Ekonomická fakulta
Faculty of Economics

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích
Ekonomická fakulta
Katedra aplikované matematiky a informatiky

Diplomová práce

Analýza stavu bezpečnosti informací ve vybraných obcích

Vypracoval: Bc. Lukáš Kubala
Vedoucí práce: doc. Ing. Ladislav Beránek, CSc.

České Budějovice 2020

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Ekonomická fakulta

Akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Lukáš KUBALA**
Osobní číslo:	**E18349**
Studijní program:	**N6209 Systémové inženýrství a informatika**
Studijní obor:	**Ekonomická informatika**
Téma práce:	**Analýza stavu bezpečnosti informací ve vybraných obcích**
Zadávající katedra:	**Katedra aplikované matematiky a informatiky**

Zásady pro vypracování

Cílem práce je analyzovat informační systém ve vybraných obcích s využitím standardů zejména ISO/IEC 27000. Práce se soustředí na dopady zákona č. 181/2014 Sb., o kybernetické bezpečnosti a regulativu GDPR na informační systém obcí a příslušné procesy. Bude navržen a proveden dotazníkový průzkum dopadů zmíněných zákonů na vybraných obcích. Na základě analýzy dotazníků a provedených analýz rizik budou navržena případná opatření včetně procesního návrhu.

Metodický postup:

1. Současný stav řešené problematiky – přehled regulatorního prostředí.
2. Analýza dopadu zákonných norem na informační systémy obcí a jejich procesy.
3. Provedení průzkumu, analýza rizik, analýza výsledků.
4. Návrh a zdůvodnění rámcového řešení zadaného problému.
5. Závěr.

Rozsah pracovní zprávy:	**50 – 60 stran**
Rozsah grafických prací:	**dle potřeby**
Forma zpracování diplomové práce:	**tištěná**

Seznam doporučené literatury:

1. DONÁT, Josef. (2017). *Nařízení eIDAS: komentář.* Praha: C.H. Beck.
2. MATES, Pavel, & SMEJKAL, Vladimír. (2012). *E-government v České republice: právní a technologické aspekty.* Praha: Leges.
3. ROHEL, Vladimír.(2013). Dopady zákona o kybernetické bezpečnosti na povinné osoby. *DSM Data Security Management*, roč. XVII, č. 4.
4. SMEJKAL, Vladimír. (2015). *Kybernetická kriminalita.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk.

Vedoucí diplomové práce: **doc. Ing. Ladislav Beránek, CSc.**
Katedra aplikované matematiky a informatiky

Datum zadání diplomové práce: **15. ledna 2019**
Termín odevzdání diplomové práce: **12. dubna 2020**

V Českých Budějovicích dne 18. března 2019

JIHOČESKÁ UNIVERZITA
V ČESKÝCH BUDĚJOVICÍCH
EKONOMICKÁ FAKULTA
Studentská 13
370 05 České Budějovice

L.S.

doc. Dr. Ing. Dagmar Škodová Parmová
děkanka

doc. RNDr. Jana Klicnarová, Ph.D.
vedoucí katedry

Prohlášení

Prohlašuji, že svou diplomovou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

Poděkování

Chtěl bych tímto způsobem poděkovat vedoucímu práce doc. Ing. Ladislavu Beránkovi CSc. za rady a pomoc při tvorbě této práce. Dále mému okolí za podporu při studiu.

Obsah

1 Úvod

V posledních letech se do povědomí veřejnosti dostalo Obecné nařízení o ochraně osobních údajů známé pod anglickou zkratkou GDPR. Snahou je zavést a zvýšit ochranu osobních údajů ve státech Evropské unie. Jde o zásadní nařízení, které může změnit fungování mnoha institucí. Součástí této normy je mimo jiné faktické posílení kybernetické bezpečnosti. Tato práce zkoumá a porovnává vliv tohoto nařízení s jinými již běžnými normami na fungování jedné ze základních institucí, obcí. Také se zabývá stavem kybernetické bezpečnosti v daných obcích.

2 Cíle a metodika

2.1 Cíle

Cílem práce je analyzovat informační a komunikační technologie ve vybraných obcích za využití standardů zejména ISO/IEC 27000. Práce se soustřední zejména na stav kybernetické bezpečnosti a dopady regulativy GDPR na systémy v obcích a příslušné procesy. Bude proveden dotazníkový výzkum těchto dopadů a na základě analýzy dotazníků a provedených analýz rizik budou navržena případná opatření.

Pro naplnění cíle práce byly zvoleny následující dílčí cíle:

- Vymezení základních pojmů souvisejících s řešeným tématem.
- Charakteristika jednotlivých standardů.
- Porovnání norem ze skupiny ISO 27000 a regulativy GDPR.
- Provést analýzu rizik vybrané obce a navrhnout případná řešení.
- Provést analýzu dotazníků a navrhnout případná řešení a doporučení.

Na základě materiálů, které byly prostudovány v této diplomové práci, budu vycházet z výzkumných otázek a hypotéz.

1. H0: Neexistuje závislost mezi finanční náročností implementace GDPR a typem obce (obec, obec s pověřeným obecním úřadem, obec s rozšířenou působností)
2. H0: Neexistuje závislost mezi časovou náročností implementace GDPR a typem obce (obec, obec s pověřeným obecním úřadem, obec s rozšířenou působností)
3. H0: Neexistuje závislost mezi tím, zda má obec dokument bezpečnostní politiky a tím, zda provádí analýzu rizik.
4. H0: Neexistuje závislost mezi tím, zda má obec informační systém a tím, jak časově náročná byla implementace GDPR do procesů obce.
5. H0: Neexistuje závislost mezi tím, zda je obec certifikována pomocí norem z rodiny ISO 27001 a časovou náročností implementace GDPR do procesů obce.

2.2 Metodika

Nejprve proběhne studium odborné literatury a literární rešerše dané problematiky. Budou představeny jednotlivé normy a standardy. Poté bude ukázán na příkladu vybrané obce jednoduchý návod, jak rychle provést analýzu rizik v malé obci. Následně bude proveden dotazníkový výzkum mezi obcemi. Na základě vyhodnocení dotazníků budou navržena případná opatření. Hypotézy budou vyhodnoceny za pomoci statistického softwaru.

3 Informační systém

Informační systém je poměrně široký pojem Z legislativního pohledu lze nalézt hned několik náhledů. Například v zákoně 365/2000 o informačních systémech veřejné správy a o změně některých dalších zákonů je psáno následující:

„Informačním systémem veřejné správy funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy. Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností.“ (Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů, 2000) (Mates & Smejkal, 2012)

Informační systém ve veřejné správě spadá pod oblast, která se nazývá E-government. Volně lze toto přeložit jako elektronická vláda. Evropská komisi pod tímto pojmem uvádí v eGovernment akčním plánu jako nástroj, který posiluje podniky, zlepšuje efektivitu, a za použití informačních a komunikačních technologií poskytuje lepší služby občanům a podnikům. (“European eGovernment Action Plan 2011-2015”, 2011) (Mates & Smejkal, 2012)

4 ISO/IEC 27000, 27001 a 27002 pro řízení informačních rizik

4.1 Úvod

Informace a informační systémy jsou důležitou součástí moderních firem. Zejména více a více vnitřních a vnitropodnikových datových přenosů a zvyšující se využívání otevřených sítí však zvyšuje riziko kompromitace přenášené informace. Pro snížení rizik a předejití škodám, musí společnosti zavést adekvátní opatření v podobě zavedení bezpečnosti informací. Pro ochranu informací a informačních systémů nabízejí standardy ISO 27000, ISO 27001, ISO 27002 příručky, návody, požadavky a cíle, při jejichž splnění dosáhnou společnosti adekvátní úrovně zabezpečení. ISO 27001 umožnuje společnosti, aby byla certifikována podle normy, čímž doloží, že bezpečnost informací je důsledně uplatňována, a to podle mezinárodně uznávaného bezpečnostní standardu. (Mates & Smejkal, 2012)

Certifikací podle ISO 27001 společnost ověřuje plnění známých a uznávaných bezpečnostních standardů a zvyšuje tak důvěru zákazníků. Stejně tak ověření souladu s mezinárodním standardem snižuje riziko pokut nebo kompenzačních plateb v důsledku soudních sporů. (Disterer, 2013)

4.2 Mezinárodní standardy

Normy vznikají vývojem podrobných popisů konkrétních charakteristik produktu nebo služeb psané odborníky a vědeckými institucemi z celého světa. Reprezentují shodu na charakteristikách jako je kvalita, bezpečnost, spolehlivost. Tyto charakteristiky by měli být udržitelné po dlouhé časové období a následně zdokumentovány a zveřejněny. Cílem vývoje norem je podporovat jednotlivce i společnosti při nákupu produktů a služeb. Poskytovatelé produktů a služeb mohou zlepšit svou pověst certifikováním v souladu s normami. ISO je organizace založená v roce 1946 a uznávaná ve 159 zemích světa. Také je předním orgánem pro vydávání mezinárodních standardů. Standardy ISO 27000 až ISO 270002 byly vytvořeny ve spolupráci s Mezinárodní elektrotechnickou komisí (IEC), která je hlavním vydavatelem mezinárodních standardů v oblasti elektrotechniky. (“International Electrotechnical Commission”, 2019), (Disterer, 2013)

4.3 Vývoj

Vznik standardů ISO 27000 až ISO 270002 lze vysledovat až do roku 1993 kdy britská asociace National Computing Centre (NCC) publikovala dokument *"PD 0003 A Code of Practice for Information Security Management"*. Britský standardizační orgán British Standards Institute (BSI) tento dokument přejal a zveřejnil jej jako národní standard *"BS 7799-1 IT—Security techniques—Code of practice for information security management"* v roce 1995. (Disterer, 2013)

Doplňující část *"BS 7799-2 Information security management systems—Specification with guidance for use"* umožnila společnostem certifikovat jejich procesy. ISO sladilo tento standard s ostatními jako ISO 9001 a vytvořilo ISO 27001 v roce 2005. Od této doby lze provádět certifikaci podle tohoto standardu.

ISO 27001 dal vzniknout celé skupině ISO 27 K, která zahrnuje různé standardy pro zabezpečení informací. V roce 2007 staré ISO 17799 bylo přiřazeno do skupiny ISO 27 K jako ISO 27002. V roce 2009 bylo vydáno ISO 27000 s cílem poskytnout přehled, úvod a vysvětlení terminologie s názvem *"IT—Security techniques—Information security management systems—Overview and Vocabulary"* (Disterer, 2013)

4.4 ISO 27000

V roce 2009 byla vydána norma ISO 27000 jako přehled řady norem ISO 27 K a společný koncepční základ. Bylo definováno 46 základních pojmů. Význam informační bezpečnosti a systematického zapojení do bezpečnostních aspektů je odvozen z rizika pro společnosti, jejichž obchodní procesy jsou stále více závislé na zpracování informací a jejichž složité a vzájemně propojené IT infrastruktury jsou náchylné k selhání a narušení. Stejně jako u jiných IT standardů se k normám skupiny ISO 27 K přidal cyklus „Plan-Do-Check-Act" (PDCA), který zdůrazňuje nutnost procesní orientace a integrace plánování operací a neustálé kontroly implementace v souladu s plánováním. (Disterer, 2013) (ISO/IEC 27000:2018: Information technology — Security techniques — Information security management systems, 2018)

Ve fázi plánování systému řízeného bezpečností informací[1] (Information Security Management Systém – ISMS) jsou definovány systémy, identifikována a vyhodnocena rizika a vhodné postupy a opatření ke snižování rizik. Zprávy generované průběžným

monitorováním operací jsou použity k odvození vylepšení a pro další zlepšení ISMS. (Disterer, 2013) (ISO/IEC 27000:2018: Information technology — Security techniques — Information security management systems, 2018)

4.5 ISO 27001

Standard ISO 270001 byl publikován v roce 2005 pod názvem „Information technology—Security techniques—Information security management systems—Requirements". Na 42 stranách popisuje požadavky které musí splňovat ISMS pro získání certifikátu. Jako rámec je norma zaměřena na společnosti ze všech odvětví a všech velikostí. O vhodnosti pro malé a střední podniky však existují pochybnosti. Konkrétní opatření pro splnění požadavků nejsou standardem stanovena, ale musí být vyvinuta a implementována na základě konkrétní společnosti. Certifikační požadavky ISO 27001 jsou objasněny vypracováním termínů a konceptů a doplněny prováděcí směrnicí v rámci ISO 27002. Těžištěm ISO 27001 je požadavek na plánování, implementaci, provoz a nepřetržité monitorování a zlepšování procesně orientovaného ISMS. Tento přístup by měl být v souladu s cyklem PDCA[2]. Pro plánování a implementaci by mělo být definováno pokrytí a zaměření ISMS. Měla by být stanovena a posouzena rizika a pro informační systémy by měly být stanoveny kontrolní cíle. Z těchto zkoumání by měla být odvozena vhodná opatření pro ochranu procesů. V příloze standardu je uvedeno a výslovně stanoveno celkem 39 kontrolních cílů a 134 opatření pro řízení bezpečnosti. Kontrolní cíle jsou dále rozděleny a popsány v normě ISO 27002. Při implementaci by mělo být provedeno školení pro získání podpory zavedení normy a její nezbytnosti. Dodržování postupů musí být neustále sledováno. Opatření by měla být kontrolována a zlepšována v a bezpečnostní rizika by měla být identifikována a posouzena, aby se neustále zvyšovala účinnost a efektivita ISMS. Požadavky, které mají být aplikovány na dokumentaci ISMS, jsou ve standardu popsány ustanovením základního obsahu, nezbytných dokumentů a specifikací a monitorovacích struktur pro správu dokumentů. Například změny procesů, verzování nebo pravidla pro přístupová práva. Jsou zde

[2] Demingův cyklus neboli též PDCA cyklus je metoda postupného zlepšování například kvality výrobků, služeb, procesů, aplikací, dat, probíhající formou opakovaného provádění čtyř činností. ("Demingův cyklus", 2016). Více také v kapitole Analýza rizik – úvod.

uvedeny povinnosti vrcholového managementu ve všech fázích cyklu PDCA. Zahrnují určování a provádění bezpečnostní politiky, definování rolí a odpovědností, nábor a přípravu potřebných personálních a materiálních zdrojů, jakož i rozhodnutí o řízení rizik. Zlepšení a další rozvoj ISMS musí být prováděn nepřetržitě, a to na základě bezpečnostní politiky, protokolování a vyhodnocování operací, výsledků testování a výsledků opatření pro zlepšení. Kromě toho by zlepšení a další rozvoj měly být prosazovány prostřednictvím pravidelných interních auditů. Vhodná implementace bezpečnostní politiky, její vhodnost a úplnost musí být zajištěna každoročními kontrolami řízení. (Disterer, 2013) (ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems, 2013)

4.6 Rozšíření ISO 27001

V roce 2010 bylo světově platných 15 625 certifikátů, z toho bylo 529 v České republice. Počet společností však nelze přesně určit, jelikož některé mohou držet více certifikátů. Aktuálně, dle zjištění výzkumu ISO 2018 bylo ke konci roku 2018 celosvětově platných 31 910 Certifikátů, z toho 543 v České republice. (Charlet, 2019), (“THE ISO SURVEY”, 2019)

4.7 Certifikační proces

Pro ověření souladu ISMS s ISO 27001 musí společnost absolvovat certifikační postup řízený autorizovanou certifikační organizací Registered Certification Bodies RCB (registrovaná certifikační autorita). Organizace ISO udržuje jejich seznam. Společnost zahajuje postup výběrem certifikační autority. V rámci předběžného zkoumání s podporou RCS lze určit, do jaké míry již existuje shoda s normou a co je třeba ještě vykonat pro úspěšnou certifikaci. V přípravném projektu by odpovídajícím způsobem měla být prováděna opatření nezbytná pro shodu s ISMS K tomu jsou nezbytné mít odpovídající znalosti a zkušenosti s certifikačními postupy, jakož i zvláštní odborné znalosti v oblasti bezpečnosti informací, a pokud je to třeba, měly by být získány najmutím externích odborníků. V první instanci zahrnuje zkoumání certifikaci (audit) všech dokumentů (bezpečnostní politiky, popisů procesů atd.) Tyto dokumenty se zasílají certifikační autoritě k posouzení. Kontrola dokumentace slouží jako příprava na hlavní audit, kde zástupci certifikační organizace provádějí během inspekce na místě podrobnou kontrolu, která trvá několik dní. To bude zahrnovat rozhovory se všemi odpovědnými osobami, které musí vysvětlovat své chápání bezpečnostní politiky, popisovat procesy,

prezentovat podrobnosti a funkcionality, vysvětlovat procesní dokumentaci a diskutovat o známých slabých místech a zahájených opatřeních ke jejich zlepšení. Certifikační organizace poté vytvoří zprávu, ve které budou vysvětleny výsledky auditu a nezbytná opatření ke zlepšení, které je třeba provést před dalším auditem. V případě pozitivního celkového výsledku společnost obdrží oficiální certifikát osvědčující shodu ISMS s požadavky ISO 27001. (Disterer, 2013) (Certification, 2013)

Implementace vhodné ISMS může trvat několik měsíců až několik let, záleží do velké míry na stavu zabezpečení IT bezpečnosti v organizaci. Čas a náklady na implementaci budou nižší, pokud jsou ve společnosti zavedeny procesy podle ISO 20000. Certifikát má platnost 3 roky. Obecně lze říci, že následná recertifikace vyžaduje mnohem menší úsilí než původní certifikace. Průběžné dodržování požadavků normy ISO 27001 a neustálé zlepšování ISMS je zajištěno prostřednictvím každoročních monitorovacích auditů. Tyto audity provádějí auditoři z RCB, přičemž první monitorovací audit musí proběhnout před uplynutím 12 měsíců od vydání certifikátu. Pokud by během monitorovacího auditu byly zjištěny závažné odchylky od požadavků normy, může RCB pozastavit nebo dokonce zrušit certifikát, dokud nebudou odchylky opraveny. (Disterer, 2013) (Certification, 2013)

4.8 ISO 27002

Kodifikované požadavky v ISO 27001 jsou rozšířeny a vysvětleny v ISO 27002 ve formě příručky. Příručka byla poprvé vydána v roce 2000 - tehdy pod názvem ISO 17799 pod názvem *"Information technology—Security techniques—Code of practice for information security management"*. V roce 2007 došlo k revizi a sladění s normami skupiny 27 K a označení bylo změněno na ISO 27002. S vývojem ISO 27002 byly běžné postupy, které se osvědčily v praxi standardizovány tak, že je lze snadno přizpůsobit specifickým požadavkům společností. Aby se vysvětlil význam informační bezpečnosti pro společnosti, jsou stanovena rizika pro informační bezpečnost společnosti a nutnost cílených a dohodnutých opatření v rámci ISMS. Jsou popsány nezbytné kroky pro identifikaci a vyhodnocení bezpečnostních rizik, aby se zajistil požadavek na ochranu informačních systémů. Pokračující vývoj ISO 27002, který je založen na normě ISO 27001, kde je podrobněji vysvětleno 39 cílů kontroly uvedených v příloze ISO 27001. Těmto cílům je přiděleno celkem 134 opatření, která jsou odůvodněna a podrobně popsána. Základní pokyny pro zajištění informační bezpečnosti musí být definovány a specifikovány ve formě bezpečnostní politiky vedením společnosti. Distribuce

a prosazování těchto zásad v rámci společnosti také slouží k zdůraznění důležitosti informační bezpečnosti a pozornosti managementu věnované těmto tématům. Informační bezpečnost musí být zakotvena ve společnosti, aby ji bylo možné účinně prosazovat a zavádět opatření. Je tedy třeba stanovit role a odpovědnosti a je třeba upřesnit zejména povinnosti při zachování důvěryhodnosti a stanovit pravidla pro komunikaci s externími stranami jako například zákazníkem, dodavateli, orgány atd. Veškerý hmotný a nehmotný majetek, který má být chráněn opatřeními pro informační bezpečnost musí být identifikován za účelem stanovení konkrétních odpovědností a pravidel manipulace. Bezpečnostní rizika jsou také způsobena zranitelností IT systémů. Zde je třeba předpokládat, že více než polovina všech útoků je iniciována interními zaměstnanci. Nicméně velká část bude také iniciována společnými akcemi interních pracovníků a externích lidí. Protože interní pracovníci mohou k útokům použít důvěrné znalosti o vnitřních procesech, zvycích, slabostech, sociálních vztazích atd., měli by být považováni za vyšší riziko než externí útočníci. S personálními opatřeními, jako je nábor, propouštění a přidělování úkolů, musí být zohledněna odpovídající rizika. Například přístupová práva uživatele musí být omezena na rozsah nezbytný k provedení práce, ke které je uživatel přihlášen. Se změnami odpovědností, povinností nebo pracovních míst by měla být přístupová práva odpovídajícím způsobem upravena a pokud jsou zaměstnanci propuštěni, měla by být přístupová práva okamžitě zrušena. Měla by být přijata opatření fyzické bezpečnosti, aby se chránila infrastruktura před neoprávněným vstupem, přístupem, krádeží, poškozením a zničením. Pro zajištění správného fungování ICT systémů by měly být ideálně rutinní operace zdokumentovány v manuálu jako standardní provozní postupy, aby se daly použít v případě nouze. Podobně by měly být stanoveny a zdokumentovány postupy pro výjimečné okolnosti, zpoždění, výpadky, poruchy nebo katastrofické události. Technické nebo organizační změny by měly být zkontrolovány z hlediska možného dopadu na provoz IT systémů před jejich zavedením. Podobně by měly být zdokumentovány bezpečnostní incidenty, analyzovány a vyhodnoceny z hlediska možného nebo podstatného zlepšení bezpečnostního systému. A také musí být zavedena vhodná opatření, aby byly splněny požadavky na soulad s normou. Standardem jsou citována zejména autorská práva a práva na užívání. Požadavky na zabezpečení a ochranu dat musí být regulovány a zajištěny ověřitelným způsobem. (Disterer, 2013) (ISO/IEC 27002:2013: Information technology — Security techniques — Code of practice for information security controls, 2013)

4.9 Další standardy skupiny ISO 27 K

Standardy skupiny ISO 27 K, či jinak ISO řady 27000 jsou publikovány pod názvem “Information technology—Security techniques” a podrobně a podrobně popisují požadavky na systém řízení informační bezpečnosti (ISMS) a na certifikaci jako takovou. Rodina standardů představuje sbírku nových i již dobře známých standardů, které byly přepracovány a revidovány tak, aby byly aktuální a také aby se sladil jejich obsah a formát. S touto skupinou ISO sleduje cíl mít soudržné standardy v oblasti informační bezpečnosti a zajistit tak kompatibilitu s ostatními standardy. Tím dosahuje cíle nabídnout komplexní podporu společnostem všech velikostí, odvětví a typů při zajišťování informační bezpečnosti. Publikování standardů řady 27 K není v tomto okamžiku dokončeno nebo uzavřeno – mnoho standardů je ve fázi vývoje, budou následovat další doplnění. ISO 27001 obsahuje požadavky, které musí být ověřeny pro certifikaci podle této normy. ISO 27006 obsahuje požadavky, které musí být splněny, aby byly organizace akreditovány jako certifikační autority. Všechny další standardy lze považovat za směrnice pro různé domény v oblasti zajištění informační bezpečnosti. (Disterer, 2013) (An Introduction to ISO 27001, ISO 27002....ISO 27008, 2019)

4.10 Shrnutí významu ISO norem

Informační a informační systémy jsou stále více vystaveny rizikům díky rostoucí podpoře podnikových procesů poskytovaných informačními technologiemi a zvýšené úrovni vytváření komunikačních sítí v rámci společností a spolupráce s externími stranami. Efektivní ISMS pomáhá snižovat rizika a předcházet narušení bezpečnosti. Normy ISO 27000, 27001 a 27002 tvoří rámec pro návrh a provoz ISMS, jsou založené na dlouhodobých zkušenostech. (Disterer, 2013)

S těmito normami se společnostem nabízí možnost sladit jejich IT postupy a metody pro zajištění odpovídající úrovně bezpečnosti informací s mezinárodním standardem. Certifikace ISMS podle ISO 27001 má také vliv pozitivní image společnosti, a to prostřednictvím ověření systematického řízení informační bezpečnosti. Tato norma je také v právních rozhodnutích vyžadována jako měřítko a základ pro posouzení předmětu informační bezpečnosti – zde certifikát podle ISO 27001 prokazuje „poskytování nejmodernějších služeb“ v oblasti informační bezpečnosti. Organizace mohou prokázat, že jsou schopny poskytovat služby IT bezpečným způsobem. Pomocí certifikátu lze provést ověření shody se standardem s ohledem na bezpečnost informací.

Normy ISO 27000, 27001 a 27002 se v Evropě a Asii široce rozšířily. Význam certifikace prokazující jistou úroveň informační bezpečnosti stále roste, a tak lze očekávat zvyšující se počet vydaných certifikátů. (Disterer, 2013) (ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems, 2013)

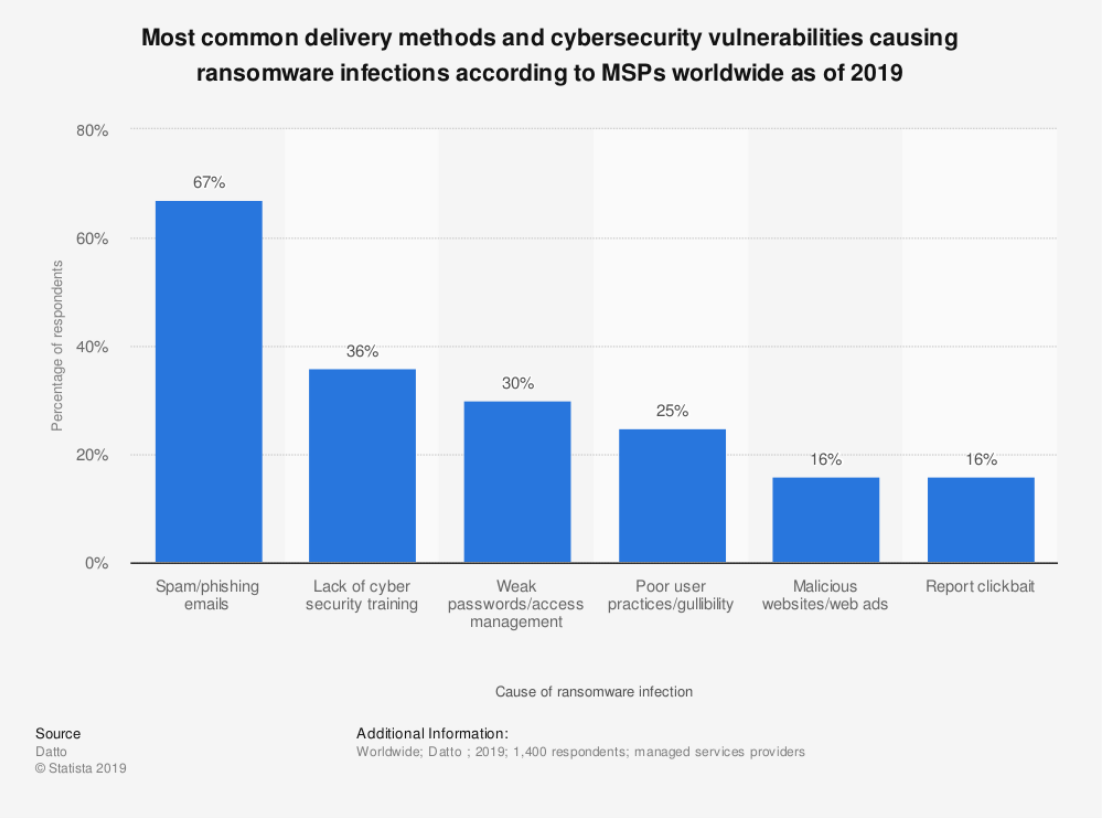
4.11 Normy jako prostředek pro zlepšení bezpečnosti

Zavedení bezpečnostních norem z rodiny ISO 27001 a GDPR může pomoci zvýšit celkovou kybernetickou bezpečnost. V poslední době se množí hackerské útoky na státní organizace, a to zejména ve formě ransomware[3]. Tento typ útoku může kompletně ochromit fungování celé infrastruktury a ohrozit tak základní služby. Navíc jeho řešení je z podstaty velmi obtížné a může trvat i několik týdnů. Bylo vydáno varování Národním úřadem pro kybernetickou a informační bezpečnost. (Hrozba kybernetických útoků na nemocnice a jiné významné cíle ČR, 2020) Z aktuálních útoků lze vybrat ten na nemocnici v Benešově, kde bylo pravděpodobně počátečním bodem stažení nebezpečného souboru běžným zaměstnancem. (Ukliknutí ‚stálo' nemocnici v Benešově 40 milionů. Kyberútok začal otevřením přílohy., 2020)

Jak je vidět na grafu nejběžnějších způsobů narušení bezpečnosti (Datto, 2019) v drtivé většině lze těmto narušením předejít, a to dodržováním či zavedením vhodných norem.

[3] „Jde o specifický druh škodlivého kódu, který se používá pro vydírání uživatelů. Po úspěšném infikování zařízení blokuje přístup k zařízení nebo šifruje definovaná data na disku. Na obrazovce se zobrazí výzva k zaplacení „výpalného", v některých případech i s informací, kolik času uživateli na zaplacení zbývá. Po uplynutí doby se požadovaná částka navýší." (Co je ransomware?, 2020)

Graf 1 Nejběžnějších způsoby narušení kybernetické bezpečnosti



Zdroj: Datto, 2019

5 ISMS

5.1 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací (Information Security Management System – ISMS) je dokumentovaný systém, ve kterém jsou chráněna definovaná informační aktiva, jsou řízena rizika bezpečnosti informací a zavedená opatření jsou kontrolována. (“Co je ISMS”, 2019)

Organizace shromažďují, ukládají a zpracovávají velké množství informací, aby dosáhly svých cílů. Některé společnosti shromažďují více informací, než je nezbytné k provozování jejich obchodních procesů. Informace jsou shromažďovány, ukládány, zpřístupňovány a zpracovávány zaměstnanci. Shromážděné informace jsou cenné nejen pro organizaci, ale také pro konkurenty. V některých případech mohou být informace zajímavé i pro širší veřejnost. Data obsahují důvěrné informace, jejichž únik může poškodit nejen organizaci, ale i partnery, uživatele a zákazníky. (Dombora, 2019) (Novák & Požár, 2014)

Informace zpracované organizacemi mohou být seskupeny podle různých kategorií. Podniky se zabývají informacemi o produktech, produkci, personálu, zákaznících, partnerech, pravidlech a předpisech, pracovních postupech, designu a vývoji, výzkumu, řízení kvality, organizační struktuře, obchodních zprávách atd. V závislosti na povaze informací, právní prostředí může vyžadovat rozvoj bezpečnostních politik a předpisů, jakož i provádění bezpečnostních opatření. Například osobní data jsou chráněna zákonem kdekoli na světě. Nejprve je však třeba upřesnit význam osobních údajů. Termín je definován právem platným v každé zeměpisné oblasti. Například v Evropské unii je význam osobních údajů definován Obecným nařízením o ochraně osobních údajů (GDPR), které mohou být doplněny místními zákony členských států EU. (Dombora, 2019)

V závislosti na povaze informací, které organizace shromažďují, ukládají a zpracovávají, by měly být chráněny v souladu s obchodními potřebami a právním prostředím. Potřeby organizace týkající se ochrany údajů řídí několik faktorů. Nejdůležitější z nich jsou následující: (Dombora, 2019) (Novák & Požár, 2014)

- podpora výroby s pomocí autentických informací,
- zajištění integrity informací pro zvýšení produktivity a kvality,

- vyhýbání se pokutám způsobeným porušením zákona zajištění ochrany citlivých informací,
- zprávy o řízení založené na autentických údajích
- využití certifikace ISO / IEC 27001 jako tržní výhody

5.2 Nejčastější problémy ISMS a jejich příčiny

Pokud jde o použití ISMS, lze učinit různá pozorování. V některých případech je ISMS vyvíjen v souladu s platnými normami a zákony a plní svou funkci ochrany informací. Existují případy, kdy je ISMS částečně funkční, a případy, kdy to nemá pro organizaci žádný význam nebo obsahuje i irelevantní údaje.

Analýzou problémů souvisejících se strukturou, obsahem, čitelností, použitelností a dodržováním místní a mezinárodní legislativy a dopadem předpisů na organizace lze pozorovat následující typy nedostatků: (Dombora, 2019) (Novák & Požár, 2014)

5.2.1 Problémy týkající se struktury ISMS

- Téměř všechna bezpečnostní pravidla jsou začleněna do jednoho velkého nařízení
- Všichni zaměstnanci musí znát a dodržovat všechna bezpečnostní pravidla a předpisy
- Nařízení o bezpečnosti informací obsahuje několik pravidel, která nejsou relevantní pro všechny zaměstnance.
- Neexistuje žádné rozdělení ISMS s ohledem k rolím
- Není jasné, která pravidla platí pro jednotlivé zaměstnance.

5.2.2 Problémy týkající se čitelnosti ISMS

- Čtení Nařízení o bezpečnosti informací zabere hodně času, a i když si jej zaměstnanci přečtou, nepamatují si jeho obsah
- Používá zkratky a odbornou terminologii, díky čemuž je pro mnoho zaměstnanců je nepochopitelná

5.2.3 Problémy týkající se použitelnosti ISMS

- ISMS je matoucí a má předpisy které se překrývají, nikdo neví, které pravidlo by mělo být použito
- ISMS obsahuje protichůdná pravidla
- Pokud zaměstnanci dodržují pravidla ISMS, nemohou plnit své každodenní úkoly, což zastavuje provoz.

- Podmínky (environmentální, technické, ekonomické atd.) provádění ISMS nejsou vhodné.
- Zásady a předpisy neodpovídají operačnímu prostředí

5.2.4 Problémy týkající se dodržování předpisů

- Zásady a předpisy nedodržují právní prostředí.
- ISMS je upravená verze příslušných zákonů nebo standardů, ale zůstává teoretická, není integrována do pracovních postupů organizace, uvádí, ale neposkytuje požadovanou ochranu.

Protože dnes téměř všechny organizace nějak závisí na dostupnosti informací, důvěrnosti a integritě, ochrana informací je proto základním požadavkem. Nezavedení funkčního ISMS představuje pro organizace vysoké riziko. (Novák & Požár, 2014)

Analýza problémů ukazuje, že implementace špatně navrženého ISMS může, kromě nedostatečné ochrany informací, způsobit bezpečnostní rizika a bránit fungování organizace. Organizace by dále měly zvážit všechny faktory související s bezpečností informací, které ovlivňují provoz a prosperitu a projevit zájem o následující: (Dombora, 2019)

- Zájem o správu důvěrných informací, poskytování přesných informací partnerům, zákazníkům a zaměstnancům za účelem zlepšení organizačních procesů
- Dodržování právního prostředí, které vynucuje nejen dodržování předpisů na regulační úrovni, ale také provádění technických ochranných opatření

Soulad s GDPR nelze zajistit bez provozních ISMS a technických bezpečnostních opatření.

5.2.5 Implementace informační bezpečnosti založené na standardech

Certifikace ISO 27001 byla dříve tržní výhodou, ale nyní se stala spíše běžným požadavkem.

Při analýze problémů ISMS lze identifikovat následující kategorie: nedostatečná struktura, nedostatečný obsah, čitelnost, použitelnost nebo nesoulad. Porovnáním nefunkčního ISMS s těmi funkčními lze pozorovat některé vlastnosti, které pomáhají zlepšovat kvalitu a použitelnost. Následující skupiny ukazují tyto vlastnosti. (Dombora, 2019) (Rohel, 2013) (Asosheh et al., 2013)

Soulad s platnými právními předpisy a normami: tato skupina parametrů pomáhá sladit právní požadavky a kontrolní systém standardů s ISMS. V této kategorii lze identifikovat následující charakteristiky: vytváření křížových odkazů na právní zákony, předpisy a kontroly norem a sledování jejich změn. Křížové odkazy jsou nezbytné u zákonů, kde pomáhají auditovat a ověřovat shodu a platnost. Bez těchto odkazů je obtížné identifikovat nebo přizpůsobit prvky politik nezbytné ke splnění požadavků vnějších předpisů, kde mohou způsobit neplnění požadavků zákonů. Sledování změn externích regulačních požadavků vytváří podněty pro aktualizaci příslušných dokumentů ISMS s odkazem na daný zákon a aktuální verzi. Obvykle se jedná o proces, který upozorní zúčastněné strany, pokud se příslušné zákony, standardy regulací změní, což znamená aktualizaci politik za účelem zachování shody. (Dombora, 2019) (Rohel, 2013) (Asosheh et al., 2013)

Aktuální a konzistentní: tyto charakteristiky pomáhají udržovat ISMS v souladu s obchodními požadavky a eliminují překrývající se politiky. Byly vytvořeny jasné definice oblasti působnosti politiky, mapa dokumentace, křížové odkazy jsou stále aktuální a jednotné a došlo k vymezení pojmů a pravidel. Jasný rozsah a dosah regulace napomáhá udržovat konzistentní zásady ISMS. Mapa dokumentace definuje rozsah každé politiky a zajišťuje transparentnost ISMS. Jednotná definice bezpečnostních pravidel a požadavků je definována pouze na jednom místě a odkázána ze všech ostatních dokumentů Křížové odkazy mezi dokumenty pomáhají eliminovat překrývání a zároveň pomáhají najít související pravidla a definice. (Dombora, 2019) (Rohel, 2013) (Asosheh et al., 2013)

Pochopitelné a interpretovatelné: Díky těmto charakteristikám jsou zásady ISMS čitelné a jednoznačné. V této kategorii je jasně stanovena jasná, přesná a srozumitelná terminologie a jazyk. Jazyk politiky musí být přesný, jasný a jednoznačný. Bezpečnostní pravidla nesmí obsahovat žádnou nejistotu. Terminologie a jazyk ISMS by měly být srozumitelné cílové skupině, a to i když nejsou odborníky na informační bezpečnost. (Dombora, 2019) (Rohel, 2013) (Asosheh et al., 2013)

Úplné a kompletní: tyto vlastnosti ISMS umožňují ochranu informací, a to tak aby pokryly všechny relevantní hrozby, které se v organizaci vyskytují během provádění obchodních procesů. To znamená, že bezpečnostní pravidla a požadavky ISMS musí pokrývat všechny relevantní hrozby pro celou organizaci, všechna oddělení a všechny pracovní toky které provádějí zaměstnanci. Bezpečnostní pravidla a předpisy musí

pokrývat všechny pracovní toky organizace. (Dombora, 2019) (Rohel, 2013) (Asosheh et al., 2013)

Nezbytná a dostatečná pravidla: je to jedna z nejdůležitějších skupin vlastností, protože to hlavně ovlivňuje funkčnost a vynutitelnost ISMS. ISMS by měl poskytovat nezbytnou úroveň ochrany, což znamená, že by měl obsahovat ochranná opatření týkající se všech informačních aktiv zajišťujících potřebnou důvěrnost, úroveň integrity a dostupnosti. Toho lze dosáhnout kontrolou všech příslušných zákonů a norem a výběrem všech příslušných požadavků na organizaci, poté vývojem a zahrnutím odpovídajících pravidel a opatření ochrany do ISMS. Čím více pravidel je zabudováno do ISMS, tím je pravděpodobnější, že se překrývají, takže je třeba odstranit zbytečná a sloučit překrývající se pravidla. Zbytečná a protichůdná pravidla brání zaměstnancům v plnění jejich každodenních úkolů. Neměly by být zahrnuty žádné textové části zákonů nebo norem, měly by být místo toho odkazovány. Neměl by být uveden žádný popis metodik, měl by na ně být uveden odkaz, protože jsou pravidelně aktualizovány. (Dombora, 2019) (Rohel, 2013) (Asosheh et al., 2013)

Hierarchická struktura a struktura založená na rolích: struktura dokumentace ISMS by měla být popsána v mapové dokumentaci, aby poskytla přehled o celé regulační struktuře, což by mělo být více než vzájemné odkazy mezi dokumenty. Všechny politiky a předpisy v ISMS by měly být kategorizovány podle kategorií politiky, regulace, postupů a podpůrných dokumentů. To pomáhá oddělit různé prováděcí úrovně, existuje zde však vzájemná interakce: úroveň politiky řídí úroveň regulace, která řídí pracovní toky a vytváří podpůrné dokumenty. Různé úrovně mají svou roli. Každá úroveň politiky obsahuje strategii a zásady, podle nichž organizace rozvíjí informační bezpečnost. Úroveň regulace stanoví obecná bezpečnostní pravidla, která mají příslušná oddělení a zaměstnanci dodržovat. Úroveň regulace by měla být založena na rolích a předpisy by měly být dostupné příslušným útvarům a zaměstnancům podle jejich role v organizaci. Úroveň postupu by se měla skládat z pracovních toků pro implementaci a udržování informační bezpečnosti. Podpůrné dokumenty popisují nastavení, autorizační dokumenty, systémové parametry, výsledky testů, záznamy údržby, záznamy o incidentech, záznamy o problémech, záznamy o změnách, záznamy auditu, systémové parametry atd. Obvykle se jedná o výsledky nebo vstupy pracovních postupů na úrovni procedur. (Dombora, 2019) (Rohel, 2013) (Asosheh et al., 2013)

Vynutitelné a proveditelné: Aby bylo možné provozovat ISMS, je důležité vyškolit zaměstnance, vysvětlit strukturu a vztah politik, předpisů, procesů a podkladů. V souladu s nezbytnými a dostatečnými charakteristikami pravidel pomáhají tyto vlastnosti minimalizovat potřebné bezpečnostní znalosti pracovníků v různých pracovních pozicích. Obecná bezpečnostní pravidla pokrývají znalosti všech zaměstnanců a musí se na ně vztahovat zásady bezpečnosti informací. Pravidla specifická pro dané oddělení musí být pokryta terénními bezpečnostními politikami příslušných oddělení. Bezpečnostní pravidla týkající se činnosti musí být začleněna do pracovních postupů. Aby byl celkový systém pravidel ISMS použitelný, neměl by obsahovat žádná konfliktní pravidla a pravidla o blokování obchodních procesů. Zaměstnanec musí znát pouze ty zásady, předpisy a procesy, které jej ovlivňují. (Dombora, 2019) (Rohel, 2013) (Asosheh et al., 2013)

Vyvážená rizika a zdroje: organizace by měla zvážit informační a bezpečnostní rizika a přidělit na ně nezbytné zdroje. ISMS by měla zvážit rizika, možná ochranná opatření a jejich náklady, aby na ně přidělila potřebné zdroje, a to s ohledem na rizika a zdroje informační bezpečnosti, které má organizace k dispozici. To znamená, že ISMS nesmí obsahovat žádná bezpečnostní pravidla, která znamenají ochranná opatření, která si organizace nemůže dovolit financovat. (Dombora, 2019) (Rohel, 2013) (Asosheh et al., 2013)

Zavádění informační bezpečnosti založené na standardu ISO 27001 v malé a střední organizaci není jednoduché a vyžaduje návody a doporučení. Vzhledem k tomu, že je nutná shoda s externím regulačním prostředím, zdroje jsou omezené, náklady jsou ovlivněny bezpečnostními opatřeními, která mají být implementována, řešením může být ISMS založený na rizicích. Tyto pokyny a výše zmíněné parametry kvality jsou proto vhodnými nástroji pro vývoj optimalizovaného, vynutitelného a rizikově založeného ISMS. (Dombora, 2019) (Rohel, 2013) (Asosheh et al., 2013)

6 General Data Protection Regulation (GDPR)

6.1 Úvod do problematiky

Obecné nařízení o ochraně údajů (GDPR) je zákon v Evropské unii (EU), který vyžaduje, aby podniky, vlády a další instituce shromažďovaly online údaje o spotřebitelích pouze legálním a transparentním způsobem a poté je ukládaly bezpečně a eticky, aby nemohly být zneužity nebo ukradeny. Data jsou jakékoli osobní informace, které lidé předávají podnikům, bankám nebo jiným skupinám online. Zahrnuje plná jména, adresy, čísla kreditních karet a další informace. (Ruth, 2017)

Úniky dat, která mají za následek odcizení těchto informací, může jednotlivce výrazně poškodit tím, že odhalí jejich soukromí a finanční informace. GDPR vyžaduje, aby všechny organizace sbírající údaje v Evropské unii a všechny organizace mimo Evropskou unii, které obchodují s občany EU, dodržovaly nařízení na ochranu údajů. Skupiny, které nedodrží zákon tím, že nesprávně zacházejí s údaji o spotřebitelích nebo neohlašují datové úniky, mohou být pokutovány miliony eur nebo mohou být zdaněna procenta jejich ročních globálních příjmů. (Ruth, 2017)

Hlavní cíl GDPR na ochranu údajů o spotřebitelích je trnem v oku mnoha organizacím. Ve věku počítačů a digitalizovaných informací je ochrana údajů nezbytná k zajištění toho, aby totožnosti spotřebitelů, soukromí a finance zůstaly v bezpečí před neoprávněným prohlížením a krádeží. (Ruth, 2017)

Data jsou osobní informace, které organizace shromažďují od spotřebitelů a ukládají na počítačích. Informace jsou obvykle velmi citlivé pro jednotlivce a není zamýšleno, aby je viděl kdokoli jiný než samotní jednotlivci a společnosti, které údaje shromažďují a analyzují. Mnoho organizací shromažďuje osobní údaje spotřebitelů, včetně maloobchodních společností, bank, nemocnic a vlád. (Ruth, 2017)

Organizace mohou shromažďovat a ukládat jména zákazníků, adresy, telefonní čísla, e-mailové adresy, informace o bankovních účtech, čísla kreditních karet a lékařské záznamy. Mezi další informační organizace, které mohou shromažďovat od spotřebitelů, patří rasa, etnický původ, sexuální orientace, politická příslušnost a trestní minulost. (Ruth, 2017)

Od sběratelů dat po celém světě se obecně očekává, že budou při získávání, uchovávání a používání spotřebitelských údajů dodržovat určité právní a etické pokyny. Zákony

upravující použití údajů se liší podle země, ale etické zásady jsou téměř univerzální. Například se očekává, že sběr údajů bude přínosem jak pro sběratele, tak pro spotřebitele. Dodržováním tohoto pokynu se zajišťuje, že data po shromáždění slouží skutečnému účelu. Další etický princip týkající se sběru dat zahrnuje progresivitu nebo schopnost odvodit co nejvíce za využití co možná nejmenšího množství dat. (Ruth, 2017)

Další důležitý etický princip, který by měli sběratelé dat použít, je známý jako sluneční test. Na základě amerických zákonů známých jako sunshine laws[4] (sluneční zákony) - které vyžadují, aby byly některé vládní aktivity zpřístupněny veřejnosti. Sluneční test doporučuje všem podnikům sbírajícím údaje, aby zvážily potenciální dopady odhalení a úniku všech údajů o svých zákaznících na veřejnost. Pokud se vedoucí pracovníci společnosti domnívají, že by taková odhalení poškodila jejich zákazníky a podnikání, musí podniknout příslušné kroky k zabezpečení a ochraně shromážděných údajů o zákaznících. (Ruth, 2017)

6.2 Přehled a původní cíle

V lednu 2012 Evropská komise, která připravuje právní předpisy a obecně dohlíží na Evropskou unii, začala plánovat aktualizaci a vylepšení zákonů týkajících se ochrany údajů. Hlavním cílem komise bylo modernizovat evropské zákony o digitální ochraně v éře počítačů a dat. Evropská unie již přijala zákon o ochraně údajů v roce 1995 (Data Protection Directive), ale jeho ustanovení byla do roku 2012 již zastaralá a každý z různých členských států EU zavedl do svého právního řádu jinak. Evropská komise považovala aktualizaci zákona za nezbytnou k oživení důvěry spotřebitelů v evropské korporace a v konečném důsledku k urychlení hospodářského růstu. (European Commission, 2012)

[4] Právní předpisy ukládající vládním agenturám, aby prováděly své operace otevřeněji. Účelem těchto zákonů je usnadnit větší kontrolu vládního rozhodování médiím a široké veřejnosti. Sluneční zákony vycházejí z teorie, že role médií v podobě hlídacího psa je vážně narušena, když vládní rozhodovací orgány uzavírají své schůzky před veřejností. Schovávání těchto schůzek před veřejnou kontrolou by mohla být chápáno jako forma mediální cenzury. K řešení tohoto vnímaného problému přijalo mnoho místních vlád, všech padesát států USA a federální vláda takzvané „sluneční zákony“, protože vyžadují, aby byla práce orgánů státní správy vystavena veřejnému dohledu. Zákony týkající se slunečního svitu obvykle vyžadují, aby určité typy schůzek byly přístupné veřejnosti a aby se povědomí o těchto schůzích šířilo dobou s odpovídající předchozímu oznámení – musí být oznámeny dostatečně s předstihem. První takový zákon přijala Florida v roce 1975. (“Sunshine laws”, 2019)

Původní ambice zákona dle tiskové zprávy z roku 2012 (European Commission, 2012) byly:

- „Jednotný soubor pravidel o ochraně údajů platný v celé EU. Budou odstraněny zbytečné administrativní požadavky, jako jsou požadavky na oznámení pro společnosti. To ušetří podnikům přibližně 2,3 miliardy EUR ročně.
- Namísto současné povinnosti všech společností oznamovat veškeré činnosti v oblasti ochrany údajů orgánům dozoru nad ochranou údajů – požadavek, který vedl ke zbytečnému papírování a podniky stojí 130 milionů EUR ročně, stanoví nařízení zvýšenou odpovědnost pro ty, kdo zpracovávají osobní údaje.
- Například společnosti a organizace musí co nejdříve informovat vnitrostátní dozorový orgán o závažném porušení údajů (pokud je to možné do 24 hodin).
- Organizace budou muset jednat pouze s jediným vnitrostátním orgánem pro ochranu údajů v zemi EU, kde mají své hlavní sídlo. Stejně tak se mohou lidé obrátit na orgán pro ochranu údajů ve své zemi, a to i v případě, že jsou jejich údaje zpracovávány společností se sídlem mimo EU. Tam, kde je pro zpracování údajů vyžadován souhlas, je vyjasněno, že musí být poskytnut výslovně, než se pouze předpokládá.
- Lidé budou mít snadnější přístup k vlastním datům a budou moci snadněji přenášet osobní údaje od jednoho poskytovatele služeb k jinému (právo na přenositelnost dat). Tím se zlepší konkurence mezi službami.
- „Právo být zapomenut“ pomůže lidem lépe spravovat rizika ochrany údajů online: lidé budou moci vymazat svá data, pokud neexistují legitimní důvody pro jejich uchování.
- Pravidla EU se musí použít vždy, pokud se osobní údaje zpracovávají v zahraničí společností, která působí na trhu EU a nabízí své služby občanům EU.
- Budou posíleny nezávislé vnitrostátní orgány pro ochranu údajů, aby mohly lépe prosazovat pravidla EU. Budou mít pravomoc pokutovat společnosti, které porušují pravidla EU o ochraně údajů. To může vést k pokutám až do výše 1 milionu EUR nebo až do 2 % celosvětového ročního obratu společnosti
- Nová směrnice bude uplatňovat obecné zásady a pravidla ochrany údajů pro policejní a soudní spolupráci v trestních věcech. Tato pravidla se budou vztahovat na vnitrostátní i přeshraniční přenosy dat.“

Jednání o podrobnostech nového zákona o ochraně údajů trvalo čtyři roky. V letech 2012 a 2013 vyjádřilo několik stran Evropského parlamentu názory na to, co o čem přesně by měl být navrhovaný zákon. V březnu 2014 Evropský parlament, který hlasuje o navrhovaných právních předpisech EU, podpořil zákon o ochraně údajů, který by chránil počítačové informace pro spotřebitele a podpořil tak růst hospodářství Evropské unie. (Ruth, 2017)

Vláda EU definovala řadu principů navrhovaného zákona do června 2015. Různé další orgány doporučovaly změny znění zákona v průběhu několika dalších měsíců. Do prosince 2015 se parlament, komise a rada dohodly na finální verzi GDPR. Zákon byl schválen v dubnu 2016, a všechny organizace sbírající údaje napříč členskými státy Evropské unie musí od května 2018 implementovat toto ustanovení. (Žůrek, 2017)

GDPR je rozsáhlý zákon, který nařizuje odpovědné nakládání s údaji jakoukoli společností v Evropské unii nebo mimo Evropskou unii, která zpracovává údaje občanů EU. To znamená, že zákon ovlivňuje i významné korporace po celém světě. (Ruth, 2017) (Žůrek, 2017)

GDPR vyžaduje, aby tyto instituce chránily jména spotřebitelů, adresy, biometrická data (jako jsou tělesná měření – typickým příkladem je otisk prstu), rasu, politickou příslušnost, sexuální orientaci, finanční informace a webové údaje, jako jsou adresy internetového protokolu (IP adresy[5]). Podniky a další skupiny musí shromažďovat údaje o spotřebitelích legálně a poté prokázat, že je chrání před zneužitím a krádeží, a to jak v rámci samotných organizací, tak před možnými zloději externích dat. Organizace musí informovat své zákazníky o tom, jak jsou jejich data využívána, a musí včas oznámit všechna úniky dat a údajů. (Ruth, 2017) (Žůrek, 2017)

Vláda EU zamýšlela pomocí GDPR stimulovat hospodářský růst a technologické inovace. Důvodem je, že v ideálním případě by existoval pouze jediný orgán upravující

[5] „IP adresa je jednoznačná síťová adresa počítače v internetu. IP adresa je dlouhá 32 bitů, obvykle se zapisuje jako čtveřice desítkových čísel v rozsahu 0–255 oddělených tečkou (např. 192.17.255.4). IP-adresy slouží pouze k propojování sítí (odtud internet protocol – doslova mezisíťový protokol). Jsou to tedy pouze logické adresy, které slouží k účelům směrování. IP-adresa a síťová maska jednoznačně určují příslušnost počítače k podsíti. Počítače se IP-adresami fyzicky neadresují. Na fyzické úrovni se používají tzv. hardwarové adresy závislé na typu sítě.“ (“IP adresa”, 2005)

ochranu údajů a umožnil tak podnikům kdekoli v Evropské unii zabudovat do svých technologií bezpečnost dat již od začátku vývoje. Podle Evropské komise by taková jednotnost zákonů o ochraně údajů v celé Evropské unii ušetřila ekonomice EU miliardy eur ročně. Dle tiskové zprávy se jedná o 2,3 miliardy eur. (European Commission, 2012)

6.3 Sankce

Sankce za nedodržení ustanovení GDPR jsou většinou finanční a jsou přísné. GDPR umožňuje dozorovacím orgánům kontrolovat instituce, zda dodržují zákon. Tyto úřady mohou varovat organizace, u nichž se zjistí, že nedodržují předpisy, aby v určité době změnily svou bezpečnostní politik. Úřady mohou také společnosti auditovat nebo je donutit, aby osobní údaje úplně smazaly nebo přestaly používat. Organizace, které nedodrží zákon, mohou být pokutovány až do dvaceti milionů eur nebo 4 procent svých ročních globálních příjmů, podle toho, co je vyšší. Přesná výše pokut závisí na povaze trestného činu a na uvážení dozorovacích orgánů. (Ruth, 2017) (Žůrek, 2017)

V měsících před tím, než GDPR vstoupil v platnost, nezávislá britská analytická firma Ovum uvedla, že 52 procent společností na celém světě předpovídalo, že budou pokutovány za nedodržení zákona v prvním roce po jeho přijetí. Bylo požadováno, aby členské státy EU začlenily pravidla GDPR do svých vnitrostátních právních předpisů do 6. května 2018. Zákon vstoupil v platnost dne 25. května 2018. (Ruth, 2017)

6.4 Dohled a kontrola

The European Data Protection Supervisor (EDPS) je nezávislým orgánem Evropské unie pro ochranu údajů. Hlavním posláním je sledovat a zajišťovat ochranu osobních údajů a soukromí, při zpracovávání osobních údajů jednotlivců orgány a institucemi EU. Poskytuje poradenství orgánům a institucím EU ve všech záležitostech týkajících se zpracování osobních údajů, na žádost nebo z vlastní iniciativy. Evropská komise konzultuje ohledně návrhů právních předpisů, mezinárodních dohod, jakož i prováděcích a delegovaných aktů s dopadem na ochranu údajů a soukromí. Dále má za úkol sledovat nové technologie, které mohou mít vliv na ochranu osobních údajů. Vstupuje do řízení před Soudním dvorem EU, aby poskytoval odborné rady ohledně výkladu práva na ochranu údajů. Spolupracuje s vnitrostátními orgány dohledu a dalšími orgány dohledu s cílem zlepšit soudržnost v ochraně osobních údajů. (“EUROPEAN DATA PROTECTION SUPERVISOR: The EU's independent data protection authority”, 2019)

6.5 GDPR versus ISMS

General Data Protection Regulation – Evropské nařízení o obecné ochraně údajů vyžaduje, aby správci a zpracovatelé údajů prováděli účinná technická a organizační opatření na ochranu soukromí jednotlivců. Nedostatek podrobností v nařízení, pokud jde o přesná opatření a postupy technické ochrany, které je třeba použít k zabezpečení toků osobních údajů a jejich umístění (s výjimkou velmi jasně stanovených: šifrování, minimalizace, pseudoanonymizace), vyvolalo vlnu domněnek, co by mělo být náležitým ochranným opatřením nebo úplným souborem odpovídajících bezpečnostních kontrol k zajištění účinné ochrany údajů jednotlivců. (Ionescu, R. C., Grab, B., & Hassani, Y. 2019) (Žůrek, 2017).

Bez ohledu na množství bezpečnostních opatření uplatňovaných na ochranu osobních údajů a zmírnění rizik pro práva a svobody jednotlivců, může dojít k incidentům, v důsledku nedostatečné informovanosti o osvědčených postupech mezi zaměstnanci. Zranitelnostmi jsou obecně slabiny infrastruktury, systému, postupů nebo interních kontrol. Identifikace zranitelných míst se provádí posouzením informačních systémů za účelem stanovení přiměřenosti bezpečnostních opatření, zjištění nedostatků a potvrzení přiměřenosti takových opatření po jejich provedení. (Ionescu, R. C., Grab, B., & Hassani, Y. 2019) (Žůrek, 2017)

Ani správci a zpracovatelé nejsou nařízením o ochraně osobních údajů nuceni zavést systém řízení bezpečnosti informací. Možnou existenci takového systému řízení přitom mohou využít jako příležitost k rychlejšímu a lepšímu dodržování evropského práva. (Ionescu, R. C., Grab, B., & Hassani, Y. 2019) (Žůrek, 2017)

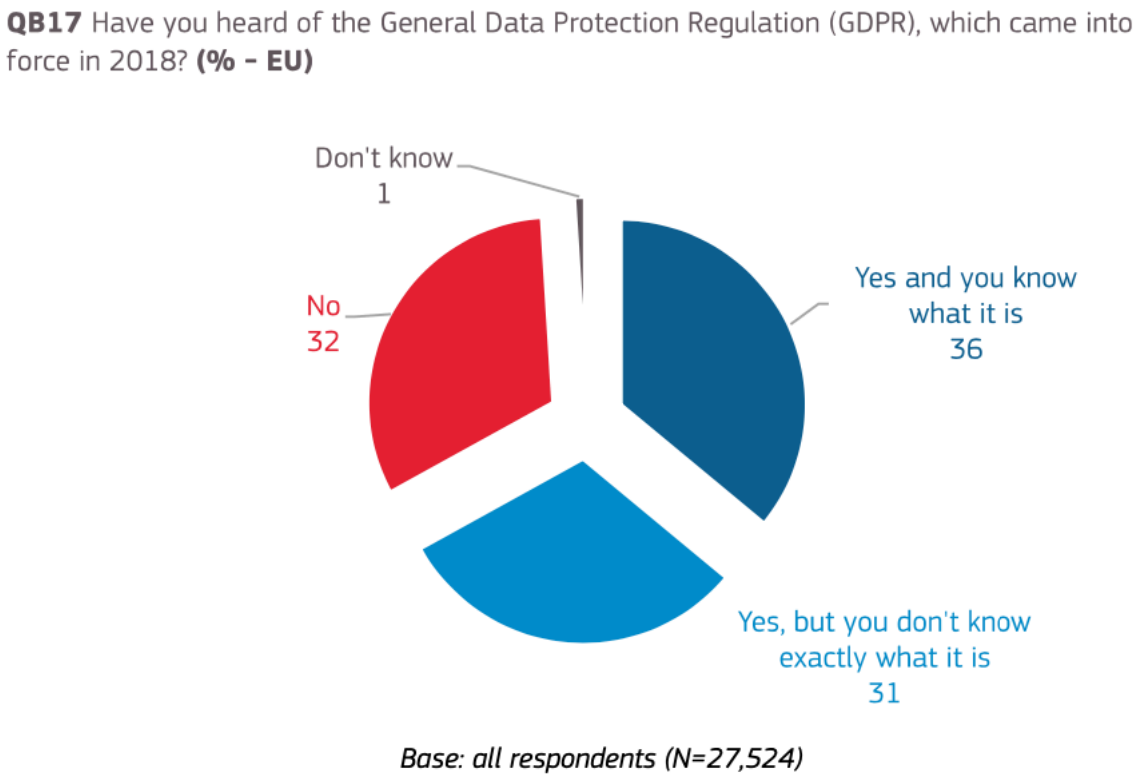
Úplný seznam bezpečnostních kontrol, které mají být zavedeny k zajištění souladu s Obecným nařízením o ochraně údajů, je obtížné specifikovat v jediném dokumentu, zejména proto, že kontroly a zpracovatelé se velmi liší, pokud jde o: objemy a kategorie zpracovaných údajů, velikost, rozpočet, technické a právní kompetence, úroveň regulačních požadavků, oblast průmyslu, zeměpisná oblast, kde působí. Systémy řízení bezpečnosti informací i obecné nařízení o ochraně údajů proto vyžadují po řešitelích, aby před zvážením vhodných ochranných opatření pro data provedli nejdříve analýzu rizik. Řešitel musí přijmout odpovídající ochranná opatření v závislosti na výsledcích této analýzy. (Ionescu, R. C., Grab, B., & Hassani, Y. 2019) (Žůrek, 2017)

Při zavádění Obecného nařízení o ochraně údajů existují v Evropské unii různé přístupy. Úroveň implementace závisí na konkrétním odvětví organizace, znalostech zaměstnanců a zdrojích poskytnutých managementem pro tyto implementace. Dalším rozdílem je právo každé země na vytvoření vlastních regionálních požadavků, při zavádění Obecného nařízení o ochraně údajů. (Ionescu, R. C., Grab, B., & Hassani, Y. 2019) (Žůrek, 2017).

6.6 Povědomí veřejnosti o GDPR

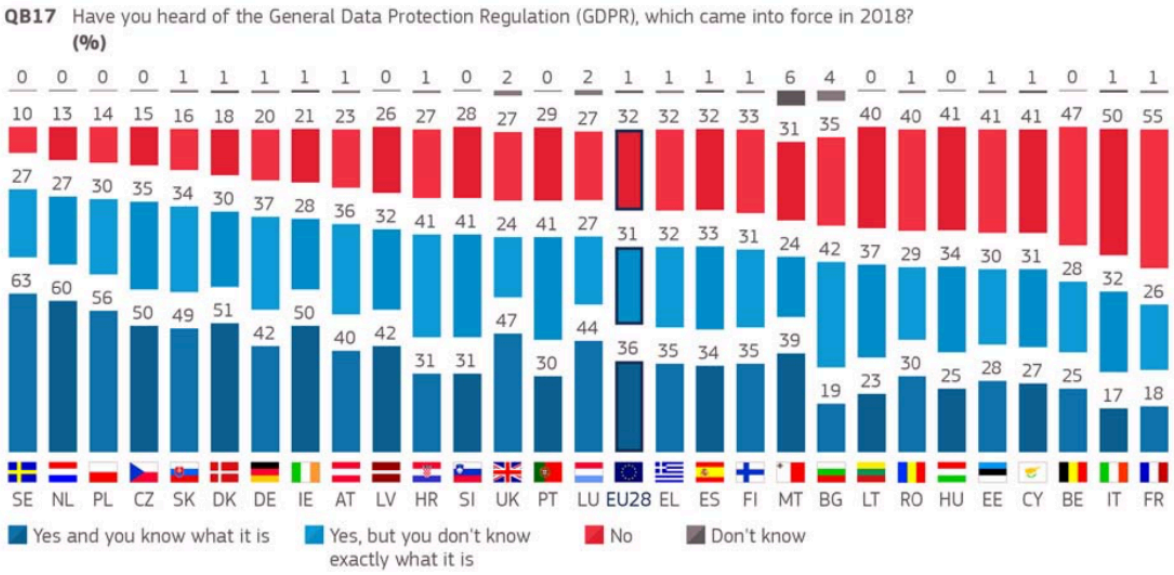
Podle výzkumu z března 2019 přes dvě třetiny občanů Evropské unie slyšeli o nařízení GDPR, z toho 36 % vědělo co jim toto nařízení přináší. (Special Eurobarometer 487 a – March 2019 "The General Data Protection Regulation" Report, 2019)

Graf 2 Povědomí o GDPR



Zdroj: Special Eurobarometer 487a – March 2019 "The General Data Protection Regulation" Report, 2019

Graf 3 Povědomí o GDPR v jednotlivých zemích EU

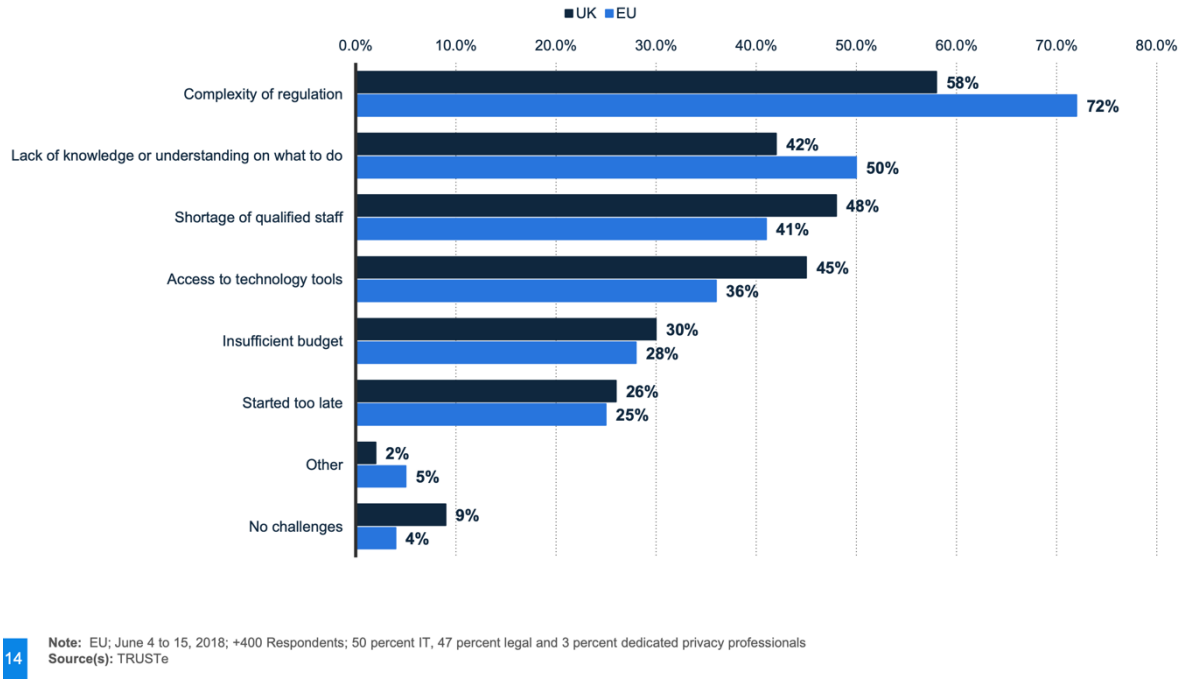


Zdroj: Special Eurobarometer 487a – March 2019 "The General Data Protection Regulation" Report, 2019

Česká republika se v rámci celé Evropské Unie umístila na čtvrtém místě v podvědomí o GDPR, kdy 50 % dotazovaných vědělo co jim toto nařízení přináší. Celkové povědomí je pak velmi dobrých 85 %.

Podle výzkumu provedeného v roce 2018 se pro organizace jeví jako hlavní problém složitost a komplexnost celé legislativy. (Coppola, 2019)

Graf 4 Hlavní problémy při zavádění GDPR



Zdroj: Coppola, 2019

6.7 GDPR versus ISO 27001

GDPR a ISO 27001 jsou dva významné standardy, které mají hodně společného. Cílem obou z nich je posílit bezpečnost údajů a zmírnit riziko jejich narušení a oba vyžadují, aby organizace zajistily důvěrnost, integritu a dostupnost citlivých dat. ISO 27001 je jedním z nejpodrobnějších standardů „best practice“ a ve skutečnosti článek 24 GDPR stanovuje, že dodržení kodexů chování a schválených certifikátů, jako je ISO 27001, lze použít jako prvek k prokazování shody s GDPR. (Middleton-Leal, 2020) (“Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)”, 2016)

Tabulka 1 Porovnání GDPR a ISO 270001

GDPR	ISO 27001
Širší rozsah dat, který vyžaduje ochranu	Management aktiv
Pro použití dat je vyžadován výslovný souhlas	Provozní bezpečnost
Rozšířená práva subjektů údajů	Řízení přístupu
Obrovské pokuty za nedodržení předpisů	Správa bezpečnostních incidentů
Přísná pravidla pro oznámení porušení údajů	Zabezpečení lidských zdrojů

Zdroj: Vlastní tvorba, (Middleton-Leal, 2020) ("Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", 2016)

Existuje mnoho oblastí, kde se ISO 27001 a GDPR překrývají. Většina z nich souvisí s bezpečností informací: ISO 27001 stanovuje podobná pravidla pro ochranu údajů, jaká jsou uvedena v článcích GDPR 5, 24, 25, 28, 30,32. Oběma standardům odpovídá několik bodů.

6.7.1 Důvěrnost, dostupnost a integrita dat

Článek 5 GPDR stanovuje obecné zásady zpracování údajů, jako je ochrana před „neoprávněným nebo nezákonným zpracováním, náhodnou ztrátou, zničením nebo poškozením". Podrobnější pokyny jsou uvedeny v článku 32, který stanoví, že organizace jsou povinny zavést, provozovat a udržovat vhodná technická a organizační opatření k zajištění bezpečnosti dat, jako je šifrování, odolnost procesních systémů a služeb, schopnost včas obnovit dostupnost osobních údajů a další. (Žůrek, 2017)

Podobně je cílem několika kontrol v ISO 27001 pomoci organizacím zajistit důvěryhodnost, dostupnost a integritu dat. Počínaje článkem 4 vyžaduje ISO 27001, aby organizace identifikovaly interní a externí problémy, které by mohly mít dopad na jejich bezpečnostní programy. Ustanovení 6 vyžaduje, aby určili své cíle v oblasti IT bezpečnosti a vytvořili program zabezpečení, který jim pomůže tyto cíle dosáhnout. Ustanovení 8 stanoví normy pro pokračující údržbu bezpečnostního programu

a vyžaduje, aby organizace dokumentovaly svůj bezpečnostní program, aby prokázaly shodu s předpisy. (Middleton-Leal, 2020) (“Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)”, 2016) (Žůrek, 2017)

6.7.2 Posouzení rizik

Jak ISO 27001, tak GDPR vyžadují přístup k zabezpečení údajů založený na riziku a jeho zhodnocení. Podle článku 35 nařízení GDPR musí společnosti provést posouzení dopadu na ochranu údajů, aby vyhodnotily a identifikovaly rizika vůči osobním údajům jednotlivých osob. Toto zhodnocení rizika GDPR je povinné před provedením vysoce rizikového zpracovávání, jako je systematické práce s mimořádně citlivými údaji.

ISO 27001 rovněž doporučuje organizacím, aby provedly důkladné zhodnocení rizik s cílem identifikovat hrozby a zranitelnosti, které by mohly ovlivnit jejich aktiva (článek 6.1.2), a vybrat vhodná opatření pro zabezpečení informací na základě výsledků tohoto posouzení rizik (bod 6.1.3). (Middleton-Leal, 2020) (“Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)”, 2016)

6.7.3 Management dodavatelů

Ustanovení 8 normy ISO 27001 vyžaduje, aby organizace určily, které procesní činnosti jsou zadávány externě, a zajistily, že jsou schopny tyto činnosti udržet pod kontrolou. Ustanovení A.15 poskytuje konkrétní pokyny ohledně vztahů s dodavateli a vyžaduje, aby organizace sledovaly a kontrolovaly dodavatelské poskytování služeb.

Podobné problémy jsou obsaženy v článku 28 GDPR, který požaduje, aby správci údajů zajistili smluvně podmínky se zpracovateli dat a vytvořili „dohodu o zpracování údajů“. (Middleton-Leal, 2020) (“Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such

data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", 2016)

6.7.4 Oznámení o narušení

Podle článků 33–34 GDPR musí společnosti informovat úřady do 72 hodin po zjištění narušení osobních údajů. Subjekty údajů musí být také informovány bez zbytečného odkladu, ale pouze v případě, že údaje představují „vysoké riziko pro práva a svobodu datových subjektů".

Ustanovení A.16 normy ISO 27001, které se týká kontrol řízení incidentů v oblasti bezpečnosti informací, nestanovuje přesný časový rámec pro oznámení o narušení bezpečnosti dat, ale uvádí, že organizace musí bezpečnostní incidenty okamžitě nahlásit a tyto události sdělit způsobem, který umožňuje „včasně podniknout nápravná opatření." (Middleton-Leal, 2020) ("Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", 2016)

6.7.5 Záměrná ochrana dat

V článku 25 GDPR se uvádí, že společnosti musí ve fázi návrhu všech projektů provádět technická a organizační opatření, aby mohly zajistit soukromí údajů hned od začátku („ochrana údajů již od návrhu"). Organizace by navíc měly standardně chránit soukromí osobních údajů a zajistit, aby se používaly pouze informace, které jsou nezbytné pro každý konkrétní účel zpracování („základní ochrana údajů") ("Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", 2016)

V normě ISO 27001 jsou podobné požadavky uvedeny v článcích 4 a 6. Ustanovení 4 vyžaduje, aby organizace rozuměly rozsahu a kontextu údajů, které shromažďují a zpracovávají, zatímco článek 6 doporučuje, aby prováděly pravidelné hodnocení bezpečnostních rizik, aby zajistily účinnost svého řízení bezpečnosti. (Middleton-Leal, 2020) ("Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with

regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", 2016)

6.7.6 Vedení záznamů

Článek 30 GDPR vyžaduje, aby organizace vedly záznamy o svých zpracovatelských činnostech, včetně kategorií údajů, účelu zpracování a obecného popisu příslušných technických a organizačních bezpečnostních opatření.

Podobně ISO 27001 říká, že organizace musí dokumentovat své bezpečnostní procesy, jakož i výsledky svých hodnocení bezpečnostních rizik a zacházení s nimi (článek 8). Podle kontroly A.8 musí být informační aktiva inventarizována a klasifikována, musí být přiřazeni vlastníci aktiv a musí být definovány postupy pro přijatelné použití dat. (Middleton-Leal, 2020)

Certifikace podle ISO 27001 může zjednodušit proces dosažení souladu s GDPR. Mezi těmito standardy však existuje několik rozdílů. GDPR je evropský standard, který poskytuje strategickou vizi toho, jak organizace musí zajistit soukromí údajů. ISO 27001 je soubor osvědčených postupů s úzkým zaměřením na bezpečnost informací; poskytuje praktické rady o tom, jak chránit informace a omezovat počítačové hrozby. Na rozdíl od GDPR nezahrnuje přímo následující otázky spojené s ochranou osobních údajů. (Middleton-Leal, 2020) ("Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", 2016)

6.8 Nejdůležitější články GDPR

Souhlas – Správci údajů musí prokázat, že subjekty souhlasily se zpracováním svých osobních údajů (články 7 a 8). Žádost o souhlas musí být podána ve snadno přístupné formě s připojeným účelem zpracování údajů. Dotčené osoby mají také právo kdykoli odvolat svůj souhlas.

Přenositelnost údajů – Jednotlivci mají právo získávat a znovu používat své osobní údaje pro své vlastní účely v různých službách a předávat je jiným provozovatelům bez omezení použitelnosti (článek 20).

Právo na zapomenutí – Jednotlivci mají právo na vymazání svých osobních údajů nebo na okamžité zastavení jejich dalšího šíření (článek 17).

Právo na omezení zpracování – Jednotlivci mají právo omezit způsob, jakým organizace používá jejich osobní údaje, pokud byly údaje nezákonně zpracovány nebo jednotlivec zpochybňuje přesnost údajů (článek 18).

Právo na vznesení námitky – Subjekty údajů mají právo vznést námitku proti zpracování údajů pro přímý marketing, plnění právních úkolů nebo pro účely výzkumu a statistiky (článek 21).

Mezinárodní předávání osobních údajů – Organizace musí zajistit, aby mezinárodní předávání údajů probíhalo v souladu s pravidly schválenými Evropskou komisí (článek 46). (Middleton-Leal, 2020) ("Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", 2016) (Žůrek, 2017)

7 Analýza rizik

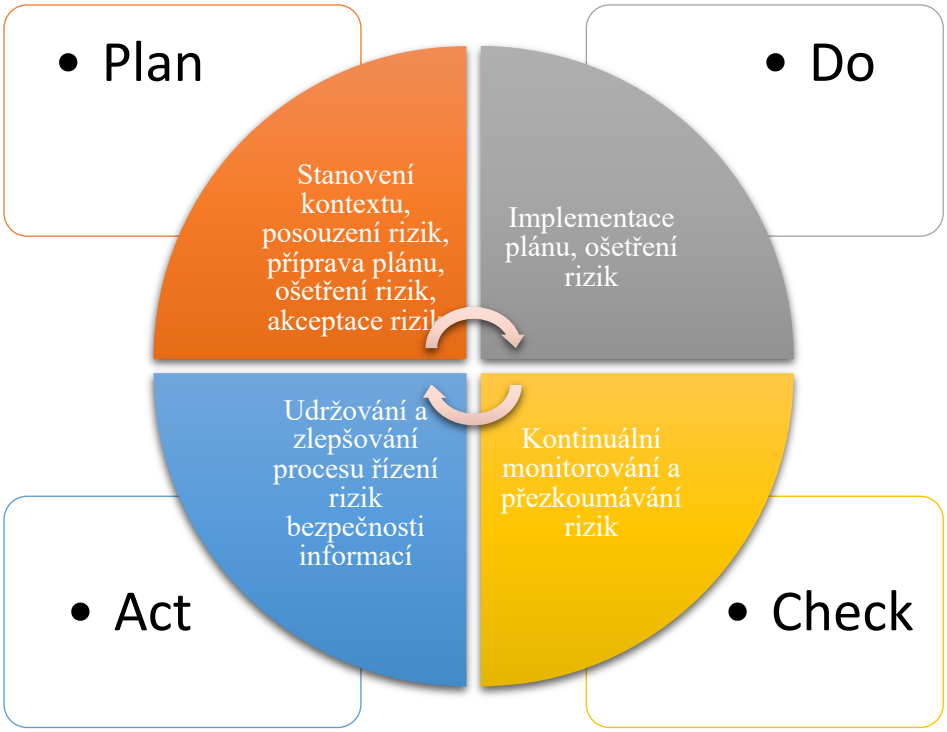
7.1 Úvod

Analýza rizik by měla odpovědět na otázku jakým hrozbám je společnost vystavena. Účelem řízení rizik bezpečnosti informací je v tomto případě soulad s právními předpisy a zvýšení důvěryhodnosti organice. Analýza rizik by měla být dle doporučení normy ISO 27001 příloha A prováděna jednou ročně. Zvláště pro malé obce může být přístup k takovéto analýze komplikovaný, proto je zde jednoduchý návod jak rychle a efektivně takovou analýzu provést.

Pro analýzu a práci s riziky v organizaci je možné využít Demingova cyklu PDCA. (“Demingův cyklus”, 2016).

„*Cyklus PDCA je řada činností zaměřených na zlepšení. Začíná studiem současné situace, během níž se shromažďují data, která se mají použít při formulaci plánu zlepšení. Jakmile je tento plán dokončen, je implementován. Poté je prováděna kontrola, zda došlo k očekávanému zlepšení. Když byl experiment úspěšný, je přijata konečná akce, jako je metodologická standardizace, aby se zajistilo, že nové zavedené metody budou neustále praktikovány pro trvalé zlepšování.*“ (Maruta, 2012)

Obrázek 1 PDCA cyklus řízení rizik podle ISO 27005



Zdroj: Vlastní tvorba, („Demingův cyklus”, 2016) (ISO/IEC 27005:2018: Information technology — Security techniques — Information security risk management, 2018)

Aplikací tohoto obecného plánu na řízení informačního rizika získáme podrobnější návod, jaké činnosti provádět.

Samotná analýza rizik z pohledu ICT využívá několik pojmů. (Analýza rizik: Jemný úvod do analýzy rizik, 2010) (“Exemplar ISMS Risk Assessment Manual Version Information Governance Toolkit”, 2019)

Aktivum = vše co má pro společnost nějakou hodnotu a je třeba to chránit. Aktiva uvedená v tabulce níže byla vybrána na základě diskuse s představiteli zkoumaných obcí. Aktiva byla ohodnocena podle důležitosti a významnosti pro obec. Číslo jedna představuje nízkou důležitost.

Hrozba = jakákoliv událost která může způsobit narušení důvěryhodnosti, integrity a dostupnosti aktiva. Hrozby, které se vztahují na jednotlivá aktiva jsou rozvedeny v Tabulce hrozeb.

Zranitelnost = vlastnost aktiva nebo slabina na úrovni fyzické, logické nebo administrativní bezpečnosti, která může být zneužita hrozbou.

7.2 Hrozby

Byly stanoveny hrozby, které mohou ohrožovat zkoumanou obec. Pravděpodobnost je možnost výskytu hrozby za časové období.

Tabulka 2 Hrozby

Body	Pravděpodobnost rizika	Popis
4	Jisté	Riziko se téměř vždy vyskytne
3	Pravděpodobné	Riziko se někdy může vyskytnout
2	Nepravděpodobné	Riziko se někdy může vyskytnout, ale je to nepravděpodobné
1	Výjimečné	Riziko se vyskytne pouze ve výjimečných případech

Zdroj: Vlastní tvorba, (ISO/IEC 27005:2018: Information technology — Security techniques — Information security risk management, 2018) (Exemplar ISMS Risk Assessment Manual Version Information Governance Toolkit, 2019).

Závažnost je dopad hrozby na obec.

Tabulka 3 Závažnost

Body	Dopad	Popis
4	Velmi vysoký	Situace zásadně omezí nebo ukončí provoz
3	Vysoký	Situace velmi nebezpečně ovlivňuje vnitřní i vnější chod firmy
2	Střední	Situace nebezpečně ovlivní vnitřní i vnější chod
1	Nízký	Situace omezuje vnitřní chod (např. dojde k časovým zpožděním do 30 dní)

Zdroj: Vlastní tvorba, (ISO/IEC 27005:2018: Information technology — Security techniques — Information security risk management, 2018) (Exemplar ISMS Risk Assessment Manual Version Information Governance Toolkit, 2019).

Významnost hrozby byla vypočtena jako Významnost = Pravděpodobnost * Závažnost

Tabulka 4 Tabulka hrozeb

Číslo	Hrozba	Pravděpodobnost 1-4	Závažnost 1-4	Významnost
1.1	Infiltrace komunikace	3	4	12
1.2	Poškození telekomunikačních kabelů	1	3	3
1.3	Poškození datového úložiště	2	4	8
1.4	Poškození archivu	2	4	8
1.5	Přírodní katastrofy	2	3	6
1.6	Selhání sítové infrastruktury	2	2	4
1.7	Přerušení dodávek elektřiny	1	2	2
1.8	Přerušení dodávek vody	1	1	1
1.9	Požár	1	3	3
1.10	Ilegální software	1	3	3
1.11	Zastaralý software	4	4	16

1.12	Chyba při údržbě	3	3	9
1.13	Nebezpečný software (viry)	4	4	16
1.14	Podvrhnutí uživatelské identity	2	4	8
1.15	Neoprávněné přesměrování uživatelské komunikace	3	3	9
1.16	Neoprávněný přístup	2	4	8
1.17	Selhání software	2	3	6
1.18	Nedostatek personálu	2	2	4
1.19	Krádež	2	3	6
1.20	Neoprávněné použití software	2	3	6
1.21	Neoprávněný přístup k úložišti	3	4	12
1.22	Neoprávněná manipulace se sítí	2	3	6
1.23	Uživatelská chyba	3	3	9
1.24	Záměrné poškození	1	2	2

Zdroj: 1 Vlastní tvorba, (ISO/IEC 27005:2018: Information technology — Security techniques — Information security risk management, 2018) (Exemplar ISMS Risk Assessment Manual Version Information Governance Toolkit, 2019).

7.3 Zranitelnost

Tabulka 5 Zneužitelnost

Body	Dopad zneužití	Popis
4	Velmi vysoký	Zásadně ovlivní důvěryhodnost, integritu a velice ohrozí obec, vede ke kompromitaci důležitých dat
3	Vysoký	Ovlivní důvěryhodnost, integritu a ohrozí obec, vede ke kompromitaci dat.
2	Střední	Má jistý vliv na důvěryhodnost, integritu ale zásadně neohrožuje.
1	Nízký	Neohrozí důvěryhodnost ani provoz obce

Zdroj: Vlastní tvorba, (ISO/IEC 27005:2018: Information technology — Security techniques — Information security risk management, 2018) (Exemplar ISMS Risk Assessment Manual Version Information Governance Toolkit, 2019).

Významnost zranitelnosti byla vypočtena jako Významnost = Zneužitelnost * Závažnost.

Tabulka 6 Tabulka zranitelností

Číslo	Zranitelnost	Zneužitelnost 1-4	Závažnost 1-4	Významnost
2.1	Nedostatek personálu	1	1	1
2.2	Neoprávněná činnost externího personálu (úklid)	2	3	6
2.3	Nedostatečná znalost bezpečnostních pravidel	3	3	9
2.4	Absence kontrolních mechanismů	3	2	6
2.5	Absence politiky pro užívání komunikačních kanálů	3	3	9
2.6	Absence / nedostatečná kontrola a evidence přístupu do budovy / místností	3	4	12
2.7	Absence / nedostatečné zabezpečené budovy (alarm)	2	3	6
2.8	Budova je umístěna v záplavové zóně	1	3	3
2.9	Nedostatečná údržba úložiště	2	2	4
2.10	Absence identifikačních a ověřovacích mechanismů	3	4	12
2.11	Nedostatečná údržba síťových prvků	4	3	12

2.12	Nedostatečná údržba koncový stanic	4	3	12
2.13	Neoprávněné kopírování	3	3	9
2.14	Nedbalost při likvidaci dokumentů	2	4	8
2.15	Nedbalost při zacházení s dokumenty	2	3	6
2.16	Absence / špatná politika hesel	4	4	16
2.17	Nekontrolované stahování a instalace software	3	3	9
2.18	Špatné přiřazení přístupových oprávnění	3	3	9

Zdroj: Vlastní tvorba, (ISO/IEC 27005:2018: Information technology — Security techniques — Information security risk management, 2018) (Exemplar ISMS Risk Assessment Manual Version Information Governance Toolkit, 2019).

7.4 Tabulka analýzy rizik

Tabulka 7 Tabulka analýzy rizik

Aktivum	Hodnota 1-4 (1-nízká, 2-střední, 3-vysoká, 4-velmi vysoká)	Hrozby	Zranitelnosti
Osobní složky	4	1.3, 1.4, 1.5, 1.9, 1.16, 1.19, 1.21, 1.23, 1.24	2.2, 2.4, 2.6, 2.7, 2.8, 2.10, 2.13, 2.14, 2.15
Smlouvy	3	1.3, 1.4, 1.5, 1.9, 1.16, 1.19, 1.21, 1.23, 1.24	2.2, 2.4, 2.6, 2.7, 2.8, 2.10, 2.13, 2.14, 2.15
Účetní doklady	2	1.3, 1.4, 1.5, 1.9, 1.16, 1.19, 1.21, 1.23, 1.24	2.2, 2.4, 2.6, 2.7, 2.8, 2.10, 2.13, 2.14, 2.15
Korespondece	1	1.1, 1.14, 1.16, 1.23	2.2, 2.4, 2.6, 2.7, 2.8, 2.10, 2.13, 2.14, 2.15
Finanční záznamy	3	1.3, 1.4, 1.5, 1.9, 1.16, 1.19, 1.21, 1.23, 1.24	2.2, 2.4, 2.6, 2.7, 2.8, 2.10, 2.13, 2.14, 2.15
Emaily	2	1.1, 1.2, 1.6, 1.11, 1.13, 1.14. 1.15, 1.16, 1.22, 1.23	2.3, 2.4, 2.5, 2.10, 2.11, 2.12, 2.16, 2.17
Počítače	1	1.1, 1.2, 1.7, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.16, 1.17, 1.20, 1.23	2.3, 2.4, 2.5, 2.9, 2.10, 2.11, 2.12, 2.16, 2.17
		1.1, 1.2, 1.7, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.16	2.3, 2.4, 2.10, 2.11

Zdroj: Vlastní tvorba

Tabulka 8 Tabulka analýzy rizik

Míra rizika 1-5 (1-nízká, 2-střední, 3-vysoká, 4-velmi vysoká, 5-maximální)	Hrozby skóre	Zranitelnosti skóre	Celkové rizikové skóre	Pozornost pro zabezpečení aktiva
5	62	68	650	2600
4	62	68	520	1560
3	62	68	390	780
3	37	68	315	315
2	62	68	260	780
4	91	85	704	1408
2	102	89	382	382
3	102	55	471	942

Zdroj: Vlastní tvorba

Tabulka 9 Tabulka analýzy rizik

Tiskárny	1	1.1, 1.2, 1.3, 1.4, 1.11	2.2, 2.13, 2.15
Telefony	1	1.1, 1.2, 1.3, 1.4, 1.11	2.3, 2.5, 2.11
Sítová zařízení	4	1.1, 1.2, 1.7, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.16, 1.17, 1.20, 1.23	2.3, 2.4, 2.10, 2.11, 2.16
Archivní prostředky	4	1.3, 1.4, 1.5, 1.9, 1.16, 1.19, 1.21, 1.23, 1.24	2.2, 2.4, 2.6, 2.7, 2.9, 2.10, 2.13, 2.14, 2.15, 2.18
Aplikační software	1	1.1, 1.2, 1.7, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.16, 1.17, 1.20, 1.23	2.3, 2.12, 2.16, 2.17, 2.18
Základní software (OS)	2	1.1, 1.2, 1.7, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.16, 1.17, 1.20, 1.23	2.3, 2.12, 2.16, 2.17, 2.18
Lidé	4	1.5, 1.9, 1.18, 1.19, 1.23, 1.24	2.1, 2.4, 2.6, 2.7, 2.8, 2.10

Zdroj: Vlastní tvorba

Tabulka 10 Tabulka analýzy rizik

1	47	21	68	68
1	47	30	77	77
5	102	55	785	3140
5	62	78	700	2800
2	102	55	314	314
2	102	55	314	628
5	30	40	350	1400

Zdroj: Vlastní tvorba

Tabulka 11 Tabulka analýzy rizik

Aktivum	Hodnota 1-4 (1-nízká, 2-střední, 3-vysoká, 4-velmi vysoká)	Hrozby	Zranitelnosti	Míra rizika 1-5 (1-nízká, 2-střední, 3-vysoká, 4-velmi vysoká, 5-maximální)	Hrozby skóre	Zranitelnosti skóre	Celkové rizikové skóre	Pozornost pro zabezpečení aktiva
Osobní složky	4	1.3, 1.4, 1.5, 1.9, 1.16, 1.19, 1.21, 1.23, 1.24	2.2, 2.4, 2.6, 2.7, 2.8, 2.10, 2.13, 2.14, 2.15	5	62	68	650	2600
Smlouvy	3	1.3, 1.4, 1.5, 1.9, 1.16, 1.19, 1.21, 1.23, 1.24	2.2, 2.4, 2.6, 2.7, 2.8, 2.10, 2.13, 2.14, 2.15	4	62	68	520	1560
Účetní doklady	2	1.3, 1.4, 1.5, 1.9, 1.16, 1.19, 1.21, 1.23, 1.24	2.2, 2.4, 2.6, 2.7, 2.8, 2.10, 2.13, 2.14, 2.15	3	62	68	390	780
Korespondece	1	1.1, 1.14, 1.16, 1.23	2.2, 2.4, 2.6, 2.7, 2.8, 2.10, 2.13, 2.14, 2.15	3	37	68	315	315
Finanční záznamy	3	1.3, 1.4, 1.5, 1.9, 1.16, 1.19, 1.21, 1.23, 1.24	2.2, 2.4, 2.6, 2.7, 2.8, 2.10, 2.13, 2.14, 2.15	2	62	68	260	780
Emaily	2	1.1, 1.2, 1.6, 1.11, 1.13, 1.14. 1.15, 1.16, 1.22, 1.23	2.3, 2.4, 2.5, 2.10, 2.11, 2.12, 2.16, 2.17	4	91	85	704	1408
Počítače	1	1.1, 1.2, 1.7, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.16, 1.17, 1.20, 1.23	2.3, 2.4, 2.5, 2.9, 2.10, 2.11, 2.12, 2.16, 2.17	2	102	89	382	382
Servery	2	1.1, 1.2, 1.7, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.16, 1.17, 1.20, 1.23	2.3, 2.4, 2.10, 2.11, 2.16	3	102	55	471	942
Tiskárny	1	1.1, 1.2, 1.3, 1.4, 1.11	2.2, 2.13, 2.15	1	47	21	68	68
Telefony	1	1.1, 1.2, 1.3, 1.4, 1.11	2.3, 2.5, 2.11	1	47	30	77	77
Sítová zařízení	4	1.1, 1.2, 1.7, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.16, 1.17, 1.20, 1.23	2.3, 2.4, 2.10, 2.11, 2.16	5	102	55	785	3140
Archivní prostředky	4	1.3, 1.4, 1.5, 1.9, 1.16, 1.19, 1.21, 1.23, 1.24	2.2, 2.4, 2.6, 2.7, 2.9, 2.10, 2.13, 2.14, 2.15, 2.18	5	62	78	700	2800
Aplikační software	1	1.1, 1.2, 1.7, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.16, 1.17, 1.20, 1.23	2.3, 2.12, 2.16, 2.17, 2.18	2	102	55	314	314
Základní software (OS)	2	1.1, 1.2, 1.7, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.16, 1.17, 1.20, 1.23	2.3, 2.12, 2.16, 2.17, 2.18	2	102	55	314	628
Lidé	4	1.5, 1.9, 1.18, 1.19, 1.23, 1.24	2.1, 2.4, 2.6, 2.7, 2.8, 2.10	5	30	40	350	1400

Zdroj: Vlastní tvorba

Hrozby skóre bylo vypočteno jako součet významností vyskytujících se hrozeb u daného aktiva. Vyjadřuje míru ohrožení aktiva.

Zranitelnosti skóre bylo vypočteno jako součet významností vyskytujících se zranitelností u daného aktiva. Vyjadřuje míru zranitelnosti aktiva.

Celkové rizikové skóre bylo vypočteno jako míra rizika * (hrozby skóre + zranitelnosti skóre). Vyjadřuje celkové riziko pro dané aktivum.

Pozornost pro zabezpečení aktiva byla vypočtena jako hodnota aktiva * celkové rizikové skóre. Vyjadřuje, kterým aktivům by měla být aktuálně věnována nejvyšší pozornost z hlediska zabezpečení a snahy eliminace rizik, protože mají vysokou důležitost pro společnost a zároveň jsou nejvíce ohrožena.

7.5 Výsledky a zhodnocení

Z tabulky analýzy rizik vyplývá jako nejohroženější aktivum síťová zařízení, na druhém místě jsou archivní prostředky a na třetím místě osobní složky. Jako nejméně ohrožené se ukázaly tiskárny a telefony. Zajímavým jevem je umístění počítačů, které mají vysoké dílčí skóre, ale díky své nízké hodnotě pro společnost jsou v tabulce relativně nízko.

7.6 Opatření a doporučení pro obec z příkladu

Hlavním požadavkem ISMS je vytvoření dokumentu bezpečnostní politiky a jeho pravidelné přezkoumávání a aktualizace. Na obci je tento dokument k dispozici. Podle průzkumu mezi zaměstnanci je ale pro ně tento dokument nesrozumitelný. Doporučujeme aktualizovat dokument (jednou ročně) bezpečnostní politiky tak aby byl srozumitelný pro všechny zaměstnance, ideálně jim umožnit sledování změn.

Pro snížení rizika doporučujeme zavést opatření uvedená ve Vyhlášce č.82/2018 Sb. a také v normách rodiny ISO 27001 příloha A.

Jako příklad jsou uvedena některá opatření pro nejohroženější aktivum, tj. síťová zařízení.

- zajištění segmentace komunikační sítě
- zajištění řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě
- pomocí kryptografie zajištění důvěrnosti a integrity dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií
- aktivní blokování nežádoucí komunikace

- pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty užívání nástroje, který zajistí ochranu integrity komunikační sítě.

(“Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti): Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 28 odst. 2 písm. a) až d) a f) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb. a zákona č. 205/2017 Sb.”)

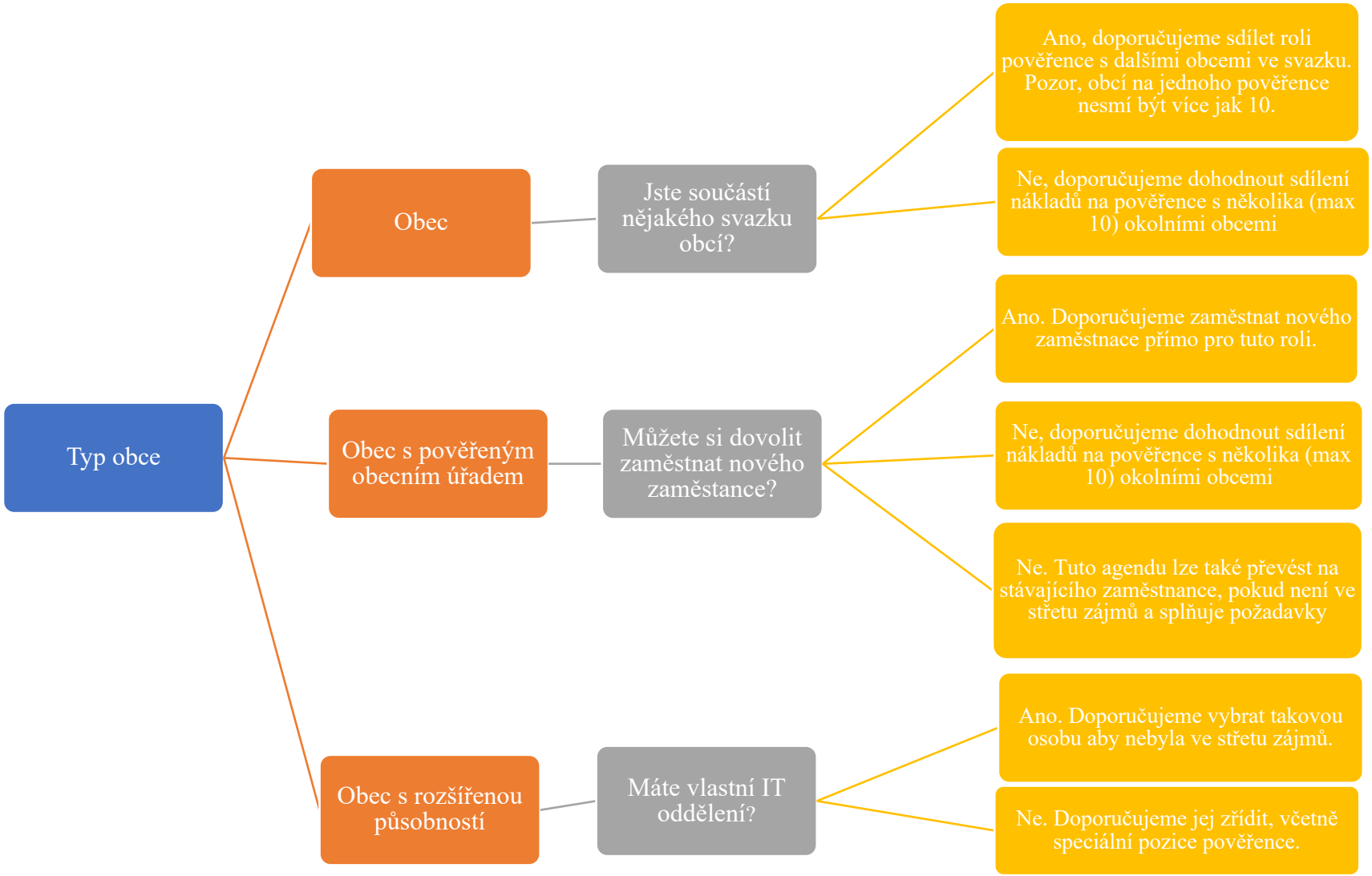
8 Pověřenec pro ochranu osobních údajů

Orgány musí z podstaty nařízení GDPR splnit svou povinnost jmenovat pověřence ochrany údajů. Buď jmenují zaměstnance jako interního pověřence ochrany údajů, nebo jmenují externího pověřence ochrany údajů. Při výběru takové osoby musí zajistit, aby interní pověřenec ochrany údajů nebyl vystaven střetu zájmů kvůli jeho práci v oddělení IT, oddělení lidských zdrojů nebo vrcholovém vedení, kde by musel dohlížet na sebe. Bez ohledu na to, která možnost je vybrána, musí mít pověřenec ochrany údajů odborné znalosti v oblasti ochrany údajů a bezpečnosti IT, v závislosti na složitosti zpracování údajů a velikosti společnosti. (Data Protection Officer, 2018) (Škorničková, 2019) ("Metodické doporučení k činnosti obcí k organizačně technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí: Podle právního stavu k 10. sprnu 2017", 2017) (Žůrek, 2017)

Pověřenec musí usilovat o dodržování všech příslušných zákonů o ochraně údajů, sledovat konkrétní procesy, jako jsou hodnocení dopadů na ochranu údajů, zvyšovat povědomí zaměstnanců o ochraně údajů a odpovídajícím způsobem je školit, jakož i spolupracovat s orgány kontroly. Zaměstnanec jednající jako inspektor ochrany údajů proto nesmí být propuštěn nebo potrestán z důvodu plnění svých úkolů. Společnost je sama odpovědná za dodržování zákonů o ochraně údajů. Proto musí zapojit pověřence ochrany údajů do všech otázek, které se týkají ochrany osobních údajů „řádně a včas". Při jmenování pověřence ochrany údajů musí společnost sdělit jmenovací a kontaktní údaje orgánům dozoru nad ochranou údajů. Úmyslné nebo nedbalostní nejmenování pověřence ochrany údajů navzdory zákonné povinnosti je porušením podléhajícím pokutám. (Data Protection Officer, 2018) (Škorničková, 2019) ("Metodické doporučení k činnosti obcí k organizačně technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí: Podle právního stavu k 10. sprnu 2017", 2017) (Žůrek, 2017)

Na grafu níže je naznačen možný proces rozhodování při výběru způsobu realizace role pověřence pro ochranu osobních údajů.

Graf 5 Možný způsob výběru role pověřence pro ochranu osobních údajů

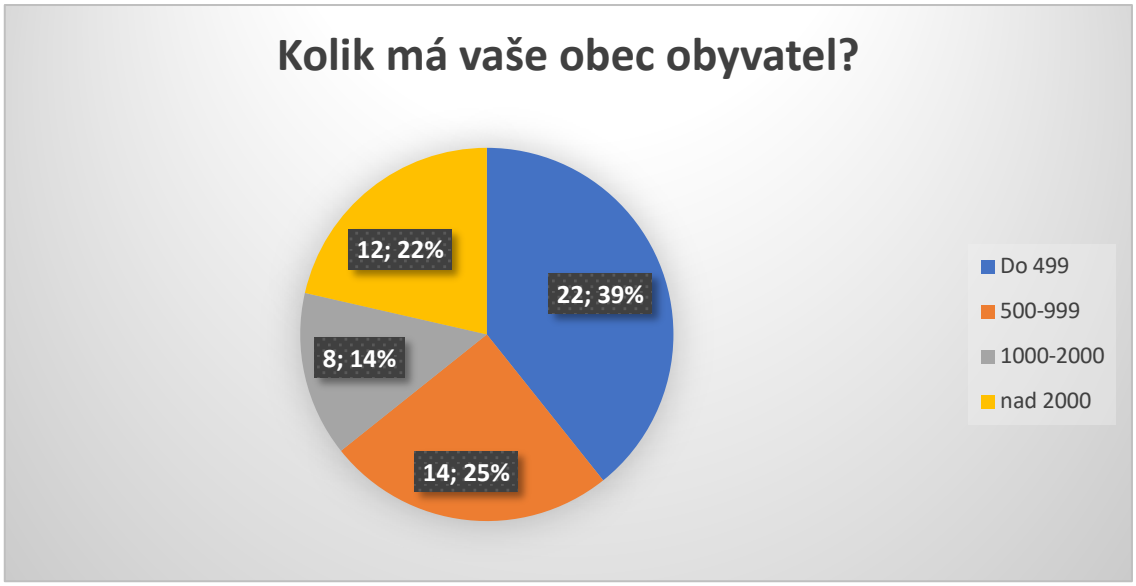


Zdroj: Vlastní tvorba

9 Dotazníkové šetření

Dotazníkové šetření bylo provedeno v obcích na území České republiky, a to kombinací osobní (návštěva obecního úřadu) a online formy (platforma Google Formuláře), osobně nebo adresným emailem bylo osloveno 51 obcí na celém území České republiky a další obce byly osloveny pomocí Svazu měst a obcí České republiky, který sdružuje 2765 obcí. Celkem se vrátilo 56 dotazníků. Přesnou procentuální návratnost nelze určit. Dotazník se skládal ze 16 otázek.

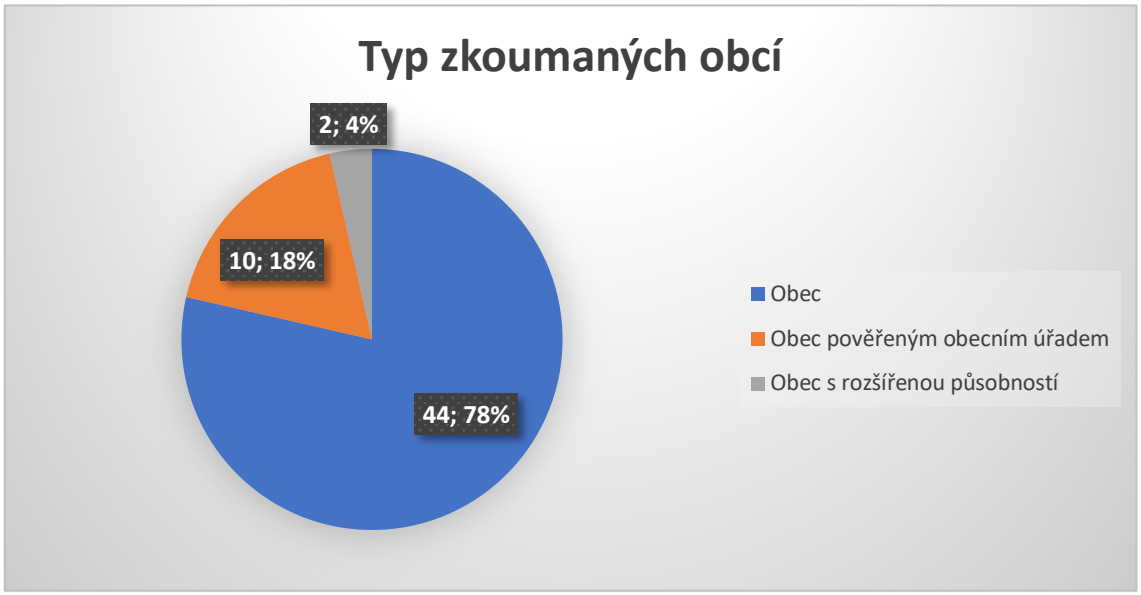
Graf 6 Počet obyvatel zkoumaných obcí



Zdroj: Vlastní tvorba

Otázka na počet obyvatel je v dotazníku z důvodu lepších možností pozdější práce s daty. Samotný graf ukazuje strukturu obcí, které odpověděli na otázky.

Graf 7 Typ zkoumaných obcí



Zdroj: Vlastní tvorba

Otázka na typ zkoumané obce je v dotazníku opět z důvodu lepších možností práce a analýzy získaných dat. Struktura typů přibližně odpovídá rozložení v rámci České republiky.

Graf 8 Bezpečnostní hrozby

Zdroj: Vlastní tvorba

Bezpečnostní hrozby na úřadech vykazují podobné trendy, s jakými se setkávají běžní uživatelé. Pouze vyšší četnost vloupání se vymyká. Aplikací bezpečnostní politiky lze těmto hrozbám předcházet případně minimalizovat dopady. Za pozitivní lze

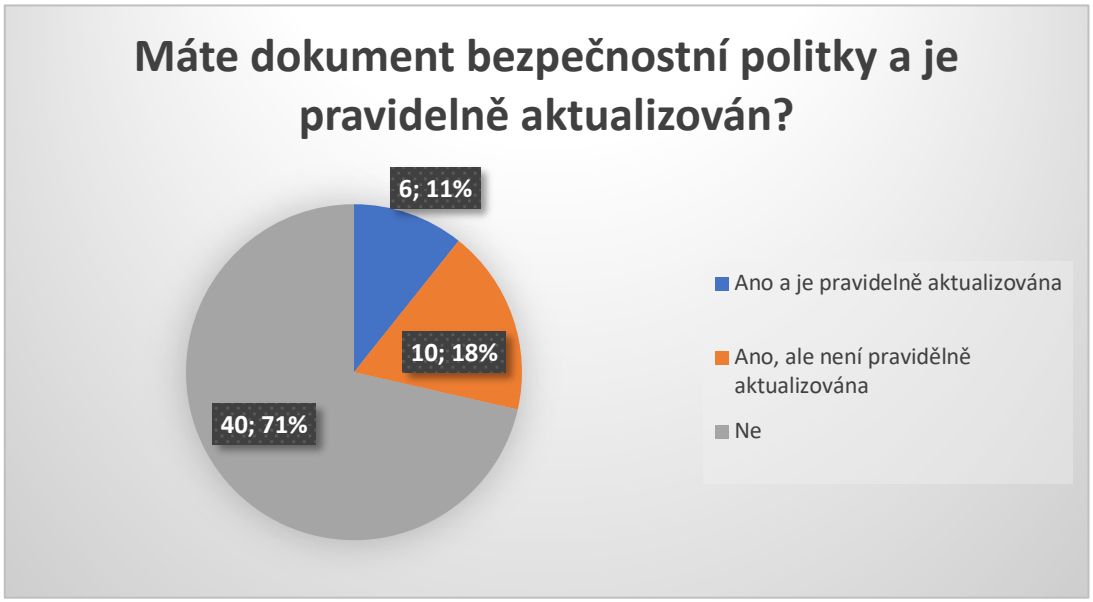
považovat, že ve všech zkoumaných obcích je alespoň základní ochrana proti škodlivému kódu pomocí antivirových programů. Jakákoliv další opatření však téměř chybí, vrcholem je zabezpečení budov pomocí alarmu či požadavek na zavedení hesel na pracovních stanicích, není ale v drtivé většině definován jakýkoliv podrobnější postup.

Graf 9 Informační bezpečnost

Zdroj: Vlastní tvorba

Externí řešení ICT a bezpečnosti hodnotím jako nepříliš ideální, nicméně je to stále lepší než převádět celou tuto komplexní agendu na běžného zaměstnance bez patřičného vzdělání či absence kohokoliv. 40 % zcela nevhodného řešení je velmi rizikové.

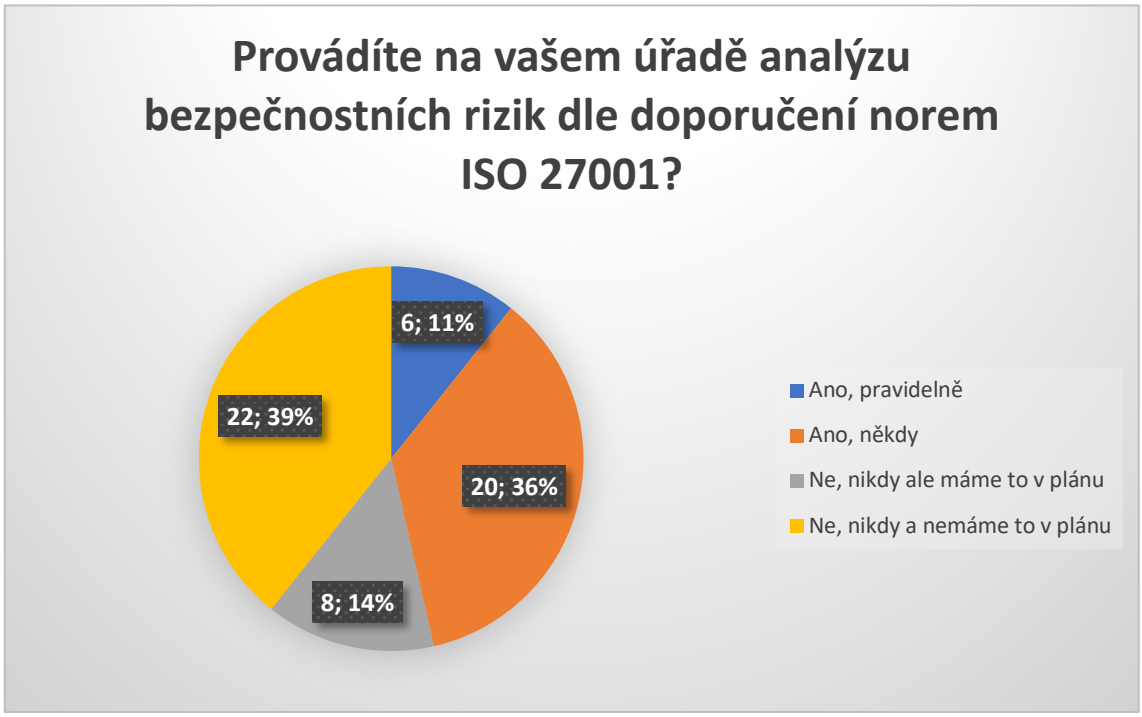
Graf 10 Bezpečnostní politika



Zdroj: Vlastní tvorba

Požadavkem ISMS je dokument bezpečnostní politiky. Ten by měl být k dispozici všem zaměstnancům a v plánovaných intervalech aktualizován. Z šetření vyplynulo zcela alarmující zjištění a to že 70 % zkoumaných obcí nemá žádnou bezpečnostní politiku. Pokud bezpečnostní politika existuje, není většinou aktuální, a navíc je nesrozumitelná pro zaměstnance. Aktualizace by měla dle normy ISO 27001 příloha A aktualizována každý rok což splňuje pouze 12 % obcí. Na otázku mohou zaměstnanci sledovat průběžné změny a postup schvalování bezpečnostní politiky (není na grafu) odpovědělo kladně pouze 12 % obcí. Možnost sledování změn bezpečnostní politiky je jedním z dalších doporučení ISO 27001 přílohy A.

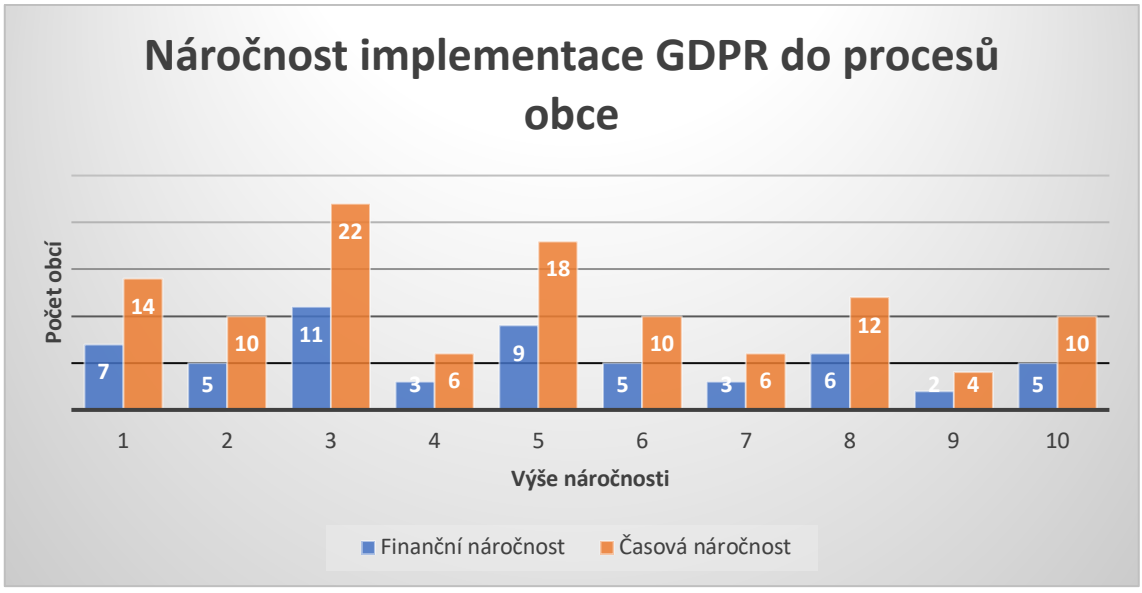
Graf 11 Analýza bezpečnostních rizik



Zdroj: Vlastní tvorba

Analýza a zhodnocení rizik je jedním z hlavních součástí norem ISO 27001. Je to nejdůležitější krok v začátku zajištění informační bezpečnosti. 39 % obcí tuto analýzu nikdy neprovedlo a ani to nemá v plánu. Jsou tak velmi ohroženi a nemají žádný základ pro řešení informační bezpečnosti. Absence této analýzy zároveň komplikuje aplikaci GDPR.

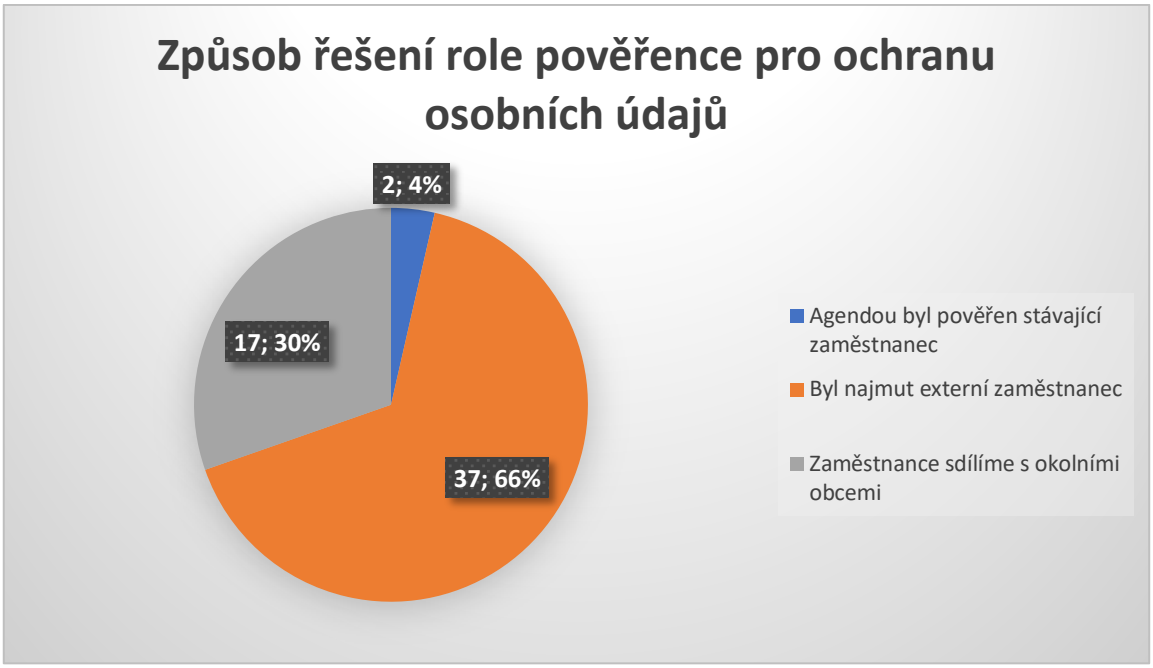
Graf 12 Náročnost implementace GDPR



Zdroj: Vlastní tvorba

Na grafu měli dotazované obce vyjádřit na škále náročnost implementace GDPR do vlastních procesů. Číslo 1 představuje nejmenší náročnost a 10 nejvyšší. Jasně převyšuje časová náročnost. Jedná se hlavně o studium nařízení, návštěvu školení a úpravu procesů tak aby odpovídaly nařízení.

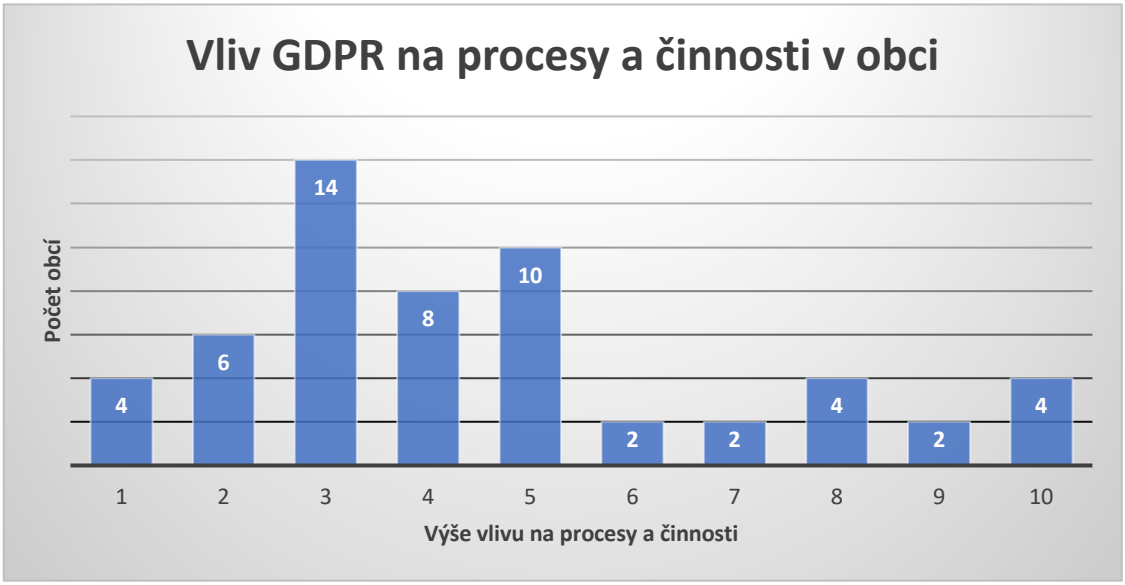
Graf 13 Způsob role řešení pověřence pro ochranu osobních údajů



Zdroj: Vlastní tvorba

Každá obec je podle nařízení povinna zřídit roli pověřence pro ochranu osobních údajů. V případě vlastního IT oddělení je nejjednodušší pověřit stávajícího zaměstnance, pokud není ve střetu zájmů. Většina zkoumaných obcí vyřešila tuto roli delegací na externího zaměstnance. Oficiální doporučení Ministerstva vnitra pak doporučuje sdílet agendu pověřence s okolními obcemi, těch může být až deset.

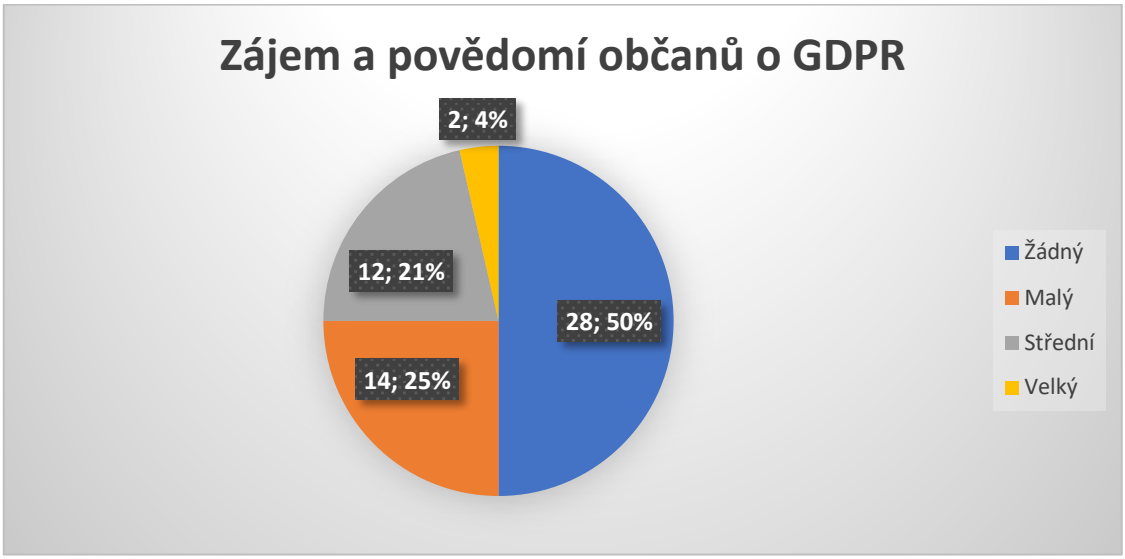
Graf 14 Vliv GDPR



Zdroj: Vlastní tvorba

Na grafu měli zkoumané obce ohodnotit vliv GDPR na samotné procesy v obci. Z výsledků vyplývá, že ve většině obcí nebyla až tolik ovlivněna z hlediska úpravy činností.

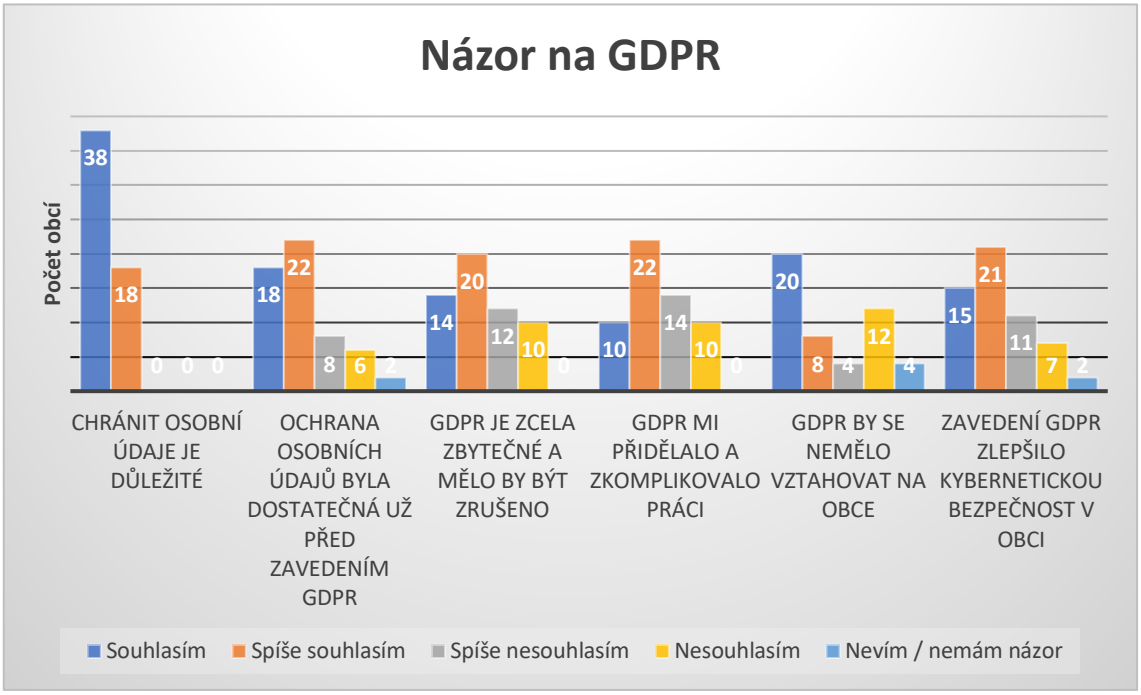
Graf 15 Zájem a povědomí občanů o GDPR



Zdroj: Vlastní tvorba

75 % občanů zkoumaných obcí nejeví o GDPR větší zájem. Toto zjištění je v kontrastu s výzkumem (*Special Eurobarometer 487a – March 2019 "The General Data Protection Regulation" Report*, 2019) který tvrdí že povědomí o GDPR v ČR je 85%.

Graf 16 Názor na GDPR



Zdroj: Vlastní tvorba

Na otázky v tomto grafu panuje mezi obcemi většinová shoda. Všichni souhlasí s tím, že se mají chránit osobní údaje, ale již nesouhlasí s prováděnou formou. Jsou toho názoru, že ochrana osobních údajů byla dostatečná již před zavedením GDPR. Většina by také toto nařízení spíše zrušila, ale zde je i zcela opačná názorová část, která by naopak nařízení nechala v platnosti. Největší rozpolcenost názorů panuje na to, zda GDPR komplikuje práci či nikoliv. Z osobních rozhovorů vyplul obecný názor, že práci komplikuje. V dotazníku je pak souhlas s tímto tvrzením ovlivněn pozicí osoby, kde pracuje. Na nižší zaměstnance úřadů (zajišťující například účetnictví) nemá totiž nařízení takový vliv, jako na sekce zajišťující vedení obce či provoz ICT. I někteří zaměstnanci, jež odpověděli že se jim osobně se práce nezkomplikovala, jsou často názoru, že obecně vzato GDPR práci spíše komplikuje. Souhlas s tvrzením, že GDPR by se nemělo vztahovat na obce pak potvrzuje trend mírného odporu s prováděnou formou ochrany údajů. Součástí GDPR je pak i důraz na kybernetickou bezpečnost a činnosti prováděné online. Zde panuje shoda, že nařízení zlepšilo úroveň bezpečnosti, což vzhledem ke zjištěnému stavu v části obcí je pozitivní zpráva.

10 Testování hypotéz

Stanovené hypotézy byly testovány pomocí T testu (Gerald, 2018) a Fisherova exaktního testu. (Fisherův exaktní test, 2020) U první, druhé a čtvrté hypotézy byly sloučeny obce s pověřeným obecním úřadem a obce s rozšířenou působností do jedné skupiny z důvodu malého počtu obcí s rozšířenou působností. Interpretaci výsledků to nevadí, jelikož hlavní snahou bylo zjistit, zda existuje rozdíl mezi běžnou, malou obcí a větší obcí s dalšími kompetencemi. Z tohoto důvodu, a protože byla pro hodnocení využita ordinální škála, byl u těchto hypotéz zvolen T test jako nejvhodnější řešení. U třetí hypotézy byl zvolen Fisherův exaktní test, protože zde jsou malá data, navíc v podobě čtyřpolní tabulky, pro kterou je tento test nejvhodnější.

Použitá hladina významnosti u všech testů je $\alpha = 0,05$. Testování bylo provedeno jazykem R v programu RStudio verze 1.3.1073.

1. H0: Neexistuje závislost mezi finanční náročností implementace GDPR a typem obce (obec, obec s pověřeným obecním úřadem, obec s rozšířenou působností)
   H1: Existuje závislost mezi finanční náročností implementace GDPR a typem obce (obec, obec s pověřeným obecním úřadem, obec s rozšířenou působností)
   Výsledek p hodnoty = p=0,379 což je větší než stanovená hladina významnosti 0,05 tím pádem zamítáme H1 o závislosti a přijímáme H0: **Neexistuje závislost mezi finanční náročností implementace GDPR a typem obce (obec, obec s pověřeným obecním úřadem, obec s rozšířenou působností)**

2. H0: Neexistuje závislost mezi časovou náročností implementace GDPR a typem obce (obec, obec s pověřeným obecním úřadem, obec s rozšířenou působností)
   H1: Existuje závislost mezi časovou náročností implementace GDPR a typem obce (obec, obec s pověřeným obecním úřadem, obec s rozšířenou působností)
   Výsledek p hodnoty = p=0,084 což je větší než stanovená hladina významnosti 0,05 tím pádem zamítáme H1 o závislosti a přijímáme H0: **Neexistuje závislost mezi časovou náročností implementace GDPR a typem obce (obec, obec s pověřeným obecním úřadem, obec s rozšířenou působností)**

3. H0: Neexistuje závislost mezi tím, zda má obec dokument bezpečnostní politiky tím, zda provádí analýzu rizik.

H1: Existuje závislost mezi tím, zda má obec dokument bezpečnostní politiky a tím, zda provádí analýzu rizik.
Výsledek p hodnoty = 0,989 což je větší než stanovená hladina významnosti a tím pádem přijímáme H0: **Neexistuje závislost mezi tím, zda má obec dokument bezpečnostní politiky a tím, zda provádí analýzu rizik.**

4. H0: Neexistuje závislost mezi tím, zda má obec informační systém a tím, jak časově náročná byla implementace GDPR do procesů obce.
   H1: Existuje závislost mezi tím, zda má obec informační systém a tím, jak časově náročná byla implementace GDPR do procesů obce.
   Výsledek p hodnoty = 0,036 což je menší než stanovená hladina významnosti 0,05 tím pádem zamítáme H0 o nezávislosti a přijímáme H1: **Existuje závislost mezi tím, zda má obec informační systém a tím, jak časově náročná byla implementace GDPR do procesů obce.**

5. H0: Neexistuje závislost mezi tím, zda je obec certifikována pomocí norem z rodiny ISO 27001 a časovou náročností implementace GDPR do procesů obce.
   H1: Existuje závislost mezi tím, zda je obec certifikována pomocí norem z rodiny ISO 27001 a časovou náročností implementace GDPR do procesů obce.
   Hypotézu se nepodařilo potvrdit ani vyvrátit z důvodu malého vzorku dat. Pouze 2 zkoumané obce jsou certifikovány pomocí norem z rodiny ISO 27001. Polovina zkoumaných obcí vůbec neví, co to ISO 27001 je a ostatní o implementaci neuvažují. Původním předpokladem při začátku psaní práce bylo, že většina obcí je certifikována, a proto jim zavedení GDPR nedalo téměř žádnou práci.

11 Shrnutí a doporučení

V rámci zkoumání bylo navštíveno a pohovořeno s mnoha představiteli i zaměstnanci obcí a obecních úřadů. Obecně panuje shoda nad jednou věcí a tím je, že tito lidé vnímají zavedení a aplikaci regulativy GDPR na obce jako další a zcela zbytečnou administrativní zátěž. Odvolávají se na Zákon o obcích č.128/2000 Sb. § 2 „*Obec pečuje o všestranný rozvoj svého území a o potřeby svých občanů; při plnění svých úkolů chrání též veřejný zájem.*“ Ten podle nich dostatečně vyjadřuje povinnost obce chránit zájmy občanů.

Pro lepší představu o přístupu ke GDPR uvádím autentický případ z jedné středně velké obce: *„Museli jsme vydat velkou částku na pověřence, aby jednou za rok přijel člověk z Prahy a řekl nám, že si musíme zabezpečit dokumenty. Tak jsme na skříňky dali petlice a zámky. On byl spokojený, dal nám potřebná razítka a my až odjel, zase petlice sundali.“*

Lepší informační kampaň ze strany státu a snaha zdůvodnit zavedení tohoto nařízení by mohl zvýšit renomé tohoto nařízení, které přijímá mnoho užitečných práv zejména pro běžné občany.

Co se týká stavu kybernetické bezpečnosti, v jednotlivých obcích se situace výrazně liší. A to přes legislativu jasně vymezující jednotlivé povinnosti. Naprosto alarmujícím zjištěním je, že 70 % zkoumaných obcí nemá jakýkoliv dokument ohledně bezpečnostní politiky. 39 % obcí pak neprovádí žádnou analýzu rizik. Zavedení GDPR by v teoretické rovině mělo alespoň částečně zlepšit tento špatný stav, v praxi se však situace příliš nezlepšila (lze tak usuzovat na základě provedeného dotazníkového výzkumu).

Obecně tak lze doporučit provádění alespoň základních činností, jako je pravidelná analýza rizik, vytvoření či upravení dokumentu bezpečnostní politiky do srozumitelné podoby pro všechny zaměstnance. Zavedením těchto opatření lze předejít většině bezpečnostních rizik se kterými se zejména malé obce setkávají.

Z prvního pohledu vypadá jako nejlepší opatření pro zlepšení stavu kybernetické bezpečnosti a souladu s regulativou GDPR zavedení norem skupiny ISO 27000, ve většině malých obcích by však tato implementace a zejména certifikace byla nepřiměřeně náročná oproti množství a rozsahu prováděných činností a procesů. Aktuální stav toto jen potvrzuje, 96 % zkoumaných obcí certifikováno není. Naopak dodržování základních

ISMS „best practices“ je určitě na místě. Povědomí o těchto praktikách je bohužel mezi obcemi malé. Důvodem je posazení informačních a komunikačních technologií na „druhou kolej“ a neochota investovat vysoké částky na jeho provoz a údržbu. Navíc jazyk legislativy, norem a jejich komplikovanost není příliš přívětivý laikům, mezi které patří drtivá většina představitelů či zaměstnanců obcí. Vytvoření jednoduchého manuálu ze strany státu pro obce by mohlo tento stav změnit.

12 Budoucnost

V roce 2020 představil Evropský úřad pro ochranu dat (European Data Protection Supervisor (EDPS)) novou strategii na roky 2020–2024, která se týká ochrany dat v Evropské unii. Tato strategie má tři základní pilíře. ("The EDPS Strategy 2020–2024: Shaping a Safer Digital Future", 2020) (Shaping a Safer Digital Future: a new Strategy for a new decade: Press Release, 2020)

- Předvídavost = *„EDPS bude i nadále sledovat právní, sociální a technologický pokrok po celém světě a informovat o své práci s odborníky, odborníky a orgány pro ochranu údajů."*
- Akce = *„V zájmu posílení dohledu, prosazování a poradních rolí evropského inspektora ochrany údajů bude evropský inspektor ochrany údajů podporovat soudržnost v činnostech donucovacích orgánů v EU a vyvine nástroje, které pomohou orgánům, orgánům a agenturám EU udržovat nejvyšší standardy v oblasti ochrany údajů."*
- Solidarita = *"Evropský inspektor ochrany údajů bude při prosazování digitální spravedlnosti a soukromí pro všechny prosazovat také odpovědné a udržitelné zpracování údajů, aby pozitivně ovlivnil jednotlivce a spravedlivým způsobem maximalizoval společenské výhody."*

Díky této strategii se Evropská unie stane světovým lídrem v bezpečnosti a ochraně dat. Vzhledem k přenositelnosti na jednotlivé země a její orgány včetně obcí lze očekávat další zesílení datové ochrany. Nicméně díky současné existenci GDPR není pravděpodobná taková zátěž na správní orgány při zavádění jednotlivých cílů strategie popsaných výše, jako tomu bylo při zavádění GDPR. Problémem se může stát zavádění výjimek, a to ze strany jednotlivých států

13 Závěr

Tato diplomová práce představila některé z normy z oblasti kybernetické bezpečnosti a porovnala je s regulativou GDPR. Byla provedena ukázková analýza rizik vhodná pro malé obce a za pomoci dotazníkového šetření byly zjištěny informace o stavu kybernetické bezpečnosti v obcích a vlivu GDPR.

Bylo zjištěno, že neexistuje závislost mezi finanční náročností implementace GDPR a typem obce (obec, obec s pověřeným obecním úřadem, obec s rozšířenou působností). Toto lze odůvodnit tím, že všechny obce si musely vyřešit roli pověřence pro ochranu osobních údajů, jehož finanční náročnost je pro všechny obce podobná. Také neexistuje závislost mezi časovou náročností implementace GDPR a typem obce. Podobně jako u finanční náročnosti, všechny obce musely provést podobné činnosti. Neexistuje závislost mezi tím, zda má obec dokument bezpečnostní politiky a tím, zda provádí analýzu rizik. Obce by měli provádět obě činnosti, zde bylo předpokladem, že pokud má obec dokument bezpečnostní politiky provádí i analýzu rizik a dbá tak na svojí kybernetickou bezpečnost, což se ale neprokázalo. Dále existuje závislost mezi tím, zda má obec informační systém a tím, jak časově náročná byla implementace GDPR do procesů obce. Informační systém se však vyskytuje pouze v menším počtu obcí a obvykle není nijak komplikovaný. Je většinou zastaralý a bez podpory, a proto jeho úpravy pro GDPR zejména díky požadavku na správnou anonymizaci zabraly čas.

Úroveň kybernetické bezpečnosti se v jednotlivých obcích výrazně liší. Obecné nařízení ochraně osobních údajů GDPR mělo jistý vliv na kybernetickou bezpečnost a procesy v jednotlivých obcích, v mnoha případech však spíše v teoretické než praktické rovině. Složitost, komplikovanost zákonů, norem navíc zlepšení stavu kybernetické bezpečnosti příliš nenapomáhá.

I. Summary and keywords

The aim of this work is to analyze information and communication technologies in selected municipalities using security standards, especially ISO / IEC 27000. The work focuses mainly on the state of cyber security and the impact of GDPR regulation on systems in municipalities and relevant processes. A questionnaire survey of these impacts was carried out and possible measures were proposed on the basis of the analysis of the questionnaires and the carried-out risk analysis.

It was found that there is no dependence between the financial demands of GDPR implementation and the type of municipality. There is also no dependence between the time required to implement GDPR and the type of municipality. There is no dependence between whether the municipality has a security policy document and whether it carries out a risk analysis. Furthermore, there is a dependence between whether the municipality has an information system and how time-consuming was the implementation of GDPR into the municipality's processes.

The level of cyber security varies significantly from municipality to municipality. The GDPR General Regulation has had some impact on cyber security and processes in individual municipalities, but in many cases on a theoretical rather than a practical level. In addition, the complexity of laws and standards does not help to improve the state of cyber security.

Keywords: GDPR, ISO 27001, cyber security, municipalities

II. Zdroje

An Introduction to ISO 27001, ISO 27002....ISO 27008. (2019). Retrieved August 15, 2020, from https://www.27000.org/contact.htm

Analýza rizik: Jemný úvod do anylýzy rizik. (2010). Cleverandsmart. Retrieved July 15, 2020, from https://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/

Asosheh, A., Hajinazari, P., & Khodkari, H. (2013). A practical implementation of ISMS. 7Th International Conference On E-Commerce In Developing Countries:with Focus On E-Security, 1-17. https://doi.org/10.1109/ECDC.2013.6556730

Certification. (2013). Retrieved September 01, 2020, from https://www.iso.org/certification.html

Co je ISMS [Online]. (2019). Retrieved November 09, 2019, from https://www.tx.cz/isms/metodika

Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), 2016 § (2016). European Parliament. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504

Coppola, D. (2019). THE GDPR AND DATA PROTECTION IN EUROPE: ONE YEAR LATER: A DOSSIERPLUS ON THE GENERAL DATA PROTECTION REGULATION AND ITS CONSEQUENCES IN EUROPE (did-65397-1). Statista. https://www.statista.com/study/65397/the-gdpr-and-data-protection-in-europe-one-year-later/

Česká republika – Ministerstvo vnitra, & Pražská znalecká kancelář. (2020). Systémová analýza působnosti obcí z hlediska obecného nařízení o ochraně osobních údajů (2018 ed.). https://www.mvcr.cz/gdpr/soubor/systemova-analyza-pusobnosti-obci-z-hlediska-obecneho-narizeni-o-ochrane-osobnich-udaju.aspx

Data Protection Officer. (2018). Retrieved July 21, 2020, from https://gdpr-info.eu/issues/data-protection-officer/

Datto (October 16, 2019). Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2019

[Graph]. In Statista. Retrieved April 22, 2020, from https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/

Demingův cyklus [Online]. (2016). Retrieved November 11, 2019, from https://managementmania.com/cs/deminguv-cyklus

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal Of Information Security, 04(02), 92-100. https://doi.org/10.4236/jis.2013.42011

Dombora, S. (2019). Parameters and Guidelines of Enforceable Information Security Management Systems [Online]. Interdisciplinary Description Of Complex Systems, 17(3), 485-491. https://doi.org/10.7906/indecs.17.3.7

Donát, J. (2017). Nařízení eIDAS: komentář. C.H. Beck.

European Commission (25 January 2012) Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses [Press release] Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46

EUROPEAN DATA PROTECTION SUPERVISOR: The EU's independent data protection authority [Online]. (2019). Retrieved November 29, 2019, from https://edps.europa.eu/edps-homepage_en

European eGovernment Action Plan 2011-2015 [Online]. (2011). Retrieved October 29, 2019, from https://ec.europa.eu/digital-single-market/en/european-egovernment-action-plan-2011-2015

European Union Agency for Fundamental Rights and Council of Europe. (2018). Handbook on European data protection law: Publications Office of the European Union [Online] (2018 edition). Luxembourg, Luxembourg: Publications Office of the European Union. Retrieved from https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

Exemplar ISMS Risk Assessment Manual Version Information Governance Toolkit. (2019). In. NHS. https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ISMS%20Risk%20Assessment%20Manual%20v1.4.pdf

Fisherův exaktní test. (2020). Retrieved August 18, 2020, from https://portal.matematickabiologie.cz/index.php?pg=aplikovana-analyza-klinickych-a-biologickych-dat--analyza-a-management-dat-pro-zdravotnicke-obory--testovani-hypotez-o-kvalitativnich-promennych--fisheruv-exaktni-test

Gerald, B. (2018). A Brief Review of Independent, Dependent and One Sample t-test. International Journal Of Applied Mathematics And Theoretical Physics, 4(2). https://doi.org/10.11648/j.ijamtp.20180402.13

Hrozba kybernetických útoků na nemocnice a jiné významné cíle ČR. (2020). Národní Úřad Pro Kybernetickou A Informační Bezpečnost. Retrieved April 22, 2020, from https://nukib.cz/cs/informacni-servis/aktuality/1425-hrozba-kybernetickych-utoku-na-nemocnice-a-jine-vyznamne-cile-cr/

Charlet, L. (2019). THE ISO SURVEY 2018. Geneva Switzerland: International Organization for Standardization, from https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

Chatzipoulidis, A., Tsiakis, T., & Kargidis, T. (2019). A readiness assessment tool for GDPR compliance certification, 2019(8), 14-19. https://doi.org/10.1016/S1361-3723(19)30086-7

International Electrotechnical Commission [Online]. (2019). Retrieved November 07, 2019, from https://www.iec.ch/about/?ref=menu

IONESCU, R. C., GRAB, B., & HASSANI, Y. (2019). Study of Effects of Information Security Management System in the Context of the E.U. General Data Protection Regulation Application. Quality – Access to Success, 20, 322–328. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=e5h&AN=135437231&lang=cs&site=eds-live

IP adresa [Online]. (2005). Retrieved November 22, 2019, from http://www.abclinuxu.cz/slovnik/ip-adresa

ISO/IEC 27000:2018: Information technology — Security techniques — Information security management systems. (2018). Retrieved 08, 2020, from https://www.iso.org/standard/73906.html

ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems. (2013). Retrieved August 15, 2020, from https://www.iso.org/standard/54534.html

ISO/IEC 27002:2013: Information technology — Security techniques — Code of practice for information security controls. (2013). Retrieved August 15, 2020, from https://www.iso.org/standard/54533.html

ISO/IEC 27005:2018: Information technology — Security techniques — Information security risk management. (2018). Retrieved August 20, 2020, from https://www.iso.org/standard/75281.html

Maruta, R. (2012/10/01). Maximizing Knowledge Work Productivity: A Time Constrained and Activity Visualized PDCA Cycle: A Time Constrained and Activity Visualized PDCA Cycle. Knowledge And Process Management, 19(4), 203-214. https://doi.org/10.1002/kpm.1396

Mates, P., & Smejkal, V. (2012). E-government v České republice: právní a technologické aspekty. Leges.

Metodické doporučení k činnosti obcí k organizačně technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí: Podle právního stavu k 10. sprnu 2017 (2017). Ministerstvo vnitra České republiky. https://www.gdpr.cz/wp-content/uploads/2017/09/Metodick%C3%A9-doporu%C4%8Den%C3%AD-k-%C4%8Dinnosti-obc%C3%AD.pdf

Middleton-Leal, M. (2020). GDPR and ISO 27001 Mapping: Is ISO 27001 Enough for GDPR Compliance?. Netwrix. Retrieved July 17, 2020, from https://blog.netwrix.com/2018/04/26/gdpr-and-iso-27001-mapping-is-iso-27001-enough-for-gdpr-compliance/

Novák, L., & Požár, J. (2014). Systém řízení informační bezpečnosti. In CyberSecurity. cz–Kybernetická bezpečnost [online]. https://www.cybersecurity.cz/data/SRIB.pdf

Nový příkaz z Bruselu: strážce dat v každé vsi. (2017). Retrieved July 20, 2020, from https://www.tyden.cz/rubriky/domaci/novy-prikaz-z-bruselu-strazce-dat-v-kazde-vsi_446982.html

Ochrana osobních údajů: často kladené dotazy. (2020). Ministerstvo Vnitra České Republiky. Retrieved July 20, 2020, from https://www.mvcr.cz/gdpr/clanek/gdpr-informace-casto-kladene-dotazy.aspx

Rohel, V. (2013). Data security management. Dsm Data Security Management, 2013(4). https://doi.org/1211-8737

Ruth, M. (2017). General Data Protection Regulation (GDPR) . Salem Press Encyclopedia. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=ers&AN=125600230&lang=cs&site=eds-live

Shaping a Safer Digital Future: a new Strategy for a new decade: Press Release. (2020). Retrieved July 22, 2020, from https://edps.europa.eu/press-publications/press-news/press-releases/2020/shaping-safer-digital-future-new-strategy-new_en

Smejkal, V. (2018). Kybernetická kriminalita (2. rozšířené a aktualizované vydání). Vydavatelství a nakladatelství Aleš Čeněk.

Special Eurobarometer 487a – March 2019 "The General Data Protection Regulation" Report. (2019). European Union. http://ec.europa.eu/commfrontoffice/publicopinion

Sunshine laws [Online]. (2019). Salem Press Encyclopedia. Retrieved from http://eds.a.ebscohost.com/eds/detail/detail?vid=1&sid=ed4c2f5a-9076-4c69-8fd6-b492db26d996%40sdc-v-sessmgr03&bdata=Jmxhbmc9Y3Mmc2l0ZT1lZHMtbGl2ZQ%3d%3d#AN=102082447&db=ers

Škorničková, M. E. (2019). DPO čili Pověřenec pro ochranu osobních údajů. Retrieved July 21, 2020, from https://www.gdpr.cz/gdpr/dpo/

The EDPS Strategy 2020–2024: Shaping a Safer Digital Future. (2020). European Data Protection Supervisor. https://doi.org/10.2804/124494

THE ISO SURVEY [Online]. (2019). Retrieved November 07, 2019, from https://www.iso.org/the-iso-survey.html

Ukliknutí ‚stálo' nemocnici v Benešově 40 milionů. Kyberútok začal otevřením přílohy. (2020). Lidovky.cz. Retrieved April 22, 2020, from https://www.lidovky.cz/domov/ukliknuti-stalo-nemocnici-v-benesove-40-milionu-kyberutok-zacal-kliknutim-na-prilohu.A200115_201359_ln_domov_vlh

Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti): Národní úřad pro

kybernetickou a informační bezpečnost stanoví podle § 28 odst. 2 písm. a) až d) a f) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb. a zákona č. 205/2017 Sb. Česká republika: Parlament České republiky, Poslanecká sněmovna.

Zákon 104/2017 Sb. kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony, 2017 § (2017). Česká republika: Parlament České republiky, Poslanecká sněmovna.

Zákon 205/2017 Sb. kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony, 205/2017 Sb. § (2017). Česká republika: Parlament České republiky, Poslanecká sněmovna.

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), 2014 § (2014). Parlament České republiky, Poslanecká sněmovna.

Zákon č. 365/2000 Sb. o informačních systémech veřejné správy a o změně některých dalších zákonů, 2000 § (2000). Česká republika: Parlament České republiky, Poslanecká sněmovna,

Zákon č. 365/2000 Sb. o informačních systémech veřejné správy a o změně některých dalších zákonů, 2000 § (2000). Česká republika: Parlament České republiky, Poslanecká sněmovna.

Zákon č. č. 412/2005 S o ochraně utajovaných informací a o bezpečnostní způsobilosti, 2005 § (2005). Česká republika: Parlament České republiky, Poslanecká sněmovna.

Žůrek, J. (2017). Praktický průvodce GDPR (1st ed.). ANAG.

IV. Seznam grafů, tabulek a obrázků

V. Seznam příloh

VI. Přílohy

Dotazník 1

Informace o obci

V této části nejprve získáme informace o vaší obci

Kolik má vaše obec obyvatel? *

- Do 499
- 500-999
- 1000-2000
- nad 2000

Vyberte typ vaší obce *

- obec
- obec s pověřeným obecním úřadem
- obec s rozšířenou působností

Kolik osob pracuje na vašem obecním úřadě? *

- 1-5
- 5-10
- 15-20
- více než 20

Informační bezpečnost

V této sekci nás zajímá stav informační bezpečnosti ve vaší obci

Jaké informační a komunikační prvky (ICT) využíváte na vašem úřadě? *

- [ ] Počítače, notebooky, tablety
- [ ] Telefony
- [ ] E-mail
- [ ] Fax
- [ ] Tiskárny
- [ ] Servery
- [ ] Informační systém
- [ ] Jiná...

Je na vašem úřadě zaměstnána osoba speciálně se zabývající informatikou / informační bezpečností? *

- ○ Ano, na hlavní pracovní poměr
- ○ Ano, externě
- ○ Ne, má ji na starosti běžný zaměstnanec jako část své agendy
- ○ Ne, vůbec

Setkali jste se někdy na vašem úřadě s nějakou z níže uvedených bezpečnostních hrozeb? *

- ☐ Škodlivý software (viry, malware)
- ☐ Podvodné jednání - phising
- ☐ Ransomware (druh škodlivého programu, který blokuje počítačový systém nebo šifruje data v něm zapsan...
- ☐ Záměrný kybernetický útok
- ☐ Vloupání / krádež
- ☐ Jiná...

Provádíte na vašem úřadě analýzu bezpečnostních rizik? *

- ○ Ano, pravidelně
- ○ Ano, občas
- ○ Ne, nikdy, ale máme to v plánu
- ○ Ne, nikdy a nemáme to v plánu

Máte na vašem úřadě nějaký dokument který by se zabýval bezpečnostní politikou? Pokud ano, je dostatečně srozumitelný? *

- ○ Ano a je srozumitelný
- ○ Ano, ale není srozumitelný
- ○ Ne

Je vaše obec certifikována pomocí norem z rodiny ISO 27001?

- ◯ Ano
- ◯ Ne, ale uvažujeme o tom
- ◯ Ne a neuvažujeme o tom
- ◯ Nevím co to je

GDPR

V této sekci nás zajímají informace ohledně zavádění a aplikování Obecného nařízení o ochraně osobních údajů známého také pod anglickou zkratkou GDPR General Data Protection Regulation

Jakým způsobem je ve vaší obci řešena role pověřence pro ochranu osobních údajů? *

- ◯ Je jím stávající pracovník úřadu na hlavní pracovní poměr
- ◯ Byl zaměstnán nový pracovník na hlavní pracovní poměr
- ◯ Byl najmut externí pracovník
- ◯ Tuto roli zajišťuje pracovník sdílený s okolními obcemi
- ◯ Tuto roli jsme ještě neřešili / nemáme ji

Jak finančně náročné bylo pro vaší obec zavedení souladu s GDPR? *

	1	2	3	4	5	6	7	8	9	10	
Málo	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Velmi

Jak časově náročné bylo pro vaší obec zavedení souladu s GDPR? *

	1	2	3	4	5	6	7	8	9	10	
Málo	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Velmi

Ovlivnilo zavedení GDPR činnosti na vašem úřadě? *

	1	2	3	4	5	6	7	8	9	10	
Vůbec	○	○	○	○	○	○	○	○	○	○	Velmi

Jaký vliv mělo zavedení GDPR na činnosti na vašem úřadě / ve vaší obci? *

- ○ Záporný
- ○ Spíše záporný
- ○ Neutrální
- ○ Spíše kladný
- ○ Kladný
- ○ Žádný
- ○ Jiná…

Ohodnoťte povědomí / zájem občanů o GDPR ve vaší obci *

	1	2	3	4	5	6	7	8	9	10	
Nevědí co GDPR je / nezajímá je to	○	○	○	○	○	○	○	○	○	○	Vědí co je GDPR / aktivně se zajímají

Vyjádřete prosím Váš názor na následující tvrzení *

	Souhlasím	Spíše souhlasím	Spíše nesouhla...	Nesouhlasím	Nevím / nemá...
Ochraňovat os...	○	○	○	○	○
Ochrana osobn...	○	○	○	○	○
GDPR je zcela z...	○	○	○	○	○
GDPR je zcela ...	○	○	○	○	○
GDPR mi přiděl...	○	○	○	○	○
GDPR by se ne...	○	○	○	○	○
Stát včas zajist...	○	○	○	○	○