MANAGEMENT BEZPEČNOSTI PROCESŮ A TECHNOLOGIÍ V SOUVISLOSTI SE ZÁVISLOSTÍ NA ICT

MANAGEMENT OF PROCESSES AND TECHNOLOGIES SECURITY IN RELATION TO A DEPENDENCE ON ICT

David Král

Abstrakt: *Příspěvek se zabývá problematikou informační bezpečnosti, konkrétně oblastí bezpečnosti procesů a technologií. Ke zmíněné oblasti je možné využít řadu doporučených postupů a norem, článek využívá přístup norem ISO/IEC 27K. Jsou zde prezentovány výsledky průzkumu v segmentu malých a středních podniků, ve kterých byla zkoumána kritéria související s uvedenou oblastí managementu informační bezpečnosti. Dále je provedeno šetření mezi subjekty v oblasti závislosti na informačních a komunikačních technologiích. Cílem článku je popsat stav bezpečnosti ve zkoumané oblasti mezi dotazovanými malými a středními podniky a prezentovat metodiku, která využívá faktor závislosti na informačních a komunikačních technologiích při stanovení úrovně managementu informační bezpečnosti.*

Klíčová slova: *management bezpečnosti informací, malé a střední podniky, bezpečnost procesů a technologií, závislost na ICT.*

Abstract: *The paper discusses the issue of information security, specifically the area of processes and technologies security. Several recommended practices and standards can be used for the area, the article uses the ISO / IEC 27K approach. The results of the survey in the segment of small and medium sized enterprises are presented, which examined the criteria related to the mentioned area of information security management. In addition, an investigation is conducted among subjects in the field of information and communication technology dependence. The aim of the article is to describe the state of security in the area investigated among the interviewed SMEs and to present a methodology that uses the information*

and communication technology dependency as a factor determining the level of information security management.

Keywords: *information security management, small and medium sized enterprises, security of processes and technologies, dependence on ICT.*

JEL klasifikace: *M12, M15.*

1 ÚVOD

Informace je možné považovat za aktivum, stejně jako jiná významná obchodní aktiva. Informace jsou často nezbytné pro podnikatelské aktivity subjektů a v důsledku toho musí být adekvátně chráněny. Informace mohou být uloženy v mnoha formách, např. digitální, hmotné nebo ve formě znalostí zaměstnanců. Je důležité mít také na paměti a vhodně chránit všechny využívané způsoby přenosu informací: elektronické, listinné nebo verbální. Bez ohledu na formu a přenos informací je vždy nutné aplikovat jejich vhodnou ochranu.[1]

Pokud posuzujeme bezpečnost informací, je třeba zkoumat jejich tři hlavní dimenze: důvěrnost, dostupnost a integritu. Informační bezpečnost obsahuje implementaci a správu bezpečnostních opatření, která mají za cíl chránit citlivá aktiva organizace, zajistit kontinuitu subjektu a minimalizovat dopad bezpečnostních incidentů. Pro efektivní management informační bezpečnosti je třeba také implementovat vhodný soubor kontrolních mechanismů, a to prostřednictvím zvoleného procesu managementu rizik. Celý soubor opatření včetně bezpečnostních politik, procedur, organizačních struktur, atd. realizovaných pro ochranu informačních aktiv je označován jako systém managementu informační bezpečnosti, v angličtině ISMS (Information Security Management System).

Nasazené kontrolní mechanismy musí být specifikovány, realizovány, monitorovány, kontrolovány a pokud je to vhodné, tak také zlepšovány. Cílem těchto opatření je tedy zajištění bezpečnosti citlivých opatření a jejich prostřednictvím také podnikatelských cílů organizace.

[1] ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary. International Organization for Standardization. 2014.

Definice informační bezpečnosti je uvedena ve standardu ISO (ISO/IEC 27000:2014)[2] - *„Informační bezpečnost zahrnuje aplikaci a management vhodných bezpečnostních opatření, která zahrnují posouzení širokého spektra hrozeb, s cílem zajistit udržitelný podnikatelský úspěch a kontinuitu a minimalizací dopadů bezpečnostních incidentů.“*

Oblast procesů a technologií, které v organizaci probíhají, resp. jsou používány, je jednou z nejdůležitějších součástí systému managementu informační bezpečnosti. V dalším textu je popsána problematika informační bezpečnosti v segmentu malých a středních podniků a jsou uvedeny bariéry, které brání těmto organizacím implementovat nejznámější normy a standardy. Dále jsou zde prezentovány výsledky kvantitativního výzkumu, který se zabýval zkoumanou oblastí, a to metodou dotazníkového šetření, které se zúčastnilo více než 300 malých a středních podniků.

2 PROBLEMATIKA INFORMAČNÍ BEZPEČNOSTI V SEGMENTU MALÝCH A STŘEDNÍCH PODNIKŮ

Segment malých a středních podniků (dále jen „MSP“) má důležitý význam pro inovace, růst a rozvoj ekonomiky na národní i evropské úrovni a měl by být prioritní oblastí ekonomické politiky vlády. Aby mohly MSP poskytovat služby zákazníkům a plnit své obchodní cíle, jsou v současné době stále více závislé na svých informačních systémech a sítích,. Drtivá většina MSP, možná vyjma kategorii mikropodniků, se spoléhá na nějaký druh informačního systému a mnoho z nich již řadu procesů realizuje online. Elektronické komunikační sítě, propojené informační systémy a digitální služby se stávají klíčovými pro stále vyšší počet MSP.

Souběžně s rostoucím vlivem ICT na MSP vzrůstají v tomto segmentu také obavy z ohrožení citlivých informací. Vzhledem k neustále se vyvíjejícím oblastem hrozeb a postupně se zvyšujícímu ohrožení firemních aktiv se MSP dnes potýkají s významnými bezpečnostními riziky, které ohrožují jejich podnikání. MSP potřebují zavést formální procesy informační bezpečnosti, technické mechanismy a organizační opatření. Bez těchto kroků mohou být MSP vážně ohroženy neúmyslnými i záměrnými útoky na jejich informační systémy a sítě, což se v důsledku může negativně projevit na jejich podnikatelských výsledcích.

[2] ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary. International Organization for Standardization. 2014.

Pro podporu organizací při přijímání nejlepších bezpečnostních postupů byl v posledním období vyvinut značný počet bezpečnostních standardů, na kterých se podílely normalizační a profesní organizace či expertní asociace. Cílem těchto norem je pomoci organizacím efektivně řídit a posilovat opatření pro bezpečnost informací a snížit tak vznikající rizika na přijatelnou úroveň. Tato opatření musejí být přitom aplikována tak, aby zachovaly konkurenční výhody dotčených subjektů a zároveň zajistily ochranu informačních aktiv.

Existuje mnoho důvodů pro MSP, aby usilovaly o přijetí standardů pro informační bezpečnost. Přesto jejich implementace v této oblasti je stále nízká a jejich přijetí není do značné míry vnímáno jako priorita. Z dostupných výzkumů a analýz vyplývá, že pro MSP existuje několik významných bariér, které brání přijetí norem v oblasti informační bezpečnosti a které mohou být překonány přijetím konkrétních opatření. Jednou z hlavních překážek je skutečnost, že v MSP je omezené povědomí o možných ekonomických přínosech standardizace v oblasti informační bezpečnosti, což na druhou stranu částečně pramení z toho, že neexistuje silná podpora pro zavádění těchto norem zaměřená primárně na MSP.

Zavádění standardů bezpečnosti informací je proto vnímáno MSP jako velmi náročný úkol. Je to do jisté míry způsobeno specifickými potřebami MSP, které nebyly během procesu vývoje norem brány do úvahy. Tím se standardy staly příliš komplikovanými pro MSP, které často řídí svoje procesy jednoduchými vnitřními postupy.

Přestože MSP již učinily určité kroky ke zvýšení bezpečnosti svých citlivých aktiv, stále existuje dlouhá cesta směrem k širokému přijetí norem v jejich segmentu jako prostředku ke zmírnění rizik plynoucích z rychlosti technologických změn a kybernetických hrozeb. MSP by měly být silněji povzbuzovány k tomu, aby podnikly odvážnější proaktivní kroky a dokázaly efektivněji čelit hrozbám a útokům na jejich aktiva.

Bariéry přijetí standardů bezpečnosti informací pro MSP:

Povědomí o dostupných standardech

- MSP jsou nedostatečně informovány o dostupných standardech, které jim mohou pomoci zmírnit bezpečnostní rizika.
- MSP čelí potížím s identifikací norem, které budou kompatibilní s jejich konkrétními podnikatelskými cíli.

Angažovanost managementu

- Implementace standardů vyžaduje zdroje, které by jinak MSP alokovaly do podnikatelských aktivit s transparentnější návratností investic.
- Management často nevnímá jasně, jak implementace těchto standardů zvyšuje hodnotu jejich organizace.

Vnímání kybernetických hrozeb zaměřených na MSP

- Stále převládá chybné vnímání, že kybernetické útoky hrozí hlavně velkým podnikům.
- Poslední výzkumy jasně ukazují, že každá forma podnikání, bez ohledu na jeho velikost, je potenciálním cílem kybernetického útoku.

Zapojení do procesu vývoje

- Návrhy norem jsou určeny především pro větší organizace a jsou zaměřeny na pokrytí jejich složitějších procesů.
- Neexistuje mnoho standardů, které by byly snadno aplikovatelné v prostředí MSP.
- Netechnologicky zaměřené MSP se na procesech rozvoje a revize norem příliš neúčastní.

Kompetence k řízení kybernetické bezpečnosti

- V MSP, které procesy týkající se informačních a komunikačních technologií realizují interně, často nedisponují zaměstnancem zodpovědným pouze za bezpečnost informací.
- V MSP, které procesy týkající se informačních a komunikačních technologií outsourcují, chybí interní lidské zdroje se znalostmi v oblasti bezpečnosti informací.
- Pro implementaci a správu bezpečnostních standardů jsou obvykle vyžadovány různé multidisciplinární bezpečnostní role, což přesahuje kapacitu a odbornost MSP.

Rozpočet a zdroje

- Zavedení standardů bezpečnosti informací může být náročné z hlediska finančních zdrojů a schválení potřebného rozpočtu od managementu může být náročnou úlohou.
- V mnoha případech je třeba, aby MSP požádaly o pomoc zkušeného konzultanta, což zvyšuje finanční náklady implementace.

Management rizik

- Mnoho MSP nemá funkční směrnice pro efektivní řízení rizik v oblasti informační bezpečnosti a existují omezené dostupné rámce pro řízení rizik, které jsou pro malé organizace aplikovatelné.
- Oblast rizik, které organizaci hrozí, musí být detailně zmapované, aby bylo možné identifikovat vhodné normy k implementaci.

Specifické standardy ochrany osobních údajů

- V posledních letech došlo v organizacích k posunu vnímání významu ochrany osobních údajů, ale existuje omezené množství evropských nebo mezinárodních standardů určených k tomu, aby pomohly malým organizacím zajistit odpovídající ochranu osobních údajů[3].

3 DOTAZNÍKOVÉ ŠETŘENÍ BEZPEČNOSTI PROCESŮ A TECHNOLOGIÍ A ZÁVISLOSTI SLEDOVANÝCH SUBJEKTŮ NA ICT

Šetření se zúčastnilo celkem 305 malých a středních podniků. Zapojené subjekty byly zařazeny a rozděleny do tří podkategorií dle doporučení EU (2003/361/ES ze dne 6. května 2003) a aplikačního výkladu MSP, který zpracovalo Ministerstvo průmyslu a obchodu a Úřad pro ochranu hospodářské soutěže[4].

Tabulka 3.1: Definice malého a středního podnikatele

Kategorie podniku	Počet zaměstnanců	Roční obrat	Bilanční suma roční rozvahy
Mikropodnik	< 10	< 2 mil. EUR	< 2 mil. EUR
Malý podnik	< 50	< 10 mil. EUR	< 10 mil. EUR
Střední podnik	< 250	< 50 mil. EUR	< 43 mil. EUR

Zdroj: http://www.czechinvest.org/definice-msp

3.1 Procesy a technologie

Při získávání primárních dat bylo zkoumáno, do jaké míry sledované organizace (malé a střední podniky) manažersky zajišťují oblast bezpečnost procesů a technologií. Vyhodnocená úroveň zabezpečení této stěžejní oblasti

[3] MANSO, C. G, REKLEITIS, E., PAPAZAFEIROPOULOS, F., and V. MARITSAS. Information security and privacy standards for SMEs

[4] http://www.czechinvest.org/data/files/definice-maleho-a-stredniho-podniku-2-1112.pdf

by měla zásadně ovlivnit vytváření nebo aktualizaci strategie managementu informační bezpečnosti organizace. Pro získávání dat byla preferována kritéria, která jsou součástí oddílů bezpečnosti, které se vztahují ke zkoumané problematice ve standardech ISO/IEC 27K, a to především v aktuálně platné normě ISO/IEC 27002[5]:

- fyzické zabezpečení prostor,
- politika povolení vstupu do prostor,
- zajištění proti přírodním hrozbám,
- ochrana před selháním napájení,
- postup bezpečné likvidace,
- ochrana před škodlivým software,
- postup zálohování dat,
- postup šifrování dat,
- ochrana výměny dat s externími partnery,
- bezpečnostní opatření v rámci smluvního partnerství,
- záznam aktivit uživatelů informačního systému,
- aplikace nápravných opatření na odstranění vzniklých chyb,
- dodržování politiky čistého stolu a obrazovky,
- postup pro registraci uživatele do informačního systému,
- odpovědnost uživatelů za činnost v informačním systému,
- dodržování tvorby tzv. silných hesel,
- postup autentizace při vzdáleném přístupu do informačního systému,
- ochrana portů pro vzdálenou diagnostiku a konfiguraci,
- politika odhlášení stanic ze systému při nečinnosti
- zásady bezpečnosti práce na mobilních zařízeních[6]

Každé kritérium v realizovaném šetření obsahovalo 4 možné varianty odpovědí, a to dle hodnocení úrovně realizace zkoumaného kritéria u dotazovaných malých a středních podniků. Každé kritérium bylo

[5] ISO/IEC 27002 - Information technology — Security techniques - Code of practice for information security controls. International Organization for Standardization. 2013.
[6] ISO/IEC 27002: 2013

ohodnoceno počtem bodů v závislosti na dosaženém stupni realizace zkoumané kategorie - viz tab. 3.2.

Tabulka 3.2: Úroveň realizace

Body	Úroveň realizace
1	nerealizováno
2	plánováno
3	částečně realizováno
4	kompletně realizováno

zdroj: vlastní zpracování

3.2 Závislost na ICT

V realizovaném průzkumu bylo dále zkoumáno, do jaké míry jsou sledované malé a střední podniky závislé na informačních a komunikačních technologiích. Důvodem tohoto šetření byl předpoklad, že z pohledu managementu informační bezpečnosti je třeba rozlišovat nebo jinak pohlížet na subjekty, které nejsou při realizaci svých procesů významně závislé na informačních a komunikačních technologiích a oproti tomu jiná úroveň zabezpečení těchto procesů bude vyžadována nebo očekávána od subjektů, pro něž jsou informační technologie klíčové a nezastupitelné pro jejich fungování.

Pro získávání dat byla zvolena následující kritéria:

- Jakého ročního obratu dosahuje Vaše společnost?
- Kolika zaměstnanci disponuje Vaše společnost?
- Do jaké míry je Vaše společnost závislá na ICT při poskytování výrobků nebo služeb Vašim zákazníkům?
- Odhadněte hodnotu duševního vlastnictví organizace uloženou v elektronické podobě.
- Jaký vliv má výpadek informačního systému na chod Vaší organizace?
- Jaký vliv má výpadek internetu na chod Vaší organizace?
- Jak jsou Vaši zákazníci citliví na bezpečnost dat a ochranu soukromí?
- Odhadněte potenciální dopad vážného bezpečnostního incidentu na pověst Vaší organizace.
- Jaké množství operací máte závislých na Vašich dodavatelích?

- Odhadněte množství citlivých dat / majetku, které by se mohly stát cílem kyber / fyzického útoku.

Podobně jako v první části průzkumu každé kritérium obsahovalo 4 možné varianty odpovědí, a to dle hodnocení úrovně závislosti zkoumaného kritéria u dotazovaných malých a středních podniků. Každé kritérium bylo ohodnoceno počtem bodů v závislosti na dosaženém stupni závislosti – viz tab. 3.3.

Tabulka 3.3: Úroveň závislosti

Body	Úroveň závislosti
1	nízká
2	střední
3	vysoká
4	velmi vysoká

zdroj: vlastní zpracování

4 VÝSLEDKY

4.1 Zhodnocení zabezpečení procesů a technologií

Prvním krokem ke stanovení úrovně zabezpečení posuzované oblasti procesů a technologií bylo vyhodnocení zkoumaných dvaceti kritérií uvedených v kapitole č. 3.1. Každá zapojená organizace získala bodové hodnocení, a to na základě úrovně realizace všech zkoumaných kritérií, a to bez započítaného vlivu závislosti organizace na informačních a komunikačních technologiích. Zabezpečení dané oblasti bylo rozděleno do 4 úrovní - nízká, střední, vysoká a velmi vysoká a ke každé z nich byly stanoveny bodové intervaly - viz tab. 4.1.

Tabulka 4.1: Úroveň zabezpečení procesů a technologií bez vlivu závislosti na ICT

Body	Bodové intervaly	Úroveň zabezpečení
1	20-40	nízká
2	41-55	střední
3	56-69	vysoká
4	70-80	velmi vysoká

zdroj: vlastní zpracování

Po provedení vyhodnocení přidělených bodů na základě výše uvedených bodových intervalů jsou popsány výsledky vyplývající z provedeného dotazníkového šetření, rozdělené do všech tří kategorií zkoumaných subjektů, tj. mikropodniků, malých podniků a podniků střední velikosti.

V průzkumu byly zastoupeny tři kategorie organizací ze segmentu malých a středních podniků. Každá z nich dosáhla jako skupina jiných výsledků, a to především v krajních úrovních zabezpečení (nízká a velmi vysoká úroveň). V kategorii mikropodniků byla identifikována mírná většina subjektů, které výsledky šetření zařadily do nízké nebo střední úrovně managementu (51 %) a pouze 11 % z nich do velmi vysoké úrovně zabezpečení. Téměř polovina subjektů z kategorie malých podniků byla zařazena do vysoké úrovně managementu (48 %), což v součtu s velmi vysokou úrovní zabezpečení (21 %) tvoří více než dvě třetiny dotazovaných malých podniků (69 %). Signifikantní rozdíl je patrný v nízké a střední úrovni zabezpečení. Zatímco kategorie mikropodniků byla zastoupena nadpoloviční většinou zapojených subjektů, v rámci kategorie malých podniků byla do těchto zmíněných úrovní zabezpečení zařazena necelá jedna třetina organizací (31 %). Pro kategorii středních podniků výsledky potvrzují zvyšování kvality managementu bezpečnosti procesů a technologií s rostoucí velikostí podniku. V této kategorii nebyl žádný subjekt zařazen do nízké úrovně zabezpečení a pouze necelá čtvrtina organizací této velikosti prokázala střední úroveň zabezpečení. Naproti tomu více než tři čtvrtiny zkoumaných subjektů této kategorie zvládá management bezpečnosti procesů a technologií na vysoké nebo velmi vysoké úrovni, a to konkrétně 77 % zapojených subjektů.

Výsledky průzkumu bezpečnosti procesů a technologií bez vlivu závislosti na ICT:

- Mikropodniky
- poměrně velká skupina zkoumaných subjektů v této kategorii byla zařazena do kategorie vysoké úrovně zabezpečení, a to konkrétně 38 % ze zapojených mikropodniků, což je pozitivní zjištění,
- na druhou stranu většina zapojených subjektů z kategorie mikropodniků, přesněji 51 % (27% nízká úroveň, 24 % střední úroveň) vykázala nízkou nebo střední úroveň zabezpečení managementu procesů a technologií, což se nedá označit za překvapivý, ale ani pozitivní výsledek,

- pouze 11 % zkoumaných mikropodniků dle zvolené metodiky je možné označit za subjekty, které zvládají management procesů a technologií v souvislosti s řízením informační bezpečnosti bez problémů, tj. na velmi vysoké úrovni.

Malé podniky

- téměř polovině, konkrétně 48 % zapojených subjektů z této kategorie malých a středních podniků byla dle použité metodiky přiřazena úroveň managementu procesů a technologií na vysoké úrovni,
- 21 % subjektů dosáhlo velmi vysoké úrovně managementu,
- 24 % zkoumaných malých podniků realizuje management procesů a technologií na střední úrovni,
- pouze 7 % zapojených malých podniků vykazuje nízkou úroveň managementu.

Střední podniky

- podobně jako u kategorie malých podniků, velká skupina, téměř polovina (46 %) zapojených subjektů střední velikosti je koncentrována do vysoké úrovně zabezpečení zkoumané oblasti,
- téměř jedna třetina subjektů (31 %) byla zařazena do velmi vysoké úrovně zabezpečení oblasti procesů a technologií,
- méně než jedna čtvrtina zařazených organizací (23 %) byla vyhodnocena jako ty, které zvládají management zkoumané oblasti na nízké nebo střední úrovni, konkrétně 0 % nízká a 23 % střední úroveň zabezpečení.

Přehledné vyhodnocení úrovně managementu procesů a technologií dotazovaných mikropodniků, malých a středních podniků je k dispozici v tabulce 4.2.

Tabulka 4.2: Zhodnocení úrovně managementu procesů a technologií bez vlivu závislosti na ICT dle kategorie subjektu

Úroveň managementu	Počet zkoumaných subjektů			Kategorie subjektu
nízká	34 (11%)	22	27 %	mikropodnik
		12	7 %	malý podnik
		0	0 %	střední podnik
střední	73 (24%)	20	24 %	mikropodnik
		40	24 %	malý podnik
		13	23 %	střední podnik
vysoká	136 (45%)	31	38 %	mikropodnik
		79	48 %	malý podnik
		26	46 %	střední podnik
velmi vysoká	62 (20%)	9	11 %	mikropodnik
		35	21 %	malý podnik
		18	31 %	střední podnik

zdroj: vlastní zpracování

4.2 Zhodnocení závislosti na ICT

Dalším krokem ke stanovení úrovně zabezpečení posuzované oblasti procesů a technologií bylo vyhodnocení deseti kritérií uvedených v kapitole č. 3.2, které zkoumaly závislost organizací na informačních a komunikačních technologiích. Každá zapojená organizace získala bodové hodnocení, a to na základě úrovně závislosti všech zkoumaných kritérií. Úroveň závislosti byla opět rozdělena do 4 stupňů - nízká, střední, vysoká a velmi vysoká a ke každé z nich byly stanoveny bodové intervaly - viz tab. 4.3.

Tabulka 4.3: Úroveň závislosti na ICT

Body	Bodové intervaly	Úroveň závislosti
1	0-17	nízká
2	18-25	střední
3	26-32	vysoká
4	33-40	velmi vysoká

zdroj: vlastní zpracování

Mikropodniky

- největší skupina subjektů v této kategorii byla zařazena do střední úrovně závislosti na ICT, a to konkrétně 41 % ze zapojených mikropodniků,
- nízká i vysoká úroveň závislosti je zastoupena podobným poměrem sledovaných mikropodniků, a to 29 %, resp. 26 %,
- pouze 4 % zkoumaných mikropodniků dle zvolené metodiky je maximálně závislých na ICT.

Malé podniky

- zastoupené malé podniky většinově vykazují střední nebo vysokou závislost na ICT, Oba tyto stupně zahrnují téměř 80 % zkoumaných subjektů,
- pouze 8 % subjektů je minimálně závislých na ICT,
- oproti tomu je 13 % zkoumaných malých podniků významně závislých na ICT.

Střední podniky

- žádný zapojený subjekt střední velikosti nevykazoval nízkou úroveň závislosti na ICT,
- více než polovina subjektů (51 %) byla zařazena do vysoké úrovně závislosti na ICT,
- zbylá polovina středních podniků byla víceméně rozpůlena do úrovní střední a velmi vysoké úrovně závislosti na ICT.

Tabulkové zhodnocení úrovně závislosti na informačních a komunikačních technologiích dotazovaných organizací je k dispozici v tabulce 4.4.

Tabulka 4.4: Zhodnocení úrovně závislosti na ICT dle kategorie subjektu

Úroveň závislosti	Počet zkoumaných subjektů			Kategorie subjektu
nízká	37 (12%)	24	29 %	mikropodnik
		13	8 %	malý podnik
		0	0 %	střední podnik
střední	112 (37%)	34	41 %	mikropodnik
		63	38 %	malý podnik
		15	26 %	střední podnik
vysoká	118 (39%)	21	26 %	mikropodnik
		68	41 %	malý podnik
		29	51 %	střední podnik
velmi vysoká	38 (12%)	3	4 %	mikropodnik
		22	13 %	malý podnik
		13	23 %	střední podnik

zdroj: vlastní zpracování

4.3 Zhodnocení zabezpečení procesů a technologií v souvislosti se závislostí na ICT

Posledním krokem ke stanovení úrovně zabezpečení posuzované oblasti procesů a technologií bylo nastavení míry vlivu závislosti organizace na informačních a komunikačních technologiích na úroveň zabezpečení zkoumané oblasti. Pro realizované šetření byla využita metodika[7], která vychází z předpokladu, že čím vyšší závislost subjektu na ICT je detekována, tím vyšší nároky jsou kladeny na bezpečnost procesů a technologií. Na druhou stranu pro subjekt s vyhodnocenou nízkou závislostí na ICT budou platit mírnější parametry pro dosažení stupně velmi vysoké úrovně managementu procesů a technologií než pro subjekt s vysokou nebo velmi vysokou závislostí na ICT.

Každá zapojená organizace získala bodové hodnocení, a to na základě úrovně závislosti na ICT a následně dle zařazení do bodového intervalu, který odpovídal dosaženému výsledku v rámci průzkumu úrovně managementu procesů a technologií. Výsledná interpretace byla opět rozdělena do 4 stupňů - nedostatečná ochrana, vyžaduje výrazné zlepšení, vyžaduje dílčí zlepšení, přiměřená ochrana - viz tab. 4.5.

[7] KRÁL, D. Informační bezpečnost podniku.

Tabulka 4.5: Bezpečnost procesů a technologií v souvislosti se závislostí na ICT

Úroveň závislost na ICT	Bodové intervaly - úroveň managementu procesů a technologií	Interpretace
nízká	20-34	nedostatečná ochrana
	35-44	vyžaduje výrazné zlepšení
	45-54	vyžaduje dílčí zlepšení
	55-80	přiměřená ochrana
střední	20-40	nedostatečná ochrana
	41-50	vyžaduje výrazné zlepšení
	51-60	vyžaduje dílčí zlepšení
	61-80	přiměřená ochrana
vysoká	20-46	nedostatečná ochrana
	47-56	vyžaduje výrazné zlepšení
	57-66	vyžaduje dílčí zlepšení
	67-80	přiměřená ochrana
velmi vysoká	20-52	nedostatečná ochrana
	53-62	vyžaduje výrazné zlepšení
	63-72	vyžaduje dílčí zlepšení
	73-80	přiměřená ochrana

zdroj: vlastní výzkum

Následovalo opět vyhodnocení přidělených bodů na základě výše uvedené metodiky a zařazení do patřičného intervalu. V následujícím textu jsou popsány výsledky, které vyplývají z provedeného dotazníkového průzkumu a které jsou znovu rozděleny do tří kategorií zkoumaných subjektů.

Po přiznání vlivu závislosti na ICT se výsledky pro všechny sledované kategorie malých a středních podniků pozitivně proměnily. V kategorii mikropodniků se většina subjektů, a to přibližně dvoutřetinová, zařadila do vysoké a velmi vysoké úrovně managementu (64 %). Zbylá třetina subjektů zůstala v problematických úrovních, tedy nízké (23 %) a střední (13 %). Také v kategorii malých podniků se efekt závislosti na ICT projevil pozitivně na celkovém hodnocení úrovně managementu, ale ne nijak dramaticky. Mírně se zvýšil podíl subjektů spadajících do vysoké a velmi vysoké úrovně managementu (74 %), ale spíše došlo k přesunu části subjektů z úrovně vysoké do úrovně velmi vysoké, která poté vykazovala zastoupení více než třetiny zkoumaných malých podniků. Pro podniky střední velikosti se vliv závislosti na ICT v nízké a střední úrovni managementu vůbec neprojevil a tyto stupně zůstaly naprosto beze změny. Přesun byl zaznamenán pouze mezi vysokou a velmi vysokou úrovní managementu. Po uplatnění

vlivu závislosti ICT byla téměř polovina dotazovaných středních podniků zařazena do nejvyšší, tedy velmi vysoké úrovně managementu bezpečnosti procesů a technologií.

Tabulkové zhodnocení úrovně zabezpečení procesů a technologií, které porovnává výsledky s vlivem i bez vlivu závislostí na informačních a komunikačních technologiích dotazovaných organizací je k dispozici v tabulce 4.6.

Tabulka 4.6: Zhodnocení úrovně zabezpečení procesů a technologií v souvislosti se závislostí na ICT dle kategorie subjektu

Interpretace / Úroveň managementu	**Počet subjektů / s vlivem závislosti na ICT**			**Počet subjektů/bez vlivu závislosti na ICT**			**Kategorie subjektu**
nedostatečná ochrana / nízká	34 (11%)	19	23 %	34 (11%)	22	27 %	mikropodnik
		15	9 %		12	7 %	malý podnik
		0	0 %		0	0 %	střední podnik
vyžaduje výrazné zlepšení / střední	52 (17%)	11	13 %	73 (24%)	20	24 %	mikropodnik
		28	17 %		40	24 %	malý podnik
		13	23 %		13	23 %	střední podnik
vyžaduje dílčí zlepšení / vysoká	110 (36%)	30	37 %	136 (45%)	31	38 %	mikropodnik
		63	38 %		79	48 %	malý podnik
		17	30 %		26	46 %	střední podnik
přiměřená ochrana / velmi vysoká	109 (36%)	22	27 %	62 (20%)	9	11 %	mikropodnik
		60	36 %		35	21 %	malý podnik
		27	47 %		18	31 %	střední podnik

zdroj: vlastní zpracování

5 DISKUSE A ZÁVĚRY

Realizovaný výzkum v oblasti managementu bezpečnosti procesů a technologií zkoumá tuto významnou oblast v systému managementu informační bezpečnosti, a to dle doporučených postupů uvedených v normách ISO/IEC 27K. Nejprve je provedeno šetření v samotné oblasti procesů a technologií, poté je zjišťována závislost zkoumaných subjektů v oblasti závislosti na informačních a komunikačních technologiích a následně je dle zvolené metodiky upraveno hodnocení úrovně managementu bezpečnosti procesů a technologií v souvislosti se zjištěnou závislostí na ICT. Z výsledků provedeného průzkumu vyplývají následující skutečnosti:

- s rostoucí velikostí subjektu roste i úroveň managementu bezpečnosti procesů a technologií,
- s rostoucí velikostí subjektu roste i úroveň závislosti na informačních a komunikačních technologiích,
- závislost na ICT se jeví jako vhodný doplňkový faktor při konstrukci metodiky hodnocení úrovně managementu informační bezpečnosti.

I přes uvedené závěry nelze velikost organizace považovat za nejdůležitější parametr přístupu k managementu informační bezpečnosti. Vliv závislosti na ICT není v současné době zanedbatelný a může přispět k nastavení vhodných doporučení při posuzování úrovně bezpečnosti procesů a technologií. Dá se ovšem očekávat, že síla tohoto faktoru bude v budoucnu klesat, poněvadž je zřejmé, že závislost na ICT bude neustále stoupat a vysoká úroveň závislosti se bude postupně týkat naprosté většiny podnikatelských subjektů.

AFILACE

Příspěvek je zpracován jako jeden z výstupů výzkumného projektu „Informační bezpečnost procesů a technologií v prostředí malých a středních podniků“ v rámci oblasti IGA_AS_03_08, podporovaného interní grantovou agenturou AKADEMIE STING.

POUŽITÉ ZDROJE

[1] ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary. International Organization for Standardization. 2014.

[2] ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization. 2013.

[3] ISO/IEC 27002 - Information technology — Security techniques - Code of practice for information security controls. International Organization for Standardization. 2013.

[4] KRÁL, D. Management bezpečnosti informací v malých a středních podnicích. In: JEŽKOVÁ, R. a kol. Podnikání a management v malých a středních podnicích: teoretické aspekty a aplikace. 1. vyd. Brno: STING, spol. s r.o., 2015. 399 s. s. 224-269.

[5] KRÁL, D. Informační bezpečnost podniku. VUT Brno: disertační práce, 2010.

[6] MANSO, C. G, REKLEITIS, E., PAPAZAFEIROPOULOS, F., and V. MARITSAS. Information security and privacy standards for SMEs. Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. ENISA, 2015. 55 s. ISBN 978-92-9204-159-5.

[7] O´HANLEY, R. a J.S. TILLER, Information Security Management Handbook. 6th. edition. Auerbach Publications, 2013. 434 s. ISBN 978-14-6656-749-8.

[8] Aplikační výklad pro vymezení pojmů drobný, malý a střední podnikatel a postupů pro zařazování podnikatelů do jednotlivých kategorií. Czechinvest: Agentura pro podporu podnikání a investic [online]. 2014 [cit. 2017-11-10]. Dostupné z: http://www.czechinvest.org/data/files/definice-maleho-a-stredniho-podniku-2-1112.pdf

[9] Definice malého a středního podnikatele. Czechinvest: Agentura pro podporu podnikání a investic [online]. c1994-2017 [cit. 2017-11-10]. Dostupné z: http://www.czechinvest.org/definice-msp

AUTOR

Ing. David Král, Ph.D., Katedra aplikovaných disciplín, AKADEMIE STING, o.p.s., Stromovka 1, 637 00 Brno, e-mail: kral@sting.cz.

AUTHOR

Ing. David Král, Ph.D., Department of Applied Disciplines, STING ACADEMY, Stromovka 1, 637 00 Brno, Czech Republic, e-mail: kral@sting.cz.