KONVERGOVANÁ BEZPEČNOST A JEJÍ PŘÍNOS PRO OBJEKTY VEŘEJNÉ SPRÁVY

CONVERGED SECURITY AND ITS CONTRIBUTION TO OBJECTS OF TERRITORIAL SELF-GOVERNMENT

Hana URBANČOKOVÁ, Jan VALOUCH
Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky
Nad Stráněmi 4511, 760 05 Zlín, Česká republika
urbancokova@utb.cz; valouch@utb.cz

Abstrakt: *Bezpečnost aktiv v objektech veřejné správy je v současné době řešena oddělenými systémy fyzické, kybernetické a provozní bezpečnosti. Informace z těchto druhů bezpečností lze vzájemně propojit tak, aby bylo možné efektivněji detekovat narušení bezpečnosti a rychleji na tuto skutečnost reagovat, čímž se také zvýší pravděpodobnost zadržení narušitele přímo při činu nebo bezprostředně po něm. Takové propojení informací z různých druhů bezpečnosti je označováno jako konvergovaná bezpečnost.*

Klíčová slova: *konvergovaná bezpečnost, zabezpečení, veřejná správa, objekty veřejné správy*

Úvod

Bezpečnost je stav, kdy vnitřní a vnější podmínky systému umožňují plnění jeho určených funkcí a jeho další rozvoj. Lze tedy říci, že systém je ve stavu bez reálné hrozby nebezpečí. Pod pojmem systém můžeme chápat jakýkoliv společenský, přírodní či technologický systém, který vznikl v zájmu člověka a společnosti. Cílem oboru bezpečnosti je chránit tyto systémy (např. objekt a jeho aktiva) a to zejména před vznikem nežádoucí újmy, nebo před negativními dopady na systém vzniklých při narušení jeho bezpečnosti. Cílem bezpečnosti je újmy a dopady minimalizovat na co nejnižší možnou úroveň.

Vlivem technologického rozvoje a nárůstu počtu jednotlivých druhů aktiv sloučených v jednom systému, narůstá i počet druhů bezpečnosti, které musí být zajišťovány v rámci ochrany daného systému. Příkladem takovéhoto systému jsou objekty veřejné správy, kterým se budeme věnovat v tomto příspěvku. Objekty veřejné správy dnes chrání svá aktiva především pomocí fyzické bezpečnosti, administrativní bezpečnosti, personální bezpečnosti, provozní bezpečnosti, kybernetické bezpečnosti a BOZP (bezpečnost a ochrana zdraví při práci) [1].

V současnosti je zaužívaný stav, kdy je každý druh bezpečnosti zajišťován nezávisle na ostatních druzích, což je poměrně neefektivní způsob řešení bezpečnosti. Jedním z negativ, které takovéto řešení přináší je neschopnost propojit informace ze senzorů oddělených druhů bezpečnosti a s tím spojená neschopnost včasného odhalení možného nebezpečí. Pokud například chce zaměstnanec neoprávněně zkopírovat data ze serveru přímo v serverovně, neexistuje v současnosti možnost okamžitého propojení informací z bezpečnostních systémů, které zajišťují některý z aspektů ochrany tohoto aktiva. Příklad rozdílu v odhalení a zajištění narušitele když není propojena fyzická, kybernetická a provozní bezpečnost a případu, kdy by se informace z těchto druhů bezpečnosti vzájemně spojovali v reálném čase, si přiblížíme ve čtvrté kapitole.

Dalším negativem oddělených bezpečnostních systémů jsou zvyšující se náklady na zajištění bezpečnosti, plynoucí z nezávislého zajištění každého druhu bezpečnosti. To se projevuje nejenom v technologickém zajištění bezpečnosti, ale také v personální náročnosti. Každý druh bezpečnosti je obvykle zajišťován samostatnou skupinou odborníků, využívá vlastní síť bezpečnostních technologií i vlastní ochranné procesy [2].

Řešením propojení vybraných druhů bezpečnosti na základě jejich vzájemných vazeb je jejich slučování do tzv. konvergované bezpečnosti, kterou si blíže popíšeme v první kapitole tohoto příspěvku. Ve druhé kapitole se budeme věnovat specifikám, které jsou typické pro objekty veřejné správy, a nejběžnějšímu zabezpečení v těchto objektech, především ve třech oblastech - fyzické bezpečnosti, kybernetické a provozní bezpečnosti. V rámci třetí kapitoly nastíníme jednoduchý příklad vyhodnocení narušení, když jsou technologie fyzické,

kybernetická a provozní bezpečnosti odděleny a příklad možné spolupráce v rámci jejich propojení v konvergované bezpečnosti. Ve čtvrté kapitole, budeme rozebírat význam aplikace konvergované bezpečnosti v objektech veřejné správy.

1 Konvergovaná bezpečnost

Potřeba zefektivnit celkové zabezpečení vybraných aktiv nás vedla k vytvoření konceptu konvergované bezpečnosti. Tento koncept je tvořen slučováním více druhů bezpečnosti, které jsou použity pro ochranu společného aktiva, a to na základě společných vazeb mezi nimi. Doposud byly tyto vazby přehlíženy a jednotlivé druhy bezpečnosti chápány jako samostatné a oddělené bezpečnostní systémy, které byly zaměřené vždy na určitý druh aktiv a využívaly vlastní nástroje pro detekci ohrožení [3].

Některými z už zmíněných druhů bezpečnosti, které jsou řešeny v objektech veřejné správy, jsou administrativní bezpečnost a BOZP. Administrativní bezpečnost zahrnuje opatření, jejichž cílem je zejména zajištění ochrany utajovaných informací. Pravidla administrativní bezpečnosti popisují postupy, které musí pracovníci dodržovat při tvorbě záznamu informací, při jejich evidenci, přepravě, zpracování, rozmnožování, ukládání, likvidaci nebo jiné manipulaci s nimi. BOZP je také soubor předpisů, jejichž cílem je stanovení podmínek pro eliminaci vlivů nebezpečných a škodlivých faktorů pracovního procesu a prostředí na zaměstnance. Administrativní bezpečnost i BOZP jsou typy bezpečností, jejichž kontrolním mechanizmem jsou především fyzické kontroly vybranými pracovníky. Protože se nejedná o druhy bezpečnosti, které by ke svému plnění běžně využívali nějaké jiné kontrolní nástroje, jejich konvergence s dalšími druhy bezpečností pro naše potřeby není možná. Z tohoto důvodu se dále budeme věnovat bezpečnosti v objektech veřejné správy jenom v rámci konvergence fyzické, kybernetické a provozní bezpečnosti.

Cílem fyzické bezpečnosti je v první řadě ochrana vůči fyzickým hrozbám, jako je požár, krádež, vloupání, úmyslné poškození majetku a zejména ochranu života a zdraví osob. Hlavním úkolem fyzické bezpečnosti je zaznamenat přítomnost narušitele v prostorech, které jsou fyzickou bezpečností sledovány pomocí komponentů zebezpečovacích systémů. Takovýmito komponenty jsou detektory poplachových zabezpečovacích a tísňových systémů (PZTS), dohledové videosystémy (DV) a/nebo systémy kontroly vstupu (SKV). Samostatnou kategorií jsou komponenty elektrické požární signalizace (EPS), jejichž instalace je dnes ve většině veřejných objektů vyžadována relevantními právními předpisy v souladu s požárně bezpečnostním řešením staveb.

Naproti tomu kybernetická bezpečnost se prioritně zaměřuje na informační technologie. Zaměřuje se na ochranu technických přístrojů, jako jsou počítače, mobilní telefony, PDA, tablety, servery a jiné zařízení, které pracují s elektronickými daty. Kybernetická bezpečnost sleduje tok dat v informační sítí pomocí softwarových a hardwarových nástrojů. Hlavním úkolem je zabránit kyberkriminalitě- krádeži dat, jejich poškození, pozměnění, blokování či vymazání, případně zajišťování informačních technologií vůči kyberútokům a šířením škodlivých kódů.

Další důležitým druhem bezpečností je provozní bezpečnost dohlížející na naplňování cílové funkce dané organizace tak, aby nedocházelo k narušení, omezení nebo úplnému zastavení provozu. K zajištění provozní bezpečnosti můžou být využity některé komponenty zabezpečovacího systému (např. systémy kontroly vstupu), ale převážně jsou využity vlastní kontrolní nástroje.

Konvergovaná bezpečnost využívá souvztažnosti jednotlivých druhů bezpečnosti v rámci vybraného aktiva. Když budeme schopni získaná data z jednotlivých druhů bezpečnosti spojit a správně interpretovat, budeme moci rychleji a lépe odhalit vznikající narušení bezpečnosti a cíleněji zajistit jeho řešení.

2 Objekty veřejné správy a jejich aktuální zabezpečení

Veřejnou správou ve funkčním pojetí se rozumí, že se jedná prakticky o výkon veřejné správy, jako výkon podzákonné a nařizovací činnosti těchto orgánů. Veřejná správa jako správa veřejných záležitostí je správou ve veřejném zájmu a subjekty, které ji realizují, ji vykonávají jako právem uloženou povinnost, a to z titulu svého postavení veřejnoprávních subjektů. Posláním orgánů veřejné správy je zákony, resp. další obecně závazné právní předpisy, zavádět a provádět při použití různých forem činnosti, tedy i odvozené normalizace.

V objektech veřejné správy se převážně zpracovávají utajované informace týkající se správy státu a osobní informace osob spojených s Českou republikou (fyzické i právnické osoby - občané České republiky, cizinci žijící na území České republiky, tuzemské i zahraniční organizace). Tyto informace jsou převážně v elektronické podobě, ale mnohé existují i v papírové formě (tiskopisy).

Jelikož objekty veřejné správy jsou často veřejně přístupné budovy, kdokoliv má možnost volného prohlédnutí vnitřní struktury budovy, umístění některých komponentů zabezpečovacího systému a vytipování si

slabých míst v zabezpečení. Volná přístupnost objektů veřejnosti dává prostor i k drobným krádežím. Ohrožení však nepřichází pouze od cizích osob, ale rovněž i ze strany zaměstnanců, kteří dokonale znají vnitřní infrastrukturu objektu. Páchání přestupků nebo trestné činnosti vlastními zaměstnanci, jako krádeže nebo vynášení citlivých informací je v dnešní době velmi časté nejen v soukromých organizacích, ale i v těch veřejných.

Zabezpečení v jednotlivých objektech veřejné správy se může lišit, a to především z hlediska, zda se jedná o obecný úřad, krajský úřad, sídlo některého ministerstva či sídlo dalších ústředních orgánů státní správy řízených přímo vládou (Český statistický úřad, Komise pro cenné papíry apod.) nebo se jedná o sídlo ostatních orgánů podřízených ministerstvům (Česká obchodní inspekce, Český telekomunikační úřad apod.).

Jako referenční objekt pro příklad běžného zabezpečení objektu státní správy byl v rámci výzkumu zvolen obecní úřad, který z bezpečnostních důvodů nebude jmenován. Tento objekt se nachází v centru města a pozůstává ze šesti nadzemních a jednoho podzemního patra. Objekt je z jedné strany připojen k sousednímu objektu, další tři strany sousedí s městkou komunikací a chodníky pro pěší. Vstupy do budovy jsou dva, zadní vchod pro zaměstnance a hlavní vchod pro veřejnost.

Z umístění objektu je zřejmé, že v rámci fyzické bezpečnosti nebude v rámci zabezpečení objektu realizována před-perimetrická, perimetrická a venkovní prostorová ochrana objektu. Plášť budovy je monitorován kamerovým systémem, který přenáší obraz na pracoviště informací, umístěné v budově úřadu v blízkosti hlavního vchodu. Zabezpečení oken magnetickými kontakty je realizováno na přízemí a v prvním patře. Vchod pro zaměstnance je otevírán pomocí přístupových karet zaměstnanců, hlavní vchod je bez jakékoliv kontroly vstupujících osob. V blízkosti obou vchodů se nachází docházkový systém pro zaměstnance. Vnitřní prostory jsou chráněny pomocí kamerového systému na chodbách a pohybovými detektory v jednotlivých místnostech objektu. Serverovna má 24 hodinové zabezpečení detektory pohybu, které jsou deaktivovány po vstupu oprávněné osoby. Vstup je podmíněn zadáním přístupového hesla oprávněné osoby a prostor je monitorován kamerovým systémem. Ve vybraných odděleních úřadu se nachází tísňová tlačítka a v celé budově je instalován systém elektrické požární signalizace. Výstup z PZTS je přenášen na dohledové poplachové a přijímací centrum (DPPC) městské policie. Výstup z EPS je také přenášen na DPPC městské policie s návazností na hasičský záchranný sbor. Obrazové záznamy z kamer DV se přenášejí na obrazovku/monitor na pracoviště informací (pracoviště recepce ve vestibulu budovy), zobrazuje se jen to, co si obsluha právě nastaví a proto se také všechny záznamy ukládají na úložiště, které se nachází přímo v budově (v serverovně). Informace z SKV se ukládají na server.

Kybernetická bezpečnost je zajišťována především samostatnou informační sítí z optických kabelů, standardními aplikacemi antivirových programů, pravidelně se měnícím přístupovým heslem každého zaměstnance, přístupností každého zaměstnance jenom k datům vyžadovaných pro jeho práci a omezení připojení zařízení k síti (v objektu se nenachází wifi, připojení do sítě je povoleno jenom prostřednictvím datové zásuvky v každé kanceláři a oprávnění každého počítače nastavuje správce sítě). Jednotliví zaměstnanci nemají v rámci počítačů oprávnění instalovat jakékoliv programy, připojit k počítači lze však jakékoliv další zařízení (USB, přenosný disky i mobilní telefon). Protože jsou zařízení připojena k internetu, zobrazované webové stránky nejsou nijak omezované a stahování příloh emailu také nepodléhá kontrole. Upozornění na možný výskyt škodlivého kódu v stahovaném souboru poskytuje antivirový program. Jednou týdně probíhají pravidelné kontroly na přítomnost a šíření škodlivých kódů a to u všech zařízení připojených do informační sítě úřadu.

V rámci provozní bezpečnosti je sledována pouze dodávka elektrické energie, kde serverovna a všechny důležité systémy jsou v případě výpadku elektrické energie automaticky propojené na napájení dieselovým agregátem a s využitím přístupového systému je k dispozici docházkový systém, který upozorňuje na nedostupnost lidských zdrojů. Další faktory narušující provozní bezpečnost objektu jsou do systému zadávány příslušným pracovníkem ručně (přerušené vytápění, klimatizace, odstávka serveru, plán revizí, výpadek telekomunikační sítě apod.).

3 Příklad narušení bezpečnosti

Příklad rozdílu v odhalení a zajištění narušitele když není propojena fyzická, kybernetická a provozní bezpečnost a případu, kdy by se informace z těchto druhů bezpečnosti vzájemně spojovali v reálném čase, bude nastíněn v této kapitole.

V případě, kdy by například zaměstnanec chtěl neoprávněně zkopírovat data ze serveru přímo v serverovně, neexistuje v současnosti možnost okamžitého propojení informací z bezpečnostních systémů, které zajišťují některý z aspektů ochrany tohoto aktiva. Do fyzické bezpečnost patří SKV, který zajišťuje vstup do prostoru serverovny pomocí přístupového hesla i kamerový systém, který je v této místnosti umístěn. Údaje o

kopírování dat přímo z USB portu na serveru, lze zase sledovat v rámci zajištění kybernetické bezpečnosti. V rámci provozní bezpečnosti lze do systému zadat plánovanou manipulaci s daty.

Při oddělených bezpečnostních systémech je odhalení odcizení dat osobou, která má oprávnění pro vstup do serverovny i pro manipulaci s daty, a její okamžité zadržení nerealizovatelné. Jednotlivé systémy nevyhodnotí jeho jednání za rizikové, protože pro fyzickou bezpečnost osoba vstupující do prostoru serverovny měla platné přístupové heslo, kamerový systém nahrává záznam a zaměstnanec na informacích si nemusí všimnout podezřelé aktivity, protože osobu na záznamu zná. Provozní bezpečnost má v plánu zadanou manipulaci s daty, ale podrobnosti už nejsou nikam interpretovány. Jediný systém, který může zaznamenat podezřelou činnost je kybernetická bezpečnost, ale pokud zaměstnanci zodpovídající za kybernetickou bezpečnost vyhodnotí získané informace, zájmová osoba bude dávno mimo objekt. Dnes je tedy na vyhodnocení rizika potřeba čas, který poskytne narušitelovi prostor na únik.

V případě propojení informací z fyzické, kybernetické a provozní bezpečnosti do uceleného systému konvergované bezpečnosti, by bylo odhalení takovéto jednání zaměstnance jednodušší. Přístupový systém by zaměstnance vpustil do prostoru serverovny, kamerový systém by zaměstnanci na informacích poskytl obrazový záznam ze serverovny a zároveň by byly k dispozici informace z provozní bezpečnosti, kde by v rámci plánu manipulace s daty museli být následující informace - datum a časový údaj, na kdy je úkon naplánován, osoba oprávněná k manipulaci a osoba/y dohlížející na správný postup. V této fázi by zaměstnanec na pracovišti informací (recepci) zaregistroval nesrovnalosti (v serverovně je jenom jedna osoba, nesouhlasí plánovaný datum nebo čas) a dále by postupoval v souladu s připravenými postupy (např. by kontaktoval určené osoby pro řešení incidentu, nebo v krajním případě by bylo technicky možné i zablokovat výstup ze serverovny). V případě, kdy by zaměstnanec na recepci nesrovnalosti nezaregistroval, zaznamenal by takové jednání systém kybernetické bezpečnosti, který by z provozní bezpečnosti měl mít přesné informace o tom, s kterými daty a v které době by se mělo manipulovat a tuto skutečnost porovnávat s daty získanými ze svých kontrolních mechanismů. Jestli by některá skutečnost neodpovídala (datum, čas, typ kopírovaných souborů), byl by vyhlášen poplach.

Konvergovaná bezpečnost nám v tomto případě poskytla dvě možnosti odhalení krádeže dat vlastním zaměstnancem. První možnost odhalení stavěla na všímavosti osoby sedící u monitoru kamerového systému, druhá možnost odhalení narušitele spoléhala na kontrolní mechanizmy jednotlivých bezpečnostních systémů. Aplikací konvergované bezpečnosti se výrazně zvýšila pravděpodobnost včasného odhalení narušitele a jeho zadržení přímo při činu.

4 Závěr / Přínos konvergované bezpečnosti pro objekty veřejné správy

Z příkladu popsaného v předešlé kapitole je zřetelné, že konvergovaná bezpečnost nám umožní lepší kontrolu nad vykonávanými procesy v objektu veřejné správy. Důležitá je především kontrola manipulace s utajovanými a jinými citlivými daty, ale systém konvergované bezpečnosti nám může pomoct i při běžném provozu objektu veřejné správy, nebo při předvídání možných hrozeb.

V rámci běžného provozu mohou být počítače nebo hesla jednotlivých zaměstnanců vázány na přístupový systém a v čase jejich nepřítomnosti v objektu by nebylo možné přihlásit se k jejich uživatelskému účtu nebo použít jejich přístupové heslo. Dokonce by bylo možné v jejich nepřítomnosti jejich počítače úplně odpojit od sítě. Takovéto odpojení počítačů by mělo význam i při zapomenutí otevřeného okna, kde prostřednictvím signálu magnetického kontaktu na okně vyhlásí PZTS poplach.

Mezi přínosy aplikace systému konvergované bezpečnosti patří především:

- naplnění aktuálních potřeb v oblasti bezpečnostního managementu a řízení kontinuity činností podniků (potřeba nerozlišovat jednotlivé druhy bezpečností, ale pracovat s jedinou bezpečností jako celkem),
- komplexní splnění požadavků zákazníka na zabezpečení a řízení technologií v objektu,
- úspora energií a zvýšení bezpečnosti,
- efektivní zhodnocení úrovně odolnosti infrastruktury sledovaného podniku, segmentu nebo i celého odvětví proti různým typům hrozeb,
- možnost vytvořit jednotný postup hodnocení odolnosti vybraných typů objektu objektů (státní správa, energetika, měkké cíle, doprava, telekomunikace atd.) z pohledu fyzické, kybernetické a provozní bezpečnosti,
- možnost analýzy dat, zaznamenaných v historii systému konvergované bezpečnosti s cílem vyhodnotit vývoj stavu odolnosti objektu a následně realizovat cílené úpravy systémů zahrnutých do konvergované bezpečnosti (zejména těch prvků, které vykazují nízkou odolnost, výkyvy odolnosti atd.),

- možnost rychlejší a efektivnější reakce na vznikající narušení bezpečnosti a cílenější zajištění jeho řešení,
- lepší pochopení vzájemných vazeb mezi fyzickou, kybernetickou a provozní bezpečností,
- přesnější specifice vlivu hrozeb z různých druhů bezpečností na konkrétní aktivum,
- snadnější identifikace kritických míst, na které by se měla organizace nebo segment zaměřit při tvorbě bezpečnostních opatření,
- zvýšení účinnosti stávajících systémů,
- získání před-poplachové informace, např. o nestandardním chování osob v daném objektu nebo v jeho blízkosti, nebo informací o nestandardních technických či klimatických změnách,
- efektivní využití centrálního ovládání a monitorování, centralizovaná obsluha,
- standard, který umožňuje připojit širokou škálu prvků zabezpečení a automatizace,
- možnost integrace subsystémů jiných výrobců, široký rozsah funkcí,
- účinné řízení přístupu osob do jednotlivých částí objektu včetně záznamu vstupu uživatelů do databáze systému,
- získání více informací o bezpečnostní situaci objektu,
- zvýšená možnost kontroly pohybu osob,
- kontrola odběru a úspora energií [4] [5] [6].

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] 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.

[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, 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.

[6] VALOUCH, Jan. Projektování integrovaných systémů. [skriptum]. Zlín: UTB, 2015. ISBN 978-80-7454-557-3 169 s.