# Ochrana podnikových informačních systémů před kybernetickými útoky

***Vladimír Smejkal,***
**Moravská vysoká škola Olomouc**
**vladimir.smejkal@mvso.cz**

***Jindřich Kodl***
**soudní znalec, Praha**
**jm.kodl@gmail.com**

***Abstrakt:*** *Vzhledem k rostoucí závislosti civilizace na informačních a komunikačních technologiích se stává zranitelnost informačních systémů a informačních technologií významnou hrozbou. Protože hlavním nástrojem obrany proti kyberútokům je prevence, je třeba budovat informační systémy jako systémy zabezpečené. To platí i pro podnikové informační systémy. Tím dojde ke snížení zranitelnosti, a tedy i k zábraně hrozeb pocházejících z řad pachatelů kybernetické kriminality či kyberteroristů. Současně musí být součástí preventivních opatření i nástroje pro zjišťování možných kyberútoků tak, aby na ně mohl vlastník aktiv reagovat, jakož i nástroje umožňující rozkrýt, co se v systému či jeho komponentě odehrálo, aby bylo možno zajistit důkazy – digitální stopy. Tyto stopy mají dvojí význam: slouží k odhalení pachatele a dokázání jeho trestné činnosti, ale současně jsou zpětnovazebním zdrojem pro další vylepšování bezpečnostních opatření.*

**Klíčová slova:** kybernetická bezpečnost; kyberkriminalita; kyberterorizmus; řízení rizik; systém řízení bezpečnosti informací; nástroje pro kybernetickou bezpečnost; dokazování; digitální stopy; podnikové informační systémy.

***Abstract:*** *Considering the growing dependency of civilization on information and communication technologies, the vulnerability of information systems and information technologies is becoming a major threat. Because the prevention is the main tool of defence against cyber-attacks it is necessary to build information systems as secure systems. That also applies to enterprise information systems. This will reduce the vulnerability and hence prevent the threats of cyber-crime emanated from cyber-terrorism offenders or cyber-terrorists. At the same time, tools for detecting potential cyber-attacks must be part of preventive measures so that the asset owner can respond to them, as well as tools to unravel what happened in the system or its component to provide digital evidence. These traces have a dual meaning: they serve to detect the perpetrator and prove his criminal activity, but also at the same time they are a feedback source for further improvement of security measures.*

**Keywords:** cyber security; cybercrime; cyber-terrorism; risk management; Information security management system; cyber security tools; proving; digital evidence; enterprise information systems.

## 1. Úvod

Kyberkriminalita, kyberterorizmus a kybernetická válka – to jsou vysoce aktuální problémy současnosti, resp. velmi blízké budoucnosti. Vzhledem k rostoucí závislosti

civilizace na informačních a komunikačních technologiích se stává jejich zranitelnost významnou hrozbou. Čím více věcí bude připojeno (stane se součástí kyberprostoru[1]), s tím větším rizikem zneužití tedy musíme počítat. Je tedy otázkou, zda jsme dostatečně připraveni na tyto útoky a jak se na ně připravovat, aby to nebylo „zbrojení na minulou válku". Přitom útoky odehrávající se v kyberprostoru mohou mířit jak na kritickou infrastrukturu státu ale tak jak se společnosti, resp. jejich informační systémy stále více otevírají různým platformám a zařízením (viz trendy přistupovat z mobilních zařízení a do cloudu, propojovat všechno se vším apod.), mohou útoky velmi účinně mířit i na ně.

Podnikové IS dnes obsluhují všechny klíčové oblasti v podniku, jakými jsou například výroba, marketing, finance, personalistika, plánování, prodej, nákup, logistika, reklamační řízení, e-obchod atd. Někdy se jedná o více propojených informačních systémů, někdy o jeden komplexní, modulárně koncipovaný (např. SAP), přičemž u ERP systémů v posledních letech vývoj směřuje k integrovaným řešením se společnou datovou základnou, dnes mnohdy s využitím cloudu. (Basl, J. & Blažíček, R., 2013, s. 61-63) Lze tedy nepochybně konstatovat, že závislost většiny podniků na funkčnosti a bezchybnosti jejich IS je fatální.

Rozhodující význam u modulárního uspořádání mají manažerské informační systémy (MIS), tj. systémy pro zpracování dat, důležitých pro celou činnost podniku. V rámci MIS jsou zpracovávány všechny hlavní informační potřeby managementu podniku, od agend vrcholového vedení až po plánování či týdenní nebo denní operativní přehledy. Tyto agendy a data s nimi spojená mohou být právě významným terčem kybernetických útoků. V blízké budoucnosti lze očekávat další nárůst ekonomicky motivovaných a cílených útoků na podnikovou infrastrukturu.

Současné populární fenomény jako „Internet věcí" (Internet of things), Průmysl 4.0, BYOD (Bring Your Own Device), nárůst řídících systémů (SCADA) a až překotný úprk k robotizaci výrazně zvyšují možná rizika vyplývající z ohrožení útoky na tyto technologie. Čím více věcí bude připojeno (stane se součástí kyberprostoru), s tím větším rizikem zneužití musíme počítat.

Podnikové IS nebo jejich části se přitom mohou stát s vysokou pravděpodobností terčem kybernetických útoků z mnoha důvodů:

**1. likvidace konkurence:**

a) útok hrubou silou na informační a komunikační infrastrukturu podniku (náhodný nebo cílený),

b) nasimulování stavu, kdy konkurence bude obviněna ze správních deliktů – např. porušení povinností dle GDPR[2] nebo ze spáchání trestného činu[3]),

[1] Podle § 2 písm. a) zákona o kybernetické bezpečnosti č. 181/2014 Sb. se kybernetickým prostorem rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací. K definici kyberprostoru více viz (SMEJKAL, V., 2015, s. 93 a násl.).

[2] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů (General Data Protection Regulation, GDPR)

[3] Viz trestní zákoník a zákon č. 418/2011 Sb. o trestní odpovědnosti právnických osob a řízení proti nim.

c) informační útok (pomluvy, nekalá soutěž),

**2. parazitování na konkurenci** (získání jeho duševního vlastnictví – know-how, software apod., osobních údajů – údajů o klientech či zákaznících, o trhu – dodavatelé, kupující, ceny a obchodní podmínky),

**3. krádež jiných aktiv** (získání přístupu k nástrojům platebního styku a odčerpání peněz z účtů; krádež hardware).

**4. vymazání nebo modifikace dat či programů v IS s motivem:**

a) pomsta zvenčí nebo zevnitř (typicky bývalý nebo stávající zaměstnanec),

b) ideologický či politicky motivovaný útok,

**5. znepřístupnění dat – např. zašifrováním za účelem vydírání (dnes např. v souvislosti s ransomware** (Smejkal, V. & Kodl, J., 2017) nebo získáním zpracovávaných osobních údajů).

Bez ohledu na to, o jaký podnikový informační systém nebo jeho část (ERP, SCM, CRM, MIS, BI, CI apod.) se bude jednat, vždy je podstatné, že bude obsahovat programy a data. Obě dvě složky představují cenná aktiva podniku a obě dvě složky se mohou stát terčem útoku. Proto je třeba, aby výše uvedené hrozby (a případně další) byly identifikovány a minimalizovány.

## 2. Kybernetický útok a reakce na něj

V dalším textu budeme souhrnně pro výše uvedená jednání, jako jsou kyberkriminalita, kyberterorizmus a kybernetická válka, používat souhrnné označení „protiprávní jednání“ a pachatele označovat jako „útočníky“ a soustředíme se na útoky směřující proti informačnímu prostředí firem. Potom můžeme rozlišit zejména následující činnosti související s protiprávním jednáním:

1. příprava útoku pachatelem,

2. vlastní útok pachatele,

3. zjištění útoku (obvykle poškozeným, tj. vlastníkem aktiva),

4. odstraňování následků útoku (vlastníkem aktiva),

5. zahlazování stop po útoku (pachatelem),

6. zajišťování důkazů – informací využitelných jako důkaz (OČTŘ),

8. realizace opatření pro snížení rizika dalšího útoku – stejného či podobného (vlastník aktiva nebo jím pověřená osoba, dodavatel výrobků a služeb apod.).

Z výše uvedeného schématu můžeme z hlediska zájmů podniku, případně vlastníka aktiva vidět dvě linie, které probíhají na sobě nezávisle:

1. Je to trestní stíhání, které by mělo vést k odhalení a potrestání pachatele, kdy funkcí trestu je funkce informační, která označuje a upozorňuje na protiprávní jednání. Další funkcí je funkce motivační, která má za cíl odstranit takové chování pachatele, které mělo za následek uložení trestu. Preventivní funkce se snaží o vyvarování se jednání, které vedlo k uložení trestu. Trest může plnit i funkci vyrovnávací, kdy hlavní roli hraje odškodnění poškozených újmou, kterou způsobil pachatel. Účelem trestu je tedy zejména ochrana společnosti před trestnými činy, zabránění pachateli v páchání další trestné činnosti, jakož i (dle názoru autora spíše idealistická) představa o převýchově pachatele a výchovném působení trestního řízení i na ostatní členy

společnosti. Samotný trest vždy musí zůstat pouze prostředkem, jímž se společnost proti páchání trestných činů brání. (Kuchta, J. & Válková, H. a kol. 2005, s. 187-188)

2. Druhou linku představuje náprava vzniklých škod včetně zajištění, aby již ke stejnému nebo obdobnému, lépe však jakémukoliv útoku nedošlo. Jde tedy o situační prevenci, která může být realizována obecně a zaměřená vůči předem neurčenému okruhu subjektů (např. zákon o kybernetické bezpečnosti), nebo konkrétně, u určitého subjektu, v daném případě u poškozeného vlastníka aktiv. Jde tedy o tzv. řízení kontinuity činností v podniku, které má za cíl bránit přerušení podnikatelských činností a chránit kritické procesy podniku před následky závažných chyb a katastrof – viz také dále.

Nejdůležitějším pravidlem úspěšného manažerského řízení krizových událostí je naučit se krizi řídit, ne na ni pouze reagovat. Jedná se tedy o proaktivní filozofii v krizovém plánování. Proaktivní krizový manažer aktivně vyhodnocuje rizika před vznikem mimořádné události, zvažuje alternativy a důsledky různých akcí a zásahů a realizuje předvídavé kroky k získání maximální kontroly nad mimořádnými událostmi. (Smejkal, V. & Rais, K., 2013, s. 434 a násl.)

Krizový management je tvořen dvěma odlišnými, leč vzájemně se doplňujícími fázemi:

I. prevence krizových událostí, a

II. reakce na krizové události.

Přitom prevence před kyberkriminalitou je důležitější nežli následné odstraňování škod, protože cílem je, aby k žádným škodám vůbec nedošlo. Bohužel představa, že nějaký složitější systém, který je součástí kyberprostoru, můžeme zabezpečit jednou provždy, je iluzorní až nemožná. Proto je otázka preventivních opatření snižujících riziko kybernetického útoku tak významná a trvale přítomná. Nelze tedy čekat na okamžik, kdy budeme bilancovat dopady útoků, ale je se na nutné se připravit již v samotném návrhu architektury informačního systému. Výhodou současných návrhů je, že již výhradně vychází ze 3-vrstvé architektury, tvořené datovou vrstvou, spravující vlastní data, funkční resp. aplikační vrstvou a presentační vrstvou, která je přímo svázána s uživateli. Z hlediska zabezpečení tak lze zpracovávané informace i procesy, které s nimi nakládají, s výhodou strukturovat.

Dalším významným aspektem ochrany informací v IS podniku je jejich modulární charakter. Proto je rozhodujícím aspektem bezpečnostních opatření vždy jejich konkrétní zaměření na oblasti a procesy, které podnikový IS nebo jeho modul pokrývá, tedy zejména:

- Řízení lidských zdrojů – spravující osobní data uživatelů, dnes tak významná problematika vzhledem k blížícímu se nabytí účinnosti Nařízení GDPR,
- Řízení financí– zahrnující finanční, nákladové a investiční účetnictví, podnikový controlling, finanční agendy (řízení cash flow, finanční plánování a rozpočty, řízení rizik, peněžní obchody, měnové transakce a cenné papíry), mzdy, výkaznictví.
- Správa majetku – řešící veškerý provoz organizace (může být součástí řízení financí),
- Řízení výroby – prodej, nákup, výroba, skladování a expedice (logistika), reklamace a poprodejní servis. Zde se můžeme setkat s moduly jako SCM (Supply Chain Management, řízení dodavatelského řetězce), MES

(Manufacturing Execution Systém, řízení výrobního procesu), případně APS (Advanced Planning and Scheduling, pokročilé plánování zdrojů),

- Obchodní činnost – marketing, e-obchod, realizované moduly jako CRM (Customer Relationship Management, řízení vztahu se zákazníkem), případně s nadstavbou v podobě CI (Competitive Intelligence, konkurenční zpravodajství),
- Řízení kvality – informace o možnostech zlepšování a skutečném stavu,
- Manažerský informační systém – dnes často v podobě BI (Business Intelligence), příp. ECM (Enterprise Content Management, správa informací),
- Řízení projektů včetně řízení projektových rizik,
- Řízení vývoje, správy a bezpečnosti IS (ISMS) a další.

V návaznosti na strategickou business analýzu a s tím spojenou analýzu podnikového IS a jeho modulů je pak rozhodujícím momentem formulování příslušných preventivních bezpečnostních činností. Lze přitom vycházet z tzv. situační prevence, která vychází ze zkušenosti, že určité druhy kriminality se objevují v určité době, na určitých místech a za určitých okolností. Prostřednictvím opatření organizační, režimové, fyzické a technické povahy se snaží situační kriminogenní faktory minimalizovat.

## 3. Zvládání rizik jako hlavní složka preventivních činností

Informační bezpečnost musí řešit veškerou ochranu informací organizace, tedy ochranu celého informačního systému, automatizované i neautomatizované části. Máme tím na mysli zejména ochranu informací v mluvené a psané formě, ale i ochranu informací při zpracování a přenosu, tedy zejména při používání telefonů a faxů prostřednictvím telekomunikační sítě, počítačových sítí typu LAN/WAN, soukromých datových sítí a veřejné datové sítě typu internetu, včetně různých variant intranetu. Při současném stupni zapojení prostředků IS/IT do práce s informacemi se sice z velmi velké většiny bude tedy zajištění informační bezpečnosti orientovat na automatizovanou složku informačního systému organizace, byť neautomatizovanou složku nelze opomíjet, a to ani v rámci analýzy rizik.

Analýza rizik je prvním krokem procesu, který nazýváme řízení rizik. Toto řízení rizik je jednou ze složek systému řízení bezpečnosti informací. Systém řízení bezpečnosti informací (Information Security Management Systém, ISMS) sestává z politik, postupů, směrnic a příslušných zdrojů a činností, které organizace řídí, aby zajistila ochranu informačních aktiv. ISMS podle normy ČSN ISO/IEC 27000 představuje systematický přístup k ustavení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování bezpečnosti informací organizace tak, aby byly dosaženy její cíle. Je založen na posuzování rizik a na úrovních přijetí rizik organizace, které byly navrženy pro efektivní ošetření rizik a pro jejich řízení.[4]

Podle cit. normy je třeba, aby organizace provedla při ustavení, monitorování, udržování a zlepšování ISMS následující kroky:

a) identifikovala informační aktiva a s nimi spojené bezpečnostní požadavky,

[4] ČSN ISO/IEC 27000 – Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník, Praha: ÚTNMSZ, 2014.

b) posoudila rizika bezpečnosti informací a ošetřila rizika bezpečnosti informací,
c) vybrala a implementovala příslušná opatření k zvládnutí neakceptovatelných rizik,
d) monitorovala, udržovala a zvyšovala efektivnost opatření spojených s informačními aktivy organizace.

Detailně je ISMS definován normou ČSN ISO/IEC 27001, podle níž mj. organizace musí definovat a aplikovat proces posuzování rizik bezpečnosti informací[5], který:

a) stanoví a udržuje kritéria rizik bezpečnosti informací, která zahrnují 1) kritéria akceptace rizik; 2) kritéria pro provádění posouzení rizik bezpečnosti informací,
b) zajistí, že opakovaná posouzení rizik bezpečnosti informací produkují konzistentní, opodstatněné a porovnatelné výsledky,
c) identifikuje rizika bezpečnosti informací a vlastníky rizik,
d) analyzuje rizika bezpečnosti informací, přičemž posuzuje potenciální následky, které by nastaly, pokud by se rizika realizovala, reálnou pravděpodobnost výskytu těchto rizik a na základě toho stanoví výslednou úroveň rizik,
e) hodnotí výsledky a stanovuje priority zjištěných rizik pro jejich ošetření.

Při posuzování rizik lze postupovat podle obecné normy ISO 31000[6] nebo podle speciální normy z řady 27000, týkající se informačních technologií, konkrétně podle ČSN ISO/IEC 27005[7].

Podrobně je proces řízení rizik rovněž popsán v rámci zákona o kybernetické bezpečnosti, coby dnes zřejmě nejpodrobnější úpravy kybernetické bezpečnosti v českém právním řádu – zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále také jen „ZKB“) – je začleněno do oblasti organizačních opatření (§ 5 odst. 2). Podrobně je řízení rizik upraveno v prováděcí vyhlášce č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti ((dále také jen „vyhláška“). Hodnocení rizik popsané v příloze č. 2 vyhlášky odpovídá více méně metodě nazvané Matice následků a pravděpodobností uvedené v normě ČSN EN 31010.[8]

## 4. Nástroje pro snižování rizika u podnikových IS

Řízení vývoje, správy a bezpečnosti IS v podniku je poměrně dobře popsáno ve zdrojích, jako jsou technické normy, metodiky (ITIL, COBIT), zákon o kybernetické bezpečnosti a jeho prováděcí vyhláška apod. Přesto se lze domnívat, že některé kroky nás ještě čekají. Jsou to například:

[5] ČSN ISO/IEC 27001 – Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky, Praha: ÚTNMSZ, 2014.

[6] ČSN ISO 31000 – Management rizik – Principy a směrnice, Praha: ÚTNMSZ, 2010.

[7] ČSN ISO/IEC 27005 – Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. Praha: ÚTNMSZ, 2013.

[8] ČSN EN 31010:2011 - management rizik – techniky posuzování rizik. Praha: ÚTNMSZ, 2011, položka B.29, s. 73 a násl.

1. jednoznačná identifikace každého prvku v kyberprostoru,
2. přechod z protokolu IPv4 na IPv6 při dodržování požadavku plné implementace bezpečnostních mechanismů IPsec9 (což se ne zcela děje),
3. budování informačních systémů jako bezpečných od samého počátku, kdy princip „Security by Design", dnes uplatňovaný v softwarových projektech, bude rozšířen na všechny komponenty IS podniku: hardware, software, procedury a postupy, lidi. Součástí tohoto přístupu by mělo být i maximální využívání principu bezpečné identifikace, autentizace a autorizace uživatelů (Smejkal, V. & Kodl., J., 2008, s. 1-6) a využívání kryptografické ochrany (Smejkal, V. & Kodl, J., 2017),
4. větší využívání služeb typu Security as a Service.

# 5. Zajišťování důkazů v kyberprostoru jako součást prevence

Součástí preventivních opatření i musí být nástroje pro zjišťování možných kyberútoků tak, aby na ně mohl vlastník aktiv reagovat, jakož i nástroje umožňující rozkrýt, co se v systému či jeho komponentě odehrálo, aby bylo možno zajistit důkazy – digitální stopy. Tyto stopy mají dvojí význam: slouží k odhalení pachatele a dokázání jeho trestné činnosti, ale současně jsou zpětnovazebním zdrojem pro další vylepšování bezpečnostních opatření. Opatřování informací o činnosti podniku a o bezpečnostních incidentech, které následně mohou sloužit jako zdroj poznatků pro zlepšování ISMS a jako důkazy pro trestní či občanskoprávní řízení, se proto díváme jako součást preventivních opatření, nikoliv jako na součást následné reakce na incident.

Každé technologické zařízení, které získává, zpracovává, předává nebo uchovává data, zanechává záznamy (odrazy) o své činnosti. Tyto záznamy z kriminalistického hlediska jsou stopami. Lze také říci, že digitální stopa je fyzikální interpretací (záznamem) nehmotné informace, zakódované do digitálního formátu. (Porada, V. & Šedivý, P., 2012)

Zákon o kybernetické bezpečnosti řadí mezi technická opatření uvedená v ust. § 5 odst. 3 zavedení nástrojů jako jsou:

1. nástroj pro ochranu integrity komunikačních sítí,
2. nástroj pro ověřování identity uživatelů,
3. nástroj pro řízení přístupových oprávnění,
4. nástroj pro ochranu před škodlivým kódem,
5. nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,
6. nástroj pro detekci kybernetických bezpečnostních událostí,
7. nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

Z hlediska zajištění důkazů a dokazování jsou pro nás nejvýznamnější nástroje ad 5., 6. a 7., kdy dochází k ukládání informací o činnostech uživatelů a administrátorů, fungování technických a programových komponent a probíhá sběr a vyhodnocení kybernetických bezpečnostních událostí. Klíčovou je právě otázka prokazatelnosti, že

[9] Viz dokumenty RFC 4301–4303, 4835 a 5996.

se stopa nacházela na určitém místě a že v procesu od jejího zajištění do ukončení znaleckého zkoumání nebyla žádným způsobem modifikována.

Z hlediska kriminalistické počítačové analýzy je pro nás klíčové, abychom mohli konformně správným a přísně legálním způsobem najít, zadokumentovat a provést důkazy zjištěné z digitálních stop. (Smejkal, V. 2016) Tyto stopy se nacházejí v počítačových systémech a na nosičích dat, případně kdekoliv v kyberprostoru. Jejich vlastnosti jsou ovšem takové, že příliš neusnadňují práci orgánů činných v trestním řízení, resp. jimi ustanovených znalců. Patří sem zejména:

a) nehmotnost digitálních stop,
b) latentnost digitálních stop,
c) časová trasovatelnost digitálních stop, resp. manipulovatelnost s časem v počítačových systémech,
d) informační hodnota digitálních stop,
e) velmi nízká životnost digitálních stop,
f) uchování a kvalita archivních záznamů,
g) velké objemy digitálních dat,
h) vysoká datová hustota digitálních záznamů,
i) dynamika vývoje digitálních technologií,
j) dynamika činnosti informačních systémů,
k) komplexnost prostředí,
l) velký geografický rozsah prostoru s digitálními stopami,
m) dostupnost kvalitní ochrany digitálních dat,
n) možnosti automatizace při identifikaci digitálních stop,
o) možnosti změny identity pachatele v kyberprostoru,
p) obnovitelnost digitálních stop,
q) problém originality digitálních stop,
r) nedůvěra v důkazní sílu digitálních stop. (Porada, V. & Straus, J., 2012, s. 306 a násl.)

Současné standardní a poměrně robustní řešení počítačové bezpečnosti jsou založena vesměs na detekci signatur – neměnných sekvencí znaků či bytů v přenášených souborech či v jiné části síťového provozu, jejichž přítomnost indikuje příslušnou nákazu. Pokročilejší řešení pracují se signaturami na úrovni sekvencí systémových volání, seznamem nežádoucích síťových identifikátorů apod. Statická povaha signatur omezuje jejich účinnost. Pokročilé útočné strategie jsou silně polymorfní, neopakují přenosy týchž binárních sekvencí, nepřistupují opakovaně na stejné servery atd. Týmy analytiků produkující signatury pro bezpečnostní. řešení proto čelí rychle rostoucímu objemu analýz, který se snadno stává nezvladatelný. (Mařík, V. a kol. 2016, s. 104 a násl.)

Je zřejmé, že kontinuální sběr, monitorování a vyhodnocování dat týkající se podniku a jeho IS, vyžaduje vytvoření komplexního systému, který bude pracovat s nástroji umožňujícími zpracovávat tzv. big data, pracujícímu v prostředí fuzzy informací, s využitím nástrojů umělé inteligence, jako jsou např. expertní systémy, které budou

spíše vyhodnocovat chování osob, užívajících IS legálně, stejně jako útočníků, kteří budou provádět určité činnosti zvenčí.

# 6. Řízení kontinuity činností jako součást prevence

Řízení kontinuity činností je nedílnou součástí řízení a správy podniku. Řízení kontinuity činností by mělo zajistit odolnost podniku tak, aby byla ochráněna a optimalizována dostupnost produktů a služeb. Strategie řízení kontinuity činností, plány a řešení by měly být založeny na kritických činnostech podniku, které jsou identifikovány pomocí analýzy rizik obsahující hodnocení dopadů.

Příprava na řešení krizové situace v podniku (například, ale nikoliv pouze v souvislosti s informačním systémem) by měla zahrnovat:

1. **Plán řešení nouzové situace**, tj. první reakce na konkrétní negativní událost. Tento plán nastupuje ihned po zjištění katastrofy a platí v nejbližších minutách až hodinách. Je zaměřen na ochranu osob a majetku, zastavení dalšího působení pohromy, zajištění nejdůležitějších aktiv podniku. Zde zřejmě nejdůležitější úlohu hraje rozdělení rolí – co, kdo, kdy a v jakém pořadí má vykonat.

2. Tento plán eskaluje do **plánu udržení na trhu** (udržení zákazníků). Jeho smyslem je zajistit jakýmikoliv prostředky, aby byly uspokojeny existující požadavky zákazníků a aby byl nalezen způsob, jak informovat všechny stakeholdery (vlastníky, management, zaměstnance, dodavatele, odběratele, státní orgány a orgány samosprávy, ekologické a jiné organizace atd.) o situaci a o jejím řešení. Provádění postupů dle tohoto plánu by mělo být záležitostí dnů, nikoliv delší.

3. Dalším krokem je realizace **plánu znovuzahájení činnosti** (výroby) – obnovy podnikání. Účelem tohoto plánu je obnovení činnosti na stejné (nebo lepší) úrovni v daném čase a při co nejefektivnějším vynaložení prostředků. Součástí jsou obvykle i způsoby financování nových investic či oprav stávajících aktiv a řízení cash-flow v době do dosažení ustáleného chodu. Zde se již můžeme pohybovat v časovém horizontu podstatně rozsáhlejším – od týdnů po měsíce. Čím delší ale bude čas do znovuzahájení činnosti, tím je větší pravděpodobnost, že pozici na trhu převezme konkurence.

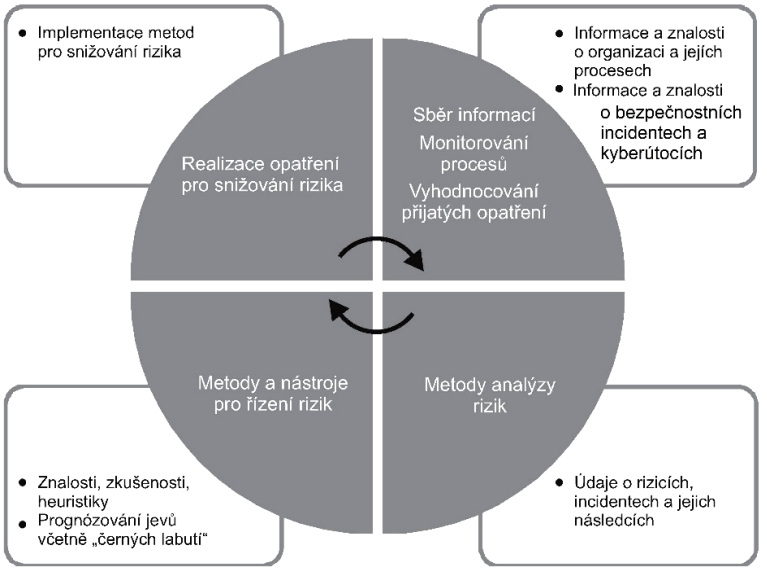
4. **Plán nápravných opatření**, který můžeme také nazvat „poučením z krizových událostí“, by měl zahájit proces přípravy podniku na další krizi, tj. zohlednit zkušenosti a poznatky z celého procesu včetně přijetí nápravných a preventivních opatření, kontrolních a testovacích mechanismů atd. (Smejkal, V. & Rais, K., 2013, s. 440)

Problematika systémů řízení kontinuity činností (Business Continuity Management System, BCMS) je podporována v současnosti již třetí normou. Původně to byla PAS 56:2003, poté BS 25999 a nyní ISO 22301, resp. celá řada norem ISO 2230x.[10]

[10] V ČR to jsou normy ČSN EN ISO 22300 – Ochrana společnosti – Terminologie, ČSN EN ISO 22301 – Ochrana společnosti – Systémy managementu kontinuity podnikání –Požadavky a ČSN EN ISO 22313 – Ochrana společnosti – Systémy managementu kontinuity podnikání – Pokyny.

# 7. Závěr

Boj proti kybernetickým útokům je nikdy nekončící spirálou mezi možnostmi nových technologií, a tedy i možnostmi, jak je zneužít, a rovněž tak možnostmi, které tyto technologie poskytují při prevenci i při odhalování a vyšetřování tohoto druhu trestné činnosti. Z toho vyplývá mj. i následující významná skutečnost: řízení rizik, ochrana dat, resp. celý boj proti kybernetické kriminalitě je iterační, nikdy nekončící proces, který trvá stejně dlouho, jako existují aktiva, jež je třeba chránit. Celý proces řízení rizik, od fáze identifikace a analýzy rizik až po uplatnění metod pro snižování rizika lze znázornit například takto:




**Obr. 1 Proces řízení rizik** *(Smejkal, V. & Rais, K., 2013, s. 131)*

Důležitou součástí procesu rozhodování o metodách a nástrojích na snížení identifikovaných rizik a na boj proti kybernetickým útokům jsou samozřejmě náklady na snížení rizika. Do opatření na snížení či odstranění rizika je vhodné investovat pouze tolik, aby náklady byly úměrné potenciální výši hrozící škody. Součástí projektu na snížení rizik tedy musí být i cost management, který bude poměřovat dopady rizik a náklady na jejich odstranění. Je ovšem třeba mít na paměti, že některé dopady lze obtížně kvantifikovat, přičemž jejich důsledky mohou být pro organizace a/nebo pro její vedení nevyčíslitelné. Existují totiž případy – např. v rámci tzv. kritické infrastruktury[11],

[11] Viz zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění nařízení č. 315/2014 Sb. a Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

že úroveň zbytkových (reziduálních) rizik musí být nastavena velice nízko. To může ovšem platit i pro IS v podnicích, které sice nejsou součástí státem vyhlášení kritické infrastruktury nebo provozovateli tzv. významných informačních systémů (podle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích), ale na základě analýzy rizik vyhodnotí, že daný IS podniku nebo jeho část jsou natolik klíčovou složkou podnikové infrastruktury, že bude vhodné aplikovat stejné postupy a opatření, jako kdyby se o KIS nebo VIS jednalo.

## Literatura

Basl, J. & Blažíček, R., 2012: *Podnikové informační systémy. Podnik v informační společnosti.* 3., aktualiz. a dopl. vyd. Praha: GRADA

Kuchta, J. & Válková, H. a kol., 2005: *Základy kriminologie a trestní politiky*. 1. vydání. Praha: C. H. Beck

Mařík, V. a kol., 2016: *Průmysl 4.0 - Výzva pro Českou republiku*. Praha: Management press

Porada, V. & Straus, J., 2012: *Kriminalistické stopy – Teorie, metodologie, praxe*. Plzeň: Aleš Čeněk, s. 306 a násl.

Porada, V. & Šedivý, P., 2012: Praktická využitelnost kriminalistických a forenzních aplikací v oblasti počítačové/kybernetické kriminality. *Karlovarská právní revue,* č. 3, s. 94–114

Smejkal, V., 2015: *Kybernetická kriminalita*. Plzeň: Aleš Čeněk

Smejkal, V., 2016: Metodika vyšetřování kybernetické kriminality. In: Porada Viktor a kol. *KRIMINALISTIKA. Technické, forenzní a kybernetické aspekty.* 1. vydání. Plzeň: Aleš Čeněk, s. 786–802

Smejkal, V. & Rais, K., 2013: Řízení rizik ve firmách a jiných organizacích. 4., aktualizované a rozšířené vydání. Praha: GRADA

Smejkal, V. & Kodl., J., 2008: Development trends of electronic authentication. In: *Proceedings of the 42nd Annual Conference 2008 IEEE International Carnahan Conference on Security Technology*, Diplomat Hotel Prague, Czech Republic, October 13–16

Smejkal, V. & Kodl, J., 2017: Encryption and protection of the legitimate interests versus the fight against cyberterrorism and other cybercrimes. (Šifrování a ochrana oprávněných zájmů versus boj proti kyberterorismu a jiným kyberzločinům.) In: *Proceeding of the 18th International Conference „IS2 – OTHER DIMENSIONS OF SECURITY...return to the drawing board "*, 24.-25. 5. 2017, Praha: TATE International, s. 71-83

**JEL Classification: K14, M15**