TVORBA KATALOGŮ PENALIZAČNÍCH FAKTORŮ

CREATION OF PENALIZATION FACTORS CATALOGS

Jan VALOUCH
Univerzita Tomáše Bati ve Zlíně
Nad Stráněmi 4511, 760 05 Zlín, Česká republika
valouch@fai.utb.cz

Abstrakt: *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. Hodnocení odolnosti může být založeno na snímání změn stavu faktorů, které podstatně ovlivňují odolnost objektu. Míra vlivu na odolnost může být vyjádřena jako penalizace, čili snížení odolnosti. V této souvislosti je možno definovat metodu penalizace, jako postup pro hodnocení odolnosti objektů z hlediska konvergované bezpečnosti. Následující článek popisuje tvorbu katalogů penalizačních faktorů, jako základních dokumentů pro aplikaci penalizační metody.*

Klíčová slova: *fyzická bezpečnost, konvergovaná bezpečnost, odolnost, penalizace, katalog.*

Abstract: *The ability of a reference object to protect assets and manage security breaches is expressed by its resilience.Resilience expresses how an object is able to resist the harmful effect and protect its assets. The resilience rating can be based on sensing changes in the status of factors that significantly affect the object's resistance. The degree of impact on resilience can be expressed as a penalty. In this context, it is possible to define a penalty method as a procedure for assessing the resilience of objects in terms of converged security. The following article describes the creation of catalogs of penalty factors as the basic documents for the application of the penalty method.*

Keywords: *physical security, converged security, resilience, penalties, catalog.*

Úvod

Při výpočtu indexů odolnosti referenčního objektu se využívají penalizační faktory, které jsou uvedeny v katalozích penalizačních faktorů. Výchozím dokumentem je **obecný katalog penalizačních faktorů**, který představuje přehled všech potencionálních vnějších a vnitřních činitelů (faktorů), které ovlivňují odolnost objektu. Mezi takové penalizační faktory patří především negativní stavy a události (absence systémů, absence bezpečnostní dokumentace, poruchy, poplachové stavy, nedostupnost informací, výpadky dodávky energií atd.) Tento katalog představuje hlavní nástroj v rámci hodnocení odolnosti objektů z hlediska konvergované bezpečnosti při využití metody penalizace [1]. Návrh postupu tvorby a aplikace obecného katalogu je popsán v následujících podkapitolách.

1 Metodika tvorby katalogu

V rámci hodnocení odolnosti referenčního objektu z hlediska konvergované bezpečnosti (fyzická, kybernetická a provozní bezpečnost) 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:

- 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),
- zpřesnění katalogu penalizačních faktorů pro jednotlivá aktiva v objektu, zahrnujícího všechny druhy bezpečnosti (fyzická, kybernetická a provozní bezpečnost),
- výpočet indexu odolnosti aktiva pro jednotlivé druhy bezpečnosti,
- 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. Potřebné údaje (informace o stavech) ke všem faktorům uvedeným v katalogu musejí být snímatelné automaticky (výstupy z technických prostředků) nebo manuálně zadatelné do online security manageru [2].

V rámci hodnocení vybraného, konkrétního 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) [3].

Jednotlivým faktorům budou dále přirazeny 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) [2].

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.

Při určování penalizačních faktorů je vhodné vycházet z kategorizace jednotlivých druhů bezpečnosti. Např. u fyzické bezpečnosti je možno provést její dekompozici do následujících oblastí:

- technická ochrana,
- režimová ochrana,
- fyzická ostraha,
- administrativní bezpečnost,
- personální bezpečnost,
- vnější vlivy, lokalita [1].

Tyto oblasti mohou v rámci obecného katalogu představovat **kategorie faktorů** a to z důvodu větší přehlednosti. V rámci těchto kategorií jsou pak **na základě expertních úvah** vydefinovány jednotlivé penalizační faktory a vytvořena jejich bližší charakteristika, např.:

- technická ochrana (kategorie faktoru),
- poplachový stav PZTS (název faktoru),
- narušení perimetru objektu (charakteristika faktoru, nebo také dílčí faktor) [4].

Příklad u provozní bezpečnosti:

- provozní technologie (kategorie faktoru),
- osvětlení (název faktoru),
- porucha osvětlení (charakteristika faktoru, nebo také dílčí faktor).

Příklad u kybernetické bezpečnosti:

- nástroje kybernetické bezpečnosti (kategorie faktoru),
- koncové stanice (název faktoru),
- šifrování dat na mobilních zařízeních (charakteristika faktoru, nebo také dílčí faktor).

Obecný katalog bude sestaven v „maximální“ podobě, s tím, že se předpokládá, že v rámci aplikace hodnotícího nástroje pro konkrétní objekt, budou vybrány a hodnoceny pouze relevantní faktory. Bude se vytvářet **výchozí katalog penalizačních faktorů** pro vybraný konkrétní referenční objekt. Např. pokud v objektu není nainstalován systém PZTS, budou relevantní dynamické faktory typu: poplachový stav PZTS, poruchový stav PZTS atd. z obecného katalogy vyřazeny. Následující tabulky č. 1, 2 a 3 prezentují ukázky části obecných katalogů pro jednotlivé druhy bezpečnosti. Počet faktorů v obecných katalozích se předpokládá cca 100 - 200 pro každý druh bezpečnosti. Samozřejmě se předpokládá možnost jeho dalšího rozšiřování.

Struktura penalizačních faktorů je následující:

- kategorie faktoru,
- název faktoru,
- charakteristika faktoru,
- výchozí penalizace pro fyzickou bezpečnost (předpokládaný dopad faktoru na fyzickou bezpečnost),
- výchozí penalizace pro kybernetickou bezpečnost (předpokládaný dopad faktoru na kybernetickou bezpečnost),
- výchozí penalizace pro provozní bezpečnost (předpokládaný dopad faktoru na provozní bezpečnost),
- senzor (zdroj informace o aktivaci faktoru),
- řešitel (předpokládaná osoba nebo organizační prvek, odpovědný za řešení problému).

	Část I. Fyzická bezpečnost							
	B. Dynamické faktory							
ID	**Kategorie faktoru**	**Název faktoru**	**Charakteristika faktoru**	**Výchozí penalizace**			**Senzor**	**Řešitel**
				FB	**KB**	**PB**		
1.	Technická ochrana	Poplachový stav PZTS	Narušení perimetru objektu	20	10	10	Detektor PZTS	Ostraha
2.			Narušení pláště objektu – technické prostupy	30	10	30	Detektor PZTS	Ostraha
3.			Narušení pláště objektu - okna	30	10	10	Detektor PZTS	Ostraha
4.			Narušení pláště objektu - dveře	40	20	20	Detektor PZTS	Ostraha
5.			Narušení vnitřního prostoru objektu	40	20	30	Detektor PZTS	Ostraha
6.			Narušení předmětové ochrany	50	30	30	Detektor PZTS	Ostraha

Tab.1: Příklad obecného katalogu penalizačních faktorů- fyzická bezpečnost [1]

	Část II. kybernetická bezpečnost							
	A. Statické faktory							
ID	**Kategorie faktoru**	**Název faktoru**	**Charakteristika faktoru**	**Výchozí penalizace**			**Senzor**	**Řešitel**
				FB	**KB**	**PB**		
1.	Nástroje kyberbezpečnosti	Síť (perimetr)	SIEM	10	30	10	audit	
2.			IDS	10	30	10	audit	
3.			IPS	10	30	10	audit	
4.			Firewall	10	40	20	audit	
5.			Reverzní proxy	10	40	20	audit	

Tab.2: Příklad obecného katalogu penalizačních faktorů- kybernetická bezpečnost [1]

	Část III. Provozní bezpečnost							
	A. Statické faktory							
ID	Kategorie faktoru	Název faktoru	Charakteristika faktoru	Výchozí penalizace			Senzor	Řešitel
				FB	KB	PB		
1	Provozní technologie	Klimatizace	Absence klimatizace	10	10	15	audit	
2	Provozní technologie	Ventilace	Absence ventilace	10	10	20	audit	
3	Provozní technologie	Vytápění	Absence vytápění	10	20	30	audit	
4	Provozní technologie	Voda	Absence vody	20	20	60	audit	

Tab.3: Příklad obecného katalogu penalizačních faktorů- provozní bezpečnost [1]

1.1 Aktualizace penalizačních údajů

Z důvodu zajištění správných výsledků při hodnocení odolnosti objektů metodou penalizace je nutné aktualizovat penalizační faktory. Aktualizace je nutno provést v případě, kdy došlo k zásahu do struktury některého systému, který se podílí na zajištění bezpečnosti aktiva a tudíž má vliv na jeho odolnost. Aktualizované budou penalizační údaje těch faktorů, které jsou navázány na systémy, ve kterých došlo k zásahu. K takovým zásahům patří např.:

- doplnění nových prvků systémů a odebírání starých (např. komponenty PZTS, DV, SKV, EPS atd.),
- aktualizace SW,
- poškození nebo poruchy prvků systémů s předpokladem dlouhodobého výpadku (vyřazení prvků ze systému),
- opravy prvků systémů po dlouhodobém výpadku (zařazení prvků do systému),
- odstranění problémů/incidentů z počátečního auditu, atd. [5].

Pokud nedojde ke změnám struktury bezpečnostních systémů, aktualizace statických penalizačních údajů se pro vybrané faktory bude vykonávat vždy po revizi souvisejících systémů, a to v doporučované minimální periodicitě 1x za rok. Dynamické faktory jsou aktualizovány průběžně (při změně v bezpečnostních systémech).

2 Aplikace katalogu v rámci výpočtu odolnosti objektu

V rámci výpočtu indexů odolnosti referenčního objektu se vychází z **obecných katalogů penalizačních faktorů**. V dalším textu je popsán postup práce s katalogy penalizačních faktorů a penalizacemi při výpočtu indexů odolnosti aktiv pro jednotlivé druhy bezpečnosti.

Stěžejním úkolem při aplikaci obecného katalogu na konkrétní objekt je provedení výběru relevantních penalizačních faktorů (**vytvoření výchozího katalogu penalizačních fak**torů) a prioritizace obecných hodnot penalizace daného penalizačního faktoru na podmínky hodnoceného objektu, resp. jednotlivých aktiv objektu. Prioritizace se provádí z důvodu posouzení vlivu faktoru na skutečné podmínky aktiva a využívá se tzv. váhování. Váhy se stanovují v rozsahu 1 – 5. Hodnota 1 znamená, že faktor má na aktivum menší vliv a dopad, hodnota 5 znamená maximální dopad. Pomocí váhy mohou být tedy hodnoty penalizací v katalogu penalizačních faktorů zvyšovány s ohledem na možné dopady v konkrétním objektu [5]. Postup aplikace obecného katalogu pro konkrétní objekt je následující:

- specifikace referenčního objektu (vymezení objektu, právní subjektivita, organizační členění, kompetence, cílové funkce, odpovědnost za bezpečnost atd.),
- specifikace aktiv (analýza rizik a určení základních aktiv referenčního objektu - život a zdraví osob, majetek, technologie, data, životní prostředí atd.),
- vytvoření výchozího katalogu penalizačních faktorů (redukcí/výběrem z obecného katalogu, na základě znalosti referenčního objektu, aktiv, vnějších a vnitřních konfiguračních a ochranných činitelů),
- zpřesnění výchozího katalogu penalizačních faktorů pro jednotlivá aktiva (výběr faktorů, které jsou s aktivy skutečně spojeny škodícím účinkem či jinými podstatnými vlivy + stanovení váhy penalizačního faktoru),
- výpočet indexu odolnosti aktiva pro jednotlivé druhy bezpečnosti,

- výpočet indexu odolnosti pro jednotlivé druhy bezpečnosti,
- výpočet indexu odolnosti pro celý referenční objekt [6].

Závěr

Článek prezentuje návrh postupu tvorby obecného katalogu penalizačních údajů, jako základního dokumentu pro aplikaci metody penalizace při hodnocení odolnosti objektů. Obecný katalog penalizačních faktorů, musí obsahovat maximum statických a dynamických faktorů, využitelných pro hodnocení odolnosti referenčních objektů a jejich aktiv. Přehledy potencionálních faktorů zpracovávají experti v rámci jednotlivých druhů bezpečnosti (fyzická, kybernetická, provozní bezpečnost). Potřebné údaje (informace o stavech) ke všem faktorům uvedeným v katalogu musejí být snímatelné automaticky (např. z výstupů poplachových systémů) nebo manuálně zadatelné (např. informace o existenci technického prostředku v objektu, revize, plánované akce v objektu a jeho okolí, které mohou ovlivnit jeho bezpečnost atd.). Katalog je rozdělen na části fyzické, kybernetické a provozní bezpečnosti. Tyto se dále dělí na statické a dynamické faktory. Struktura katalogu by měla být tvořena následujícími údaji: ID faktoru, kategorie faktoru, název faktoru, charakteristika faktoru, výchozí penalizace (vliv faktoru), senzor a řešitel, odpovídající za reakci na aktivaci faktoru. Při aplikaci obecného katalogu na konkrétní objekt, bude proveden výběr relevantních penalizačních faktorů (zpravidla redukcí) a tím se vytvoří výchozí katalog penalizačních faktorů pro hodnocený objekt.

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] 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.

[2] 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.

[3] VALOUCH, Jan, URBANČOKOVÁ, Hana. Katalog penalizačních kritérii 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.

[4] 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.

[5] 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.

[6] 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.