BEZPEČNOST PROCESŮ A TECHNOLOGIÍ

SECURITY OF PROCESSES AND TECHNOLOGIES

David Král

Abstrakt: *Článek se věnuje problematice bezpečnosti procesů a technologií v rámci systému managementu informační bezpečnosti, a to v segmentu mikro a malých podniků. Popisuje oblast standardizace systémů managementu informační bezpečnosti s důrazem na oblasti procesů a technologií. V článku je popsán a vyhodnocen průzkum v segmentu mikro a malých podniků, který mapuje ve výše zmíněných oblastech kvalitu zabezpečení mezi zkoumanými subjekty. Cílem článku je prezentovat výsledky provedeného průzkumu a poukázat na důležitost této oblasti při tvorbě strategie managementu informační bezpečnosti.*

Klíčová slova: *management bezpečnosti informací, mikro a malé podniky, bezpečnost procesů a technologií*

Abstract: *The paper discusses the issue of security of processes and technologies in an information security management system, mainly in the segment of micro and small enterprises. It describes the standardization of information security management systems with an accent to the field of processes and technologies. The paper describes and evaluates a survey among micro and small enterprises, which maps the quality of security in the above mentioned areas. This article aims to present the results of the survey and to highlight the importance of this sphere in developing a management strategy for information security.*

Keywords: *information security management, micro and small enterprises, security of processes and technologies*

JEL klasifikace: *M12, M15*

1 ÚVOD

Informace se stávají stále důležitějším aktivem pro podnikání organizace a v důsledku toho je nutné je adekvátně zabezpečit. Informace mohou být uloženy v mnoha rozličných formách a přenášeny různými prostředky komunikace. Management bezpečnosti informací je disciplínou, která identifikuje citlivá aktiva, jejich zranitelnost a hrozby, které mohou způsobit ztrátu jejich dostupnosti, integrity a důvěrnosti.

Definice informační bezpečnosti je uvedena například ve standardu ISO (ISO/IEC 27000:2014)[14] - *„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.“*

Informační bezpečnost je standardně implementována prostřednictvím pevně daných pravidel, která vyplynou z analýzy informačních rizik, která je prvním krokem celého procesu. Vytvořená bezpečnostní politika je poté řízena pomocí systému managementu bezpečnosti informací. Bezpečnostní pravidla musí být korektně specifikována, realizována, monitorována, přezkoumávána a tam, kde je to nutné, tak aktualizována.

Jednou z nejdůležitějších součástí systému informační bezpečnosti je samotná ochrana procesů a technologií, které v dané organizaci probíhají, resp. jsou využívány. V dalších kapitolách článku je provedena základní analýza této zkoumané oblasti a provedeno vyhodnocení kvantitativního výzkumu metodou dotazníkového šetření, které bylo realizováno na vzorku téměř 250 mikropodniků a malých podniků převážně Jihomoravského kraje.

2 INFORMAČNÍ BEZPEČNOST PROCESŮ A TECHNOLOGIÍ

Existuje řada norem a postupů zpracovaných pro management bezpečnosti informací. Soubor norem ISO/IEC 27K definuje požadavky týkající se politiky, rolí, odpovědností a pravomocí zaměstnanců zainteresovaných na informační bezpečnosti. Kromě toho vyžaduje funkčnost procesů, postupů a organizačních struktur, které budou předcházet, odhalovat a reagovat na různé typy hrozeb. Tento systém managementu je schopen chránit

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

důvěrnost, integritu a dostupnost informací v kooperaci s aplikací procesu managementu rizik a dává tak jistotu zainteresovaným stranám, že rizika jsou odpovídajícím způsobem řízena.

Zavedení a implementace jakékoliv normy pro bezpečnost informací závisí na strategické orientaci organizace a je ovlivněna řadou aspektů, včetně potřeb a cílů daného subjektu, požadavcích na bezpečnost, organizačních procesech, velikosti a struktuře organizace. V dalším textu je uveden popis klíčových oblastí informační bezpečnosti, které zajišťují ochranu procesů a technologií, tak jak je charakterizuje norma ISO/IEC 27002[15].

Management aktiv

Cílem této oblasti je identifikovat aktiva organizace a definovat odpovědnosti za jejich ochranu. Dále je nutné zajistit, aby tyto informace byly adekvátně zabezpečeny vzhledem k jejich důležitosti pro danou organizaci. V neposlední řadě je také třeba zabránit neoprávněnému přístupu, modifikaci, odcizení či zničení informací uložených na médiích.

V této oblasti by měl být identifikován vlastník aktiv a další zainteresované osoby, které mají být zodpovědné za bezpečnost aktiv a za jejich klasifikaci a nakládání s nimi. Veškerá technická zařízení pro zpracování informací by také měla být identifikována a udržována. Navíc se tato oblast zabývá kontrolou řízení vyměnitelných médií, likvidací médií a fyzického přenosu médií.

Řízení přístupu

Cílem této oblasti je omezit přístup k citlivým informacím a k zařízením na jejich zpracování. Dále je třeba zajistit přístup k informacím autorizovaným uživatelům a zabránit neoprávněným přístupům k systémům a službám.

Tato oblast je zaměřena na ochranu proti záměrnému i náhodnému poškození nebo ztrátě aktiv. V ideálním případě by to měli být vlastníci aktiv, kteří stanoví vhodná pravidla pro řízení přístupu, přístupová práva a omezení pro specifické uživatelské role vůči těmto aktivům. To vyžaduje zdokumentovanou bezpečnostní politiku týkající vytvoření, odstranění a revizi přístupových práv, včetně fyzického přístupu a přístupu k síťovým službám.

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

Fyzická bezpečnost a bezpečnost prostředí

Cílem této oblasti je zabránit neoprávněným fyzickým přístupům, poškození nebo zničení informací a zařízení na jejich zpracování. Dále je třeba předcházet ztrátě, krádeži nebo ohrožení aktiv a zabránění tak případnému přerušení provozu organizace.

Řízení této oblasti zahrnuje fyzické zabezpečení perimetru kancelářských či dalších prostor a zařízení, ochranu před vnějšími a živelnými hrozbami, zabezpečení proti ztrátě, zničení, krádeži nebo poškození aktiv, ochranu zařízení před výpadky napájení, ochranu kabeláže před poškozením, údržbu zařízení.

Bezpečnost provozu

Cílem této oblasti je zajistit bezpečný provoz zařízení pro zpracování informací. Dále se předpokládá, že informace a zařízení na jejich zpracování jsou chráněny proti malware, jsou zaznamenávány bezpečnostní události a zajišťovány důkazy, je zajištěna integrita operačních systémů, je zabráněno zneužívání technických zranitelností aktiv.

Tato oblast se zabývá schopností organizace zajistit korektní a bezpečný provoz. Řízení zahrnuje provozní postupy a odpovědnosti pro ochranu před malware, zálohování, logování a monitorování, řízení operačních systémů, management zranitelností.

Bezpečnost komunikací

Cílem této oblasti je zajistit ochranu informací v oblasti sítí a souvisejících podpůrných zařízení pro zpracování informací. Dále je třeba zajistit ochranu citlivých dat při jejich přenosu v rámci organizace nebo na jakýkoliv externí subjekt.

Tato oblast řeší schopnost organizace zajistit ochranu informací v systémech a aplikacích v sítích a jeho podpůrných zařízeních pro zpracování informací. Řízení zahrnuje bezpečnost informací v sítích a souvisejících služeb před neoprávněným přístupem, zásady a postupy pro transfer dat, bezpečný přenos obchodních informací mezi organizací a externími subjekty, pravidla týkající se používání elektronické pošty.

Vztahy s dodavateli

Cílem této oblasti je zajistit ochranu aktiv organizace, které jsou přístupné pro externí subjekty. Dále je cílem zachování dohodnuté úrovně bezpečnosti informací a poskytování služeb v souladu s dodavatelskými smlouvami.

Tato oblast se zabývá řízením vztahů s dodavateli, včetně politiky zabezpečení informací a procesů, řešení bezpečnosti v rámci dodavatelských smluv, komunikací a povědomím o užívaných technologiích v rámci dodavatelského řetězce a řízením dodávky služeb.

3 PRŮZKUM BEZPEČNOSTI PROCESŮ A TECHNOLOGIÍ

Průzkumu se zúčastnilo celkem 248 mikro a malých podniků. Zapojené subjekty byly zařazeny do této kategorie dle evropské legislativy[16].

Tabulka 3.1: Kategorie malých a středních podniků

Kategorie podniku	Počet zaměstnanců	Obrat
Mikropodnik	< 10	< 2 mil. EUR
Malý podnik	< 50	< 10 mil. EUR

Zdroj: http://ec.europa.eu/growth/smes

V rámci tohoto průzkumu bylo zkoumáno, do jaké míry sledované mikro a malé podniky řídí problematiku bezpečnosti procesů a technologií. Zjištěná kvalita zabezpečení této oblasti je poté jedním z klíčových aspektů při tvorbě strategie managementu informační bezpečnosti. V průzkumu byla zkoumána kritéria, která jsou považována za významná pro tuto oblast ve standardech ISO/IEC 27K:

- 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,

[16] http://ec.europa.eu/growth/smes

- 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

Každá z otázek v rámci průzkumu měla čtyři varianty možných odpovědí, a to podle hodnocení úrovně realizace daného kritéria u zapojených subjektů. Každé kritérium bylo ohodnoceno body ze škály 1-4 a podniku byla přidělena úroveň zabezpečení.

Tabulka 3.2: Zhodnocení úrovně realizace

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

zdroj: vlastní zpracování

Fyzické zabezpečení prostor

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda jsou prostory, které obsahují zařízení pro zpracování informací, chráněny bezpečnostními perimetry / bariérami.

Tabulka 3.3: Fyzické zabezpečení prostor

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	17	29 %	nerealizováno
		17	29 %	plánováno
		17	29 %	částečně realizováno
		8	13 %	kompletně realizováno
malý podnik	189	20	11 %	nerealizováno
		28	15 %	plánováno
		91	48 %	částečně realizováno
		50	26 %	kompletně realizováno

zdroj: vlastní zpracování

Politika povolení vstupu do prostor

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda je do prostorů organizace, které obsahují citlivé informace nebo zařízení, povolen vstup pouze oprávněným osobám.

Tabulka 3.4: Politika povolení vstupu do prostor

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	4	7 %	nerealizováno
		12	20 %	plánováno
		21	36 %	částečně realizováno
		22	37 %	kompletně realizováno
malý podnik	189	19	10 %	nerealizováno
		17	9 %	plánováno
		59	31 %	částečně realizováno
		94	50 %	kompletně realizováno

zdroj: vlastní zpracování

Zajištění proti přírodním hrozbám

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda je organizace zajištěna proti vnějším a přírodním hrozbám.

Tabulka 3.5: Zajištění proti přírodním hrozbám

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	16	27 %	nerealizováno
		12	20 %	plánováno
		23	39 %	částečně realizováno
		8	14 %	kompletně realizováno
malý podnik	189	14	7 %	nerealizováno
		20	11 %	plánováno
		80	42 %	částečně realizováno
		75	40 %	kompletně realizováno

zdroj: vlastní zpracování

Ochrana před selháním napájení

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda jsou zařízení, která zpracovávají informace, chráněna před selháním napájení a před dalšími formami přerušení způsobenými poruchami podpůrných zařízení.

Tabulka 3.6: Ochrana před selháním napájení

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	12	20 %	nerealizováno
		18	31 %	plánováno
		16	27 %	částečně realizováno
		13	22 %	kompletně realizováno
malý podnik	189	17	9 %	nerealizováno
		25	13 %	plánováno
		77	41 %	částečně realizováno
		70	37 %	kompletně realizováno

zdroj: vlastní zpracování

Postup bezpečné likvidace

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda existuje v organizaci postup bezpečné likvidace a odstraňování majetku po autorizaci oprávněné osoby tak, aby neunikly citlivé informace.

Tabulka 3.7: Postup bezpečné likvidace

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	12	20 %	nerealizováno
		11	19 %	plánováno
		26	44 %	částečně realizováno
		10	17 %	kompletně realizováno
malý podnik	189	20	11 %	nerealizováno
		26	14 %	plánováno
		65	34 %	částečně realizováno
		78	41 %	kompletně realizováno

zdroj: vlastní zpracování

Ochrana před škodlivým software

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda jsou veškeré stanice v organizaci dostatečně chráněny proti škodlivým programům a kódům.

Tabulka 3.8: Ochrana před škodlivým software

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	3	5 %	nerealizováno
		11	19 %	plánováno
		27	46 %	částečně realizováno
		18	30 %	kompletně realizováno
malý podnik	189	10	5 %	nerealizováno
		22	12 %	plánováno
		74	39 %	částečně realizováno
		83	44 %	kompletně realizováno

zdroj: vlastní zpracování

Postup zálohování dat

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda existuje v organizaci postup pravidelného a bezpečného zálohování dat.

Tabulka 3.9: Postup zálohování dat

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	4	7 %	nerealizováno
		15	25 %	plánováno
		21	36 %	částečně realizováno
		19	32 %	kompletně realizováno
malý podnik	189	4	2 %	nerealizováno
		16	9 %	plánováno
		70	37 %	částečně realizováno
		99	52 %	kompletně realizováno

zdroj: vlastní zpracování

Postup šifrování dat

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda jsou důvěrná, osobní či citlivá data šifrována a související šifrovací klíče náležitě chráněny.

Tabulka 3.10: Postup šifrování dat

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	16	27 %	nerealizováno
		10	17 %	plánováno
		20	34 %	částečně realizováno
		13	22 %	kompletně realizováno
malý podnik	189	35	18 %	nerealizováno
		29	15 %	plánováno
		71	38 %	částečně realizováno
		54	29 %	kompletně realizováno

zdroj: vlastní zpracování

Ochrana výměny dat s externími partnery

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda jsou veškeré výměny programového vybavení a informací v rámci organizace nebo v rámci výměny s externími partnery vhodným způsobem chráněny.

Tabulka 3.11: Ochrana výměny dat s externími partnery

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	8	13 %	nerealizováno
		11	19 %	plánováno
		29	49 %	částečně realizováno
		11	19 %	kompletně realizováno
malý podnik	189	25	13 %	nerealizováno
		21	11 %	plánováno
		88	41 %	částečně realizováno
		55	29 %	kompletně realizováno

zdroj: vlastní zpracování

Bezpečnostní opatření v rámci smluvního partnerství

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda obsahují smlouvy s partnery organizace dodávajícími výrobky/služby opatřeny výčtem bezpečnostních opatření a sankcemi, pokud tato opatření partneři nedodržují.

Tabulka 3.12: Bezpečnostní opatření v rámci smluvního partnerství

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	13	22 %	nerealizováno
		13	22 %	plánováno
		22	37 %	částečně realizováno
		11	19 %	kompletně realizováno
malý podnik	189	33	17 %	nerealizováno
		18	10 %	plánováno
		58	31 %	částečně realizováno
		80	42 %	kompletně realizováno

zdroj: vlastní zpracování

Záznam aktivit uživatelů informačního systému

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda jsou po dostatečně dlouhou dobu zaznamenávány aktivity všech uživatelů v informačním systému organizace, výjimky a události související s bezpečností informací.

Tabulka 3.13: Záznam aktivit uživatelů informačního systému

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	13	22 %	nerealizováno
		15	25 %	plánováno
		17	29 %	částečně realizováno
		14	24 %	kompletně realizováno
malý podnik	189	32	17 %	nerealizováno
		31	17 %	plánováno
		61	32 %	částečně realizováno
		65	34 %	kompletně realizováno

zdroj: vlastní zpracování

Aplikace nápravných opatření na odstranění vzniklých chyb

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda jsou zjištěné údaje analyzovány a přijímány příslušná opatření na odstranění vzniklých chyb.

Tabulka 3.14: Aplikace nápravných opatření na odstranění vzniklých chyb

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	10	17 %	nerealizováno
		12	20 %	plánováno
		25	43 %	částečně realizováno
		12	20 %	kompletně realizováno
malý podnik	189	28	15 %	nerealizováno
		27	14 %	plánováno
		79	42 %	částečně realizováno
		55	29 %	kompletně realizováno

zdroj: vlastní zpracování

Dodržování politiky čistého stolu a obrazovky

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda je v organizaci dodržována politika čistého stolu a obrazovky.

Tabulka 3.15: Dodržování politiky čistého stolu a obrazovky

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	13	22 %	nerealizováno
		14	24 %	plánováno
		18	30 %	částečně realizováno
		14	24 %	kompletně realizováno
malý podnik	189	43	23 %	nerealizováno
		31	16 %	plánováno
		73	39 %	částečně realizováno
		42	22 %	kompletně realizováno

zdroj: vlastní zpracování

Postup pro registraci uživatele do informačního systému

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda existuje postup pro registraci uživatele do informačního systému organizace, a přidělení práv pro přístup do oblastí IS dle klasifikace uživatele.

Tabulka 3.16: Postup pro registraci uživatele do informačního systému

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	16	27 %	nerealizováno
		12	20 %	plánováno
		17	29 %	částečně realizováno
		14	24 %	kompletně realizováno
malý podnik	189	22	12 %	nerealizováno
		18	9 %	plánováno
		42	22 %	částečně realizováno
		107	57 %	kompletně realizováno

zdroj: vlastní zpracování

Odpovědnost uživatelů za činnost v informačním systému

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda mají všichni uživatelé informačního systému jedinečný identifikátor (ID) tak, aby bylo možné dosledovat odpovědnost za jejich činnosti.

Tabulka 3.17: Odpovědnost uživatelů za činnost v informačním systému

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	14	24 %	nerealizováno
		9	15 %	plánováno
		22	37 %	částečně realizováno
		14	24 %	kompletně realizováno
malý podnik	189	28	15 %	nerealizováno
		25	13 %	plánováno
		43	23 %	částečně realizováno
		93	49 %	kompletně realizováno

zdroj: vlastní zpracování

Dodržování tvorby tzv. silných hesel

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda jsou uživatele donuceni systémem tvořit pouze tzv. silná hesla.

Tabulka 3.18: Dodržování tvorby tzv. silných hesel

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	17	29 %	nerealizováno
		13	22 %	plánováno
		19	32 %	částečně realizováno
		10	17 %	kompletně realizováno
malý podnik	189	41	22 %	nerealizováno
		26	14 %	plánováno
		46	24 %	částečně realizováno
		76	40 %	kompletně realizováno

zdroj: vlastní zpracování

Postup autentizace při vzdáleném přístupu do informačního systému

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda jsou aplikovány zvláštní postupy autentizace při vzdáleném přístupu do informačního systému organizace.

Tabulka 3.19: Postup autentizace při vzdáleném přístupu do informačního systému

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	18	31 %	nerealizováno
		20	34 %	plánováno
		16	27 %	částečně realizováno
		5	8 %	kompletně realizováno
malý podnik	189	46	24 %	nerealizováno
		27	14 %	plánováno
		69	37 %	částečně realizováno
		47	25 %	kompletně realizováno

zdroj: vlastní zpracování

Ochrana portů pro vzdálenou diagnostiku a konfiguraci

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda jsou bezpečně chráněny porty pro vzdálenou diagnostiku a konfiguraci.

Tabulka 3.20: Ochrana portů pro vzdálenou diagnostiku a konfiguraci

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	18	31 %	nerealizováno
		13	22 %	plánováno
		22	37 %	částečně realizováno
		6	10 %	kompletně realizováno
malý podnik	189	35	18 %	nerealizováno
		30	16 %	plánováno
		68	36 %	částečně realizováno
		56	30 %	kompletně realizováno

zdroj: vlastní zpracování

Politika odhlášení stanic ze systému při nečinnosti

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda jsou stanice po určené době nečinnosti odhlášeny od systému.

Tabulka 3.21: Politika odhlášení stanic ze systému při nečinnosti

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	19	32 %	nerealizováno
		11	19 %	plánováno
		13	22 %	částečně realizováno
		16	27 %	kompletně realizováno
malý podnik	189	29	13 %	nerealizováno
		15	8 %	plánováno
		45	24 %	částečně realizováno
		104	55 %	kompletně realizováno

zdroj: vlastní zpracování

Zásady bezpečnosti práce na mobilních zařízeních

V rámci tohoto kritéria se zástupci oslovených subjektů vyjadřovali k otázce, zda existují v organizaci zásady a postupy bezpečné práce na mobilních výpočetních prostředcích a zařízeních.

Tabulka 3.22: Zásady bezpečnosti práce na mobilních zařízeních

Kategorie subjektu	Počet zkoumaných subjektů			Úroveň realizace
mikropodnik	59	13	22 %	nerealizováno
		11	18 %	plánováno
		24	41 %	částečně realizováno
		11	19 %	kompletně realizováno
malý podnik	189	35	19 %	nerealizováno
		29	15 %	plánováno
		69	36 %	částečně realizováno
		56	30 %	kompletně realizováno

zdroj: vlastní zpracování

4 VÝSLEDKY

Celková úroveň zabezpečení oblasti procesů a technologií byla určena vyhodnocením zkoumaných kritérií. Úroveň kvality zabezpečení byla podniku přidělena na základě získaného bodového hodnocení, a to na základě bodových intervalů uvedených v tabulce 4.1.

Tabulka 4.1: Úroveň kvality zabezpečení oblasti procesů a technologií

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

Na základě výše uvedených bodových intervalů jsou dále uvedeny základní výsledky vyplývající z provedeného průzkumu, rozdělené do obou kategorií zkoumaných subjektů - mikropodniků a malých podniků.

Vzhledem k zastoupení dvou kategorií subjektů ze segmentu malých a středních podniků v provedeném průzkumu, je třeba hodnotit jednotlivé kategorie podniků rozdílně. V kategorii mikropodniků se nacházela většina subjektů, které vyhodnocení průzkumu zařadilo do nízké nebo střední úrovně managementu (58 %) a pouze 8 % z nich do kategorie velmi vysoké úrovně. Většina malých podniků se koncentrovala do kategorie vysoké úrovně managementu (51 %), společně s velmi vysokou úrovní (21 %) tvoří téměř tři čtvrtiny zastoupených malých podniků (72 %). Zatímco skupina malých podniků zařazených do nízké a střední úrovně managementu procesů a technologií, která v rámci mikropodniků byla zastoupena nadpoloviční většinou zapojených subjektů, je v rámci malých podniků zastoupena pouze 28 % zapojených subjektů, tj. přibližně jednou čtvrtinou.

Mikropodniky

- největší skupina zapojených subjektů z této kategorie mikropodniků a malých podniků vykázala úroveň managementu procesů a technologií na střední a vysoké úrovni, tohoto výsledku v obou uvedených úrovních zabezpečení dosáhla 34 % mikropodniků,
- naproti tomu téměř čtvrtina těchto subjektů (24 %) dosáhla nízké úrovně managementu lidských zdrojů,
- pouze 8 % zkoumaných mikropodniků dle zvolené metodiky je možné označit jako ty, kteří zvládají management procesů a technologií v souvislosti s řízením informační bezpečnosti na velmi vysoké úrovni.

Malé podniky

- více než polovina, konkrétně 51 % zapojených subjektů z této kategorie mikropodniků a malých podniků vykázala úroveň managementu procesů a technologií na vysoké úrovni,
- 21 % subjektů dosáhlo velmi vysoké úrovně managementu,
- 19 % zkoumaných malých podniků realizuje management procesů a technologií na střední úrovni,
- pouze 9% zapojených malých podniků vykazuje nízkou úroveň managementu.

Kompletní zhodnocení úrovně managementu procesů a technologií zapojených mikropodniků a malých podniků je uvedeno v tabulce 4.2.

Tabulka 4.2: Zhodnocení úrovně managementu procesů a technologií dle kategorie subjektu

Úroveň managementu	Počet zkoumaných subjektů			Kategorie subjektu
nízká	31 (12%)	14	24 %	mikropodnik
		17	9 %	malý podnik
střední	56 (23%)	20	34 %	mikropodnik
		36	19 %	malý podnik
vysoká	117 (47%)	20	34 %	mikropodnik
		97	51 %	malý podnik
velmi vysoká	44 (18%)	5	8 %	mikropodnik
		39	21 %	malý podnik

zdroj: vlastní zpracování

5 DISKUSE A ZÁVĚRY

Výzkum v oblasti managementu procesů a technologií provádí audit základních parametrů doporučeného přístupu ke zmíněné oblasti informační bezpečnosti tak, jak k ní přistupuje norma ISO/IEC 27K. Z výsledků průzkumu na jedné straně vyplývá, že velká skupina zapojených subjektů přistupuje k této problematice zodpovědně, na druhou stranu je z hodnocení jednotlivých parametrů i z hodnocení celkového patrné, že není možné považovat segment malých a středních podniků, minimálně v této oblasti, za homogenní skupinu. Existují zde významné rozdíly mezi hodnocením jednotlivých subjektů v rámci zařazených kategorií podniků a ukazuje se zde

jistá závislost mezi velikostí subjektu a úrovní managementu v rámci zkoumané oblasti. Zatímco malé podniky vykazují v naprosté většině kvalitní přístup k managementu procesů a technologií, mikropodniky mají v této oblasti managementu větší nedostatky a jejich hodnocení je kvalitativně na horší úrovni. Velikost podniku ale není samozřejmě možné považovat za zásadní měřítko přístupu k informační bezpečnosti. I mikropodnik může být zcela závislý na informačních a komunikačních technologiích a vybraný bezpečnostní incident mu může způsobit problémy i existenciálního charakteru.

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. ISBN 978-80-87482-30-8.

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.