

ÚVOD DO KONVERGOVANÉ BEZPEČNOSTI

THE CONVERGED SECURITY INFORDUCTION

Luděk LUKÁŠ

Univerzita Tomáše Bati ve Zlíně

Nám. T. G. Masaryka 5555, 76001 Zlín

lukas@utb.cz

Abstrakt: Bezpečnost patří mezi základní atributy a funkce společnosti. Cílem bezpečnosti jako oboru je chránit referenční objekt (člověka, organizaci, podnik, stát atd.) a zejména jeho aktiva před vznikem újmy nebo negativního dopadu. Referenční objekt si svoji bezpečnost zajišťuje aktivně pomocí druhů bezpečnosti. Zejména vlivem technologického rozvoje však narůstá počet druhů bezpečnosti, které musí referenční objekt v rámci své ochrany zajišťovat. Pro referenční objekt typu výrobní podnik tato situace znamená, že musí uvedená opatření realizovat na vrub zisku. Proto se hledají způsoby, jak uvedenou situaci řešit. Jednou z možností je slučovat vhodné druhy bezpečnosti do jednoho celku. Uvedený koncept se nazývá konvergovaná bezpečnost. Základem konvergence jsou společná aktiva a splývání technologií. V článku je analyzován koncept konvergované bezpečnosti a jeho přínosy.

Klíčová slova: bezpečnost, konvergovaná bezpečnost, odolnost, zranitelnost, systém ochrany.

Úvod

Bezpečnost patří mezi významné fenomény dnešní doby. Zejména díky rozvoji technologií společnost identifikuje čím dále větší počet aktiv. Ještě donedávna měla tato aktiva především hmotný charakter. S vynálezem počítačů a rozvojem digitálních komunikačních a informačních technologií však vznikla aktiva, která mají logickou či nematerializovanou povahu. Jedná se o data, která jsou využita k realizaci či podpoře čím dále většího spektra činností. Od sdělování, přes řízení, vzdělávání, zábavu, sociální činnosti až po modelování a realizaci inteligentních činností. Aby nedocházelo k narušení uvedených činností, došlo k zavedení souborů opatření, zavedení druhů bezpečností. V současnosti existuje několik desítek druhů bezpečností. Nejenže dochází ke vzniku druhů bezpečnosti v nových oblastech bezpečnostního prostředí, ale i k atomizaci původních druhů bezpečnosti. Zejména v podnicích a organizacích začíná uvedená skutečnost způsobovat obtíže. Zajištění bezpečnosti představuje pro organizaci službu „ochrany podmínek“ k naplňování její cílové funkce, tedy výroby či poskytování služeb.

Náklady na zajištění bezpečnosti se musí promítnout do ceny produkce, nebo jdou na vrub zisku. Náklady na bezpečnost zlepšují kvalitu produkce, ale umožňují, aby byla realizována ve stanovených podmínkách. Proto se hledají cesty, jak bezpečnost zajistit v podmínkách, kdy organizace zajišťuje několik druhů bezpečnosti. Mezi tyto druhy bezpečnosti patří fyzická bezpečnost, informační bezpečnost, kybernetická bezpečnost, administrativní bezpečnost, bezpečnost a ochrana zdraví při práci, požární ochrana, environmentální bezpečnost, případně provozní bezpečnost. Jednou z cest je uplatnění konceptu konvergované bezpečnosti. Základní myšlenkou uvedeného konceptu je slučování vhodných druhů bezpečnosti do jednoho celku. Výzkum v této oblasti se teprve rozbíhá a praxe se s ním postupně seznamuje. Hledá se při tom správná rovnováha a užitečnost slučování.

Problematika bezpečnosti provází lidstvo po jeho celou dobu jeho civilizované historie. S rozvojem civilizace docházelo k postupnému rozšiřování bezpečnostních problémů, které byly postupně zařazovány do agendy bezpečnosti. Výrazný vliv na tuto skutečnost měla především institucionalizace bezpečnosti ve formě státu a rovněž také rozvoj technologií. Institucionalizace znamenala svěření ochranné funkce společnosti organizaci zvané „stát“. Zajištění bezpečnosti na kvalitativně vyšší úrovni a potřeba „ochranné funkce“ byly jedním z impulsů ke vzniku státu. Současně s tím začal stát plnit řadu dalších funkcí, zejména ekonomickou, politickou, organizační, právní a správní. K nim se postupně přidaly další funkce státu, zejména sociální, vzdělávací a kulturní. Rozvoj technologií si vyžádal, aby byla bezpečnost zajišťována v těch celcích a odvětvích, které mohly svými negativními událostmi (havárie, nehody) a dopady společnost či jedince ohrožovat. Případně na nich byla společnost výrazně závislá.

1. Vymezení druhu bezpečnosti

Druh bezpečnost představuje soubor opatření, řešících specifickou skupinu bezpečnostních problémů. Jedná se o soustavné a opakované řešení nežádoucích jevů narušení bezpečnosti určitého typu. Cílem zavedených a realizovaných opatření je zamezit vzniku újmy nebo alespoň minimalizovat dopady, způsobené narušeními bezpečnosti. Příkladem druhu bezpečnosti je fyzická bezpečnost, informační bezpečnost, bezpečnost a ochrana zdraví při práci, bezpečnost silničního provozu, mezinárodní bezpečnost.

Druhy bezpečnosti vznikají na základě potřeb praxe jejich institucionalizací. Zajištění bezpečnosti je prosazováno řadou nástrojů, mezi něž patří zejména 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 či 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.

V současnosti existuje více jak 50 druhů bezpečnosti, které jsou dány právním řádem České republiky. Ve většině případů jsou tyto druhy bezpečnosti vymezeny zákonem nebo celostátní vyhláškou. Jednotlivá kritéria a požadavky jsou navíc uvedeny normách ČSN. Nedodržování bezpečnostních požadavků je pak vynucováno a trestáno. Tím, že jsou organizace povinny naplňovat požadavky právního řádu, zajišťují bezpečnost ve vyžadovaných druzích bezpečnosti. Aby došlo ke snížení nákladů, případně zvýšení kvality ochrany, je snaha slučovat některé nebo všechny druhy bezpečnosti do jednoho celku. Dochází tak k zavádění konvergované nebo integrální bezpečnosti.

2. Konvergovaná bezpečnost, principy a východiska řešení

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. Jestli například chce zaměstnanec firmy neoprávněně zkopírovat data ze serveru přímo v servrovně, neexistuje v současnosti v rámci kybernetické bezpečnosti možnost jej odhalit díky propojení data z přístupového systému servrovny, kamerovým systémem sledujícím vstup do servrovny, s údaji o kopírování dat přímo z USB portu serveru. 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 souvztáhnosti 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. Na Obr. 1 je zobrazena konvergovaná bezpečnost, zahrnující provozní bezpečnost, fyzickou bezpečnost a kybernetickou bezpečnost.

Konvergovaná bezpečnost



Obr. 1 Koncept konvergované bezpečnosti

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.

Mezi základní principy, na nichž je konvergovaná bezpečnost postavena, lze zařadit následující skutečnosti:

- 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 mohou 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.

3. Přínosy konvergované bezpečnosti

Konvergovaná bezpečnost 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.

Nasazení konvergované bezpečnosti současně umožňuje snižovat zranitelnost systému ochrany. Jedná se především o rychlejší reakci, založenou na identifikaci narušení bezpečnosti díky využití souvztažnosti údajů a informací. Vznikající narušení bezpečnosti může být odhaleno dříve, než dojde k poškození aktiva. Filtry událostí, vyhodnocující bezpečnostní situaci, mohou díky korelaci narazit na vektory dat, které identifikují vznikající narušení bezpečnosti v jeho počáteční fázi. Vyhodnocovat se budou nejen jednotlivé události a vztahy mezi nimi, ale také jejich posloupnost a časové relace. Základem hodnocení bude katalog vektorů narušení, obsahující soubory dat demaskujících příznaků a jejich časových relací. Kvalita katalogu bude vyjadřovat míru odolnosti a zranitelnosti systému ochrany. Tím se celkově zvýší odolnost a sníží zranitelnost systémů ochrany referenčních objektů. Průběžná a aktuální znalost stavu odolnosti systému ochrany bude umožňovat jednotlivá narušení bezpečnosti řešit a přijímat účinná opatření k nápravě.

Dalším přínosem konvergované bezpečnosti bude celostní pohled bezpečnostního managementu na bezpečnostní situaci. Situace již nebude vnímána jako soubor nezávislých pohledů, ale jako průnik pohledů, umožňující vidět vzájemné vazby mezi jednotlivými prvky bezpečnostního prostředí. Uvedené pojetí pak může vést k odstraňování duplicit při zajištění bezpečnosti.

Závěr

V současnosti se bezpečnost zajišťuje po jednotlivých druzích bezpečnosti. Každý druh bezpečnosti obvykle funguje nezávisle na ostatních. Tato situace přináší řadu komplikací především při zajištění celkové bezpečnosti. Problémem je i ekonomická otázka ve formě zvýšených nákladů na bezpečnost. Řešením tohoto problému je aplikace konceptu konvergované bezpečnosti, spočívající ve sloučení slučitelných druhů bezpečnosti do jednoho celku. Sloučit lze např. fyzickou, kybernetickou a provozní bezpečnost. Výhodou řešení je možnost sledovat vazby mezi událostmi, získávanými z prostředků jednotlivých druhů bezpečnosti a identifikovat vektory dat, spojené s narušeními bezpečnosti. Koncept konvergované bezpečnosti umožňuje zlepšit vyhodnocování souvztažnosti demaskujících příznaků a odhalit narušení bezpečnosti v jeho počáteční fázi. Umožňuje také vidět zajištění bezpečnosti celostně a odhalovat tak duplicitu v jejím zajištění. To bude moci snižovat náklady na zajištění bezpečnosti.

Tento článek vznikl za podpory grantového projektu VI20172019054 "Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti", podpořeného Ministerstvem vnitra České republiky v letech 2017-2019.

Literatura

- [1] LUKÁŠ, Luděk. Teorie bezpečnosti I. Zlín : Radim Bačuvčík - VeRBuM, 2017, s. 89-100. ISBN 978-80-87500-89-7.
- [2] MALÍK, Petr. Konvergovaná bezpečnost. In: LUKÁŠ, L. Teorie bezpečnosti I. Zlín : Radim Bačuvčík - VeRBuM, 2017, s. 202 - 215. ISBN 978-80-87500-89-7.
- [3] 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