených kritických subjektů a zajistí, aby tyto kritické subjekty byly informovány o svém určení jako kritických subjektů do jednoho měsíce od tohoto určení, přičemž budou rovněž informovány o svých povinnostech.

2.6 Významné narušení

Při určování významnosti narušení členské státy zváží tyto okolnosti:

a) počet uživatelů, kteří jsou závislí na službě poskytované daným subjektem;
b) závislost dalších odvětví podle přílohy II na této službě;
c) možný dopad incidentů, pokud jde o jejich intenzitu a délku trvání, na ekonomické a společenské činnosti, na životní prostředí nebo na veřejnou bezpečnost;
d) podíl tohoto subjektu na trhu s takovýmito službami;
e) zeměpisnou oblast, která by mohla být incidentem ovlivněna, včetně případných přeshraničních dopadů;
f) důležitost subjektu, pokud jde o udržování dostatečné úrovně dané služby, s přihlédnutím k dostupnosti alternativních způsobů zajištění této služby.

Členské státy předloží Komisi do [tří let a tří měsíců po vstupu této směrnice v platnost] tyto informace:

a) seznam služeb;
b) počet kritických subjektů určených pro každé odvětví a pododvětví uvedené v příloze a službu nebo služby uvedené v čl. 4 odst. 1, které každý subjekt poskytuje;
c) případné mezní hodnoty použité k upřesnění jednoho nebo více kritérií.

2.7 Příslušné orgány a jednotné kontaktní místo

Každý členský stát určí jeden nebo více příslušných orgánů odpovědných za správné uplatňování této směrnice na vnitrostátní úrovni a v případě potřeby vymáhání pravidel v této směrnici uvedených.

Každý členský stát určí v rámci příslušného orgánu jednotné kontaktní místo pro výkon styčné funkce k zajištění přeshraniční spolupráce s příslušnými orgány jiných členských států a se skupinou pro posílení odolnosti kritických subjektů.

Každý členský stát oznámí Komisi určení příslušného orgánu a jednotného kontaktního místa do tří měsíců od tohoto určení, včetně jejich přesných úkolů a povinností podle této směrnice, jejich kontaktních údajů a veškerých následných změn. Každý členský stát zveřejní určení příslušného orgánu a jednotného kontaktního místa.

2.8 Podpora členských států kritickým subjektům

Členské státy podpoří kritické subjekty při posilování jejich odolnosti. Tato podpora může zahrnovat vypracování poradenských materiálů a metodik, podporu organizace cvičení sloužícího k otestování jejich odolnosti a zaměstnancům kritických subjektů poskytovat školení.

2.9 Posouzení rizik kritickými subjekty

Posouzení rizik zohlední všechna příslušná rizika, která by mohla vést k narušení poskytování základních služeb. Zohlední i případnou závislost jiných odvětví uvedených v příloze na základní službě poskytované kritickým subjektem, včetně odvětví v sousedních členských státech a případně třetích zemích, a dopad, který narušení poskytování základních služeb v jednom nebo více z těchto odvětví může mít na základní službu poskytovanou kritickým subjektem.

2.10 Opatření k zajištění posílení odolnosti kritických subjektů

Členské státy zajistí, aby kritické subjekty přijaly vhodná a přiměřená technická a organizační opatření k zajištění posílení své odolnosti, včetně opatření nezbytných za účelem:

a) předcházení vzniku incidentů, mimo jiné prostřednictvím snižování rizika katastrof a opatření na přizpůsobení se změně klimatu;
b) zajištění přiměřené fyzické ochrany citlivých oblastí, zařízení a další infrastruktury, včetně oplocení, bariér, nástrojů a postupů pro monitorování hranic objektu, jakož i detekčních zařízení a kontrol přístupu;
c) odolávání a zmírňování důsledků incidentů, včetně provádění postupů a protokolů pro řízení rizik a krizí a výstražných postupů;
d) zotavení se z incidentů, včetně opatření pro zajištění kontinuity činnosti a určení alternativních dodavatelských řetězců;
e) zajištění přiměřeného řízení bezpečnosti zaměstnanců, mimo jiné stanovením kategorií zaměstnanců vykonávajících zásadní funkce, stanovením přístupových práv k citlivým oblastem, zařízením a jiné infrastruktuře a citlivým informacím, jakož i určením konkrétních kategorií zaměstnanců;
f) zvyšování povědomí příslušných pracovníků o opatřeních.

Členské státy zajistí, aby kritické subjekty zavedly a používaly plán odolnosti nebo rovnocenný dokument či dokumenty, kde budou podrobně popsána opatření.

2.11 Ověření spolehlivosti

Členské státy zajistí, aby kritické subjekty mohly podávat žádosti o ověření spolehlivosti u osob, které spadají do určitých konkrétních kategorií jejich zaměstnanců, včetně osob, u kterých se zvažuje, že budou přijaty na pozice spadající do těchto kategorií, a aby tyto žádosti byly urychleně posouzeny orgány příslušnými k provádění takovýchto ověření spolehlivosti.

V souladu s příslušnými právními předpisy Unie a vnitrostátními právními předpisy se v rámci ověření spolehlivosti:

a) určí totožnost dotčené osoby na základě písemných dokladů;
b) uvedou případné záznamy v rejstříku trestů nejméně za posledních pět let a nejvýše deset let týkající se trestných činů souvisejících s náborem na konkrétní pozici v členském státě nebo členských státech, jejichž je tato osoba státním příslušníkem, a v kterémkoli z členských států nebo třetí zemi, kde má během tohoto období pobyt;
c) uvede předchozí zaměstnání, vzdělání a případné mezery ve vzdělání nebo zaměstnání v životopisu osoby za posledních nejméně pět let a nejvýše deset let.

2.12 Hlášení o incidentech

Členské státy zajistí, aby kritické subjekty informovaly příslušný orgán o incidentech, které významně narušují nebo mohou významně narušit jejich provoz. Hlášení musí obsahovat veškeré dostupné informace nezbytné k tomu, aby příslušný orgán mohl pochopit povahu, příčinu a možné důsledky incidentu, a to i za účelem stanovení případného přeshraničního dopadu incidentu. Takové hlášení nezakládá u kritického subjektu vyšší míru právní odpovědnosti.

K určení závažnosti narušení nebo možného narušení provozu kritického subjektu v důsledku incidentu je třeba vzít v úvahu zejména tyto parametry:

a) počet uživatelů postižených narušením nebo možným narušením;
b) doba trvání narušení nebo předpokládaná doba trvání možného narušení;
c) zeměpisná oblast ovlivněná narušením nebo možným narušením.

Na základě informací poskytnutých v hlášení kritickým subjektem informuje příslušný orgán prostřednictvím svého jednotného kontaktního místa jednotná kontaktní místa ostatních dotčených členských států, pokud incident má nebo může mít významný dopad na kritické subjekty a kontinuitu poskytování základních služeb v jednom nebo více ostatních členských státech.

Při tom jednotná kontaktní místa v souladu s právními předpisy Unie nebo vnitrostátními právními předpisy, které jsou v souladu s právem Unie, zacházejí s informacemi způsobem, který respektuje jejich důvěrnost a chrání bezpečnost a obchodní zájmy dotčeného kritického subjektu.

2.13 Skupina pro posílení odolnosti kritických subjektů

Skupina pro posílení odolnosti kritických subjektů je zřízena s účinkem od [šest měsíců po vstupu této směrnice v platnost]. Podporuje Komisi a usnadňuje strategickou spolupráci a výměnu informací o otázkách týkajících se této směrnice.

Skupina pro posílení odolnosti kritických subjektů má tyto úkoly:

a) podporuje Komisi v rámci pomoci členským státům při posilování jejich kapacity přispívat k zajištění odolnosti kritických subjektů v souladu s touto směrnicí;

b) hodnotí strategie pro posílení odolnosti kritických subjektů a stanoví ve vztahu k těmto strategiím osvědčené postupy;
c) usnadňuje výměnu osvědčených postupů, pokud jde o určení kritických subjektů členskými státy, a to i v souvislosti s přeshraničními závislostmi a ohledně rizik a incidentů;
d) na žádost přispívá k přípravě pokynů a případných aktů v přenesené pravomoci a prováděcích aktů podle této směrnice;
e) každoročně posuzuje souhrnné zprávy;
f) zajišťuje výměnu osvědčených postupů týkající se výměny informací souvisejících s hlášením incidentů;
g) analyzuje zprávy poradních misí a poskytuje k nim rady;
h) zajišťuje výměnu informací a osvědčených postupů v oblasti výzkumu a vývoje, pokud jde o posilování odolnosti kritických subjektů v souladu s touto směrnicí;
i) v náležitých případech zajišťuje výměnu informací v záležitostech týkajících se posilování odolnosti kritických subjektů s příslušnými orgány, institucemi, úřady a agenturami Unie.

2.14 Provádění a vymáhání

Za účelem posouzení, zda subjekty, které členské státy označily jako kritické subjekty, dodržují povinnosti uvedené v této směrnici, členské státy zajistí, aby příslušné orgány měly pravomoci a prostředky k:

a) provádění kontrol na místě v prostorách, které kritický subjekt používá k poskytování svých základních služeb, a dohledu nad opatřeními kritických subjektů;
b) provádění nebo nařízení auditů ve vztahu k těmto subjektům.

Členské státy zajistí, aby příslušné orgány měly pravomoci a prostředky požadovat, je-li to pro plnění jejich úkolů podle této směrnice nezbytné, aby subjekty, které určily jako kritické subjekty, poskytly v přiměřené lhůtě stanovené těmito orgány:

a) informace nezbytné k posouzení, zda opatření přijatá těmito subjekty k zajištění jejich odolnosti splňují požadavky;

b) důkazy o účinném provádění těchto opatření, včetně výsledků auditu provedeného nezávislým a kvalifikovaným auditorem, kterého daný subjekt vybere a provede na své náklady.

Pokud příslušný orgán žádá o poskytnutí těchto informací, uvede účel svého požadavku a upřesní informace, které jsou požadovány

2.15 Závěr kapitoly

Analyzovaná Směrnice o posílení odolnosti kritických subjektů je z i z dlouhodobého pohledu vnímána jako strategický dokument s celospolečenským dopadem. Pochopení jeho účelu je základem pro budoucí normativní, institucionální a legislativní rámec zajištění funkční kontinuity společnosti. Text této kapitoly citoval nejvýznamnější aspekty, resp. povinnosti orgánů státní zprávy a současné tak povinnosti provozovatelů kritických služeb v kontextu kritických subjektů. Dochází zde k syntetizaci požadavků.

2.16 Hodnocení

Tak jak již bylo konstatováno, změna v bezpečnostním prostředí a relativní dominance některých typů bezpečnostních hrozeb zvýšili potřebu aktualizovat evropské přístupu k bezpečnosti a odolnosti kritických infrastruktur, resp. kritických subjektů. Nově formulované povinnosti provozovatelů a orgánů státní zprávy členských státu vytváří konkrétní prostor pro rozvoj a výzkum přístupů k objektivizaci rizik v přeneseném významu na odolnost kritické infrastruktury.

2.17 Možný vývoj

Možný vývoj:

- Posilování významu řízení rizik ve vazbě na odolnost kritických subjektů,
- Změna perspektivy ze subjektů kritické infrastruktury na kritické subjekty,
- Tvorba nových nástrojů a metod pro posilování kritických subjektů.

ZÁVĚR

Tento materiál vznikl v rámci poslední etapy řešení projektu. Materiál byl zaměřen do 2 hlavních oblastí a to: ochrana a odolnost kritické infrastruktury s využitím přístupů ku konvergenci druhů bezpečnosti a dopadová studie Směrnice Evropského parlamentu a rady o posílení odolnosti kritických subjektů. Na základě uvedených byly nalezeny možné cesty pro vývoj předmětných oblastí. Obecně se jednalo o vytvoření bezpečnostních platforem pro komunikaci mezi odborníky, používání nových technologií a větší zapojování externích odborníků či implementace analyzovaných přístupů do praxe.

SEZNAM POUŽITÉ LITERATURY

ČANDÍK, Marek. Objektová bezpečnost II. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 8073182173

ČESKO. Zákon č. 133 ze dne 17. prosince 1985 o požární ochraně. In: Zákony pro lidi.cz [online]. AION CS 2010–2019 [cit. 2019-05-06]. Dostupné z: https://www.zakonypro-lidi.cz/cs/1985-133

ČESKO. Zákon č. 258 ze dne 14. července 2000 o ochraně veřejného zdraví a o změně některých souvisejících zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2019 [cit. 2019-05-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-258

ČESKO. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: Zákony pro lidi.cz [online]. AION CS 2010–2019 [cit. 2019-05-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

HROMADA, Martin, HRŮZA, Petr, KADERKA, Josef, LUŇÁČEK, Oldřich, NEČAS, Bohumil PTÁČEK, Miroslav, SKORUŠA, Leopold a SLOŽIL, Richard. Kybernetická bezpečnost: teorie a praxe. Praha: Powerprint, 2015. ISBN 978-80-87994-72-6

JANEČKOVÁ, Eva. GDPR: řešení problémů v praxi obcí. Praha: Grada Publishing, 2019. Právo pro praxi. ISBN 978-80-247-2925-1

Kolektiv autorů pod vedením Ministerstva zahraničních věcí ČR. Bezpečnostní strategie České republiky [online]. Praha: Ministerstvo zahraničních věcí České republiky, 2015 [cit. 2019-05-06]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf. ISBN 978-80-7441-005-5

LUKÁŠ, Luděk. Teorie bezpečnosti a typologie druhů bezpečnosti. In: Sborník 21. vědecké konference s mezinárodní účastí Riešenie krízových situácií v špecifickom prostredí, 25. – 26. května 2016, Žilina: EDIS. ISBN 978-80-554-1213-9

LUKÁŠ, Luděk. Teorie bezpečnosti I. Zlín: Radim Bačuvčík – VeRBuM, 2017. ISBN 978-80-87500-89-7

PROCHÁZKOVÁ, Dana. Bezpečnost kritické infrastruktury. Praha: České vysoké učení technické v Praze, 2012. ISBN 978-80-01-05103-0

ŠENK, Zdeněk. Bezpečnost a ochrana zdraví při práci: prakticky a přehledně podle normy OHSAS. 2., aktualiz. vyd. Olomouc: ANAG, 2012. Práce, mzdy, pojištění. ISBN 978-80-7263-737-9

UHLÁŘ, Jan. Technická ochrana objektů. Praha: Vydavatelství PA ČR, 2005. ISBN 8072511890

ČESKO. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) – Sbírka zákonů České republiky č. 82/2018, částka 43, strana 1122–1165

ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) – Sbírka zákonů České republiky č. 181/2014. částka 75, strana 1926–1936

ČSN EN ISO/IEC 2700x. Skupina norem 27000 až 27005 se společným názvem – Informační technologie – Bezpečnostní techniky, aktuální vydání každé normy

ČSN EN ISO 22301 (012306). Ochrana společnosti - Systémy managementu kontinuity podnikání – Požadavky, 2013

LUKÁŠ, Luděk a kolektiv. Teorie bezpečnosti I. Zlín: Radim Bačuvčík – VerBuM, 2017, ISBN 978-80-87500-89-7

Nařízení komise v přenesené pravomoci (EU) 2018/762 ze dne 8. března 2018, kterým se stanoví společné bezpečnostní metody týkající se požadavků na systém zajišťování bezpečnosti podle směrnice Evropského parlamentu a Rady (EU) 2016/798 a kterým se zrušuje nařízení Komise (EU) č. 1158/2010 a (EU) č. 1169/2010. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32018R0762&from=EN

Směrnice Evropského parlamentu a Rady EU 2016/798 ze dne 11. května 2016 o bezpečnosti železnic. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016L0798&from=CS

© EU Agency for Railways – Guidance for safety certification and supervision – Safety management system requirements for safety certification or safety authorisation – Version 1. 2. (04/09/2018). Dostupné z: https://www.era.europa.eu/sites/default/files/activities/docs/guide_sms_requirements_en.pdf

Informace o změnách zákona o kybernetické bezpečnosti. Verze 2.1. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2019

Zákon č. 110/2019 Sb., o zpracování osobních údajů

ŠKORNÍČKOVÁ, Eva. Co je GDPR? GDPR.cz [online]. [cit. 2019-02-25]. Dostupné z: https://www.gdpr.cz/gdpr/

SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9

HORÁK, Aleš. Nástroje kybernetické bezpečnosti pro mobilní platformu. Zlín, 2019. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Lukáš Králík.

Základní příručka k GDPR. Úřad pro ochranu osobních údajů [online]. [cit. 2019-02-25]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=4720

Kybernetická bezpečnost. CyberSecurity.cz: Kybernetická bezpečnost a obrana [online]. 2017 [cit. 2018-10-31]. Dostupné z: https://www.cybersecurity.cz/basic.html

ČERMÁK, Miroslav. Řízení rizik: Jemný úvod do řízení rizik. Clever and Smart [online]. [cit. 2019-05-26]. Dostupné z: https://www.cleverandsmart.cz/rizeni-rizik-jemny-uvod-do-rizeni-rizik/

LONGSTAFF, P. H, MERGEL, I., ARMSTRONG, N. Insitute for National Security and Counterterrorism, Workshop Report: Resilience in Post-Conflict Reconstruction and Natural Disasters, Syracuse University, 2009, Syracuse

LUKÁŠ, Lukáš, HROMADA, Martin. Možnosti hodnocení odolnosti kritické infrastruktury/ qvaluating the Resilience of Critical Infrastructure. In: Bezpečnost v informační společnosti, Brno, 2009, p. 56, ISBN 978-80-7231-653-3

WALKER, B. Section 1.5 to practitioner: Resilience Alliance [online]. 2009 Specified and General Resilience

Holling, C.S. Resilience and Stability of Ecological Systems. Annual Review of Ecological and Systematics, 4, 1–23, 1973. http://dx.doi.org/10.1146/annurev.es.04.110173.000245

Wildavsky, A. . Searching for Safety. Transaction, New Brunswick NJ, 1991

Horne, J. and Orr, J. Assessing Behaviors That Create Resilient Organizations. Employment Relations Today, 24, 29–39, 1998

Mileti, D. Disasters by Design: A Reassessment of Natural Hazards in the United States. Joseph Henry Press, Washington, DC, 1999

Comfort, L. Shared Risk: Complex Systems in Seismic Response. Pergamon, New York. Global Environmental Change Part B Environmental Hazards 2 (3): 129–130, 1999. DOI: 10.1016/S1464-2867(01)00006-7

Adger, W. Social and ecological resilience: Are they related? Progress in Human Geography, 24, 347–364, 2000. https://doi.org/10.1191/030913200701540465

Gunderson, L. H., and C. S. Holling, editors. 2002. Panarchy: understanding transformations in human and natural systems. Island Press, Washington, D.C., USA.

Fiksel, J. 2003. Designing resilient, sustainable systems. Environmental Science and Technology, 37 (23): 5330–5339

Rose, A. and Liao, S. Y.: Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions, J. Reg. Sci., 45, 75–112, 2005

Tierney, K. and Bruneau, M. Conceptualizing and Measuring Resilience: A Key to Disaster Loss, Reduction, TR News, May–June, 250, 14–17, 2007

United States Department of Homeland Security, „Social Network Analysis for Building Resilient Communities," DHS Solicitation Number BAA10–15

Critical Infrastructure Resilience Final Report and Recommendations, U.S. Department of Homeland Security, Washington, D.C., 2009

Carlson, J.L. et al. Resilience: Theory and Application. Lemont: Argone National Laboratory, 2012. DOI: 10.2172/1044521

Béné, C., Wood, R.G., Newsham, A., Davies, M. Resilience: New Utopia or New Tyranny? Reflection about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability Reduction Programmes. IDS Working Papers 405: 1–61, 2012. DOI: 10.1111/j.2040-0209.2012.00405.x

Hromada, M., Lukáš, L., Matejdes, M., Valouch, J., Nečesal, L., Richter, R., Kovářík, F. Systém a způsob hodnocení odolnosti kritické infrastruktury. Ostrava: Sdružení požárního a bezpečnostního inženýrství. 177 s. 2013. ISBN 978-80-7385-140-8.

Richter, R. Resilience and Critical Infrastructure. The Science for Population Protection, 7 (1): 71–76. 2015

Chandra, A. Synergy between biology and systems resilience [Master theses]. United States: Missouri University of Science and Technology. 143 p., 2010

ŘEHÁK D., Průběžná zpráva za rok 2017 projektu RESILIENCE 2015: Dynamické hodnocení odolnosti souvztažných subsystémů kritické infrastruktury, WP4: Výzkum dynamického hodnocení odolnosti kritické infrastruktury pro naplnění potřeby zvyšování ochrany a odolnosti kritické infrastruktury z pohledu potenciálních dopadů na systém, 34 s. 2018

Berkeley, A.R. et al. A Framework for Establishing Critical Infrastructure Resilience Goals. National Infrastructure Advisory Council. 85 p., 2010

Keeping the Country Running: Natural Hazards and Infrastructure. A Guide to improving the resilience of critical infrastructure and essential services. London: Cabinet Office. 98 p., 2011

Critical Infrastructure Resilience Final Report and Recommendations, U.S. Department of Homeland Security, Washington, D.C., 2009

Fekete, A. Resilienz — wie widerstands- und anpassungsfähig sind wir?: Die Verbindung von Aspekten des Risiko und Krisenmanagements im BBK. Bevölkerungsschutz: Risikomanagement, 20-23. 2011

Da Silva, J. City resilience Index. The Rockefeller Foundation, Arup International Development. 34 p. 2015

LUKÁŠ, Luděk. Metodika hodnocení odolnosti z pohledu konvergované bezpečnosti. [Výzkumná zpráva]. Projekt: VI 20172019054 „Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti“. Praha: TTC TELEKOMUNIKACE, s.r.o., 2018. 84 s.

LUKÁŠ, Luděk, VALOUCH, Jan, URBANČOKOVÁ, Hana, HROMADA Martin. Metodika hodnocení odolnosti z pohledu fyzické bezpečnosti. [Výzkumná zpráva]. Projekt: VI

20172019054 „Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti“. Praha: TTC TELEKOMUNIKACE, s.r.o., 2017. 28 s.

VALOUCH, Jan, URBANČOKOVÁ, Hana. Katalog penalizačních kritérií fyzické bezpečnosti objektů. [Výzkumná zpráva]. Projekt: VI 20172019054 „Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti“. Praha: TTC TELEKOMUNIKACE, s.r.o., 2018. 13 s.

VALOUCH, Jan, URBANČOKOVÁ, Hana. Obecný katalog penalizačních faktorů [Výzkumná zpráva]. Projekt: VI 20172019054 „Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti“. Praha: TTC TELEKOMUNIKACE, s.r.o., 2019. 28 s.

VALOUCH, Jan, URBANČOKOVÁ, Hana. Identifikace vhodných aktiv v infrastruktuře – veřejná správa. [Výzkumná zpráva]. Projekt: VI 20172019054 „Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti“. Praha: TTC TELEKOMUNIKACE, s.r.o., 2017. 29 s.

VALOUCH, Jan, URBANČOKOVÁ, Hana. Hodnocení odolnosti infrastruktury státní správy. [Výzkumná zpráva]. Projekt: VI 20172019054 „Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti“. Praha: TTC TELEKOMUNIKACE, s.r.o., 2018. 55 s.

VALOUCH, Jan. Security Assessment of the Object in terms of Alarm system design. In the Science for Population Protection. Lázně Bohdaneč: MV – GŘHZS, Institut ochrany obyvatelstva. Vol. 4. p. 185–190. ISSN 1803-568X

LUKÁŠ, L. a kol. Konvergovaná bezpečnost. Zlín: Radim Bačuvčík - VeRBuM, 2019, 206 s. ISBN 978-80-87500-99-6.

Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o posílení odolnosti kritických subjektů COM/2020/829 final.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BCMS Business Continuity Management Systém (Systém řízení kontinuity činností)

BOZP Bezpečnost a ochrana zdraví při práci

BPI Business Process Improvement (Kontinuální zlepšování procesů)

BPR Business Process Reengineering (Radikální zlepšování procesů)

CERT Computer Emergency Response Team (Skupina pro reakci na počítačové hrozby)

CSIRT Computer Security Incident Response Team (Skupina pro řešení počítačových bezpečnostních incidentů)

DDoS Distributed Denial of Services (Distribuovaný útok odepření služeb)

EMS Environmental Management Systém (Systém environmentálního managementu)

GIS Geographic information system (Geografický informační systém)

IDS Intruder Detection System (Systém pro odhalení průniku)

IPS Intruder Prevention System (Systém prevence průniku)

IT Informační technologie

KI Kritická infrastruktura

MPBP Místní provozní bezpečnostní předpis

MW Microwave (Mikrovlna)

NU Nežádoucí událost

OHSAS Occupational Health and Safety Assessment Specification (Systém managementu bezpečnosti a ochrany zdraví při práci)

PCO Pult centralizované ochrany

PDCA Plan-Do-Check-Act (Naplánuj-Proveď-Ověř-Jednej)

PIR detektor Pasiv Infra Red detector (Pasivní infračervené čidlo)

PZTS Poplachový zabezpečovací a tísňový systém

QMS Quality Management Systém (Systém řízení jakosti)

SIEM Security Information and Event Management (Management bezpečnostních informací a událostí)

SMS Systems Management Service (Systém managementu služeb)

VSS Video Surveillance Systems (Dohledový videosystém)

VVN Velmi vysoké napětí

US Ultrasonic (Ultrazvuk)