

VÝVOJ KONVERGOVANEJ BEZPEČNOSTI VYBRANÉHO MÄKKÉHO CIEĽA ŠTÁTU

THE PROGRESION OF THE COVERGED SECURTY OF THE SELECTED SOFT TARGET

Lucia MRÁZKOVÁ (ĎURICOVÁ), Dora LAPKOVÁ

Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky

Nad Stráněmi 4511, Zlín, Česká Republika

lmrazkova@utb.cz, dlapkova@utb.cz

Abstrakt: Mäkké ciele sú objekty (fyzické stavby alebo priestranstvá zoskupujúce veľké množstvo osôb) úzko spojené s vysokou mierou pravdepodobnosti prevedenia útoku na skupinu osôb, kedy dochádza k ohrozeniu života a zdravia týchto osôb v objekte. Vzhľadom na fakt, že mäkké ciele sú objekty verejného záujmu s voľne riadeným prístupom je aplikácia akýchkoľvek opatrení, ktoré by znížili pravdepodobnosť prevedenia útoku, v dobe prevádzky veľmi komplikovaná. Hlavným účelom článku je popísať aplikáciu metodiky konvergovanej bezpečnosti a penalizačných faktorov na špecifickú oblasť objektov mäkkých cieľov.

Kľúčová slova: mäkké ciele, konvergovaná bezpečnosť, odolnosť mäkkých cieľov, útok

Úvod

Článok popisuje aplikáciu metodiky na hodnotenie konvergovanej bezpečnosti na objekty spadajúce do kategórie mäkkých cieľov. V úvode dochádza k popisu samotného výpočtu konvergovanej bezpečnosti podľa uvedenej metodiky. Následne dochádza k popisu vybraného scenáru, ktorý je použitý pre prípadovú štúdiu. V prípadovej štúdii dochádza k aplikácií uvedených penalizačných faktorov na vybraný objekt. Vybraný objekt je univerzitná budova. Je potrebné podotknúť, že oboznámenie sa s procesmi vybraného objektu je základný predpoklad pre správne určenie konvergovanej bezpečnosti objektu.

Prípadová štúdia popisuje prevedenie vybraného scenára (*napadnutie skupiny študentov na výuke*), ktorý je podrobne popísaný v kapitole 2 uvedeného článku. Útok je realizovaný zo strany cudzieho návštevníka objektu, ktorý sa infiltruje do skupiny študentov postupne a to premyslene. Je potrebné poznamenať, že podobné útoky sú založené práve na získaní dôvery zo strany skupiny, a tým pádom nie je útočník v skupine nijak identifikovaný. Jedná sa o prevedenie útoku vo verejnom objekte, ktorého vstup v prevádzkových hodinách nie je kontrolovaný na všetkých úrovniach a zavedenie kontroly vstupu nie je reálne možné. Jedná sa o univerzitnú budovu, ktorá síce disponuje prístupovým systémom do učební a kľúčovou službou, ktorú prevádzkuje vrátnica budovy, avšak tieto opatrenia neriadia vstup návštevníkov do budovy. Taktiež je potrebné poznamenať, že daný typ útoku môže realizovať aj útočník priamo patriaci do skupiny študentov, a teda jeden zo študentov. V tomto prípade je nepravdepodobné, že bude útočník odhalený pred samotným prevedením útoku.

1 Metoda konvergovanej bezpečnosti

Metoda konvergovanej bezpečnosti je u mäkkých cieľov riešená rovnakým spôsobom ako u ostatných typov objektov, a to za pomoci statických a dynamických penalizačných faktorov. Obmedzenie je v chránených aktivitách, kedy sa jedná o jediné chránené aktívum, a to človeka. Limitované sú taktiež hrozby, a to len na násilné útoky.

Statické faktory sú faktory v čase bez zásahu nemenné a s dlhodobým pôsobením na objekt. Patria sem penalizačné faktory, ktoré reflektujú problémy/ incidenty, ktoré vychádzajú väčšinou z neexistencie procesov nutných pre zaistenie bezpečnosti, neexistencii bezpečnostnej politiky, neexistencii prvkov fyzickej, kybernetickej alebo prevádzkovej bezpečnosti, prípadne nesúlada s platnou legislatívou. Obvykle sa statické faktory viažu na bezpečnostný štandard referenčného objektu. Tento bezpečnostný štandard deklaruje, ako by systém ochrany referenčného objektu mal byť vytvorený a čo všetko v jednotlivých druhoch bezpečnosti

zahrňuje. Prvý krok pre stanovenie aktuálnej odolnosti objektu je na základe auditu vybraných relevantných statických penalizačných faktorov vypočítať statickú odolnosť objektu.

$$I_{ods} = 100 - \frac{\sum_{i=1}^n P_{si} \cdot V_i}{P_{smax}} * 100 \quad (1)$$

I_{ods} index statickej odolnosti

P_{si} i-tý aktívny statický penalizačný faktor

i poradie penalizačného faktoru, platného v danom časovom okamžiku

n celkový počet platných penalizačných faktorov pre dané aktívum

V_i váha statického penalizačného faktoru vzhľadom k danému aktívu (pohybuje sa v rozmedzí 1 – 5; implicitne 3)

P_{smax} suma všetkých statických penalizačných faktorov pre dané aktívum

Dynamické faktory predstavujú faktory, ktoré sa samy v čase menia, a doba ich pôsobenia nie je presne odhadnuteľná. Patrí sem napríklad detekcie pohybu pomocou kamerového systému, narušenie bezpečnosti hlásené detektorom narušenia, výpadok elektrickej energie, skenovanie portov počítačovej siete, kopírovanie dát, výpadok služby a iné. U dynamických penalizačných faktorov je nutné stanovenie sledovaného časového pôsobenia faktorov. Po dobu pôsobenia je faktor identifikovaný ako incident a podieľa sa na znížení odolnosti objektu. Po uplynutí doby je faktor archivovaný a odolnosť objektu je opäť zvýšená. Na základe poskytnutých nástrojov a metrik z hodnotenia statickej odolnosti je možné sledovať dynamické faktory a hodnotiť tak dynamickú zložku odolnosti. Pri hodnotení dynamickej odolnosti sa postupuje obdobne ako u odolnosti statickej.

$$I_{odd} = \frac{\sum_{j=1}^m P_{dj} \cdot V_j}{P_{dmax}} * 100 \quad (2)$$

I_{odd} index dynamickej odolnosti

P_{dj} j-tý aktívny dynamický penalizačný faktor

j poradie penalizačného faktoru, platného v danom časovom okamžiku

n celkový počet platných penalizačných faktorov pre dané aktívum

V_j váha dynamického penalizačného faktoru vzhľadom k danému aktívu (pohybuje sa v rozmedzí 1 – 5; implicitne 3)

P_{dmax} suma všetkých dynamických penalizačných faktorov pre dané aktívum

Výsledná odolnosť je daná rozdielom statickej a dynamickej odolnosti. Vstupná hodnota je daná statickou odolnosťou, v prípade, že nie je možné množstvo dynamických faktorov merať a monitorovať, bude i výstupná hodnota odolnosti veľmi nízka a nebude dochádzať ku skresleniu celkového výsledku nízkym počtom dynamických faktorov.

$$I_{od} = I_{ods} - I_{odd} \quad (3)$$

2 Napadnutie skupiny študentov na výuke

Vybraný scenár pre prípadovú štúdiu aplikácie uvedenej metodiky na objektoch mäkkých cieľov štátu je napadnutie skupiny študentov na výuke. Je potrebné podotknúť, že uvedený typ scenáru – útoku je špecifický práve pre vybraný typ objektu (univerzitná budova). To znamená, že pre jednotlivé kategórie objektov sú rôzne typy scenárov/ útokov, ktoré môžu v objekte nastať. Nižšie dochádza k popisu práve vybraného scenáru.

Hrozba: úmyselné napadnutie skupiny, pod vyhrážaním sa útokom nožom na vybranom študentovi

Charakteristika: Útok je realizovaný zo strany cudzieho návštevníka objektu, pre ktorého objekt nie je určený. Útočník svojim vzhľadom a vekom odpovedá charakteristickej skupine študentov. Využije nekontrolovaný vstup do objektu. Na začiatku semestra sa niekoľkokrát pripletie na výuku vybranej skupiny študentov. Po určitej dobe si vytupuje spôsob prevedenia útoku. Dôvod útoku je potreba uznania a vplyv drog.

Aktívum: Vyučujúci, študenti, a iní zamestnanci.

Popis újmy: Újma sa môže dotýkať psychického a fyzického zdravia osôb nachádzajúcich sa v objekte. Hrozí ohrozenie zdravia a života osoby, alebo skupiny osôb súčasne.

Nižšie uvedená tabuľka zobrazuje vývoj jednotlivých fáz útoku vo vybranom referenčnom objekte. Dochádza k popisu fáze a popisu spôsobu narušenia aktíva. Následné je určená príčina a dôsledky narušenia. V neposlednej rade dochádza k určeniu opatrení na základe predchádzajúcich zistení – analýza jednotlivých fáz útoku.

Názov fáze	Charakteristika fáze	Ako je narušené aktívum	Príčina	Dôsledky	Opatrenie
Preniknutie páchatel'a do objektu	Páchatel' sa dostal do objektu. Objekt je bez kontroly vstupu do objektu. Na vrátnici sedí bezpečnostný pracovník, ktorý prevažne vydáva kľúče a prijíma poštu.	Aktívum nie je narušené. Objekt je verejne dostupný. Nie sú nastavené pravidlá pre vstup do objektu. Predpokladá a, že osoby, pre ktoré objekt nie je určený, alebo nemajú dôvod k návšteve, objekt nenavštevujú.	- Nenastavená kontrola vstupu do objektu. - Nízka kontrola záujmu návštevníkov pre vstup do objektu mimo verejne prístupné akcie.	Vstup nepovolennej osoby do objektu.	- Nastavenie pravidiel pre normálnu prevádzku objektu. - Nastavenie úrovne kontroly.
Preniknutie do skupiny študentov a na výuku	Dochádza k vytipovaniu si skupiny študentov, ktorí nie sú príliš skupinovo integrovaní. Nie je pre uvedenú skupinu podozrivé, že prišiel niekto nový. Väčšinou prvé ročníky štúdia, prípadne kombinované formy štúdia.	Vybraná skupina študentov je narušená cudzím návštevníkom. Postupne dochádza k získaniu interných informácií o prevádzke fakulty. Dochádza k nadobudnutiu dôvery medzi útočníkom a ostatnými študentami.	- Nízka úroveň vytvárania skupín medzi študentami. - Nízka úroveň reakcie na cudzieho návštevníka vybranej skupiny študentov. - Nízka úroveň kontroly študentov zo strany vyučujúceho.	- Získanie interných informácií o chodu fakulty. - Získanie informácií o výuke.	- Kontrola študentov zo strany vyučujúceho. - Vytváranie skupín pre prácu vo výuke. - Prípadné technické riešenie.
Podpora integrácie v skupine	Dochádzanie na pravidelnú výuku vybranej skupiny.	Útočník si získava dôveru študentov ale aj vyučujúcich vo vybranej skupine. Cíti sa byť integrovaný a má pocit, že sa mu jeho cieľ podarilo dosiahnuť.	- Nízka úroveň kontroly identity študentov. - Nízka úroveň kontroly zoznamov študentov – uvedený aj študenti, ktorí sú napríklad na Erazme. - Nízka úroveň komunikácie študenta s vyučujúcim o dochádzka.	- Pocit dôležitosti pre potenciálneho útočníka. - Skupina je ohrozená.	- Kontrola študentov zo strany vyučujúceho. - Pravidelné kontrolovanie aktuálnosti zoznamu študentov. - Zaznamenanie študentov na výjazde do informačného systému pre vyučujúcich, aby ostatný vyučujúci o tejto skutočnosti vedeli.
Vyvolanie konfliktu zo strany vyučujúceho – priama konfrontácia	Vyučujúci si všimne, že na výuke je viac študentov ako obvykle má byť, pretože sa dostavili všetci.	Študenti sú v priamom ohrození, pretože vyučujúci ohrozí dosiahnutie cieľa pre útočníka. Útočník stráca istotu.	- Priama konfrontácia útočníka. - Priame identifikácie útočníka. - Pocit sklamanie pred skupinou – možnosť vyvolania reakcie zo strany útočníka.	Priame ohrozenie života a zdravia študentov a vyučujúceho.	- Typové činnosti vyučujúcich pri výuke – ako sa správne zachovať. - Technické riešenie – tiesňové tlačidlo na stole vyučujúceho.
Útok na študenta	Útočník je vybudенý k útoku. Dochádza k reakcii pod stresom. Útok je realizovaný na najbližšieho študenta.	Študenti sú v priamom ohrození života a zdravia. Vyučujúci nevie reagovať. V väčšine prípadov nedochádza k monitoringu situácie na výuke.	- Vyvolanie reakcie priamou konfrontáciou útočníka. - Nízka úroveň zabezpečenia reakcie na podobné útoky. - Nízka úroveň schopnosti reakcie zo strany vyučujúceho. - Nízka technická podpora zvládania situácií.	- Priame ohrozenie života a zdravia študentov a vyučujúceho. - Nedochádza k možnosti uvedomenia záchranných zložiek.	- Typové činnosti vyučujúcich pri výuke – ako sa správne zachovať. - Technické riešenie – tiesňové tlačidlo na stole vyučujúceho.
Reakcia na útok	Útočník reaguje na paniku a stres pred koncom výuky. Dochádza k strate na životoch. Nakoniec zabije aj seba.	Študenti sú v priamom ohrození života a zdravia. Vyučujúci nevie reagovať. V väčšine prípadov nedochádza k monitoringu situácie na výuke.	- Vyvolanie reakcie priamou konfrontáciou útočníka. - Nízka úroveň zabezpečenia reakcie na podobné útoky. - Nízka úroveň schopnosti reakcie zo strany vyučujúceho. - Nízka technická podpora zvládania situácií.	- Priame ohrozenie života a zdravia študentov a vyučujúceho. - Nedochádza k možnosti uvedomenia záchranných zložiek.	- Typové činnosti vyučujúcich pri výuke – ako sa správne zachovať. - Technické riešenie – tiesňové tlačidlo na stole vyučujúceho.

Tab.1: Scenár: Napadnutie skupiny študentov vo výuke

Záverom danej kapitoly je možné vysloviť záver, že pre podrobnú analýzu odolnosti objektu je potrebné poznať jednotlivé etapy vývoja incidentu v danom objekte. Na základe podrobného rozpisu scenárov možného narušenia objektu je možné stanoviť následne odolnosť objektu a navrhnúť opatrenia, ktoré zvýšia odolnosť objektu, a tým znížia pravdepodobnosť prevedenia útoku. Pri vybranom objekte vysokej školy je veľmi dôležitým aspektom čas, v ktorom je prevedený útok. Pokiaľ hovoríme o čase, myslíme tým časť roka, v ktorom sa útok odohrá, ale aj čas počas dňa. V prípade útoku mimo vyučovanie je dopad na objekt menší ako v prípade prevedenia útoku v čase prebiehajúcej výuky.

3 Prípadová štúdia použitia penalizačných faktorov na vybraný objekt

V danej časti aplikácie do prípadovej štúdie je nutné poznamenať, že kategória objektov „mäkké ciele“ je špecifická kategória objektov, a to hlavne z dôvodu typu útokov, ktoré v objekte hrozia. Jedná sa o fakt, že v prípade útoku na mäkký cieľ štátu sú využívané práve verejné objekty a koreňová príčina napadnutia súvisí s nastavenými procesmi a vedomosťami a znalosťami samotných zamestnancov. Zamestnanci by mali byť na dané typy špecifických útokov preškolení, aby dokázali včasne identifikovať potenciálneho páchateľa.

V prípade uvedenej prípadovej štúdie dochádza k aplikácii uvedenej metodiky na univerzitnú budovu. V tomto prípade nedochádza k presnej identifikácii budovy, ktorá je predmetom prípadovej štúdie v článku, a to z dôvodu bezpečnosti daného objektu.

Penalizačné faktory nedokážu identifikovať schopnosť vyučujúceho identifikovať páchateľa v skupine. Penalizačné faktory sú také, ktoré dokážu byť v čase monitorované a merateľné. Avšak detekcie podozrivého chovania nie je merateľná a záleží na schopnosti a zručnosti zamestnanca (v tomto prípade vyučujúceho) včasne identifikovať charakteristické chovanie páchateľa. Na druhú stranu pravidelné cvičenia a vzdelávanie môže zvýšiť schopnosť vyučujúceho páchateľa identifikovať a reagovať na prípadný útok s využitím technických prostriedkov implementovaných do riadenia prevádzky objektu.

Uvedený typ útoku (napadnutie skupiny študentov na výuke) má nasledujúce fázy:

1. Preniknutie páchateľa do objektu
2. Preniknutie do skupiny študentov a na výuku
3. Podpora integrácie v skupine
4. Vyvolanie konfliktu zo strany vyučujúceho – priama konfrontácia
5. Útok na študenta
6. Reakcia na útok

V uvedenej časti článku nižšie dochádza k zostaveniu grafov, ktoré vizualizujú vývoj jednotlivých troch druhov bezpečnostných parametrov prípadne celkovej odolnosti objektu. Nasledujúca tabuľka zobrazuje vstupnú analýzu objektu a výpočet statickej analýzy na základe statických faktorov pre fyzickú bezpečnosť.

Fyzická bezpečnosť – statická analýza					
Kategória faktoru	Názov faktoru	Statická penalizácia			Váha
		FB	KB	PB	
Technická ochrana	Zabezpečenie perimetru	80	5	5	3
	Zabezpečenie vonkajšieho kontrolovaného priestoru	80	5	5	3
	Zabezpečenie plášťa budovy	60	10	10	3
	Zabezpečenie vnútorného kontrolovaného priestoru	70	15	15	3
	Zabezpečenie hlavného vstupu do vnútorného chráneného priestoru	60	20	20	3
	Zabezpečenie ostatných vstupov do vnútorného chráneného priestoru	70	20	20	3
	Zabezpečenie vnútorného obzvlášť chráneného priestoru	0	0	0	3
	Inštalácia a prevádzka zabezpečovacích zariadení	0	0	0	3
Režimová ochrana	Režimové opatrenia	0	0	0	3
Fyzická ostraha	Opatrenia fyzickej ostrahy	60	5	10	3
Proces pri strate dokumentov a ich nosičov		10	10	10	3
Personálna bezpečnosť	Preverovanie zamestnancov	10	10	10	3

	Dohody o ochrane informácií	0	0	0	3
	Podmienky výkonu pracovnej činnosti	5	5	5	3
	Školenie zamestnancov	90	5	20	3
	Reakcie na bezpečnostné incidenty	80	60	60	3
	Disciplinárny proces	20	20	20	3
	Ukončenie pracovného vzťahu	0	0	0	3
Vonkajšie vplyvy - lokalita	Miera kriminality	20	0	0	3
	Index kriminality	20	0	0	3
	Počty priestupkov	15	0	0	3
	Medziročná zmena trestnej činnosti	0	0	0	3
P_sMAX		4728	1121	1403	
P_s		750	190	210	
P_s* váha		2250	570	630	
I_{ods}		52,41	49,15	55,10	
Konvergovaná bezpečnosť		52,22			

Tab.2: Statická analýza fyzickej bezpečnosti vybraného objektu

Váha pre jednotlivé faktory je implicitne nastavená na hodnotu 3, a to z dôvodu, že uvedené kritériá nemajú špecifický význam pre uvedený typ objektu. Výsledné hodnotenie nám definuje index statickej odolnosti (I_{ods}) pre jednotlivé kategórie bezpečnosti (FB=52,41 KB=49,15 PB=55,10). Následne dochádza k aplikácii prípadovej štúdie – scenár: „Napadnutie študentov vo výuke“ – scenár popísaný v kapitole 2. tohto článku.

Prípadová štúdia je aplikovaná od fáze útoku číslo 5, a to útok na študenta. Jedná sa o aplikáciu v tejto fázy z dôvodu, že predchádzajúce fáze útoku nie je možné identifikovať za pomoci penalizačných faktorov.

Fyzická bezpečnosť – dynamická analýza					
Scenár: Napadnutie študentov na výuke / Fáza: útok na študenta					
Kategória faktoru	Názov faktoru	Dynamická penalizácia			Váha
		FB	KB	PB	
Technická ochrana	Poplachový stav PZTS	0	0	0	3
	Ďalšie stavy PZTS	0	0	0	3
	Poplachový stav detekovaný dohľadovým videosystémom	0	0	0	3
	Ďalšie stavy dohľadového videosystému	0	0	0	3
	Stav prístupového systému	0	0	0	3
	Stav EPS	0	0	0	3
	MZS	0	0	0	3
Režimová ochrana	Vstup/ výstup osôb	0	0	0	3
	Vjazd/ výjazd vozidiel	0	0	0	3
	Kľúčové hospodárstvo	0	0	0	3
Fyzická ostraha	Incidenty výkonu fyzickej strahy	0	0	0	3
Personálna bezpečnosť	Zahájenie trestného stíhania zamestnanca	0	0	0	3
Vonkajšie vplyvy - lokalita	Riziková akcia v okolí objektu	0	0	0	3
	Nariadená evakuácia objektu	0	0	0	3
	Informácia o hrozbe	90	0	30	3
P_dMAX		3065	565	900	
P_d		90	0	30	
P_d* váha		270	0	90	
Fáza: útok na študenta I_{odd}		8,81	0	10,00	
I_{od}=I_{ods}-I_{odd}		43,60	49,15	45,10	
Konvergovaná bezpečnosť		45,95			

Tab.3: Dynamická analýza fyzickej bezpečnosti pre scenár napadnutie študentov na výuke – fáza 5

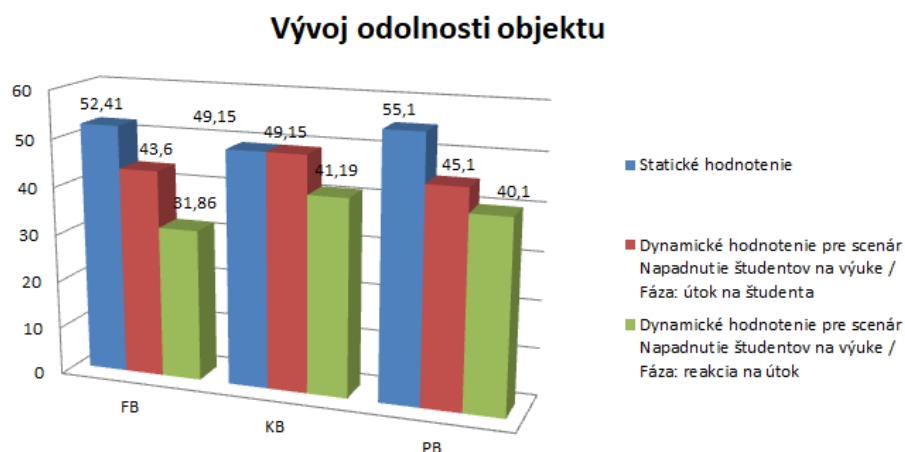
Vzhľadom na to, že pre popisovaný scenár sa jedná o prevedenie útoku za normálneho vyučovacieho procesu, tak nie je možné identifikovať pokles penalizačných faktorov do fáze: útok na študenta a prenesenie informácie na vrátnicu budovy. Žiadne monitorovacie a detekčné zariadenie nevykazuje detekovanú penalizáciu, ktorá by identifikovala vznik incidentu – prípadne ohrozenie objektu. Následne (po prenesení informácie na vrátnicu) je možné použiť dohľadový video systém inštalovaný v učebni, prípadne zistiť stav prístupového systému do učebne, kedy môže dôjsť zase k ďalšiemu poklesu, ako je uvedené v nasledujúcej tabuľke. Tento aspekt už ale môže byť identifikovaný, a tým pádom môže dôjsť k rýchlej schopnosti reagovať na vzniknutý

incident, čím sa zníži pravdepodobnosť úspešného prevedenia útoku a zníži sa dopad na ohrozené aktívum (v tomto prípade študentov).

Fyzická bezpečnosť – dynamická analýza					
Scenár: Napadnutie študentov na výuke / Fáza: reakcia na útok					
Kategória faktoru	Názov faktoru	Dynamická penalizácia			Váha
		FB	KB	PB	
Technická ochrana	Poplachový stav PZTS	0	0	0	3
	Ďalšie stavy PZTS	0	0	0	3
	Poplachový stav detekovaný dohľadovým videosystémom	0	0	0	3
	Ďalšie stavy dohľadového videosystému	60	5	5	3
	Stav prístupového systému	60	10	10	3
	Stav EPS	0	0	0	3
	MZS	0	0	0	3
Režimová ochrana	Vstup/ výstup osôb	0	0	0	3
	Vjazd/ výjazd vozidiel	0	0	0	3
	Kľúčové hospodárstvo	0	0	0	3
Fyzická ostraha	Incidenty výkonu fyzickej strahy	0	0	0	3
Personálna bezpečnosť	Zahájenie trestného stíhania zamestnanca	0	0	0	3
Vonkajšie vplyvy - lokalita	Riziková akcia v okolí objektu	0	0	0	3
	Nariadená evakuácia objektu	0	0	0	3
	Informácia o hrozbe	90	0	30	3
P_{dMAX}		3065	565	900	
P_d		210	15	45	
P_d* váha		630	45	135	
Fáza: reakcia na útok I_{odd}		20,55	7,96	15,00	
I_{od}=I_{ods}-I_{odd}		31,86	41,19	40,10	
Konvergovaná bezpečnosť		37,72			

Tab.4: Dynamická analýza fyzickej bezpečnosti pre scenár napadnutie študentov na výuke – fáza 6

Uvedené výsledné hodnoty sme spracovali do grafu pre ukážku vývoja jednotlivých faktorov v čase a celkovej odolnosti v čase. Jedná sa o celkovú odolnosť vypočítanú v rámci fyzickej bezpečnosti objektu popisovaného vo vybranej metodike.



Graf 1: Vývoj odolnosti fyzickej bezpečnosti prípadovej štúdie

Nasledujúca časť článku zobrazuje použitie rovnakej metodiky **prevádzkovú bezpečnosť**. Postup aplikácie metodiky je rovnaký, ako v prípade fyzickej bezpečnosti. Penalizácie sú nastavené podľa popisovaného katalógu penalizácií.

Prevádzková bezpečnosť – statická analýza					
Kategória faktoru	Názov faktoru	Statická penalizácia			Váha
		FB	KB	PB	
Prevádzkové technológie	Klimatizácia	0	0	0	3
	Osvetlenie	0	0	0	3
	Rozhlasy	0	0	0	3
	Lokalizácia aktív	30	5	10	3
	Záložné napájanie	10	10	10	3
	Rádiová komunikácia	0	0	0	3
	Komunikácia cez telefónnu sieť organizácie	0	0	0	3
	Komunikácia cez VTS	0	0	0	3
	Kamerový systém	0	0	0	3
Riadiaci systém pre zaistenie prevádzky organizácie	Riadiaci systém	5	5	10	3
	Záložné zdroje	3	2	10	3
Prevádzkové informácie	Informácie o obmedzení prevádzky	0	0	0	3
		0	0	0	3
Personál	Ľudské zdroje	0	0	0	3
		70	5	25	3
		70	15	25	3
Procesy/ Role	BOZP	0	0	0	3
	PO	0	0	0	3
	Riadenie rizík	20	5	5	3
	Bezpečnostné audity	20	5	5	3
	Bezpečnostná politika	20	10	10	3
	Bezpečnostný manažér	20	20	20	3
	Personálna bezpečnosť	0	0	0	3
	Kybernetická bezpečnosť	0	0	0	3
	Krízová a havarijná pripravenosť	30	20	30	3
	Zaškolenie pri nástupu do funkcie	100	40	30	3
	Plány obnovy	40	40	40	3
	Zodpovednosti a role	20	20	20	3
	Komunikačný strom	0	0	0	3
Prevádzkové udalosti	Kľúčové procesy	0	5	30	3
Prevádzkové udalosti – rutinné udalosti	Nastavenie a zastupiteľnosť kľúčových funkcií	0	0	0	3
Prevádzkové udalosti – znalosti a schopnosti zamestnancov	Zbrojný preukaz	0	0	0	3
	Školenie o PO	0	0	0	3
	Školenie o BOZP	0	0	0	3
	Certifikácie	0	0	0	3
	Iné školenia	0	0	0	3
P _s MAX		946	1121	1403	
P _s		458	207	280	
P _s * váha		1374	621	840	
I _{ods}		45,24	83,72	70,38	
Konvergovaná bezpečnosť		66,45			

Tab.5: Statická analýza prevádzkovej bezpečnosti vybraného objektu

V prípade vybraného útoku: „napadnutie študentov na výuke“ dochádza k jediným dvom druhom informácií, ktoré sa dostanú na vrátnicu uvedeného objektu, kde sa nachádza nonstop personál. Jednou z druhu informácií je tiesňové volanie na vrátnicu v prípade napadnutia. Druhou oznámenou udalosťou je po preverení kamerového systému (pokiaľ daná učebňa má kamerový systém) viditeľnosť incidentu zo stanoviska vrátnice. Ďalšou možnou informáciou môže byť prístupový systém, ktorý identifikuje vstup vyučujúceho, čo avšak pre nás nemá až taký význam (môže byť využitý na uzamknutie miestnosti – invakuácia). V tomto prípade sa jedná o výpočet dynamickej analýzy podľa nižšie uvedenej tabuľky.

Prevádzková bezpečnosť – dynamická analýza					
Kategória faktoru	Názov faktoru	Statická penalizácia			Váha
		FB	KB	PB	
Prevádzkové udalosti	Invakuace	30	5	15	3
	Kamerový systém	30	10	60	3
PdMAX		1181	318	888	
Pd		60	15	75	
Pd* váha		180	45	225	
Fáza: reakcia na útok Iodd		5,08	4,72	8,45	
Iod=Iods-Iodd		40,15	83,01	61,93	
Konvergovaná bezpečnosť		61,7			

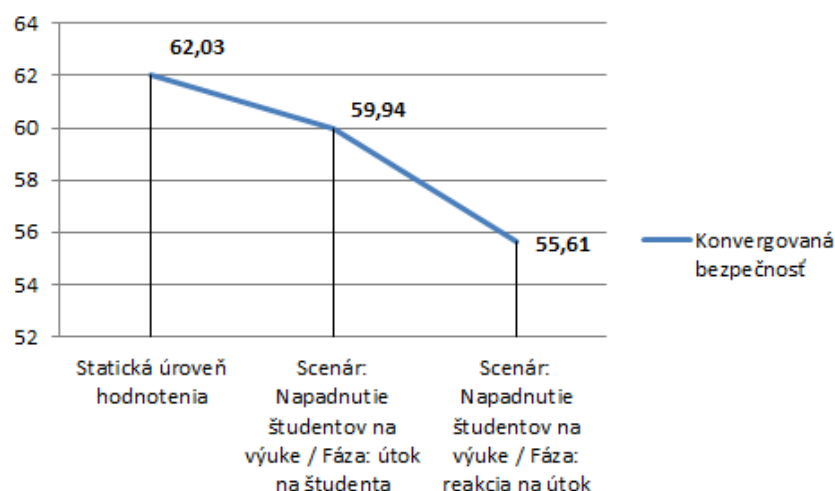
Tab.6: Dynamická analýza prevádzkovej bezpečnosti objektu

Pre kybernetickú bezpečnosť nie je v prípade daného útoku potrebné počítať vývoj kybernetickej bezpečnosti, a to z dôvodu, že daný typ útoku sa nijak nedotýka zmeny stavu kybernetickej bezpečnosti. V tomto prípade započítame do konvergovanej bezpečnosti index statickej bezpečnosti pre kybernetickú bezpečnosť.

Kybernetická bezpečnosť – statická analýza					
Kategória faktoru	Názov faktoru	Statická penalizácia			Váha
		FB	KB	PB	
Nástroje kyberbezpečnosti	Sieť (perimeter)	0	0	0	3
	Koncové stanice	19	30	22	3
		13	20	15	3
Bezpečnostná politika	BYOD	0	0	0	3
	Práva, povinnosti a chovanie užívateľov	8	12	9	3
		29	45	33	3
		22	35	26	3
Riadenie procesov	Krizový incident management	32	50	37	3
		34	53	39	3
		32	50	37	3
		22	34	25	3
	Organizačné opatrenia s vplyv 3. strany	19	30	22	3
P _s MAX		412	643	476	
P _s		230	359	265	
P _s * váha		690	1077	795	
I _{ods}		67,67	67,5	67,08	
I _{od} =I _{ods} -I _{odd}		67,67	67,5	67,08	
Konvergovaná bezpečnosť		67,42			

Tab.7: Statická analýza kybernetickej bezpečnosti vybraného objektu

Vývoj konvergovanej bezpečnosti v jednotlivých fázach útoku je znázornený na uvedenom grafe nižšie.



Graf 2: Vývoj konvergovanej bezpečnosti v jednotlivých fázach vybraného útoku

Na uvedenom grafe je možné vidieť vývoj stavu konvergovanej bezpečnosti v uvedených fázach útoku. Ako útok, na ktorom bola prevedená prípadová štúdia, bol zvolený útok: „*napadnutie študentov na výuke*“. V prvej identifikovateľnej fáze (5. fáza popisovaného útoku - útok na študenta) je možné spozorovať pokles bezpečnosti o **3,3 %**. V druhej fáze (6. fáza popisovaného útoku – reakcia na útok) reakcie na útok je pokles o **10,3%**. Je potrebné avšak poznamenať, že uvedený typ útoku nie je možné identifikovať skôr, ako uvedený útok nastane. Jedná sa o preniknutie do skupiny študentov dlhodobým pôsobením na skupinu. Najvyššiu mieru účinnosti opatrenia by v tomto prípade malo **školenie vyučujúcich**, ktorí by boli nútení zaznamenávať každú zmenu študenta v skupine, prípadne vstup na základe prístupovej karty, ktorý by avšak musel byť riadený tak, aby nedochádzalo k preniknutiu a vynechaniu prístupu.

Záver

Záverom je možné konštatovať, že uvedená metodika má veľký význam v prípade včasnej reakcie vyučujúceho a prepojenia systému tak, aby bolo možné rýchlo a efektívne riadiť prevádzku objektu už v prípade prevedenia daného typu útoku. V tomto prípade je možné vidieť pokles konvergovanej bezpečnosti, ktorý by následne viedol k riadeniu evakuácie objektu cestami mimo napadnutú časť objektu – učebňu. Prípadne by zamedzil nárastu ohrozenia ostatných návštevníkov objektu.

Tento článok 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. 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.
- [2] LAPKOVÁ, Dora, MRÁŽKOVÁ, Lucia. Metodika hodnocení odolnosti z pohledu měkkých cílů. Zlín: UTB, 2019. [Výzkumná zpráva], 86 s.
