Josef Požár, Milan Kný

Kybernetické hrozby a jejich trendy v bezpečnostním managementu

Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje nr 23, 228-239

2016

Kultura Bezpieczeństwa
Nauka – Praktyka – Refleksje
Nr 23, 2016 (228–239)

KYBERNETICKÉ HROZBY A JEJICH TRENDY V BEZPEČNOSTNÍM MANAGEMENTU

THE CYBER THREATS AND THEIR TRENDS IN SECURITY MANAGEMENT

ASSOC. PROF. RNDR. JOSEF POŽÁR, CSC.
Fakulta bezpečnostního management,
Policejní akademie České republiky v Praze

ING. MILAN KNÝ, CSC.
Fakulta bezpečnostního management,
Policejní akademie České republiky v Praze

Abstract

Target processes of institutions management (from the enterprise, through the administration, to the alliances) are dependent on the provision and reliability of information and knowledge. Total digitization and "cybernation" of most of the processes require durability and protection against attacks and incidents of a new type. To anticipate timely the new risks is more difficult than to react flexibly to new socially pathological and criminal attacks. Reactive approach can't avoid the initial losses, but this approach is pragmatic.

The paper deals with some cyber threats and trends of attacks in an environment of the security management of the organization.

Key words: Security management, cyberspace, cyber threats and trends, critical infrastructure

Abstract

Cílové procesy managementu institucí od podniku, přes správu po aliance jsou závislé na zajištění a spolehlivosti informací a znalostí. Totální digitalizace a kybernetizace většiny procesů vyžaduje odolnost a ochranu proti útokům a incidentům nového typu. Předjímat včas nová rizika je obtížnější než flexibilně reagovat na nový výskyt sociálně patologických a kriminálních ataků. Reaktivní přístup se nevyhne počátečním ztrátám, je však pragmatický.

Příspěvek se zabývá vybranými kybernetickými hrozbami a trendy útoků v prostředí bezpečnostního managementu organizace.

Institucionální struktura kybernetické bezpečnosti v České republice je tvořena systematicky shora od zákonných norem k implementaci, paralelně však ze zkušenosti s bezpečnostními systémy v klasickém prostředí a s ochranou podnikových informačních systémů.
Key words: Bezpečnostní management, kybernetický prostor, kybernetické hrozby a trendy, kritická infrastruktura.

The institutional structure of cyber security in the Czech Republic is formed systematically from above (on the basis of the legal standards to be implemented). It is, however, simultaneously based on the experience with the security systems in the classical environment and the protection of corporate information systems.

1. Úvod

Prostředí, které ovlivňuje činnost jakékoliv organizace, prochází dynamickými změnami. Jeho předvídatelnost se vzhledem k rostoucí provázanosti bezpečnostních trendů a faktorů snižuje. Výrazný nárůst používání informačních technologií v současném světě vede k vytvoření informační společnosti, urychlení komunikace a velkému rozvoji služeb. Závislost společnosti a jejího fungování na informačních technologiích rapidně narůstá, a to ve všech oblastech (nejedná se pouze o služby informační společnosti jako je internetový obchod, ale i o fungování informačních systémů, na jejichž funkci je závislá celá řada základních služeb jako například řízení dopravy, přenos energií, výkon veřejné moci apod.).

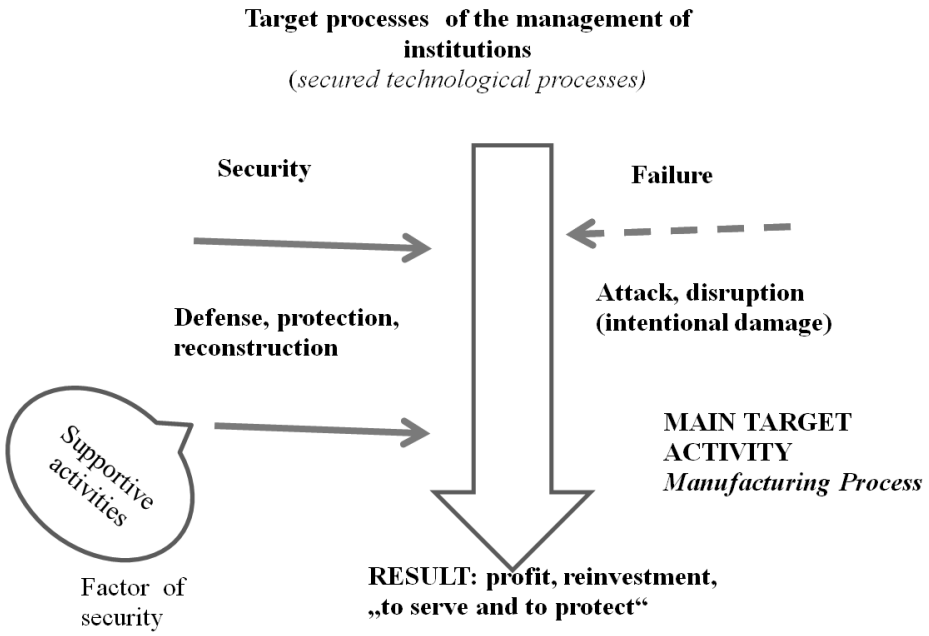
Se vzrůstající závislostí společnosti na informačních technologiích zároveň vzrůstá i zneužívání těchto technologií.

Útoky proti informačním technologiím jsou přitom stále sofistikovanější a komplexnější. Ze sféry přímého ekonomického prospěchu individuálních útočníků se útoky přesouvají do oblasti průmyslové špionáže a terorismu. Útočníci se stále více zaměřují na prvky kritické infrastruktury, jako jsou energetické systémy, produktovody, zdravotnické systémy a informační systémy veřejné správy.

Cílem článku je poukázat na nejčastější hrozby kybernetické bezpečnosti v oblasti bezpečnostního managementu. Je zřejmé, že vyčerpat a uvést všechny možné kybernetické hrozby není účelem, neboť není možné postihnout všechny stavy a situace v průběhu činnosti podniku či organizace. Předtím se pokusíme nastínit pojem bezpečnostní management.

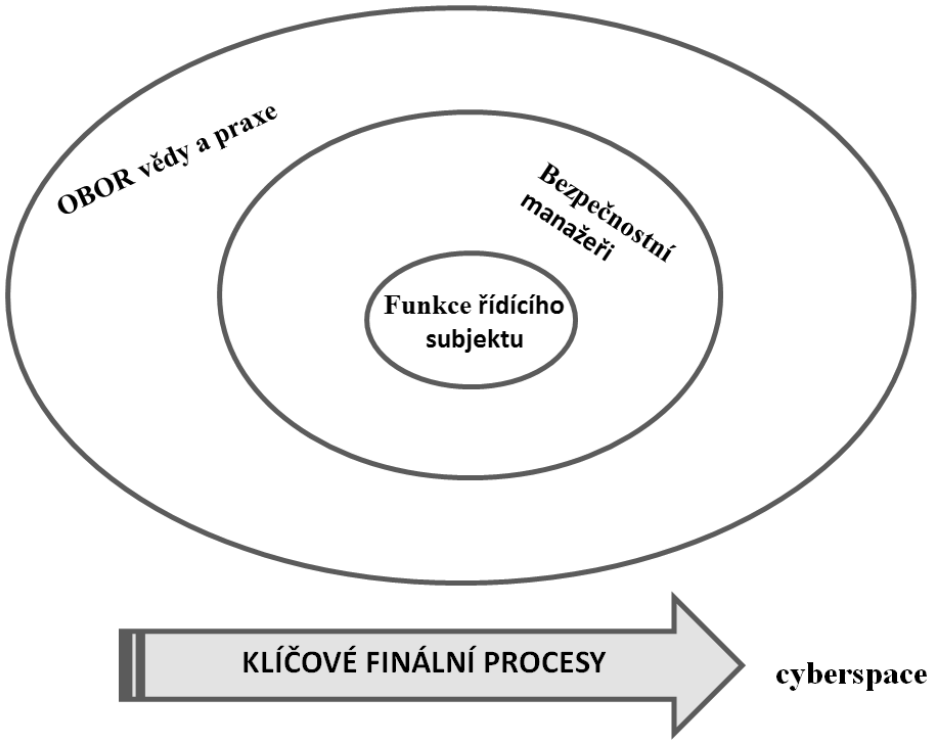
2. Bezpečnostní management v organizaci

Bezpečnostní management, vnímaný jako aplikované odvětví vědy a součást bezpečnostní praxe využívá konceptu základních a průběžných manažerských funkcí. Obvyklé kategorie oblastí činností manažerů mají u bezpečnostních manažerů specifika. Organizace, ve kterých působí, jsou udržovány ve funkčním stavu připravenosti k řešení bezpečnostních situací. Zárukou kompetentnosti plnění rolí je plná kvalifikace manažerů s odpovídající strukturou osobnosti a vybaveností relevantními znalostmi.



Obr. 1 Cílové procesy managementu

Bezpečnostní management v této práci chápeme jako obor znalostí k působení manažerů za účelem dosahování optimální bezpečnosti řízené organizace. Bezpečnost je obecně relativní vlastnost reálných systémů, která je významná k odolnosti vůči hrozbám.



Obr. 2 Role bezpečnostního managementu

Každý podnik, každá racionálně fungující organizuje, pečuje prioritně o „hlavní cílovou činnost", která přináší zejména hospodářské výsledky, pro které byla firma zřízena. Tato činnost modelově představuje složitý výrobní proces, jehož produktem jsou hmotné výrobky i nehmotné služby. Množina podpůrných činností, procesů, zabezpečuje harmonický a bezpečný chod organizace. Bezpečnostní aspekt řízení počítá se všemi relevantními hrozbami ve slabých stránkách bezpečnostního subsystému. Současný podnik řeší stále více informační vrstvu v kybernetickém prostoru vnitřních i vnějších sítí. Manuální formy informačních procesů na klasických nosičích, papírový tiskopis apod. jsou nahrazeny elektronickými, které jsou pro lidské vnímání relativně nové. Tím vznikají nové hrozby narušení provozu a zcizení hodnot organizace. Pomocí, někdy však překážkou je právní systém, který je pro

legální složku závazný, pro útočníka kybernetického útoku nikoliv. Tím se jako v každé sociálně patologické oblasti dostává zločinec do konkurenční výhody, jak časové, tak technologické. Prevence má omezené možnosti až při zvýšení četnosti stejného typu incidentů.

Klíčové finální procesy organizace představují hlavní cílovou (výrobní, servisní) činnost organizace (podniku, úřadu, bezpečnostní složky) pro kterou byla organizace zřízena a plní stěžejní hodnotu výstupu.

Bezpečnostní management lze interpretovat jako obor praktického zabezpečení a způsobu ochrany fungování organizací a také jako novou vědní disciplínu, která problematiku řízení k optimální bezpečnosti řeší. Vychází se z obecného managementu, který tradiční vědní disciplínu dlouho představuje.

3. Hrozby kybernetické bezpečnosti

Hrozbami jsou především kybernetické útoky. Kybernetický prostor je velmi specifický neexistencí geografických hranic a relativizací vzdálenosti mezi zdroji hrozeb a potenciálním cílem. Díky své asymetričnosti pak umožňuje státním i nestátním aktérům poškodit strategické a významné zájmy každého státu bez využití konvenčních prostředků. Neustále se zvyšuje počet a sofistikovanost kybernetických útoků proti veřejné a soukromé sféře. Tyto útoky mohou způsobit selhání zejména komunikačních, energetických a dopravních sítí či dopravních procesů, průmyslových nebo finančních systémů, mající za následek významné hmotné škody. Závislost všech státních i soukromých organizací na informačních a komunikačních systémech může mít vliv na správné fungování. S kybernetickými útoky zároveň úzce souvisí problematika politické a ekonomické špionáže.

V této souvislosti není účelem vyjmenovávat všechny hrozby kybernetické bezpečnosti, o nich se zmíníme v další části článku.

Ohrožení funkčnosti kritické infrastruktury[1].

Výkladový slovník kybernetické bezpečnosti chápe na s. 65 kritickou informační infrastrukturu jako „Komplex informačních a komunikačních systémů (naplňující stanovená průřezová kritéria a odvětvová kritéria v oblasti kybernetické bezpečnosti), jejichž nefunkčnost by mohla způ-

[1] P. Jirásek, P. Novák, J. Požár, *Výkladový slovník kybernetické bezpečnosti*, PA ČR, AFCEA, Praha 2015. ISBN 978-80-7251-436-6. See also: http://www.cybersecurity.cz/data/slovnik_v310.pdf.

sobit závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu". Kritická infrastruktura představuje klíčový systém prvků, jejichž narušení nebo nefunkčnost by měla závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva nebo ekonomiku státu. S ohledem na vysoký stupeň vzájemného propojení jednotlivých odvětví je kritická infrastruktura ohrožena komplexně, a to přírodními, technologickými a asymetrickými hrozbami. Zejména funkčnost energetické infrastruktury je ohrožována jak politickými tlaky, tak hrozbami s kriminální podstatou. Příkladem těchto ohrožení jsou politicky motivované manipulace s dodávkami strategických surovin, vstup cizího kapitálu s potenciálně rizikovým původem a cíli do kritické infrastruktury ČR, sabotáže, kybernetické útoky či hospodářská kriminalita.

V souvislosti s hrozbou kybernetických útoků patří k prioritám vlády zajištění bezpečnosti kritické informační infrastruktury a významných informačních systémů pomocí vládního koordinačního místa pro okamžitou reakci na kybernetické bezpečnostní incidenty. ČR podporuje budování takových systémů, které umožňují širokou spolupráci všech aktérů, tedy i těch, kteří nejsou součástí veřejné správy a přispívají k výměně zkušeností z řešení kybernetických incidentů na národní a mezinárodní úrovni. Vláda prosazuje legislativní i nelegislativní opatření tak, aby byla v souladu s principy vývoje informační společnosti a s Národní strategií kybernetické bezpečnosti na období let 2015–2020.

Internet věcí bude zranitelnější

Internet věcí se stává mohutnou hybnou silou schopnou ideálně řešit problémy vzdělávání, životního prostředí, zdraví, efektivity práce a celkově kvality lidského života. Obecně je to považováno za velkou výhodu. Technologie se rychle uplatňují v oblasti domácích vymožeností do nástrojů boje proti změnám klimatu nebo podpory zdraví. Chytrá města, Smart Cities, se mění ze snů na realitu, městské aglomerace akceptují internet věcí až s překvapivou rychlostí. Kybernetická bezpečnost se stává samostatnou oblastí. Digitálně propojené technologie se stanou součástí každodenního života, jejich bezpečnost je vnímána jako nutná součást osobní i národní bezpečnosti. Internet věcí tak nabízí velké výhody pro veřejný život, ale na druhé straně se budou projevovat obrovské zranitelnosti technologií internetu věcí, který se mezitím stane významným činitelem funkčnosti

státu a udržování veřejného blaha. Protivníci jich velmi rychle využívají a namísto zneužívání jednotlivých zařízení, ovládají a zneužívají rovnou celé sítě internetu věcí.

4. Trendy kybernetické bezpečnosti

V trendech kybernetické bezpečnosti se odrážejí hrozby a kybernetická kriminalita vůbec. Kybernetická kriminalita je různými autory definována poměrně souhlasně. Kybernetickou kriminalitu chápeme v souladu s publikací Výkladový slovník kybernetické bezpečnosti[2] jako „Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti."

Každý, kdo se věnuje sledování trendů a předpovídání dalšího vývoje, může očekávat velké množství vlivů a útoků, které nemusí být predikovány. Na základě analýzy událostí z minulých let očekáváme pravděpodobné trendy:

a) Mohou vzrůstat útoky na veškerá data umístěná v cloudu

Většina organizací si ukládají veškerá svá data do cloudu. Jsou to nejen data o zákaznících, ale také o svých projektech či majetku. Dá se tedy predikovat, že se v následujících létech setkáme s útoky, které budou zaměřeny na koncové body, mobilní zařízení a bezpečnostní autentizační protokoly a tak se útočníci budou snažit získat přístupy ke cloudům organizace. Nelze přesně předpovědět, jaké technologie a techniky pro útoky počítačoví zločinci využijí. Budou používat techniky škodlivého softwaru typu ransomware[3], který je založený na zablokování přístupu k infikovanému počítači.

Ransomware bude zaměřený nejen na lokální počítače a dokumenty, ale právě také na data uložená v cloudu, bez ohledu na jakákoliv data. Útoky tohoto typu nevyužívají šifrování, protože se zaměří zejména na vydí-

[2] P. Jirásek, P. Novák, J. Požár, *Výkladový slovník kybernetické bezpečnosti*, PA ČR, AFCEA, Praha 2015. ISBN 978-80-7251-436-6. See also: http://www.cybersecurity.cz/data/slovnik_v310.pdf.

[3] Ransomware je program, který zašifruje data a nabízí jejich rozšifrování po zaplacení výkupného (např. virus, trojský kůň).

rání související s pohrůžkou zveřejnění osobních či tajných dat. Zde bude jediná ochrana, která se zaměří na silná hesla a výborně nastavenou bezpečnostní politiku organizace.

Platí stále staré heslo, že bezpečnost je dobrá jen tak, jak dobře je zabezpečený nejslabší článek vaší informační architektury. Je zřejmé, že nejslabšími články jsou zvláště koncové body s operačním systémem Windows a mnohdy i nedostatečné znalosti o bezpečnostních hrozbách na straně běžných uživatelů.

b) Hrozby budou spojeny s finančně motivovaným malwarem

Úspěchy přetrvávajících pokročilých hrozeb (APT), které se týkají především ekonomické špionáže, budou zřejmě kopírovat postupy finančního malwaru. Kybernetičtí zločinci, kteří využívají klasický typ malwaru s cílem dosáhnout finančního zisku, budou stále více používat techniky z oblasti APT.

V poslední době programátoři zdokonalují bezpečnost operačních systémů a u uživatelů se zvyšuje povědomí o počítačových hrozbách a tak se zvyšuje celková úroveň bezpečnosti.

Útoky současného malwaru mohou zahrnovat komponenty a mechanismy šíření, které budou od samého začátku zaměřeny na specifické cíle a oběti. Rozdíly mezi tradičním malwarem a přetrvávajícími pokročilými hrozbami se budou zmenšovat.

c) Operační systém Android bude složitější a malware se proto zaměří se na nové cíle

V minulých letech narůstal malware pro operační systém Android v počtu nových variant a vzorků škodlivého kódu a tím se také zvýšilo množství postižených počítačů. Programátoři Androidu nadále pracují na zvýšení bezpečnosti této platformy, ale přijímání bezpečnostních opatření bude pro uživatele pomalé.

Uživatelé budou i nadále vystavováni jednoduchým útokům využívajícím sociální inženýrství. Počítačoví piráti samozřejmě budou stále hledat nové cesty, jak pomocí malwaru pro Android získat nějaké zajímavé finanční prostředky. Možnosti programátorů této platformy nejsou rozsáhlé, a proto představují mobilní zařízení odrazový můstek pro útoky na sociální sítě a cloudové služby. Malware bude různorodější a více specializovaný.

Nyní neexistuje na operačním systému Android dominantní slupina malwaru a lze vysledovat zastoupení jednotlivých variant škodlivého softwaru. Nejčastěji detekovaným malwarem je Andr/BBridge-A. Tento trojský kůň k instalaci dalších aplikací na mobilní telefony využívá chyby při zvyšování oprávnění. Tento nebezpečný malware může být dlouhodobě nebezpečný.

Rozmanitost finančně motivovaného malwaru odrážejí rozdíly mezi různými geografickými a ekonomickými regiony. Tento trend již lze pozorovat u technik sociálního inženýrství, které bývají pro jednotlivé země velmi specifické. Odlišnosti se týkají i záměrů jednotlivých útoků.

Lze oprávněně očekávat i to, že mechanismy bezpečnostních incidentů se budou lišit podle úrovně ochrany oběti a potenciální hodnoty útoku. Osobní data budou ohrožena v mobilních aplikacích i na sociálních sítích. Mobilní bezpečnost jedním z klíčových témat i pro další léta. Budou vznikat nové aplikace pro osobní i firemní komunikaci. To však povede k dalšímu nárůstu útoků, zejména pak v oblasti podvodů pomocí sociálního inženýrství při pokusech krádeže dat.

d) Škodlivý software bude infiltrovat přímo mechanismy obrany

V boji mezi počítačovými zločinci a poskytovateli bezpečnostních řešení lze očekávat nové prostředky a mechanismy zaměřené na nejnovější obranné mechanismy. Útokům tak budou vystaveny hodnotící služby, cloudové databáze s informacemi o bezpečnostních hrozbách, seznamy privilegovaných aplikací i jednotlivé vrstvy oddělující procesy běžící se stejným oprávněním.

V budoucnu se můžeme setkat s malwarem, který se podepíše odcizenými digitálními identitami a s pokusy zcela paralyzovat bezpečnostní mechanismy. Budou se napadat telemetrické analýzy nebo nové techniky detekce izolace procesů a přemostění programového kódu. Bude se zvyšovat zastoupení 64bitového malwaru. Ve světě osobních počítačů se postupně prosazují 64bitové varianty operačních systémů. Proto také očekáváme nárůst malwaru, který již nebude možné spustit na 32bitových platformách.

e) Primární hrozbou pro Windows budou i nadále exploitkity

V systému Windows bylo dosaženo velkého technologického pokroku, který výrazně znesnadňuje využívání programátorských chyb. S koncem životního cyklu operačního systému Windows XP bude obrovský nárůst zájmu útočníků o tuto již neaktualizovanou platformu. Nicméně dnešní

uživatelé jsou stále chytřejší a umějí již do značné míry odlišit zlé úmysly od neškodných. Proto budou autoři malwaru zdokonalovat své přesvědčovací techniky a útoky lépe cílit.

f) Nadále se budou zvyšovat tzv. nízkoúrovňové útoky na hardware, infrastrukturu i software

Události, ke kterým v minulých letech došlo v souvislosti s vládními agenturami a špionáží, ukázaly nejen to, jaké jsou možné typy útoků na infrastrukturu, ale také to, že k nim skutečně dochází. Zadní vrátka přitom nejsou dominantou pouze vládních organizací, ale setkáváme se s nimi i v komerční sféře. V letošním roce byste měli přehodnotit důvěru v používané bezpečnostní technologie a v různé firmy a organizace, se kterými se setkáváme.

Bohužel většina společností nebude mít na boj s tímto typem hrozby dostatečné prostředky a znalosti. Přesto by bylo moudré pozorně sledovat práci bezpečnostních laboratoří a informace o nových hrozbách.

g) Hackeři budou nadále napadat databáze a cloudy

Během letošního roku bude pokračovat trend využívání různorodých zařízení, která navíc budou uchovávat a zpracovávat citlivá obchodní data. Bezpečnostní ekosystém je mnohdy kolem mobilních zařízení tak rozvinutý, jako je tomu ve světě osobních počítačů.

Vzhledem k rozmanitosti jednotlivých zařízení a celkově nižší úrovni zabezpečení budou pro útočníky zajímavými cíli zejména domácnosti a kanceláře ale také i koncové body metropolitních systémů.

Nadále budou napadány bankovní asociace v oblasti nových elektronických měn a platebních technik. Budou také pokračovat tradiční útoky na kreditní a debetní karty. Tyto kybernetické hrozby jsou dnes vnímané nesystémově jako finanční ztráty v elektronickém bankovnictví (e-banking), dále jako ztráty a zneužití osobních dat v elektronickém podsystému státní a veřejné správy (e-government), jako narušení elektronického podnikání (e-business), znemožnění rozvoje elektronických obchodů a obchodování (e-commerce, e-shop na Internetu apod.) nebo při užití kybernetického terorismu (kyberterorismu) v oblasti aktivit organizovaného zločinu nebo šíření desinformací. Důležitou součástí je také role nutných systémových integrací prostředků bezpečnosti v kyberprostoru a jejich možného zneužívání k průmyslové, vojenské a politické špionáži.

5. Závěr a doporučení

Kybernetické hrozby se budou nadále vyvíjet a vyhledávat zranitelná místa v novém softwaru, aplikacích a zařízeních. Uživatelé informačních a komunikačních technologií se mohou chránit dodržováním rozumných bezpečnostních opatření online, udržováním aktuálního stavu svého bezpečnostního softwaru a aktualizováním veškerých jejich aplikací pomocí nejnovějších oprav zabezpečení.

Kybernetická bezpečnost si zaslouží podstatně větší a koordinovanou pozornost než jí dosud věnují zákonodárci, policejní orgány i uživatelé počítačů, protože škody jí vzniklé mají stále vzestupnou tendenci, přičemž používané metody a prostředky pachatelů jsou na velmi vysoké technické a intelektuální úrovni.

Odborníci působící v oblasti prevence a represe proti kybernetické kriminalitě budou muset mnohem více disponovat mezioborovými znalostmi. To vyžaduje hluboké znalosti policistů od informačních a komunikačních technologií přes bezpečnost informačních systémů až po právní disciplíny. Důležité je i vytvořit systém právní výchovy a propagace v boji proti kybernetické kriminalitě, který zahrnuje celou veřejnost od žáků a studentů až po podnikatele. Boj proti kybernetické kriminalitě je problémem vedení resortu Ministerstva vnitra ČR a Policejního prezídia P ČR. Je proto nutné zvýšit aktivitu při stíhání pachatelů složitých a náročných trestných činů především ze strany vyšetřovatelů. Z tohoto hlediska je vysokou potřebou technické vybavení, personální obsazení, zahraniční kontakty, literatura a školení centrálního policejního útvaru zabývajícího se touto problematikou. V personálním obsazení se orientovat hlavně na výrazně mladší odborníky, čerstvé absolventy škol a fanoušky disponujícími jazykovými znalostmi.

Literatura

1. Jirásek, P., Novák L., Požár, J.,. *Cyber security glossary*. Praha: PA ČR, AFCEA, 2015, 240 pp. ISBN 978-80-7251-436-6.
2. Kný, M., Požár, J., *Current Concept and Trends in Security Management and information Security.* Brno: Tribun, 2010. ISNB 978-80-7399-067-1
3. MacDonnell Ulsch, *Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks.* John Wiley and Sons, 2014, pp. 103 – 112. ISBN 978-1-118-83635-4.
4. Požár, J. *Informační bezpečnost.* Plzeň, 2005, ISBN 80-86898-38-5.

5. Požár, J. *Manažerská informatika.* Plzeň, 2010, ISBN 978-80-7380-276-9.
6. Požár, J., Kný, M., *Reflexe funkcí bezpečnostního managenentu*. Praha: PA ČR, 2015. ISBN 978-80-7251-445-8.

Josef Požár – The Dean of the Faculty of Security Management of the Police Academy of the Czech Republic in Prague. He graduated at the Faculty of Science in Brno in the field of Mathematics and Physics. He passed viva-voce examination in the field of Mathematical Analysis and he completed extramural research assistantship in the field of Technical Cybernetics at the Faculty of Engineering of the Technical University in Prague. He was awarded a degree of Senior Lecturer in the field of Security Services at the Academy of the Police Force in Bratislava.
Since 1992 he has been working at the Police Academy of the Czech Republic in Prague, where he has been teaching the following subjects: Protection of Computer Data, Information Security, Managerial Informatics and Information Security Theory.
He is the author of university texbooks such as Information Security, Managerial Informatics and of other study texts Managerial Informatics II. He is the co-author of Basics of Police and Security Activity Theory II, Basics of Information Security Theory, Selected Aspects of Information Security, Current Approach and Trends of Security Management and Information Security, and a large number of articles and speeches at conferences on information security. A member of the Czech chapter AFCEA. E-mail: pozar@polac.cz

Milan Kný – Absolvent VŠE v Praze, fakulta národohospodářská, obor mechanizace a automatizace řídících prací. Vědecká aspirantura v Ekonomickém ústavu ČSAV s graduační školou dále v UJEP (MU) v Brně, obhájeno na VŠE 1993 v oboru teorie plánování a řízení.
Praxe technika od 1958 ve vodních stavbách a v projekci organizace výstavby metra. Výzkumné a vývojové pracoviště tělovýchovy a vrcholového sportu od 1967, od roku 1990 ve služebním poměru u federální kriminální policie a od 1992 na Policejní akademii na katedře managementu a informatiky jako akademický pracovník, člen akademického senátu. Publikuje a řeší výzkumné projekty v oboru bezpečnostní management, sociální patologie mládeže a kybernetická bezpečnost. V doktorském programu garantem předmětu informační management a školitelem v oboru bezpečnostní management a kriminalistika. Je dlouholetým členem AFCEA. E-mail: kny@polac.cz