doc. RNDr. Josef Požár, CSc.
Fakulta bezpečnostního managementu PA ČR v Praze
Katedra managementu a informatiky

Vybrané hrozby informační bezpečnosti organizace

Abstrakt: Článek se zabývá možnou klasifikací hrozeb v organizaci z hlediska zajištění informační bezpečnosti. Článek uvádí některé hrozby kritické infrastruktury a její vlivy na bezpečnost organizace.

Abstract: This article deals with possible classifacion of risks and threats in the organizasion whith standpoint protection of information security. This issues shows to any threats of critical infrastructures.

Klíčová slova: Informační bezpečnost, hrozba, riziko, kybernetická kriminalita,

Key words: Information security, threat, risk, cyber crime.

Úvod

Úroveň bezpečnosti každého státu vůči vnějším i vnitřním ohrožením je přímo úměrná kvalitě prováděné bezpečnostní politiky státu. Východiskem bezpečnostní politiky je především analýza bezpečnostních hrozeb a rizik, možnosti výběru a efektivita protiopatření ke snížení rizik, limity disponibilních zdrojů, omezení a povinnosti vyplývající z mezinárodních závazků apod. Proto musí každý stát reagovat na dynamický a často i dramatický vývoj bezpečnostního prostředí v uplynulém období.

Rychlé rozšíření informačních a komunikačních technologií má za následek jednak zvyšování rychlosti a kvality informačního procesu, ale také je nezbytné se věnovat ochraně dat a informací v informačních systémech. Současně s tím také útočníci hledají stále nové způsoby útoků na informační systémy za účelem změny, zničení či jen průniku do těchto systémů. Souvisí to také s novým fenoménem trestné a jiné protispolečenské činnosti, která se nazývá kybernetická kriminalita. Ta ohrožuje nejen důvěrnost, integritu či dostupnost počítačových systémů, ale také bezpečnost rozhodujících kritických infrastruktur státu. Technologický pokrok dále dává vzniknout různým formám rozvoje, včetně kriminálních činů. Proto vznikají různé problémy vyplývající z kybernetické kriminality, které odrážejí rozdíly ve znalostech a úrovni technologií spektru tzv. „digitální propasti“. Při boji s touto kriminalitou čelí vyšetřovatelé, státní zástupci i soudci řadě složitých forenzních problémů. Je to zčásti proto, že digitální procesy vznikly v souvislosti s nehmotnou a přechodnou povahou digitálních důkazů. Kromě toho vyžaduje účinné vyšetřování a stíhání kybernetické kriminality často sledování kriminálních aktivit a jejich důsledků prostřednictvím řady různých poskytovatelů internetu, v některých případech i mimo hranice daného státu, což může vést ke složitým otázkám týkajícím se pravomoci a suverenity.

Tento článek byl zpracován v rámci Projektu vědeckovýzkumného úkolu č. 4/4 „Informační bezpečnost a kybernetická kriminalita v organizaci“, který je součástí Integrovaného výzkumného úkolu na léta 2010-2015, realizovaný Fakultou bezpečnostního managementu Policejní akademie České republiky v Praze.

Informační bezpečnost

Informační bezpečnost je velmi frekventovaný pojem, jehož důležitost má vzestupnou tendenci s ohledem na rostoucí hodnotu informací v oblasti soukromého podnikání i státní správy. Informace, které je třeba chránit, mají rozličnou podobu a to od té elektronické, přes tištěnou až třeba po informace, které se dají vypozorovat z logistických procesů či rozmístění pracovišť. Rizika úniku a zneužití informací hrozí nejen z vnějšího prostředí ale zejména zevnitř[1] organizace. Ne všechna nezabezpečená místa jsou zřejmá a o to užitečnější je rada profesionálů s mnohaletými zkušenostmi.

Informační bezpečnost znamená komplexní pohled, který organizaci pomáhá poznat a chránit své cenná data a také vede praktickými opatřeními k eliminaci či výraznému snížení dopadů v případě mimořádných událostí.

Pojem „Informační bezpečnost“ znamená komplexní přístup k ochraně informací jako celku[2]. Pro účinnou ochranu je třeba pochopit, jaké data a informace organizace má a jakou hodnotu pro ni mají. Je důležité uvědomit si cíle a reálné fungování organizace a teprve na základě toho lze navrhnout účinný a efektivní systém řízení informační bezpečnosti. Cílem však není pouhé zavedení, ale i další dlouhodobá funkčnost a rozvoj tohoto systému reagujícího na změny organizace i jejího okolí.[3]

Zavedením funkčního systému řízení informační bezpečnosti je možné v organizaci či podniku pomoci minimalizovat rizika spojená s únikem informací. Systém řízení napomáhá snížení nákladů na informační a komunikační technologie a celkově přispívá k efektivitě procesů. Je výraznou oporou v rozhodovacích procesech na úrovni managementu organizace.

Účelem je zavádět systémy řízení, které přispívají ke zkvalitnění nejen interních služeb a procesů, ale i služeb či procesů určených klientům organizace či státní instituce.

Vyřešení informační bezpečnosti znamená rovněž pro organizaci nemalý přínos. Nezřídka je v některých oborech zavedený systém řízení informační bezpečnosti přímo podmínkou pro vytváření nových obchodních či podnikatelských vztahů.

Hlavním důvodem implementace informační bezpečnosti organizace je:

- vzájemné ovlivňování ekonomik a dalších odvětví hospodářství prostřednictvím informačních a komunikačních technologií,
- digitalizace světa, kdy je neustále více dat předáváno v digitální formě, přičemž významnější a důležitější data z pohledu celé organizace jsou uložena v informačních systémech, v poslední době v tzv. cloud comupting[4] tak, aby nebyla ohrožena akceschopnost infrastruktur,
- způsoby a techniky přenosu dat v sítích jsou všeobecně známé ve formách přenosových a komunikačních standardů, a proto tato data mohou být útočníky ohrožena.

---

1 Lidský činitel je nejčastější slabou stránkou bezpečnostních systémů.

2 Ochrana je formou aktivního řízení bezpečnosti organizace.

3 Informační bezpečnost. [cit. 2009-8-1]. Dostupné na WWW: <http://www.iteg.cz/informacni-bezpecnost/>.

4 Cloud computing, aplikace provozované formou pronájmu nebo služby ve vzdálených datacentrech a spočívá v outsourcingu části informační struktury mimo vlastní organizaci nebo počítač koncovéno uživatele.

Problematika informační bezpečnosti je disciplína, která se velice rychle rozvíjí, vznikají nové a nové programy jak v oblasti ochrany dat a informací tak programy, které vytváří různí útočníci jako např. hackeři, kriminální živly, teroristé aj. Proto samotné zajištění a řízení bezpečnosti organizace jedním z průřezových profilů managementu organizace, firmy, podniku.

Všechny státní organizace i soukromé podniky musí budovat a neustále inovovat svou informační bezpečnost. Proto také nejvíce ohroženou oblastí úniku a ztrát dat a informací jsou jednak užívané informační a komunikační technologie a jednak lidské zdroje, tedy lidé, zaměstnanci organizace. Podle výzkumů problematiky informační bezpečnosti jsou právě lidí nejrizikovějším faktorem vyzrazení, kompromitace, modifikace, úniku a zničení citlivých dat a informací v organizaci.

Informační bezpečnost má bezesporu zásadní význam pro instituce, jež ji prodávají jako součást své produkce. Softwarové, právnické, zpravodajské a konzultační firmy ji dokonce prodávají jako svou hlavní komoditu. Ovšem i jinde je bezpečnost informací kritickým znakem jakosti produkce. Závada v technické dokumentaci, společně s lidským selháním a technickou závadou, se řadí ke třem hlavním příčinám nežádoucích provozních událostí v jaderném průmyslu i v letectví.

Informační bezpečnost zavádí celou řadu nových pojmů a definic. Blíže tyto definice uvádí Dobda[5]. Pro názornost uvedeme pouze některé z nich.

Bezpečnost (Security). Pod pojmem bezpečnost chápeme vlastnost nějakého objektu, anebo subjektu (informačního systému či technologie), která určuje stupeň, míru jeho ochrany proti možným škodám a hrozbám.

Hrozba (Threat) je skutečnost, událost, síla nebo osoby, jejichž působení (činnost) může způsobit poškození, zničení, ztrátu důvěry nebo hodnoty aktiva. Hrozba může ohrozit bezpečnost (např. přírodní katastrofa, hacker, zaměstnanec aj.).

Riziko (Risk) je pravděpodobnost, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní hrozby, která působí na slabou stránku této hodnoty. Je to tedy míra ohrožení konkrétního aktiva.

Zranitelné místo. Slabinu informačního systému využitelnou ke způsobení škod nebo ztrát útokem na informační systém, nazýváme zranitelné místo. Existence zranitelných míst je důsledek chyb, selhání v analýze, v návrhu a/nebo v implementaci informačního systému, důsledek vysoké hustoty uložených informací, složitosti softwaru, existence skrytých kanálů pro přenos informace jinou než zamýšlenou cestou apod.

Hrozby informační bezpečnosti a jejich klasifikace

Hrozby využívají zranitelností, tj. chyb v programu nebo v jeho konfiguraci, která umožní útočníkovi získat neoprávněný přístup k datům. Část těchto chyb odhalí útočníci, kteří je neohlásí výrobcům software a ani je nezveřejní. Chyby pak využívají k útokům na inkriminovaný systém. Může se jednat jak o úmyslné využití (zneužití) nebo náhodné (například nehody, poruchy, živelné události). Hrozby se pro účely zkoumání bezpečnosti informačního systému ohodnocují. Jedná se subjektivní, relativní hodnocení, které bere v potaz četnost výskytu události u náhodných hrozeb a míru složitosti a motivace u úmyslných útoků. Četnost výskytu určité události lze za některých podmínek spočítat. Příkladem může být četnost výpadku napájení - tu lze stanovit na základě sledování tohoto jevu v minulosti. Hodnocení míry hrozby u úmyslných útoků je mnohem složitější a většinou bývá prováděno pomocí

[5] DOBDA, Luboš. *Ochrana dat v informačních systémech*. Praha : Grada, 1998, s. 13-14.

kvalifikovaného odhadu.

Hrozbou může být například také požár, přírodní katastrofa, krádež, získání informací neoprávněnou osobou a další. Škoda, způsobená hrozbou se nazývá dopad hrozby. Do škody, kterou hrozba způsobí, se přičítají náklady na její obnovu. Úroveň hrozby se posuzuje dle následujících rysů:

- Nebezpečnost hrozby je schopnost způsobit škodu.
- Přístup hrozby je pravděpodobnost, že se hrozba dostane k aktivu. Dalším parametrem je i frekvence výskytu hrozby.
- Motivace hrozby je zájem vyvolat hrozbu vůči aktivu.

Pojmem *hrozba* označuje Staudek a Hanáček[6] možnost využitkovat zranitelné místo informačního systému k útoku na něj – ke způsobení škody na aktivech. Stejně jako u hrozby se určuje úroveň zranitelnosti, která se liší dle následujících faktorů:

- Citlivost zranitelnosti a náchylnost aktiva, objektu.
- Kritičnost a důležitost aktiva.

Velmi obecně definuje hrozbu Jirovský[7], že pod hrozbou můžeme chápat cokoliv, co nějakým způsobem může vést k nežádoucí změně informace, chování systému nebo ovlivnit jeho parametry. Dále uvádí, že útok je faktickou realizací hrozby.

Hrozby lze kategorizovat na[8]:

- objektivní
  - přírodní, fyzické jako např. požár, povodeň, výpadek napětí, poruchy apod., u kterých je prevence obtížná a kde je třeba řešit spíše minimalizaci dopadů vhodným plánem obnovy; v tomto případě je třeba vypracovat havarijní plán,
  - fyzikální, např. elektromagnetické vyzařování,
  - technické nebo logické jako porucha paměti, softwarová "zadní vrátka", špatné propojení jinak bezpečných komponent, krádež, resp. zničení paměťového média, nebo nedokonalé zrušení informace na něm,
- subjektivní, tj. hrozby plynoucí z lidského faktoru
  - neúmyslné, např. působení neškoleného uživatele nebo správce informačního systému,
  - úmyslné, představované potenciální existencí *vnějších útočníků* (špioni, teroristé, kriminální živly, konkurenti, hackeři) i *vnitřních útočníků* (odhaduje se, že 80 % útoků na informační technologie je vedeno zevnitř, útočníkem, kterým může být propuštěný, rozzlobený, vydíraný, chamtivý zaměstnanec); velmi efektivní z hlediska vedení útoku je součinnost obou typů útočníků.

Jiné, ale obdobné dělení je uvedenona Internetu.[9] Hrozbu můžeme definovat jako náhodnou nebo úmyslně vyvolanou událost, která může mít negativní dopad na důvěrnost, integritu a dostupnost aktiv. Každý informační systém je vystaven působení mnoha různých hrozeb. Pokud chce organizace těmto hrozbám čelit, musí nejprve zjistit, které to jsou. Vzhledem k tomu, že většina informačních systémů bývá obvykle vystavena působení stejných hrozeb, hovoří se o tzv. obecných neboli

---

[6] STAUDEK, Jan; HANÁČEK, Petr. *Bezpečnost informačních systémů.* Praha : UIS, 2000, s. 14.
[7] JIROVSKÝ, Václav. *Kybernetická kriminalita.* Praha : Grada, 2007, s. 20.
[8] POŽÁR. Josef. *Informační bezpečnost*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005, s. 40.
[9] Analýza rizik: indentifikace hrozeb. [Cit. 2010-09-12]. Dostupné z www: < http://www.cleverandsmart.cz/analyza-rizik-identifikace-hrozeb/>.

generických hrozbách, jejichž výčet bývá často uveden v nejrůznějších standardech a metodikách. Kromě těchto hrozeb by se však měla organizace zamyslet i nad tím, zda její systém neohrožují ještě nějaké jiné, pro něj specifické hrozby a pokud ano, měl by je do svého seznamu hrozeb přidat. Tento výše uvedený proces se v analýze rizik označuje pojmem identifikace hrozeb.

Nejčastěji tito autoři dělí hrozby podle úmyslu a umístění zdroje hrozby.

Podle úmyslu:

- **náhodné hrozby** (accidental threat) – jedná se o hrozby, které byly způsobeny zcela náhodně (původce hrozby se označuje jako threat event);
- **úmyslné hrozby** (deliberate/intentional threat) – jedná se o hrozby, které byly naplánovány (původce hrozby se označuje jako threat agent).

Podle zdroje:

- **vnitřní hrozby** (internal/insider threat) – zdroj (příčina) hrozby se nachází uvnitř organizace;
- **vnější hrozby** (external/outsider threat) – zdroj (příčina) hrozby se nachází mimo organizaci.

Kombinací výše uvedeného způsobu dělení získáváme matici, která zachycuje čtyři základní typy hrozeb.

hrozby	náhodné	úmyslné
externí	přírodního původu	hacking
interní	technické selhání lidská chyba	sabotáž

Jiné možné členění hrozeb je podle dopadu na systém. Toto dělení již není tak časté, ale umožňuje stanovit, na jaký atribut bezpečnosti (důvěrnost, integrita, dostupnost) hrozba působí:

- **aktivní hrozby** (active threat) – dochází ke změně stavu systému v důsledku narušení integrity a dostupnosti,
- **pasivní hrozby** (passive threat) – nedochází ke změně stavu systému, dochází k úniku informací, resp. dat.

Pro vlastní provedení analýzy rizik nemá výše uvedené dělení hrozeb příliš velký smysl. Ovšem v okamžiku, kdy se definuje hloubka analýzy rizik, může být takovéto dělení přínosem, neboť je tímto způsobem možné přibližně vymezit typ hrozeb, které budou předmětem analýzy. Stejně tak nám ve fázi vyhodnocení rizik může zařazení hrozby do odpovídající kategorie poskytnout obráz o tom, který typ hrozeb představuje pro organizaci největší riziko. Vzhledem k tomu, že ne všechna aktiva jsou vystavena působení všech hrozeb, je vhodné hrozby seskupit podle toho na jaké aktivum působí:

- operační systém (operating system threats),
- aplikace (application threats),
- databáze (database threats),
- síť (network threats),
- klient (host threats).

V okamžiku, kdy se bude posuzovat míra zranitelnosti aktiva vůči působení hrozby, již se nebude ztrácet čas vyhodnocováním, zda je daná hrozba relevantní či nikoliv.

Charakteristikou hrozby je její zdroj (např. vnější nebo vnitřní), motivace potenciálního útočníka (finanční zisk, získání konkurenční převahy), frekvence a kritičnost uplatnění hrozby. Jako příklady typických hrozeb pro informační technologie lze uvést orientační přehled generických hrozeb pro distribuované systémy informační technologie: neautorizovaná modifikace informací, informačních zdrojů a služeb, tj. porušení integrity odchytáváním a modifikací zpráv, vkládáním a replikacemi zpráv, neautorizované zpřístupnění informace odposlechem na přenosovém médiu, analýzou toku vyměňovaných zpráv nebo jejich délek, resp. frekvencí zasílání, analýza adres zdrojů a cílů zpráv, neoprávněné kopírování z dočasných paměťových míst (vyrovnávací paměti). K neautorizovanému zpřístupnění informací může útočník využít např. škodlivý software nebo elektromagnetické vyzařování. Hrozbou mohou být agregace citlivých informací z méně citlivých dílčích informací, dedukce ze znalosti, že jistá informace je uložena v databázi, dedukce z informací neoprávněně dostupných na veřejných zdrojích (např. z mnohých nedostatečně chráněných systémových tabulek), odposlech pomocí zařízení pro práci se zvukem, instalovaných na mnoha počítačích. Dalším typem hrozeb je neautorizované použití zdrojů (krádeže hardwarových a softwarových komponent, včetně používání jejich neoprávněných kopií), neautorizované používání informačních systémů a služeb jimi poskytovaných, znepřístupnění služeb, tj. akce a události, které brání autorizovaným subjektům využívat informační systém na dohodnuté úrovni poskytovaných služeb, popírání odpovědnosti za akce citlivé z hlediska bezpečnosti, např. popírání aktu zaslání nebo přijetí zprávy, popírání autorství dané zprávy[10].

Hrozby kritické informační infrastruktury

Společnost Symantec zveřejnila výsledky studie Ochrana kritické informační infrastruktury.[11] Ze studie vyplývá, že 53 % subjektů kritické infrastruktury bylo v posledních 5 letech průměrně 10krát napadeno kybernetickými útoky. Výsledky studie rovněž ukázaly, že nejlépe jsou připraveny čelit útokům energetické společnosti, zatímco nejhůře je na tom odvětví komunikací. Subjekty kritické infrastruktury mají zásadní význam pro národní ekonomiky i celou společnost, a úspěšný útok by mohl ohrozit národní bezpečnost.

Realizace jednotlivých útoků jsou účinné, ale také velmi nákladné. Respondenti odhadli, že 3 z 5 útoků byly dokonce velmi efektivní. Průměrné náklady na takový útok byly kolem 16 milonů Kč (850 000 $). Pouze jedna třetina subjektů kritické infrastruktury se domnívá, že je důkladně připravena na všechny typy útoků. Naopak 31 % subjektů je připraveno jen velmi málo. Zlepšení v této oblasti se jeví zdokonalení a vyšší frekvence bezpečnostních školení, v pochopení hrozeb vedením organizací, v zabezpečení koncových zařízení, v rychlosti bezpečnostní reakce a odezvy na bezpečnostní incident. Současně v personální bezpečnosti se musí zefetivnit bezpečnostní prověrk zaměstnanců a organizací. Největší nebezpečí výskytu bezpečnostního incidentu jsou vystaveny malé podniky a organizace, které zejména šetří na náklady na zajištění své informační bezpečnosti.

---

[10] Odpovědnost lze prokázat např. vedením evidenčních záznamů o provedených akcích s cílem provádění analýzy auditem nebo podpisováním informací vytvářených při takových akcích.

[11] Ochrana kritické informační infrastruktury. [cit. 2010-11-10] Dostupné z www: http://pcworld.cz/novinky/je-ochrana-kriticke-informacni-infrastruktury-dostatecna-11941.

Nabízí se celá řada doporučení. Zejména se jedná o prosazování bezpečnostní politiky a její řízení a cílem automatizovat ověřovací procesy. Je třeba klasifikovat jednotlivé hrozby a rizika, stanovit jejich pořadí podle důležitosti a definovat bezpečnostní politiku. Většina organizací se právě definováním a prosazováním své bezpečnostní politiky nezabývá. Přitom právě automatizace bezpečnostních ochran je mnohdy velmi účinná. To umožní identifikovat hrozby a bezpečnostním incidentům předejít. V praxi existuje celá řada nástrojů jako IPS a IDS.[12]

Je proto nutné proaktivně chránit informace (IPS). Zabezpečení dat umožňuje zjistit, kde se citlivá data skutečně nachází, kdo k nim má přístup a jak je chránit při jejich přenosu. K zabezpečení dat je velmi vhodné jejich šifrování. Tím se zamezí přístupu nepovolaných osob k těmto datům.

Každá organizace by měla používat prostředků autentizace a autorizace přístupu k datům. Jedná se o ověřování identity, aby přístup k systému měli oprávnění uživatelé. Ověřování rovněž funguje jako prevence před zneužitím. Informační systém prověřuje, zda je identita zařízení, systému nebo aplikace důvěryhodná.

Pro správu informačních systémů je nutné využívat bezpečné operační prostředí, definovat a prosazovat různé úrovně přístupu, automatizovat procesy, zajistit stálý výkon. Stav přístupu uživatelů do databází se využívá auditní záznamy a jejich automatické vyhodnocování.

Proto je nezbytné chránit infrastrukturu zabezpečením koncových bodů, webu při přenostu dat. Prioritou by rovněž mělo být zabezpečení kritických interních serverů a použití zálohování a obnovy dat. Organizace musí zajistit transparentnost celé strategie a odpovídající znalosti, aby mohly na hrozby rychle reagovat.

To také souvisí se strategií správy dat. Organizace se potřebují zbavit záložního zálohování a reduplikace dat a nahradit je plnohodnotným archivačním systémem a pokročilými technologiemi prevence ztráty dat. Proto se využívají jak hardwarové prostředky např. RAID pole tak i prostředky software.

Organizace i státní správa by měly spolupracovat se specialisty a dále rozšiřovat povědomí o plánech a organizacích, které se věnují zabezpečení kritické informační infrastruktury. Vždy by měl být k dispozici plán, jak reagovat tváří v tvář celostátnímu kybernetickému útoku, jaká je role vlády, kdo jsou kontaktní osoby pro dané odvětví na regionální a celostátní úrovni a jak vláda a soukromé subjekty sdílejí informace v případě nouze.

Organizace by měly mít na zřeteli, že jen zabezpečení není postačující k ochraně před kybernetickými útoky. Subjekty kritické infrastruktury a podniky obecně by měly také zajistit, aby jejich informace byly uložené, zálohované, strukturované, s přiřazenou prioritou a dostupné jen ověřeným uživatelům.

Závěr

V uplynulých letech byly zaznamenány ohromné změny a pokrok ve vývoji informačních a komunikačních prostředků. Informační a komunikační technologie se staly našimi každodenními společníky a také nepostradatelnými doplňky pro mnoho našich aktivit. Rozšířily způsoby obchodování, podnikání, kontaktů se svými blízkými či ovládat své finance. Moderní výpočetní prostředky také otevírají nové možnosti kontaktu státní správy s občany. V demokratických společnostech je pozorováno úsilí o vstřícnost a otevřenost vůči občanovi. Veřejná správa se tak snaží do určité míry

[12] IPS – Intrusion prevention systém (systém prevence narušení); IDS – Intrusion detection systém (systém detekce narušení).

usnadnit nezbytný kontakt občanů s úřady. Elektronizovaná státní správa pak může znamenat významný příspěvek k tomuto úsilí.

Úkol poskytovat informační základnu pro budoucí strategii je náročný. Výzkum kybernetické kriminality je dosud v počátcích. Zasvěcené osoby a instituce ve veřejném i soukromém sektoru nemusejí z důvodů komerčních, politických či národně bezpečnostních být ochotny své znalosti výzkumným pracovníkům sdělovat. Informace, jež si najdou cestu na veřejnost, často nemusejí být kompletní či přesné. Navzdory těmto obtížím je významné budovat informační základnu, tak, aby úsilí zmenšit digitální propast začalo přinášet výsledky.

K poskytnutí základních údajů o výskytu a nebezpečnosti různých druhů kybernetické kriminality je třeba použít široké škály výzkumných metod a komparativních přístupů. Vedle toho má zásadní význam výzkum účinnosti nové právní úpravy, policejních strategií a trestního stíhání prostřednictvím případové analýzy a studií ztrát (attrition studies). Výzkum se nesmí omezit na policejní či soudní údaje, a tyto zdroje by často měly být konkrétnější a jednotnější. Mezi oblasti, které vyžadují výzkum nejnaléhavěji, patří chování oběti a pachatele, jakož i sledování vývoje legislativy a prosazování práva po celém světě.

Strategie v oblasti informační bezpečnosti a kybernetické kriminality by měla být založena na poznatcích a podrobena přísnému hodnocení k zajištění účinnosti a účelnosti. Proto by mělo být vyvinuto společné a koordinované úsilí na mezinárodní úrovni k zajištění mechanismů financování praktického výzkumu a omezování mnohých druhů nově se objevující kybernetické kriminality. Je však stejně důležité zajistit, aby byl výzkum mezinárodně koordinován, a aby byly jeho výsledky široce dostupné.

Seznam použité literatury

1. POŽÁR. Josef. *Informační bezpečnost.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk,s.r.o.,2005, 309 s. ISBN 80-86898-38-5.
2. POŽÁR, Josef a kol. *Základy teorie informační bezpečnosti*. Praha : PA ČR, 2007,s. 219. ISBN 978-80-7251-250-8.
3. POŽÁR, Josef, HNÍK, Václav. Některé problémy boje proti kybernetické kriminalitě. *In Bezpečnostní teorie a praxe. Sborník PA ČR.* Praha : PA ČR, zvláštní číslo 2008, s. 13 – 24.
4. POŽÁR, Josef. Kybernetická kriminalita v podniku. In *Medzinárodná vedecká konferencia "Ekonomika, financia a manažment podniku – rok 2009".* Bratislava : Ekonomická fakulta, 2009, 9 s. ISBN 978-80-225-2808-5.
5. POŽÁR, Josef. Odhalování a vyšetřování kybernetické kriminality. In *Sborník přednášek Mezinárodní konference "CYTER 2009"*. Praha : CVUT, MV ČR, 2009, s. 29 – 40. ISBN 978-80-01-04372-1.
6. POŽÁR, Josef; KNÝ Milan. Pojetí a tendence bezpečnostního managementu a informační bezpečnosti" Brno : knihovnička, 2010, 134 s. ISBN 978-80-7399-067-1.

Adresa:
Doc. RNDr. Josef Požár, CSc.
děkan
Fakulta bezpečnostního managementu Policejní akademie ČR v Praze
Katedra managementu a informatiky
Lhotecká 667/9
143 01 Praha 4
Tel.: +420974828010
pozar@polac.cz