Univerzita Hradec Králové

Fakulta informatiky a managementu

DIPLOMOVÁ PRÁCE

2016 **Ondřej Škeřík**

Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Systém řízení bezpečnosti informací prostřednictvím normy ČSN/EN ISO/IEC 27001

Diplomová práce

Autor: Ondřej Škeřík

Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Pardubice květen 2016

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Pardubicích dne Ondřej Škeřík

Poděkování

Rád bych poděkoval pracovníkům společnosti Mana Consulting s.r.o., za jejich cenné rady, připomínky, náměty a mnoho praktických informací, bez kterých by tato práce v tomto rozsahu nikdy nemohla vzniknout.

Velké díky patří také vedoucímu práce, panu Mgr. Josefovi Janu Horálkovi Ph.D., za ohromnou vstřícnost, velký zájem a zejména neomezenou dostupnost a rychlé odpovědi na všechny mé dotazy.

Vděk cítím také ke všem, kteří se zúčastnili nebo alespoň se pokusili zúčastnit mého dotazníku. Uvědomuji si, že v některých případech jste museli vynaložit dodatečné úsilí v podobě snahy o schvalování vašeho příspěvku vedením organizace.

Na závěr, ale snad nejvíce, bych chtěl poděkovat svému otci, Ing. Jaroslavu Škeříkovi, za ohromnou trpělivost při vysvětlování různých souvislostí, za celkovou podporu, ale také za pomoc při slohové korekci textu.

V následujícím textu je i ohromný kus vaší práce. Všem vám za ni děkuji!

Anotace

Cílem práce je představit normu ČSN/EN ISO/IEC 27001. Vysvětlit okolnosti a důvody jejího vzniku, jejího vztahu k informační bezpečnosti a vztahu k legislativě České republiky, zejména zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejících prováděcích právních předpisů (vyhlášek a vládních nařízení). Představena bude struktura normy, popsány jednotlivé části, postup implementace a certifikace a na závěr budou představeny také alternativy a doplňky.

V praktické části autor ukáže některé z důležitých dokumentů normy ČSN/EN ISO/IEC 27001 na třech modelových organizacích různého typu a zhodnotí rozdíly při zavádění normy mezi různé typy organizací. Součástí této části bude také získávání informací pomocí průzkumu dotazníkovou formou.

Annotation

Title: Information Security Management System via Standard ČSN/EN ISO/IEC 27001

The goal is to introduce standard ČSN/EN ISO/IEC 27001 and explain circumstances and reasons for its establishment, explain relationship to information security and relationship to the Czech legislation, especially Act no. 181/2014 Coll. about cybersecurity and related implementing legislation (decrees and goverment regulations). There will be introduced the structure of this ISO standard, implementation procedure, certification and also alternatives and supplements.

In the practical part, author reveals some important documents of ČSN/EN ISO/IEC 27001 standard on three virtual organizations of various types. He will evaluate differences in the implementation of standard between these organizations. Part of this section is gathering informations through a survey questionnaire form.

Obsah

1. Úvod

Cílem práce je představení normy ISO/IEC 27001. Pro vytvoření uceleného obrazu jejího kontextu a významu se bude autor v textu věnovat okolnostem jejího vzniku, procesu certifikace a aplikace do organizace, vztahu k právním požadavkům České republiky, vztahu k připravované legislativě Evropské unie a také vztahu s jinými normami a postupy pro zvýšení informační bezpečnosti.

Prvním cílem práce je představit nejdůležitější části normy a identifikovat a zhodnotit dílčí rozdíly při aplikaci normy na různé typy organizací. Díky spolupráci se zástupci společnosti Mana Consulting s.r.o., která má na poli zavádění politik normy mnohaleté zkušenosti, může býti k tomuto úkolu využito více přístupů.

Autor vytvoří tři virtuální modelové organizace, jejichž parametry budou podobné organizacím z běžné praxe. Pro tyto modelové organizace bude vytvořeno několik dokumentů tak, jak požaduje norma. Identifikace rozdílu proběhne porovnáním těchto dokumentů.

Druhý přístup bude založen na praktickém výzkumu. Autor vytvoří dotazník a osloví zástupce organizací, u kterých předpokládá zkušenosti s normou ISO 27001. Lze očekávat, že nalézt tyto organizace a především správné a ochotné zaměstnance, stejně tak jako vůli se o své zkušenosti podělit, bude obtížné. Autor však doufám v alespoň desítku získaných odpovědí, ze kterých se pokusí vyvodit relevantní závěry.

Poslední způsob zhodnocení rozdílu bude interpretace informací a názorů získaných od zástupců poradenské společnosti Mana Consulting s.r.o. Očekává se, že tyto tři přístupy dohromady vytvoří ucelený zajímavý pohled na problematiku bezpečnosti informací v souvislosti s normou ISO 27001 v České republice.

Protože má norma silnou souvislost s právní legislativou České republiky, bude také představen kybernetický zákon. V práci budou uvedeny důvody vzniku, vztah s normou a soulad s požadavky Evropské unie.

2. Teorie informační bezpečnosti

2.1. Definice pojmů

Pro správné pochopení pojmu informační bezpečnost, resp. bezpečnost informací, je nutné nejprve samostatně rozebrat obě složky tohoto spojení. Začněme tedy s tím, co chápeme pod pojmem informace.

2.1.1. Informace

Je důležité si uvědomit, že chápání pojmu informace může být hodně subjektivní. Obecně jej můžeme shrnout jako údaj o prostředí, který svojí existencí snižuje entropii (míru neurčitosti) takového prostředí. Množství informace je pak možné vnímat jako rozdíl entropie prostředí mezi stavy před a po přijetí informace. Jinými slovy lze říci, že informace je údaj o prostředí, jeho stavu, struktuře a procesech v něm probíhajících.

V běžném životě je informace považována za znalost, kterou lze předávat, případně za obsah sdělení. Tomu ostatně odpovídá také normativní výklad pojmu informace podle normy ČSN ISO 5127-2003 (Informace a dokumentace – slovník), který informaci definuje jako sdělování znalosti při procesu komunikace s cílem zvýšení znalostí.

Pro potřeby kybernetických systémů je však vhodnější rozvinout původní obecnou definici. Z technického pohledu tedy informaci chápeme jako vlastnost objektu nebo systému, vyjadřující jeho strukturu, fixovanou ve znakové podobě na fyzickém nebo elektronickém nosiči (Databáze národní knihovny ČR, 2014).

2.1.2. Data

Pro výklad ve smyslu informační bezpečnosti je nutné pojem informace dále upřesnit. Informaci zde chápeme jako data (vybrané či jinak zpracované údaje) ve snadno čitelné formě a pochopitelné pro subjekt, kterému jsou určeny. Mohou se vyskytovat v elektronické nebo listinné formě, být vyřčené či zaznamenané na jiném médiu (CyberSecurity.cz, 2015).

2.1.3. Informační aktiva

Informace a data lze souhrnně sdružit do pojmu informační aktivum, přičemž aktivum je definováno jako cokoliv, co má pro organizaci nějakou hodnotu (Robert Gogela, 2015).

Informační aktiva se dělí na primární a podpůrná. Za primární jsou považovány informace samotné, zatímco podpůrná aktiva zahrnují všechny prostředky na uložení, zpracování a zabezpečení primárních aktiv. Podpůrná aktiva tedy zahrnují také:

- prostory v nichž se primární aktiva nacházejí,
- technologie, které slouží k uchování, zpracování a zabezpečení primárních aktiv,
- lidské zdroje, které s primárními aktivy pracují nebo přicházejí do styku.

2.1.4. Informační/kybernetická bezpečnost

Definicí pojmu bezpečnost existuje celá řada. Může se vztahovat k ekonomice, sociologii atd. Obecně lze bezpečnost definovat jako schopnost systému nebo jeho částí odolávat vnějším i vnitřním hrozbám, které na něj mohou působit (Ministerstvo vnitra ČR, 2015). Z informačního pohledu lze říci, že je to schopnost systému zachovat si atributy popsané níže v této kapitole, tedy důvěrnost, integritu, dostupnost a spolehlivost (ČSN ISO/IEC 27000, 2014, s. 11).

Tím se dostáváme k samotné definici pojmu informační bezpečnost, resp. bezpečnost informací. Setkat se lze také s výrazem kybernetická bezpečnost. Těmito pojmy rozumíme odvětví výpočetní techniky, které se zabývá ochranou zejména počítačových systémů a sítí, z pohledu funkčního i majetkového, před odcizením, korupcí nebo jiným nepředvídatelným nežádoucím působením vnějších i vnitřních jevům. Cílem je zachovat dostupnost, zamezit ztrátě důvěrnosti, integrity a spolehlivosti, tj. uchovat informační systémy dostupné a bez nežádoucích změn podle požadavků jejich uživatelů (CyberSecurity.cz, 2015).

2.1.5. Hrozba

Hrozba je potencionální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva (Vyhláška o kybernetické bezpečnosti č. 316/2014 Sb., 2014).

Hrozbou tedy rozumíme každé nežádoucí působení na aktiva, které může způsobit poškození, zneužití nebo nedostupnost aktiva. V případě kybernetické bezpečnosti je možné sledovat hrozby působící na primární aktiva zejména prostřednictvím podpůrných informačních procesů. Chráněná primární aktiva (informace) jsou zpravidla cílem působením hrozeb, protože mají svoji cenu. Prostředkem pro odvrácení hrozeb se stávají podpůrná aktiva (prostory, technologie a lidé).

Systémy podpůrných aktiv, které přicházejí do kontaktu s primárními aktivy, bývají obvykle složité a nedokonalé. Zahrnují řadu slabých míst, tzv. zranitelností. Ty mohou být zneužity hrozbami k poškození primárního aktiva.

Z pohledu příčiny, resp. druhu využití podpůrných aktiv, lze hrozby členit následujícím způsobem:

- přírodní hrozby, např. povodně, zemětřesení nebo různé klimatické jevy,
- technické hrozby, např. selhání hardwaru nebo softwaru, poruchy podpůrných zařízení technologického charakteru, přerušení dodávky

komunikačních služeb nebo energií, škodlivé kódy jako viry, spyware, trojské koně, apod.,

- společenské a organizační hrozby, např.: kybernetický útok z vnější komunikační sítě, zneužití vnitřních prostředků, sabotáž, zneužití identity jiné osoby, odcizení nebo poškození fyzického zařízení, pochybení ze strany zaměstnanců, nedodržení nebo zneužití pravidel, odpovědností, smluvních závazků, aj.,
- APT (Advanced Persistent Threat) hrozby, které mohou být také označeny jako „trvale (dlouhodobě) působící pokročilé hrozby“. Tyto hrozby kombinují technické, společenské i organizační prostředky a bývají dlouhodobě připravovány.

2.1.6. Zranitelnost

Zranitelnost je slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami (Vyhláška o kybernetické bezpečnosti č. 316/2014 Sb., 2014).

Jak je uvedeno v předchozí kapitole, podpůrná aktiva (prostory, technologie a lidé) zpravidla vytvářejí poměrně složité struktury a systémy pro uchování a zpracování primárních aktiv (informací). Existuje tedy zpravidla mnoho vzájemně působících technických prvků a lidských faktorů, které vytvářejí množství příležitostí pro hrozby k zneužití nebo poškození aktiva. Tyto příležitosti představují slabá místa, tedy zranitelnosti, v systému zabezpečení informací.

Úroveň bezpečnost informací je dána soustavnou schopností vyhledávat a odstraňovat slabá místa v řetězcích souvisejících podpůrných aktiv, která by mohla být zneužita hrozbami.

Zranitelnost vzniká v místech působnosti podpůrných aktiv, kde chybí organizační nebo technické opatření proti hrozbám nebo kde je takové opatření nedostatečně účinné.

2.1.7. Riziko

Rizikem se rozumí možnost, že určitá hrozba využije zranitelnosti informačního systému a způsobí poškození aktiva (Vyhláška o kybernetické bezpečnosti č. 316/2014 Sb., 2014).

Z definice rizika je zřejmé, že samotná hrozba nemusí být pro aktivum nebezpečná, pokud neexistuje hrozba. Jestliže nějaká hrozba existuje, může se uplatnit pouze tehdy, pokud existuje zranitelnost aktiva vůči takové hrozbě. Tento stav je pak označován jako riziko. Například hrozba kybernetického útoku z vnější sítě není rizikem vzhledem k zařízením, která nejsou k vnější síti napojena. V případě připojení k vnější síti je riziko závisle na existenci všech zranitelností souvisejících s takovým připojením.

2.1.8. Bezpečnostní incident

Vyhláška o kybernetické bezpečnosti č. 316/2014 Sb. neobsahuje přímou definici pojmu bezpečnostní incident. Server Management Mania jej definuje jako „pojem označující nějakou nestandardní či nepříjemnou bezpečnostní událost, která vede k narušení pravidel bezpečnosti v organizaci“ (Management Mania, 2016).

V praxi obecně bezpečnostní incident chápeme jako nežádoucí událost, která znamená, že určitá hrozba skutečně využila zranitelnost informačního aktiva a způsobila negativní dopad na aktivum.

Incidenty lze dělit podle příčiny na:

- způsobené kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo omezení dostupnosti služeb,
- způsobené škodlivým kódem,
- způsobené překonáním technických opatření,
- způsobené porušením organizačních opatření,

- spojený s projevem trvale působících hrozeb,
- ostatní bezpečnostní incidenty způsobené kybernetickým útokem.

Nebo podle dopadu na incidenty:

- způsobující narušení důvěrnosti aktiv,
- způsobující narušení integrity aktiv,
- způsobující narušení dostupnosti aktiv,
- způsobující kombinaci dopadů výše uvedených.

(Vyhláška o kybernetické bezpečnosti č. 316/2014 Sb., 2014.)

2.1.9. Příklad hrozby a souvisejících zranitelností

Primární informační aktivum: elektronická nabídka k veřejné zakázce.

Hrozba: únik obsahu nabídek.

Riziko: zneužití znalosti obsahu nabídky konkurenční společnosti nebo společností ke zvýšení šance na vítězství jiné nebo jiných společností, které spolu soutěží o vítězství ve stejné veřejné zakázce.

Stanovaná bezpečnostní opatření:

- zadavatel stanovil politiku (pravidla) pro zpracování a zasílání nabídek,
- zadavatel vzdělává zaměstnance v oblasti bezpečného používání informací,
- zadavatel provádí pravidelné kontroly v průběhu zpracování a předání nabídky,
- zadavatel stanovil povinnost použití zabezpečených komunikačních kanálů a bezpečných způsobů přepravy dokumentů s nabídkami zakázek,
- zadavatel stanovil povinnost zašifrování obsahu nabídky a její ochránění heslem.

Zranitelnosti:

- nedodržení bezpečnostní politiky ze strany zaměstnanců,
- obsah zakázky není zašifrován nebo zaheslován,
- k zašifrování nebo zaheslování obsahu je použito slabého algoritmu nebo hesla,
- předepsané kontroly nejsou pravidelně prováděny,
- do prostor, kde se nachází chráněný dokument, mají před jeho odesláním přístup zaměstnanci dodavatelů (např. uklízecí firma),
- aplikace pro zpracování nabídek je napadena škodlivým softwarem,
- zaměstnanec pro zpracování nabídky vykazuje korupční jednání,
- outsourcer služeb informačních technologií má administrátorský vzdálený přístup, apod.

Z uvedeného příkladu je zřejmé, že i když byl vytvořen zdánlivě účinný soubor organizačních i technických opatření, existuje řada významných zranitelností. Výsledná bezpečnost primárního informačního aktiva je vždy určena nejslabším místem v systému zabezpečení podpůrných aktiv. Úroveň zabezpečení je dána schopností odhalit slabá místa, která mohou být zneužita i přes zdánlivě silný systém běžně aplikovaných opatření.

Obrázek 1: diagram pojmů a jejich vztahů

2.2. Standardy informační bezpečnosti

2.2.1. Vývoj

S rozvojem počítačových systémů na konci osmdesátých a počátku devadesátých let vznikla potřeba reagovat na nové technologie a hrozby, které tento vývoj přinesl. Centrum počítačové bezpečnosti (Commercial Computer Security Centre) oddělení obchodu a průmyslu vlády Spojeného království (United Kingdom Goverment's Department of Trade and Industry) bylo pověřeno se touto problematikou zabývat. Cílem bylo vytvořit hodnotící kritéria bezpečnosti informačních systémů a soubor správných bezpečnostních postupů pro tvorbu a správu takových systémů.

Hodnotící kritéria vznikla jako dokument s označením ITSEC (Information Technology Security Evaluation Criteria), který vyšel v roce 1991. Tyto kritéria následně přijala za své řada dalších evropských zemí a později se z nich stala norma ISO/IEC 15408, Informační technologie – Bezpečnostní techniky – Hodnotící kritéria pro zabezpečení informačních technologií (Information technology – Security techniques – Evaluation criteria for IT security), známa také pod označením Common Criteria (zkrácené označení celého názvu Common Criteria for Information Technology Security Evaluation).

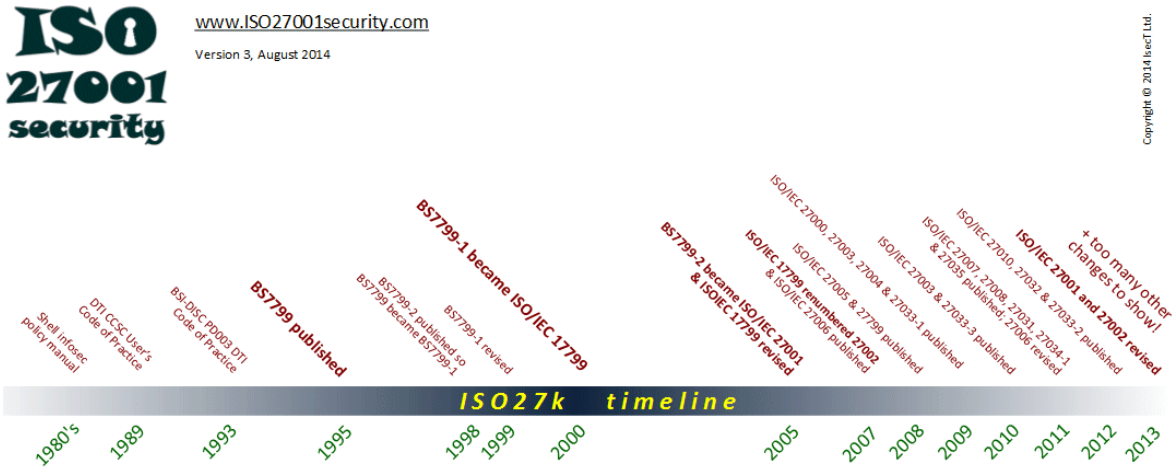
Soubor bezpečnostních postupů vznikl jako dokument s označením BSI-DISC-PD003 (British Standards Insitution – Delivering Information Solutions to Customers – Public Document) v roce 1993. Později jeho správu převzala britská instituce pro standardy BSI a roku 1995 dokument začala vydávat pod označením BS7799.

Poté se v roce 1998 vývoj standardu rozdělil do dvou dokumentů, prvního BS7799-1 (Code of Practice for Information Security Management) jako pokračování původní normy BS7799, a druhého BS7799-2 (Information Security Management Systems – Specification with guidance for use), známého také pod zkratkou ISMS.

První norma BS7799-1 byla v roce 2000 označena mezinárodní organizací pro standardizaci jako ISO/IEC 17799, Informační technologie – Bezpečnostní techniky –

Soubor postupů pro management bezpečnosti informací (Information technology – Security techniques – Code of Practice for Information Security Management) a později v roce 2007 přeznačena na ISO/IEC 27002. Její obsah zůstal při přeznačení beze změny zachován.

Druhá norma BS7799-2 byla rozšířena v roce 2002, mimo jiné o známý „Plan-Do-Check-Act“ cyklus, a přijata jako mezinárodní norma s označením ISO/IEC 27001, Informační technologie, Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky (Information technology – Security techniques – Information security management systems – Requirements) v roce 2005.



Obrázek 2: vývoj normy ISO 27001 [8]

Uvedení původní normy BS, ze kterých současné ISO/IEC normy vycházejí, není jen věcí historického charakteru. Při porovnání britských norem s těmi současnými se ukazuje značná míra podobnosti a souladu. Jinými slovy, tyto normy prošly za více jak 20 let vývoje pouze změnami evolučního charakteru. Důvodem je vysoká míra systémového charakteru původních norem. Tato skutečnost demonstruje, jak kvalitní dokumenty tehdy ve Velké Británii vznikly. Ještě více uznání si zaslouží, pokud si uvědomíme, jakým překotným vývojem prošlo prostředí informačních technologií od doby prvních pokusů o normalizaci informační bezpečnosti. Přestože tehdy byla rychlost a směr vývoje IT odvětví jen těžce předvídatelná, vznikly standardy, které se pouze s formálními obměnami používají dodnes.

2.2.2. Současnost

Výše zmíněné platné mezinárodní normy pod hlavičkami organizací ISO (International Organization for Standardization) a EIC (International Electrotechnical Commission) přijala celá řada zemí po celém světě a v mnoha z nich z těchto původně britských norem vychází současně platné zákony a vyhlášky o bezpečnosti informací. Česká Republika je jednou z nich.

Pro ověření, zda organizace splňují politiky předepsané v mezinárodních ISO/IEC normách, vznikla mezinárodní asociace IQnet. Jedná se o síť certifikačních autorit působících v různých zemích. Její členové jsou oprávněni vydávat certifikáty o splnění podmínek příslušných norem. Více o certifikátech a certifikačním procesu pojednává kapitola 4.3.2.

Obrázek 3: počet udělených certifikací ISO 27001 v jednotlivých zemích [41]

Dnes máme pro řízení informačních systémů k dispozici celou rodinu norem ISO/IEC 27000. Následující tabulka uvádí kompletní výčet (včetně těch připravovaných, které jsou označeny kurzívou) a krátké shrnutí jejich účelu a významu.

Tabulka 1: rodina norem ISO 27000

Označení	**Stručný popis**
ISO 27000	Terminologický slovník pro ostatní normy s rodiny 27000.
ISO 27001	Hlavní norma systému řízení bezpečnosti informací (ISMS). Je návodem pro organizace, jak postupovat při implementaci bezpečnostní politiky.
ISO 27002	Norma určena zejména certifikačním autoritám, které podle ní postupují při udělování certifikaci.
ISO 27003	Návod jak implementovat ostatní normy rodiny 27000.
ISO 27004	Pomůcka k měření a prezentaci efektivity systému řízení bezpečnosti informací (ISMS).
ISO 27005	Doporučení a techniky pro analýzu informačních rizik.
ISO 27006	Rozšiřuje a doplňuje požadavky obsažené v normě ISO 27001, aby byl zajištěn soulad s normou ISO 17021 (požadavky na certifikační orgány provádějící audity systémů řízení).
ISO 27007	Sada doporučení k provádění auditů podle normy ISO 27001 pro zajištění souladu s normou ISO 19011 (směrnice pro audity systému managementu jakosti a systému environmentálního managementu).
ISO 27008	Doporučení pro auditory kontrolující implementaci ISMS podle normy ISO 27002.
ISO 27009	*Norma bude definovat požadavky používání ISO 27001 ve specifických odvětvích. Cílovou skupinou této normy jsou subjekty produkující normy specifické pro určité odvětví, které se zároveň vztahují k normě ISO 27001.*
ISO 27010	Doporučení jak sdílet informace mezi více organizacemi nebo státy.
ISO 27011	Norma určená speciálně pro zavádění systému řízení bezpečnosti informací (ISMS) u telekomunikačních operátorů.
~~*ISO 27012*~~	Norma měla poskytovat doporučení pro přijetí procesů a opatření z normy ISO 27002 v oblasti státní správy. Práce však byly v roce 2009 ukončeny zejména díky vyjádření národních subjektů ve smyslu, že stačí současné normy ISO 27001 a ISO 27002 a není proto nutné k tomuto účelu vytvářet normu specializovanou.

ISO 27013	Doporučení pro realizaci jednotné informační bezpečnosti a systému pro řízení IT služeb založené na standardech ISO 27001 a ISO 20000.
ISO 27014	Doporučení pro správu bezpečnosti informací (Governance of information security).
ISO 27015	Rozšíření normy ISO TR 13569 (Banking Information Security Guildlines) pro finanční instituce, aby obsahovala doporučení z norem ISO 27001 a ISO 27002.
ISO 27016	Publikována ve formě technické zprávy (Technical Report), která má pomoci managementu ocenit a pochopit finanční dopad informační bezpečnosti na organizaci.
ISO 27017	*Doplnění pro již vydanou normu 27018, kterou budou rozšiřovat o téma bezpečnosti informací v cloud computingu.*
ISO 27018	Doporučení pro provozovatele cloudových služeb ohledně ochrany osobních údajů jejich klientů.
ISO 27019	Publikována ve formě technické zprávy (Technical Report), která má pomoci organizacím z energetického průmyslu aplikovat normu ISO 27002.
ISO 27023	Publikována ve formě technické zprávy (Technical Report), která měla být původně pouze pro interní potřeby ISO/IEC. Cílem je mapovat rozdíly mezi jednotlivými verzemi norem ISO 27001 a ISO 27002.
ISO 27031	Norma popisuje koncept a principy přípravy informačních a komunikačních technologií na mimořádné události.
ISO 27032	Doporučení ohledně kybernetické bezpečnosti mimo běžnou informační infrastrukturu. Poskytuje řešení pro sdílení informací a koordinaci řízení incidentů mezi organizacemi nebo vládami.
ISO 27033	Doporučení pro implementaci protiopatření v oblasti bezpečnosti sítí. Odvozena ze standardu ISO 18028 (IT network security).
ISO 27034	Doporučení pro tvorbu, implementaci a užívání softwaru. Prozatím k dispozici pouze první část (ISO 27034-1).
ISO 27035	Norma zaměřená na řízení incidentů bezpečnosti informací (přeznačena z ISO 18044 v roce 2004).

ISO 27036	Řeší hodnocení a snižování rizik ve vztahu k pořizování zboží a služeb od dodavatelů. Zahrnuje například outsourcing nebo cloudové služby.
ISO 27037	Doporučení pro shromažďování a ochranu digitálních soudních důkazů, zejména ve smyslu sdílení na mezinárodní úrovni.
ISO 27038	Doporučení pro správu a publikaci digitálních dokumentů.
ISO 27039	*Doporučení ohledně zavedení systémů pro odhalení a prevenci nežádoucích aktivit v počítačových sítích, tzv. IDPS (Intrusion Detection and Prevention System) systémů.*
ISO 27040	*Doporučení pro bezpečné ukládání dat.*
ISO 27041	*Doporučení pro zajištění digitálních důkazních materiálů.*
ISO 27042	*Doporučení pro zajištění a analýzu digitálních důkazních materiálů.*
ISO 27043	*Doporučení a postupy pro vyšetřování digitálních důkazních materiálů.*
ISO 27044	*Doporučení a implementace řízení bezpečnosti informací a událostí SIEM (Security Information and Event Management) v rámci systému řízení bezpečnosti informací (ISMS).*
ISO 27050	*Pod tímto označením by měl vyjít soubor norem řešící problematiku elektronických stopování, uchovávání stop v elektronickém formátu ESI (Electronically Stored Information) a jejich výměnou mezi organizacemi nebo státy. Navazuje na normy z rodiny ISO 27000 týkajících se digitálních důkazních materiálů.*
ISO 27799	Doporučení a seznam nejlepších praktik pro implementaci ISO 27002 v oblasti zdravotnictví.

Rozsah celé rodiny norem ISO 27000 je možné shlédnout online v přehledném grafickém provedení včetně roku posledního vydání na internetové adrese http://www.rac.cz/rac/homepage.nsf/CZ/ISO27000/$FILE/Family%2027000%20150421.png (odkaz ze dne 2. 10. 2015).

2.2.3. Česká Republika

O normy v České republice se stará Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Označují se zkratkou ČSN a číselným kódem. Normám převzatým se označení zachovává, pouze se na začátek přidá právě označení ČSN. V případě zmiňovaných norem je to např.: ČSN ISO/IEC 27001.

Normy takto označené jsou přeložené do českého jazyka. Oficiální autority (např. při certifikaci) mohou postupovat pouze podle norem ČSN, tedy norem v češtině. Když vyjde aktualizace normy ISO/EIC, certifikační autorita operující na území České republiky nemůže s touto aktualizací pracovat, dokud není přeložena. Z toho plyne určité zpoždění v zavádění úprav mezinárodních norem. Po vydání a přeložení nové verze normy je možné postupovat podle předchozí verze po dobu jednoho roku od uvedení nového vydání.

Jak již bylo zmíněno, certifikaci norem zaštiťuje asociace IQnet. Českým zástupcem v této asociaci je od roku 1998 Sdružení pro certifikaci systémů jakosti CQS (Association for Quality System Certification). Bylo založeno v roce 1993 a dnes zastřešuje několik organizací provádějících zkoušky a certifikace na území České republiky, jako je např. Elektrotechnický zkušební ústav (EZÚ). Těmto organizacím vydává akreditaci k provádění certifikací Český institut pro akreditaci (ČIA).

Bezpečnosti informací v České republice se mimo norem věnují také právní úpravy. Jak bylo již dříve zmíněno, v současnosti jsou právní úpravy v České republice do značené míry odvozené právě od zmiňovaných britských a později mezinárodních norem (více informací viz kapitola 5).

Demonstrací budiž § 29 vyhlášky o kybernetické bezpečnosti č. 316/2014 Sb. k zákonu o kybernetické bezpečnosti č. 181/2014 Sb., který praví: „Orgán a osoba..., jejíž informační systém..., který byl certifikován podle příslušné technické normy[1)] akreditovaným certifikačním orgánem..., splňuje požadavky na zavedení bezpečnostních opatření podle zákona a této vyhlášky.“

Jinými slovy, pokud organizace získá certifikaci ISMS podle normy ISO/IEC 27001 a povede potřebnou dokumentaci (která je ve zmíněné vyhlášce vymezena, ale pro zkrácení v rámci přehlednosti byl tento úsek z citace výše vyňat), automaticky splňuje kybernetický zákon. Norma ISO/IEC 27001 tedy poskytuje téměř kompletní návod, jak vyhovět zákonným požadavkům České republiky na bezpečnost informací.

Kromě zákona o kybernetické bezpečnosti funguje v České republice od roku 2014 Národní centrum kybernetické bezpečnosti (NCKB), které vzniklo jako součást usnesení vlády č. 781 z roku 2011. Úlohou centra je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetických útoků i návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům. Přijaté usnesení č. 781 mimo jiné ustanovuje Národní bezpečnostní úřad gestorem pro problematiku kybernetické bezpečnosti a zároveň národní autoritou v této oblasti pro Českou republiku. NCKB je také spolu s Ministerstvem vnitra oprávněn upravovat vyhlášku č. 316/2014 Sb., o kybernetické bezpečnosti (Národní centrum kybernetické bezpečnosti a CyberSecurity.cz, 2015)

2.3. Požadavky na bezpečnost informací

Cílem požadavků na bezpečnost informací je stanovit základní parametry informačních aktiv pro zachování jejich důvěrnosti, dostupnosti, integrity a spolehlivosti, viz kapitola 2.5. Tyto požadavky lze vnímat ve třech rovinách.

První je rovina právní, kde státní orgán zákonem stanoví, které informace je nutné chránit, jak je chránit, kdo je povinen je takto chránit a proti čemu je chránit. Jedná se o minimum, které musí každá organizace dodržet při provádění své činnosti, pokud se jí zákon týká.

Druhou rovinu představují normy, které vydávají doporučení pro co nejlepší výsledky v oblasti, kterou postihují.

Poslední rovinou jsou požadavky samotné organizace, které mohou být vyšší než minimální požadavky právní nebo doporučené požadavky norem.

2.3.1. Legislativní požadavky

V České republice se této problematice věnuje již dříve zmíněný zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Ten říká, jak je potřeba informace chránit a určuje, které organizace tak musí činit. K tomuto účelu vymezuje pojmy kritická infrastruktura a významný informační systém. Jejich definice však samotný zákon neřeší. Věnují se jí až vyhlášky č. 315/2014 Sb. o kritériích pro určení prvku kritické infrastruktury a č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích. Lze tedy zjednodušeně říci, že zákon stanoví jak informace chránit a vyhlášky kdo je povinen tak činit.

Jaké informace pod tuto ochranu spadají samotný zákon o kybernetické bezpečnosti ani jeho přidružené vyhlášky neřeší. Tento úděl plní celá řada dalších zákonů, jako např. zákon č. 101/2000 Sb. o ochraně osobních údajů.

2.3.2. Normativní požadavky

Normy jsou výsledkem zkušeností z praxe, napsané zpravidla jako soubor doporučení, které byly přijaty širokou odbornou komunitou. Rodina norem ISO/IEC 27000 se ve velké míře zaměřuje na systémy řízení rizik ISMS (Information Security Management System), které pomáhají organizacím nalézt přijatelnou ochranu v kontrastu s akceptovatelnými náklady na zavedení a provoz daných bezpečnostních opatření.

Pro tyto normy je důležitá možnost certifikace jejich úspěšné aplikace do prostředí organizace. Společnost, která se může prokázat mezinárodním certifikátem, se stává potenciálně spolehlivým partnerem, se kterým je možné sdílet citlivé informace.

V České republice je výhodou této certifikace splnění většiny právních požadavků daných zákonem č. 181/2014 Sb., o kybernetické bezpečnosti.

ISO normy však nejsou jedinými normami, které se používají pro zajištění bezpečnosti informací. Jmenovat lze například normu pro standardy kategorizace informací FIPS PUB 199 (Federal Information Processing Standards Publication), normu pro minimální požadavky na bezpečnost informací FIPS PUB 200 nebo normu pro posuzování, výběr a implementaci bezpečnostních opatření NIST SP 800 (National Institute of Standards and Technology Special Publication). Tyto tři normy jsou platné v USA, kde platí souběžně s normami ISO/IEC. Dalšími alternativami se více zabývá kapitola 6.

2.3.3. Interní požadavky

Systém řízení rizik je nástrojem pro organizace, který porovnává zranitelnost určitých informačních aktiv a dopady jejich případné korupce. Na jedné straně máme odhadnutou pravděpodobnost vzniku incidentu a na druhé finančně vyjádřeny náklady spojené s řešením následků incidentu (pokuty, právní spory, náklady na obnovení provozu atd.). Takto získáme míru rizika, které daný incident představuje. Podle něho lze pak navrhovat nákladově adekvátní bezpečnostní opatření.

Existují však i další ukazatele poškození, např. ztráta důvěry zákazníků, obchodních partnerů nebo dobrého jména společnosti. Proto organizace si může určitá informační aktiva cenit více a požadavky na jejich bezpečnost mít vyšší, než určuje platná legislativa nebo doporučují normy.

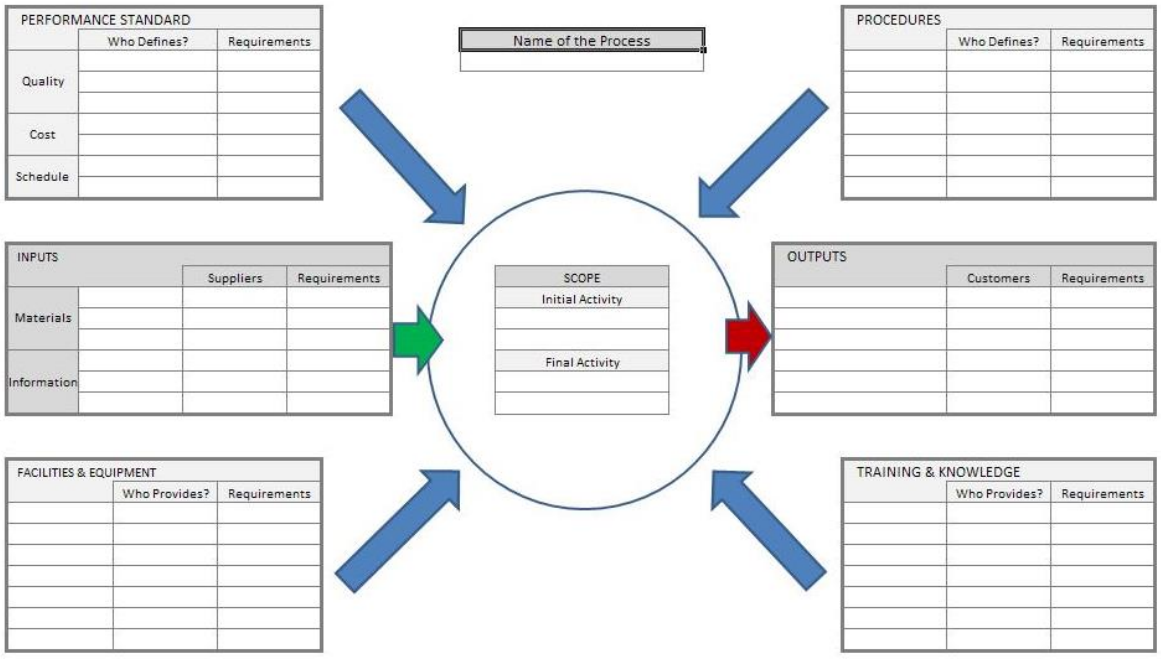
2.4. Systémy řízení informační bezpečnosti

Řízení bezpečnosti informací se obyčejně uvádí zkratkou ISMS (Information Security Management Systems). Jedná se o systém, který má za cíl ustavit, zavést, provozovat, monitorovat, udržovat a zlepšovat bezpečnosti informačních aktiv.

Nástrojů, které nám mohou pomoci s tímto úkolem, je celá řada. V textu již byla mnohokrát zmíněna norma ISO/IEC 27001. Dále máme k dispozici standard ISO/IEC

20000 pro management služeb se zaměřením na zlepšování kvality, snižování nákladů a zvyšování efektivity IT procesů. Zapomínat bychom neměli ani na knihovnu ITIL (Information Technology Infrastructure Library), která vychází z nejlepších praktických zkušeností a je považována za mezinárodní standard pro oblast řízení IT služeb ITSM (Information Technology Service Management). Více o knihovně ITIL a dalších podobných dokumentech pojednává kapitola 6.

Klíčovým nástrojem pro řízení bezpečnosti informací je Demingův model, známý zejména pod zkratkou PDCA (Plan, Do, Check, Act). Jedná se o systém nekončící smyčky plánování, provedení, kontroly a vyhodnocení, který management organizace aplikuje na informační systémy. Tento model nás učí, že zavádění, vyhodnocování a zlepšování systémů není jednorázová událost, ale nekonečný koloběh, kterým systémy zůstávají aktuální s vývojem informačních technologií v čase. Tento model je často prezentován pomocí tzv. želvího diagramu.



Obrázek 4: příklad želvího diagramu [34]

Abychom mohli PDCA cyklus využít, potřebujeme nejprve popsat všechna aktiva organizace, kterých se informační bezpečnost má týkat. Dalším krokem je provedení ohodnocení těchto aktiv. Každá organizace si ohodnocuje svá aktiva sama podle vlastních potřeb nebo za pomoci k tomu účelu vytvořené normy ISO/IEC 13335,

resp. jejího nástupce ISO/IEC 27005 – „Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací“. Tato norma poskytuje doporučení pro řízení rizik bezpečnosti informací v rámci organizace, podporuje obecný koncept specifikovaný v ISO/IEC 27001 a je strukturována, aby dostatečně podporovala implementaci informační bezpečnosti založené na přístupu řízení rizik. Systém řízení rizik je též nedílnou součástí normy ISO 27001, viz kapitola. 3.3.

Analýza rizik má za úkol na základě pravděpodobnosti výskytu incidentu a míry jeho dopadu na organizaci najít největší potenciální nebezpečí pro organizaci. S takto vzniklým seznamem rizik a jednotlivých aktiv můžeme vstoupit do PDCA cyklu, začít plánovat, realizovat a vyhodnocovat nápravná opatření. Více o analýze rizik pojednává kapitola 4.2.3.

2.5. Struktura požadavků na informační bezpečnost

Aby informace byla považována za zabezpečenou, musí splňovat zejména podmínky důvěrnosti, integrity a dostupnosti. Může však také zahrnovat podmínky autenticity, nepopiratelnosti a spolehlivosti (ČSN ISO/IEC 27000, 2014, s. 11).

Důvěrnost: zajištění, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům (ČSN ISO/IEC 27000, 2014, s. 9).

Integrita: zajištění správnosti, přesnosti a úplnosti informace (ČSN ISO/IEC 27000, 2014, s. 11).

Dostupnost: zajištění přístupnosti a použitelnosti na žádost oprávněné entity (ČSN ISO/IEC 27000, 2014, s. 8).

Spolehlivost: zajištění souladu mezi zamýšleným chováním a výsledky (ČSN ISO/IEC 27000, 2014, s. 14).

Autenticita: zajištění ověření identity entity (ČSN ISO/IEC 27000, 2014, s. 8).

Nepopiratelnost: zajištění schopnosti prokázat výskyt údajné události nebo činnosti entit, které je vyvolaly (ČSN ISO/IEC 27000, 2014, s. 13).

Autenticita a nepopiratelnost se v některých případech považují za součást spolehlivosti. Tedy pokud se mluví o zajištění spolehlivosti dat, rozumí se tím zajištění i autenticity a nepopiratelnosti.

2.6. Praktické možnosti realizace informační bezpečnosti

Zajištění výše uvedených podmínek pro všechny zpracovávané informace je v reálném provozu zpravidla velmi náročný a drahý proces. Protože v praxi jsou na různé skupiny informací kladeny rozdílné požadavky, organizace zavádí klasifikaci těchto informací dle požadavků na zachování jejich důvěrnosti, dostupnosti, integrity a spolehlivosti. Zavedení klasifikace informací z pohledu udržení základních požadavků na informace (důvěrnost, dostupnost, integrita, spolehlivost) má velký praktický význam i dopad. Soubory organizačních opatření (pravidel) i technických opatření (technologií) je možné členit a drahá nebo jinak náročná opatření je možné uplatňovat pouze pro omezený rozsah informací.

V případě důvěrnosti a dostupnosti informací bývají požadavky značně odlišné pro různé agendy. Proto dochází ke členění primárních aktiv podle jejich citlivosti na zachování důvěrnosti a dostupnosti. Požadavky na integritu, případně i spolehlivost obsahu informací jsou někdy z důvodu jednoduchosti řešeny jednotným souborem organizačních i technických opatření, které se vztahují na všechny primární aktiva organizace bez rozdílu. V těchto případech není klasifikace nutná, resp. existuje pouze jedna klasifikační skupina. V jiných případech, např. pro oblast zdravotnictví, je výhodné provádět klasifikaci primárních aktiv také dle požadavků na integritu a zejména také dle požadavků na spolehlivost obsahu informací. Příkladem je pacientská dokumentace.

Praktický přístup k požadavkům informační demonstruji na třech typech organizací: státní, soukromé a zdravotnické.

2.6.1. Státní organizace

Důvěrnost

Důvěrnost informací se ve státních organizacích obvykle klasifikuje následujícím způsobem.

Utajované informace a zvláštní skutečnosti

Nakládání s těmito informacemi podléhá režimu, který je určen příslušnou legislativou, tj. zákonem č. 412/2005 Sb., o ochraně utajovaných informací, a zákonem č. 240/2000 Sb., o krizovém řízení.

Osobní údaje

Nakládání s těmito informace určuje zákon č. 101/2000 Sb., o ochraně osobních údajů.

Interní informace

Nakládání s těmito informacemi je obvykle určeno vnitřními předpisy organizace.

Ostatní informace

Na ostatní informace z hlediska důvěrnosti nejsou kladeny žádné požadavky.

Dostupnost

Kritická dostupnost (online systémy)

Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení organizace nebo lidí. Pro ochranu

dostupnosti jsou využívány záložní systémy a obnova poskytování služeb musí proběhnout zcela automaticky a krátkodobě. Toho lze zpravidla dosáhnout pouze za použití redundantních technologií.

Vysoká dostupnost

Narušení dostupnosti aktiva by nemělo překročit dobu několika málo hodin. Aktiva jsou považována jako kritická. Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy či výměnou technických aktiv.

Do této skupiny by měly být zařazeny pouze agendy, u kterých je to vyžadováno legislativou (portály veřejné správy) nebo existují závažné interní důvody související s možným ochromení chodu celého úřadu v případě delší nedostupnosti agendy.

Střední dostupnost

Narušení dostupnosti aktiva by nemělo překročit dobu jednoho pracovního dne. Pro ochranu dostupnosti jsou využívány metody zálohování a obnovy (transakční metody). Jsou uzavřeny smlouvy se všemi dodavateli všech souvisejících aktiv (hardware i software).

Do této skupiny by měly být zařazeny pouze agendy, které jsou sdíleny celým úřadem nebo více odbory a které by v případě delšího výpadku mohly způsobit ochromení chodu celého úřadu (spisová služba, interní pošta, apod.).

Nízká (běžná) dostupnost

Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (několik dnů až nejvýše 1 týden), a proto je postačující pravidelné zálohování.

Do této skupiny by měly být zařazeny běžné agendy, u kterých nejsou legislativou stanoveny kratší lhůty, a které v případě výpadku nenaruší chod celého úřadu.

Integrita a spolehlivost

Klasifikace z hlediska integrity, spolehlivosti a případně též autenticity může být jednotná. Jednotný přístup pro oba tyto požadavky navrhuje též metodika Národního bezpečnostního úřadu prostřednictvím vyhlášky o kybernetické bezpečnosti č. 316/2014 Sb. (Příloha 1 – Hodnocení a úrovně důležitosti aktiv a Příloha 4 – Struktura bezpečnostní dokumentace, I. Struktura bezpečnostní politiky, (4) Politika klasifikace aktiv).

Kritická – nejvyšší požadavky na udržení integrity a spolehlivosti informací.

Narušení integrity vede k velmi vážnému poškození zájmů organizace s přímými a nevratnými dopady. Pro ochranu integrity aktiva musí být využity účinné prostředky, které provedené změny propojí s individuální odpovědností osoby např. pomocí digitálního podpisu. Data musí být uloženy v robustních databázových systémech. Musí být prováděny validace dat, pravidelné sofistikované (transakční) metody zálohování, ověřována čitelnost záloh atd.

Vysoká – vysoké požadavky na udržení integrity a spolehlivosti informací.

Aktivum je citlivé z hlediska integrity. Narušení integrity aktiva vede k poškození zájmů organizace s přímými dopady. Pro ochranu integrity aktiva by měly být využity prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu.

Střední – běžné požadavky na udržení integrity a spolehlivosti informací.

Narušení integrity aktiva může zapříčinit poškození zájmů společnosti, přičemž se projeví především nepřímými dopady, které nebudou významné. Pro ochranu integrity je postačující použití standardních nástrojů, např. běžné způsoby zálohování, omezení přístupových práv pro zápis apod.

Nízká – bez požadavku na integritu spolehlivost informací.

Není vyžadována žádná ochrana integrity ani spolehlivosti informací.

2.6.2. Soukromé organizace

Tyto organizace zpravidla kladou vysoké požadavky na důvěrnost i v případě interních informací. Je pro ně důležité, aby jejich know-how nemohlo být zneužito konkurencí. Zde je příklad klasifikace informací z hlediska požadavků na jejich důvěrnost v soukromé organizaci.

- Nechráněné informace
- Chráněné informace
    - Firemní (interní) informace
        - Informace výhradně pro interní využití
        - Informace schválené pro zpřístupnění jiným subjektům
        - Informace zákazníků a dodavatelů
    - Citlivé informace
    - Osobní údaje

Požadavky na dostupnost informací bývají značně rozdílné v závislosti na předmětu činnosti organizace. Například organizace poskytující informační a datové služby, služby on-line, elektronických nástrojů apod., zařazují kritická data do skupiny na úrovni kritické dostupnosti popsané v předchozí kapitole, zatímco se všemi ostatními běžnými agendami lze nakládat na úrovni střední dostupnosti. Klasifikace z hlediska dostupnosti informací je u takových organizací žádoucí a obvyklá. Menší

soukromé organizace si zpravidla vystačí i s jednotným způsobem řešení informační (datové) integrity, protože všechna data bývají umístěna na jednom nosiči (serveru) a používají stejnou metodu zálohování. V takovém případě, kdy objem dat nehraje významnou roli z hlediska ceny služeb, není ani důvod informační bezpečnost komplikovat zaváděním klasifikace dle dostupnosti. Podobná situace se týká také integrity a spolehlivosti.

2.6.3. Zdravotnické organizace

Zdravotnické organizace zpracovávají velké množství dokumentace v listinné i elektronické formě, jejíž nakládání upravuje příslušná zdravotnická legislativa a zároveň spadá do působnosti zákona č. 101/2000 Sb., o ochraně osobních údajů. Klasifikace informací z hlediska důvěrnosti je tedy obvykle podobná, jako u státních organizací. U zdravotnických organizací jsou také kladeny velmi vysoké požadavky na dostupnost informací, na jejich integritu, spolehlivost a autenticitu. Na správném obsahu zdravotnických informací, na jejich správném přiřazení k pacientům a na jejich dostupnosti v případě jejich potřeby jsou závislé životy a zdraví osob. V případě zdravotnických organizací je proto důležité provádět klasifikaci informací také z hlediska požadavků na dostupnost, integritu a spolehlivost.

Je zřejmé, že struktura klasifikace informací, zejména z hlediska požadavků na jejich důvěrnost, může být složitější. Způsob nakládání s některými skupinami informací podléhá legislativním požadavkům, zatímco pro jiné skupiny informací jsou pravidla určeny pouze interními předpisy a postupy.

Aby se v této problematice zaměstnanci organizace dokázali orientovat, organizace svými vnitřními předpisy pro každou klasifikovanou skupinu určují konkrétní pravidla a postupy.

Zaměstnanci musí znát klasifikační skupiny (stupně) a musí umět rozpoznat, které informace patří do které skupiny. Tento úkol lze řešit buď značením informací, nebo vytvářením seznamů informací. Pro potřeby vytváření seznamů informací je

nejdříve nutné sdružit informace do celků podle účelu jejich zpracování nebo využití. Takové skupiny informací se obvykle označují jako agendy. Agendou rozumíme soubor informací, které jsou sdruženy podle účelu jejich užití, resp. jejich zpracování.

Pro každou agendu lze přiřadit příslušnou skupinu podle důvěrnosti. K agendám je také možné přidat další požadavky na jejich vlastnosti, např. požadavek na dostupnost, spolehlivost, integritu atd. Pro zjednodušení bezpečnostního systému bývají požadavky na integritu a spolehlivost určeny jednotně, tedy bez další klasifikační struktury. V příloze 13 – Registr agend je uveden příklad seznamu informací strukturovaných dle jednotlivých agend. U větších organizací mohou být agendy dále seskupovány, resp. sdružovány podle útvarů organizace nebo podle podobného účelu, např. agendy obchodní, agendy právní, agendy personální apod. Uvedený registr ukazuje jednoduchý způsob klasifikace všech informací organizace podle všech požadavků na informační bezpečnost, tj. dle požadavků na důvěrnost, dostupnost, integritu a spolehlivost.

Jestliže organizace pro každou klasifikační skupinu definuje přesná pravidla pro zpracování a zabezpečení informací, pak zaměstnanci odpovědní za zpracování konkrétních agend musí být informování o tom, jak jsou konkrétní agendy klasifikovány z hlediska bezpečnostních požadavků na důvěrnost, dostupnost integritu a spolehlivost.

Pro tento účel je vhodné vytvořit přehlednou matici, kde všechny agendy jsou zařazeny do řádků tabulky a všechny bezpečnostní požadavky jsou zařazeny do sloupců stejné tabulky, jak je vidět v příloze 13 – Registr agend.

3. Informační bezpečnost podle normy ISO 27001

Norma stanoví základní požadavky na bezpečnost informací v kapitolách 4 až 10. Prostřednictvím přílohy A jsou definována jednotlivá konkrétní opatření a jejich cíle, které musí organizace splnit pro zajištění souladu s normou, resp. pokud chce splnit podmínky pro certifikaci této normy.

3.1. Kontext organizace (kapitola 4 normy)

Kontext organizace je povinný dokument, jehož cílem je:

- porozumění organizaci, tj. porozumění její činnosti a potřebám,
- porozumění prostředí, v němž organizace působí, zejména vztahům a očekávání zainteresovaných stran, tj. zákazníků, dodavatelů, veřejnosti, zájmových skupiny, atd.

Kontext organizace by měl obsahovat tzv. interní a externí aspekty. Interními aspekty se rozumí takové aspekty, které organizace může sama přímo ovlivnit. Externí aspekty organizace ovlivnit nemůže nebo je může ovlivnit jen nepřímo. Např. mediální obraz organizace, který se utváří nezávisle na organizaci, avšak organizace jej může částečně ovlivnit prostřednictvím svého úsilí a vlastním působením na veřejný sektor.

Zde je výčet položek, které by dokument kontext organizace měl obsahovat:

- Interní aspekty:
    - základní informace o organizaci (název, sídlo atd.),
    - předmět činnosti organizace, poskytované produkty a služby,
    - organizační struktura a uspořádání, organizační vztahy a provozovny,
    - interní normy a předpisy společnosti,
    - lidské zdroje.
- Externí aspekty:
    - mediální obraz společnosti (jak je společnost vnímána svým okolím),

- zainteresované strany (zákazníci, dodavatelé, smluvní partneři, instituce atd.) a jejich požadavky a očekávání,
- konkurenční prostředí a hlavní rizika činnosti společnosti,
- legislativa, která významně ovlivňuje činnost společnosti, případně přímo souvisí s informační bezpečností.

Norma neurčuje formu ani konkrétní obsah kontextu organizace. Podobu dokumentu si organizace vytváří sama. Přílohy 1 – KO – státní správa, 2 – KO – zdravotnictví a 3 – KO – soukromá organizace jsou příklady různého přístupu organizací k tomuto dokumentu. V případě kontextu soukromé organizace je tento dokument společným kontextem pro systémy řízení kvality (QMS dle ISO 9001), řízení bezpečnosti informací (ISMS dle ISO 27001) a environmentálního managementu, tj. řízení životního prostředí (EMS dle ISO 14001).

3.2. Vůdčí role (kapitola 5 normy)

Organizace musí definovat základní politiku bezpečnosti informací a také musí stanovit odpovědnosti zaměstnanců za bezpečnost informací.

3.2.1. Vůdčí role a závazek

Vrcholové vedení organizace musí prosazovat systém řízení bezpečnosti informací a to zejména prostřednictvím:

- závazku vedení k neustálému zlepšování,
- integrace všech bezpečnostních požadavků do činnosti organizace,
- zajišťování potřebných zdrojů.

Závazek vedení k prosazování bezpečnostních prvků do všech činností (procesů) a ke stálému zlepšování by měl být deklarován zřetelně, např. formou písemného veřejného prohlášení. Integrace bezpečnostních požadavků do činnosti organizace znamená, že všechna bezpečnostní opatření z přílohy A normy ISO 27001

budou zaváděna v rozsahu předmětu činnosti organizace, tedy v souladu s kontextem organizace. Pro realizaci potřebných opatření musí vedení organizace zajistit potřebné zdroje finanční, materiální i personální.

3.2.2. Politika

Organizace určí základní bezpečnostní politiku, která je přiměřená, tzn. je v souladu s kontextem organizace. Bezpečnostní politika je dalším povinným dokumentem organizace, který musí být komunikován v rámci organizace, např. formou školení zaměstnanců, a přiměřeně dostupný zainteresovaným stranám, např. prostřednictvím zveřejňovaných informací o společnosti.

3.2.3. Role, odpovědnost a pravomoci organizace

Odpovědnosti zaměstnanců za bezpečnost informací musí být v souladu s jejich kompetencemi tak, aby systém řízení bezpečnosti informací byl ve shodě s požadavky normy ISO 27001. Tyto požadavky jsou určeny přílohou A normy.

3.3. Plánování (kapitola 6 normy)

Jedná se o plánování bezpečnostních opatření na základě identifikovaných rizik. Organizace musí posoudit informační rizika, která jsou relevantní zejména s ohledem na kontext organizace, tedy rizika související s předmětem činnosti organizace a s prostředím, v němž organizace činnost vykonává, včetně zainteresovaných stran.

Organizace musí definovat a aplikovat proces identifikace, posuzování a akceptace informačních rizik. Jedná se o velmi důležitou a zároveň obtížnou činnost. Aby organizace byla schopná identifikovat a posoudit skutečně významná rizika, musí umět odhalit všechny podstatné informační zranitelnosti. Základem úspěchu je dobrá

znalost všech primárních i podpůrných aktiv. V kapitole 2.6 jsou podrobně vysvětleny potřeby klasifikace primárních aktiv a obvyklý způsob provedení.

Jestliže organizace má úplný seznam informačních aktiv, který je klasifikován (tedy členěn a strukturován) podle jejich významu ve vztahu k základním bezpečnostním požadavkům na důvěrnost, dostupnost, integritu a spolehlivost, pak se organizace může soustředit na taková aktiva nebo skupiny aktiv, která jsou pro ni nejvíce významná. Při hledání zranitelností je třeba posoudit všechna významná aktiva vůči relevantním hrozbám v rozsahu daném kontextem organizace, tj. v rozsahu daném předmětem činnosti organizace a souvisejícího prostředí, v němž organizace předmět činnosti vykonává (zainteresované strany, legislativní prostředí, konkurenční prostředí, hlavní rizika prostředí atd.), viz kapitola 3.1.

Z uvedeného je zřejmé, že správně definovaný kontext organizace a současně správné pochopení významu a hodnoty vlastních informačních aktiv jsou zásadní předpoklady pro schopnost odhalovat podstatné zranitelnosti a rizika organizace.

Pro systematickou identifikaci rizik je potřeba posoudit všechny relevantní hrozby vůči zranitelnostem podpůrných aktiv. Je nutné si uvědomit, že všechna primární informační aktiva (informace) jsou uchovávána a zpracována prostřednictvím podpůrných aktiv (prostory, informační technologie a lidé). Je zřejmé, že kterákoliv hrozba, jejíž cílem jsou primární aktiva, se může uplatnit pouze prostřednictvím zranitelností podpůrných aktiv. Podpůrná aktiva jsou zranitelná, jestliže nejsou dostatečně zabezpečena (chybí ochranná opatření nebo nejsou dostatečně účinná) vůči hrozbám, které mohou narušit důvěrnost, dostupnost, integritu nebo spolehlivost primárních aktiv. Proto je při hledání významných zranitelností potřeba posoudit, zda jsou instalovaná technická i organizační opatření, zda se tato opatření vztahují na všechna významná podpůrná aktiva, zda jsou dostatečně účinná a zda jsou přiměřená významu (ceně) primárních aktiv v souladu s jejich klasifikací.

Zjednodušeně lze konstatovat, že je potřeba zkoumat rozsah, účinnost a efektivitu stávajících opatření. Tam, kde opatření chybí nebo je nedostatečně účinné, mluvíme o bezpečnostním nedostatku, resp. zranitelnosti podpůrného aktiva.

Proces identifikace zranitelností aktiv musí probíhat systematicky. Tato činnost je velmi náročná, protože podpůrných aktiv je obvykle velké množství. Pomůckou pro zkoumání, zda jsou zavedena opatření pro všechny oblasti informační bezpečnosti, slouží příloha A normy ISO 27001.

Pokud není zavedena celá sada opatření v přiměřeném rozsahu, může dojít k tzv. obejití ostatních instalovaných opatření. Častým případem bývá instalace účinných a někdy i velmi drahých technických bezpečnostních opatření při absenci organizačních opatření. Pokud například lze snadno obelstít zaměstnance a vylákat z nich přístupové údaje, pak sebedokonalejší a drahá technická opatření selhávají.

3.3.1. Posuzování informačních rizik

Pro posuzování informačních rizik musí organizace stanovit metodiku a určit kritéria hodnocení významu rizik a kritéria akceptace rizik, tj. stanovit metriky. Norma ISO 27001 přesně nespecifikuje, jakou metodiku a jaká hodnotící kritéria zvolit. Způsob hodnocení rizik by měl být přiměřený významu aktiv a možným škodám. Zároveň by hodnocení mělo být konzistentní v čase, tj. výsledky opakovaných hodnocení by měly být souměřitelné. Jestliže organizace v odůvodněných případech změní metodiku nebo kritéria hodnocení rizik, musí provést novou výchozí analýzu rizik.

Určitým vodítkem pro organizaci mohou být jiné standardy, např. norma ISO/IEC 27005 - Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací. Tato norma poskytuje organizacím sadu doporučení jak řídit informační rizika. Další možnosti nabízejí jiná řešení popsaná v kapitole 6.

Významný posun v České republice nastal přijetím zákona č. 181/2014 Sb., o kybernetické bezpečnosti. V rámci tohoto zákona vydal Národně bezpečnostní úřad (NBÚ) jednotnou metodiku i metriky (kritéria hodnocení a akceptace rizik) pro organizace v působnosti kybernetického zákona, tzn. organizace, které spadají do působnosti tzv. významných informačních systémů nebo tzv. kritické infrastruktury. Tato metodika a metriky jsou obsaženy ve vyhlášce č. 316/2014 Sb., o bezpečnostních

opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (zkráceně vyhlášce o kybernetické bezpečnosti). Problematice řízení rizik se věnuje § 4.

Nespornou výhodou tohoto kroku je významný posun ke standardizaci hodnocení rizik v rámci České republiky. Národní bezpečnostní úřad tímto krokem zavedl jednotící standard při hodnocení rizik, kterým se mohou řídit jak organizace spadající do působnosti kybernetického zákona (tzv. povinné osoby), tak i ostatní organizace, které buď usilují o certifikaci dle normy 27001, nebo mají potřebu odhalovat a řídit informační rizika ve své společnosti. Nicméně je vhodné doplnit, že vyhláška o kybernetické bezpečnosti prostřednictvím odstavce 3) zmíněného paragrafu ponechává prostor pro organizace, aby při implementaci řízení rizik postupovaly podle jiných než uvedených metodik a metrik, pokud takové postupy zajistí stejnou nebo vyšší úroveň řízení rizik.

Ať už organizace je nebo není tzv. povinnou osobou z hlediska působnosti kybernetického zákona, lze shrnout výhody přijetí metodiky a metrik hodnocení rizik dle vyhlášky NBÚ takto:

- jednotný standard pro všechny organizace,
- konzistentní způsob hodnocení,
- možnost srovnání výstupů analýzy rizik s ostatními organizacemi podobného typu,
- soulad s kybernetickým zákonem pro případ, že bude působnost kybernetického zákona rozšířena.

Účelem analýzy rizik je:

- identifikace podstatných zranitelnosti, tj. slabých míst v systému řízení bezpečnosti informací,
- zvyšování informační bezpečnosti plánováním efektivních opatření podle jejich naléhavosti (posouzení možných škod),
- plnění legislativních, resp. normativních požadavků na informační bezpečnost,

- zajištění, že nebudou opomenuta ochranná opatření organizačního charakteru,
- zajištění, že nebudou opomenuty skryté zranitelnosti,
- snížení pravděpodobnosti závažných incidentů s negativními dopady na organizaci.

Postup při analýze rizik je obvykle tento:

- posouzení základních registrů,
    - registru informačních aktiv,
    - registru hrozeb,
    - registru zranitelností,
    - registru opatření,
- vyhodnocení rizik,
- ošetření rizik.

3.3.2. Posouzení základních registrů

Registr informačních aktiv

Posoudit informační aktiva znamená určit možné škody při porušení jejich důvěrnosti, dostupnosti, integrity a spolehlivosti.

Informační aktiva podle normy ISO 27001

Norma rozlišuje pět skupin informačních aktiv:

- informace (data),
- hardware,
- software,
- prostory,
- lidi.

Způsob identifikace a kritéria pro hodnocení aktiv si organizace stanoví sama.

Informační aktiva podle NBÚ

Informační aktiva jsou členěna na dvě základní skupiny:

- primární,
- podpůrná.

Za primární informační aktiva jsou považovány agendy organizace vedené v analogové (např. listinné) formě nebo v digitální (elektronické) formě. Za podpůrná aktiva jsou považovány všechny prostředky, jejichž prostřednictvím jsou primární informační aktiva ukládána a zpracována. Patří sem:

- veškeré informační technologie,
- prostory, v nichž jsou technologie umístěny,
- lidé, kteří s technologiemi pracují.

Primární aktiva jsou cílem hrozeb, protože některé mají pro útočníka cenu. Podpůrná aktiva jsou prostředkem zneužití hrozeb, protože pouze prostřednictvím jejich zranitelností je možné „dosáhnout“ na primární aktiva.

Proto jsou určena kritéria hodnocení dopadů a škod primárních aktiv v případě porušení jejich důvěrnosti, dostupnosti integrity a spolehlivosti.

Tabulka 2: stupnice pro hodnocení důvěrnosti primárních aktiv

Úroveň	**Popis**
Nízká (1)	Aktiva jsou veřejně dostupná nebo byla určena ke zveřejnění, např. na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy organizace, a proto není vyžadována žádná ochrana důvěrnosti.
Střední (2)	Aktiva nejsou veřejně dostupná a tvoří know-how organizace. Ochrana těchto informací není vyžadována žádnou zákonnou či regulatorní povinností nebo smluvním závazkem. Pro ochranu důvěrnosti jsou využívány běžné prostředky, jako je řízení přístupu.
Vysoká (3)	Aktiva nejsou veřejně dostupná a jejich ochrana je regulována legislativními požadavky nebo smluvními závazky, např. obchodní

	tajemství podle zákona č. 89/2012 Sb., občanský zákoník, osobní údaje podle zákona č. 101/2000 Sb., o ochraně osobních údajů, apod. Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Elektronické přenosy by měly být chráněny pomocí kryptografických prostředků.
Kritická (4)	Aktiva jsou vysoce citlivá z hlediska důvěrnosti a vyžadují nadstandardní míru ochrany. Jedná se např. o strategická obchodní tajemství, citlivé osobní údaje apod. Pro ochranu důvěrnosti je požadována důsledná evidence osob, které k aktivům přistoupily. Metody ochrany by měly bránit kompromitaci ze strany administrátorů.

Tabulka 3: stupnice pro hodnocení integrity primárních aktiv

Úroveň	**Popis**
Nízká (1)	Aktivum není citlivé z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy organizace, a proto není vyžadována žádná ochrana integrity.
Střední (2)	Aktivum může být citlivé z hlediska integrity. Narušení integrity aktiva může zapříčinit poškození oprávněných zájmů společnosti, přičemž se projeví především nepřímými dopady. Pro ochranu integrity je postačující použití standardních nástrojů, např. omezení přístupových práv pro zápis.
Vysoká (3)	Aktivum je citlivé z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů organizace s přímými dopady. Pro ochranu integrity aktiva by měly být využity speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu.
Kritická (4)	Aktivum je vysoce citlivé z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů organizace s přímými a nevratnými dopady. Pro ochranu integrity aktiva musí být využity speciální prostředky, které provedené změny propojí s individuální odpovědností osoby, např. pomocí digitálního podpisu.

Tabulka 4: stupnice pro hodnocení dostupnosti primárních aktiv

Úroveň	**Popis**
Nízká (1)	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu, přibližně do

	jednoho týdne. Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední (2)	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů organizace. Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká (3)	Narušení dostupnosti aktiva by nemělo překročit dobu několika málo hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů organizace. Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy či výměnou technických aktiv.
Kritická (4)	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost v řádu několika minut vede k vážnému ohrožení povinností organizace. Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Tabulka 5: stupnice pro hodnocení vlivu podpůrných aktiv v na primární aktiva

Úroveň	**Popis**
Nízká (1)	Integrita, důvěrnost a dostupnost primárních aktiv jsou jen omezeně závislé na funkčnosti a bezpečnosti podpůrného aktiva.
Střední (2)	Nepřímý vliv podpůrných aktiv. Integrita, důvěrnost a dostupnost primárních aktiv jsou zprostředkovaně nebo jen částečně závislé na funkčnosti a bezpečnosti podpůrného aktiva.
Vysoká (3)	Přímý vliv podpůrných aktiv. Integrita, důvěrnost a dostupnost primárních aktiv jsou bezprostředně závislé na funkčnosti a bezpečnosti podpůrného aktiva.

Registr hrozeb

„Bezpečnostní hrozba (Information security threat) je potenciální příčina nežádoucí události, která může mít za následek poškození informačního systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.“ (Výkladový slovník kybernetické bezpečnosti, 2013, s. 20)

Hrozby podle normy ISO 27001

Registr hrozeb a kritéria pro hodnocení pravděpodobnosti vzniku hrozby definuje sama organizace.

Hrozby podle NBÚ

Registr hrozeb a kritéria pro hodnocení hrozeb jsou obsahem přílohy 1 – Hodnocení a úrovně důležitosti aktiv vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti a zahrnuje hrozby rozdělené do dvou skupin pro:

- organizace spadající do působnosti zákona v oblasti tzv. významných informačních systémů (VIS),
- organizace spadající do působnosti zákona v oblasti tzv. kritické informační infrastruktury (KII).

Tabulka 6: stupnice pravděpodobnosti uplatnění hrozby

Úroveň	**Popis**
Nízká (1)	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední (2)	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká (3)	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická (4)	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Registr zranitelností

Identifikovat bezpečnostní zranitelnosti znamená najít chyby a nedostatky podpůrných aktiv, ale také chybějící ochranná opatření v systému bezpečnosti informací.

Posoudit míru zranitelnosti znamená určit účinnost souboru bezpečnostních opatření instalovaných pro potřeby ochrany informačních aktiv proti účinkům hrozeb.

Zranitelnosti podle normy ISO 27001

Registr zranitelností není normou stanoven. Organizace musí zranitelnosti identifikovat sama. Určitou pomůckou může být seznam povinných opatření a jejich cílů, který je stanoven v příloze A normy. Porovnáním již zavedených opatření s přílohou A lze identifikovat případná chybějící opatření.

Zranitelnosti, které se týkají firmware zařízení, jsou buď známé a publikované, ale výrobcem ještě neošetřené, nebo jsou skryté a neobjevené. V případě skrytých zranitelností existuje riziko, že budou zneužity hrozbou před jejich objevením.

Zranitelnosti podle NBÚ

Registr zranitelností je obsažen přílohou 2 - Hodnocení rizik vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti. Je definováno celkem jedenáct zranitelností, které organizace musí posoudit a ohodnotit dle stanovených kritérií.

Součástí zákona o kybernetické bezpečnosti je rovněž seznam povinných opatření, která jsou více konkrétní než v případě normy ISO 27001 a jsou také důsledně členěna dle svého charakteru na opatření organizační a opatření technická. I v tomto případě lze hledat chybějící relevantní opatření (potenciální zranitelnosti systému) prostřednictvím existujícího uceleného seznamu všech možných opatření.

Souborům opatření se věnuje kapitola 3.3.4.

Tabulka 7: stupnice vyjadřující pravděpodobnost úspěšnosti uplatnění hrozby

Úroveň	**Popis**
Nízká (1)	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní prvky, které jsou schopny včas detekovat možné slabiny nebo případné pokusy o překonání bezpečnostních prvků.
Střední (2)	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní prvky, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních prvků včas detekovat možné slabiny nebo případné pokusy o překonání bezpečnostních prvků je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních prvků.
Vysoká (3)	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní prvky existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních prvků.
Kritická (4)	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní prvky nejsou realizovány anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních prvků. Jsou známé úspěšné pokusy překonání bezpečnostních prvků.

Registr opatření

Registr opatření je „Soubor opatření k dosažení požadované úrovně důvěry v ochranu komunikačních, informačních a jiných elektronických i ne-elektronických systémů a informací ukládaných, zpracovávaných nebo přenášených v těchto systémech s ohledem na důvěrnost, integritu, dostupnost, neodmítnutelnost a autentičnost.“ (Výkladový slovník kybernetické bezpečnosti, 2013, s. 47)

Opatření podle normy ISO 27001

Registr opatření a jejich cílů je určen přílohou A normy. Organizace musí zdůvodnit aplikování nebo vyloučení příslušných opatření přílohy A. Zavedení všech nevyloučených opatření je nutnou podmínkou certifikace.

Opatření podle NBÚ

Registr opatření je obsažen vyhláškou č. 316/2014 Sb., o kybernetické bezpečnosti.

Je stanoveno, která opatření jsou povinná pro správce kritické informační infrastruktury a která se týkají správců významných informačních systémů. Jednotlivá opatření jsou rozdělena mezi organizační a technická opatření.

Organizace musí všechna opatření postupně zavést. Pro jejich zavedení stanoví priority na základě výstupů z analýzy rizik.

3.3.3. Hodnocení rizik

Jedná se o „proces porovnání výsledků analýzy rizik s kritérii rizik k určení, zda je míra rizika přijatelná (akceptovatelná).“ (Výkladový slovník kybernetické bezpečnosti, 2013, s. 41)

Hodnocení rizik podle normy ISO 27001

Kritéria pro hodnocení rizik si určí organizace sama.

Hodnocení rizik podle NBÚ

Kritéria pro hodnocení rizik jsou obsažena v příloze 2 - Hodnocení rizik vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti.

Tabulka 8: stupnice hodnotící míru rizika a přípustných úrovní akceptovatelných a zbytkových rizik

Úroveň	**Popis**
Nízká (1)	Riziko je považováno za přijatelné.
Střední (2)	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko přijatelné.
Vysoká (3)	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritická (4)	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

3.3.4. Ošetření rizik

Ošetřením nebo zvládnutím rizika se rozumí „proces pro modifikování (změnu) rizika." (Výkladový slovník kybernetické bezpečnosti, 2013, s. 117)

Zvládnout rizika znamená realizovat vhodná opatření pro ochranu aktiv podle jejich významu. Soubory opatření definované přílohou A normy ISO 27001, resp. vyhláškou č. 316/2014 Sb., o kybernetické bezpečnosti, poskytují systémový a komplexní přístup pro stanovení vhodných ochranných opatření.

Registr opatření stanovený vyhláškou na rozdíl od přílohy normy poskytuje více konkrétních technických opatření, resp. nástrojů k zajištění ochrany informačních aktiv (např. § 18 Nástroj pro ověřování identity, odst. (3) stanoví minimální požadavky pro heslo, jako je minimální délka, minimální počet číslic, velkých písmen atd.).

Účelem registru opatření je:

- výběr vhodných variant ošetření rizik,
- ověření, že žádné z možných opatření nebylo opomenuto,
- plánování zdrojů pro zvládání rizik,
- stanovení odpovědnosti, resp. schválení opatření vlastníky rizik a akceptace zbytkových rizik.

Při plánování opaření organizace musí zvážit:

- Opatření pro snížení pravděpodobnosti vzniku hrozeb:
    - vyhnutí se rizikům (omezení rozsahu aktiv a technologií na nezbytné minimum, např. omezení vzdáleného přístupu, oddělení sítí, apod.),
    - zkrácení doby působení hrozby (např. vypínání zařízení nebo odpojení při nečinnosti).
- Opatření pro snížení dopadů:
    - Pojištění drahých zařízení, služeb a lidských chyb.
    - Zakotvení sankcí a náhrad škod ve smluvních ujednáních s dodavateli.
- Opatření pro snížení zranitelnosti:
    - plánování bezpečnostních opatření v místech, kde jsou uvedeny vyšší hodnoty zranitelnosti. Při plánování opatření se posuzuje jejich efektivnost a vzájemnou účinnost. I nákladné technické opatření, které lze administrativně nebo jinak obejít, je neúčinné a neefektivní,
    - administrativní a nízkonákladová opatření (zavedení pravidel, stanovení odpovědnosti, školení zaměstnanců, apod.) lze provést i pro hodnoty středních rizik.
- Posouzení naléhavosti opatření v souladu s významem rizik.

Opatření je potřeba zavádět dle jejich naléhavosti. Pro urgentní rizika je nutné implementovat opatření neprodleně, pro vysoká a střední rizika je vhodné opatření plánovat.

3.3.5. Stanovení cílů bezpečnosti informací

Stanovení cílů bezpečnosti informací je povinný dokument. Cíle by měly být měřitelné z hlediska vyhodnocení, zda jich bylo dosaženo. Měly by být splnitelné (přiměřené kontextu organizace) a konzistentní. Pro plnění cílů musí organizace určit odpovědnosti, zdroje, termíny a způsob hodnocení.

3.4. Podpora (kapitola 7 normy)

Organizace musí zajistit potřebné zdroje pro zavedení, udržení a stálé zlepšování systému řízení bezpečnosti informací. K tomu organizace musí určit nezbytné kompetence osob, zvyšovat povědomí zaměstnanců a zajistit vhodný způsob interní a externí komunikace.

Organizace musí vytvářet a průběžně aktualizovat dokumentované informace (požadované normou nebo samotnou organizací), které jsou nezbytné pro řízení bezpečnosti informací. Dokumentované informace tvoří dokumentované postupy a záznamy o činnostech.

Proces tvorby a aktualizace dokumentovaných informací a seznamování zaměstnanců s nimi musí být řízen.

3.5. Provozování (kapitola 8 normy)

Organizace musí provádět plánování jako součást řízení všech procesů nutných pro splnění požadavků bezpečnosti informací. Musí vést dokumentaci v nezbytném rozsahu, aby existoval důkaz, že procesy probíhaly dle plánu.

Dále musí organizace přijímat opatření ke snížení nepříznivých dopadů incidentů a provádět pravidelné přezkoumání účinnosti těchto opatření.

Posuzování rizik musí probíhat pravidelně a vždy, když nastanou významné změny, viz kapitola 3.3.1. Organizace musí také implementovat plán zvládání rizik a vést dokumentované informace o jeho plnění, jak je popsáno v kapitolách 3.3.3 a 3.3.4.

3.6. Hodnocení výkonnosti (kapitola 9 normy)

Organizace musí analyzovat a hodnotit efektivnost systému bezpečnosti informací. K tomu účelu se stanoví, které procesy, resp. prvky bezpečnostního systému,

bude monitorovat a měřit. Další významnou činností pro získání zpětné vazby o stavu systému jsou interní audity a proces tzv. přezkoumání vedením organizace.

3.6.1. Monitorování, měření a hodnocení

Organizace určí rozsah monitoringu a kontrol, tedy co se bude monitorovat a kontrolovat. Dále také definuje použité metody monitorování a měření, stanoví kritéria pro měření, hodnocení a analýzy výstupů z monitorování a měření.

Záznamy z monitorování patří mezi povinné záznamy, které organizace musí uchovávat jako důkaz o stavu bezpečnostního informačního systému.

3.6.2. Interní audit

Účelem interních auditů je ověřovat shodu systému řízení bezpečnosti informací s požadavky normy a s vlastními požadavky organizace.

Auditní činnost organizace musí být řízena, tj. organizace musí plánovat termíny interních auditů, musí stanovit program interních auditů, definovat kritéria auditu, určit auditory, zajistit objektivitu, nestrannost a musí seznamovat vedoucí pracovníky s výsledky auditu. Organizace rovněž musí uchovávat záznamy zjištění z interních auditů.

3.6.3. Přezkoumání vedením organizace

Vrcholové vedení organizace musí plánovat a v pravidelných intervalech provádět přezkoumání systému řízení bezpečnosti informací.

Přezkoumání systému je potřeba provádět s ohledem na kontext organizace, zejména je nutné posoudit případné změny interního a externího aspektu, které mohou souviset se systémem bezpečnosti informací.

Vrcholové vedení posuzuje a přezkoumává zejména:

- řešení incidentů (neshod),
- výstupy monitoringu a kontrol,
- výsledky interních i nezávislých auditů,
- závěry z analýzy rizik, plán ošetření rizik,
- požadavky, případně stížnosti zainteresovaných stran,
- trendy v oblasti systému bezpečnosti informací,
- příležitosti pro zlepšování systému.

Přezkoumání vedením organizace je významným požadavkem normy, který poskytuje nezbytnou zpětnou vazbu pro efektivní řízení (vyhodnocování a plánování) informační bezpečnostní situace organizace.

3.7. Zlepšování (kapitola 10 normy)

Organizace musí být schopna řídit incidenty, tj. neshody a závažné nedostatky. Za neshodný stav je považován takový reálný stav, který není ve shodě se stanovenými legislativními nebo interními požadavky. Organizace musí být schopna identifikovat neshodný stav prostřednictvím monitoringu, kontrol a auditní činnosti. Zjištěný neshodný stav musí organizace přezkoumat, určit příčiny a provést přiměřená opatření (nápravná a preventivní) k zajištění souladu s požadavky a snížení rizika opakování neshodného stavu.

Organizace musí vést a uchovávat záznamy o řešení incidentů a neshod.

4. Informační bezpečnost v praxi

Pro porovnání rozdílných typů organizací z hlediska přístupu k bezpečnosti informací podle normy ISO 27001 vytvořím tři smyšlené (virtuální) organizace, jejichž modelové charakteristiky odrážejí reálné charakteristiky existujících organizací podobného typu působících na území České Republiky. Pro každou z nich bude formou příloh předložen konkrétní obsah některých povinných dokumentů a záznamů. Tyto dokumenty pomohou přiblížit požadavky normy ISO 27001 a identifikovat některé rozdíly v přístupu k informační bezpečnosti.

Budu se zabývat soukromou organizaci působící na poli energetiky, nemocnicí okresního typu a státní správou v podobě městského magistrátu.

V případě magistrátu města budeme předpokládat, že organizace zavedly a certifikovaly pouze systémy bezpečnosti informací podle normy ISO 27001. V případě velkých soukromých organizaci je běžné, že mají zavedeno více standardů. Takové organizace obvykle vytvářejí tzv. integrované systémy řízení (ISŘ), protože jednotlivé standardy se v řadě oblastí překrývají a proto některé řídicí dokumenty, dokumentované postupy a záznamy bývají společné pro více standardů. Aby bylo zřejmé, jak se dají tyto standardy spojit, je pro modelový případ zvolena velká společnost, která integrovaly systémy ISO 9001, ISO 14001, ISO 27001 a další standardy.

4.1. Charakteristiky oblasti působení modelových organizací

Následující tři odstavce budou popisovat specifické charakteristiky oblastí, ve kterých působí tři zvolené organizace.

4.1.1. Státní správa

Státní správa je definována jako veřejná správa uskutečňovaná státem. Pojem je užíván jako:

- organizační pojetí, kdy se jím rozumí orgány státní správy,
- funkčním pojetí, kdy jde prakticky o výkon podzákonné nařizovací činnosti těchto orgánů (Madar, 1995).

Jak vyplývá z definice, oblasti působnosti státní správy jsou velmi široké a jsou zpravidla upraveny zvláštními zákony. Z pohledu informační bezpečnosti jde obvykle o správu značného rozsahu informací jak v elektronické, tak i listinné formě. Některé skupiny informací se týkají občanů a zahrnují osobní a citlivé údaje, vztahují se na ně tedy zákony č. 412/2005 Sb., o ochraně utajovaných informací a č. 101/2000 Sb., o ochraně osobních údajů. Jsou zde kladeny zvýšené nároky na důvěrnost, spolehlivost a integritu dat. Zvýšené požadavky na dostupnost se mohou vyskytnout při řešení mimořádných a krizových stavů, které legislativa popisuje v zákoně č. 240/2000 Sb., o krizovém řízení.

4.1.2. Zdravotnictví

Zdravotnictví je charakteristické značným rozsahem zpracovávaných dat v listinné i elektronické formě a vysokým podílem citlivých údajů. Vztahuje se na ně tedy opět zákon č. 101/2000 Sb., o ochraně osobních údajů. Dále jsou zde důležité klíčové požadavky na důvěrnost, dostupnost a spolehlivost informací. Případy nesplnění těchto kritérií mohou mít dopad na zdraví nebo životy osob, proto jsou upraveny zákonem č. 258/2000 Sb., o ochraně veřejného zdraví.

Zvláštností je, že žádné zdravotnické zařízení v České republice k dnešnímu dni (první polovina roku 2016) nespadá do působnosti zákona č. 181/20014 Sb. o kybernetické bezpečnosti. Proč tomu tak je pomůže rozkrýt kapitola 5 a určitou osobní úvahu na toto téma si dovolím předložit v kapitole 7.

4.1.3. Soukromá organizace

Pro soukromé firmy je důležitý zejména zákon č. 513/1991 Sb., obchodní zákoník. Zákon č. 101/2000 Sb., o ochraně osobních údajů, se také vztahuje i na soukromé organizace. Některé mohou také spadat do působnosti kybernetického zákona. Jedná se zejména o organizace poskytující základní komunikační infrastrukturu, dodávky energií apod. Další legislativa a z ní vyplývající povinnosti soukromé sféry se vztahují k předmětu působení organizace a nelze je jednoduše zobecnit.

4.2. Povinné dokumentované informace

Dokumentací, které jsou vyžadovány pro splnění požadavků normy ISO 27001, je velké množství. Není v možnostech tohoto textu obsáhnout všechny vzorové dokumenty pro tři různé organizace. Zvoleny tedy byly pouze některé, které považuji za klíčové.

Jedná se o kontext organizace, prohlášení o aplikovatelnosti, analýzu rizik a plán zvládání rizik.

4.2.1. Kontexty modelových organizací

Následující odstavce obsahují základní informace, které by měl obsahovat dokument kontext organizace. Protože v tomto dokumentu může být větší množství textu, jsou dále uvedeny jen jeho podstatné části (výčet všech informací, které by měl dokument obsahovat, je obsažen v kapitole 3.1). Konkrétní podoby kompletních dokumentů tak, jak mohou vypadat v praxi, jsou v přílohách 1 – KO – státní správa, 2 – KO – zdravotnictví a 3 – KO – soukromá organizace.

Státní správa

Základní informace o organizaci

Magistrát města Nové Město, sídlem v Masarykovo náměstí 1, Novém Městě.

Předmět činnosti organizace, produkty a služby

Předmětem činnosti magistrátu je:

- plnění úkolů jemu uložených zastupitelstvem a radou města,
- výkon přenesené působnosti v rozsahu jemu svěřenému příslušnými zákony,
- zpracovávání informací občanů, jiných orgánů veřejné správy a dalších organizací a dodavatelů,
- zpracování strategických informací, obchodních tajemství a informací podléhajících režimu zákona o ochraně utajovaných informací, zákona o krizovém řízení a zákona o ochraně osobních údajů.

Zainteresované strany a jejich požadavky

- Občané
- Zaměstnanci
- Dodavatelé
- Jiné orgány veřejné správy
- Zájmové skupiny

Zainteresované strany očekávají, že s jejich důvěrnými informacemi bude nakládáno bezpečným způsobem v souladu s platnou legislativou a smluvními podmínkami, a že v případě podaných stížností nebo zjištěných incidentů bude neprodleně sjednána náprava.

Konkurenční prostředí a související rizika

Při plnění úkolů (služeb) v oblasti působnosti samosprávy města a státem delegované části veřejné zprávy se nejedná o typické konkurenční prostředí.

Hlavní rizika v oblasti působnosti magistrátu města lze nalézt v oblastech:

- častých legislativních změn,
- změn politických vedení města a vlivu samosprávy,
- rozdílných protichůdných zájmech občanů, politických a zájmových skupin,
- častých finančních, tj. rozpočtových změn.

Zdravotnictví

Základní informace o organizaci

Nemocnice Zdraví, a.s., sídlem v Nemocniční 321, Praze 1. Kapacita zařízení je 123 lůžek.

Předmět činnosti organizace, produkty a služby

Organizace zajišťuje základní zdravotní péči v souladu s:

- platnou legislativou, a to zejména s:
    - zákonem č. 372/2011 Sb., o zdravotních službách,
    - vyhláškou č. 92/2012 Sb., o požadavcích na minimální technické a věcné vybavení zdravotnických zařízení a kontaktních pracovišť domácí péče,
    - vyhláškou 98/2012 Sb., o zdravotnické dokumentaci,
- interními předpisy organizace, a to zejména s:
    - základní politikou ISMS,
    - organizačním řádem organizace,
    - postupy informační bezpečnosti,
- smluvními požadavky třetích stran, a to zejména se:

    - smlouvami s pojišťovnami podle Registru smluv,
    - smlouvami se zřizovatelem podle Registru smluv,
    - smlouvami s dodavateli a třetími stranami podle Registru smluv,
- se svými cíli.

Zainteresované strany a jejich požadavky

Zřizovatel očekává, že organizace:

- bude plnit předmět své činnosti v souladu s platnou legislativou,
- zajistí standardní kvalitu zdravotní péče,
- při dosažení požadované kvality se bude chovat efektivně a hospodárně,
- bude plnit základní kritéria a kvalitativní parametry stanovené interními předpisy,
- budou dodržovány normy a postupy léčebné péče.

Pacient očekává, že:

- mu bude poskytnuta kvalitní zdravotní péče,
- jeho léčbu budou provádět kvalifikovaní a zkušení odborníci s využitím spolehlivých informací,
- pro jeho léčbu budou využity moderní postupy a technologie,
- s jeho osobními a citlivými údaji bude nakládáno bezpečně, zejména uchování důvěrnosti.

Dodavatel očekává, že:

- budou plněny smluvní závazky,
- bude poskytována potřebná vzájemná součinnost,
- problémy, které mohou mít vliv na činnost organizace dodavatele, budou včasně oznamovány a projednávány,
- s informacemi dodavatele bude nakládáno bezpečným způsobem.

Zdravotní pojišťovna očekává, že:

- zdravotní péče bude vyúčtována v souladu se smluvními podmínkami, včas a bezchybně.

Ostatní zainteresované strany:

- Zdravotní záchranná služba,
- Policie ČR,
- veřejně prospěšné spolky a organizace,
- státní instituce a
- soudy České Republiky

očekávají, že jim bude poskytnuta nezbytná a včasná součinnost při řešení případů, v nichž je nebo může být organizace zainteresována, a to v souladu s platnou legislativou a dobrými mravy.

Konkurenční prostředí a související rizika

Rozsah činnosti organizace lze plánovat pouze částečně, proto jsou vytvořeny rámcové dohody o spolupráci s blízkými zdravotnickými zařízeními podobného typu.

Významná rizika pro organizaci:

- informační rizika:
    - únik citlivých informací (porušení důvěrnosti informací),
    - nedostupnost informací o zdraví pacientů (porušení dostupnosti),
    - záměna informací, chybné informace o zdraví pacientů (porušení autenticity nebo spolehlivosti obsahu),
- rizika bezpečnosti práce,
    - nedodržení pracovních postupů,
    - neprovedení revizí,
- finanční rizika:
    - jako je nedodržení platebních podmínek ze strany pojišťoven,
    - neodpovídající úroveň tarifů za provedené výkony nebo
    - chyby ve výkazech výkonů,

- ostatní rizika:
    - legislativní změny,
    - chyby a nedostatky při poskytování odborné lékařské (chybná diagnóza, záměna léků apod.).

Soukromá organizace

Základní informace o organizaci

EEE-energie, a.s., založena 1. 1. 2000, sídlem v Uličce 12, Novém Městě.

Předmět činnosti organizace, produkty a služby

Organizace působí v oblasti energetického průmyslu, výroby, výstavby a projektování. Zajišťuje podporu a služby v těchto oblastech:

- rozvodny a elektrárny,
- kabely a vnější vedení,
- průmyslová automatizace,
- projektování,
- výstavba a montáže.

Zainteresované strany a jejich požadavky

Hlavními partnery naší organizace jsou:

- Skupina ČEZ,
- Eon,
- Siemens,
- ABB,
- Alstom,
- Agrofert.

Důležitými požadavky našich partnerů jsou:

- dobrý mediální obraz naší společnosti,
- dodržování platné legislativy naší společností,
- dlouhá tradice a zkušenosti naší společnosti v oboru,
- zabezpečení partnerských neveřejných informací, které s naší společností sdílejí.

Konkurenční prostředí a související rizika

Energetický průmysl v České Republice je napojen na evropský trh s energií. Na trhu se nachází více tuzemských společností stejně tak se o zdejší trh ucházejí společnosti zahraniční.

Konkurenční prostředí je ovlivněno trhem s energiemi a zároveň a Energetickým regulačním úřadem (ERÚ).

Hlavní rizika:

- časté Legislativní změny,
- zásahy a regulativní opatření ERÚ,
- zastaralá přenosová soustava, která není koncipována pro velké množství malých zdrojů,
- nerovnoměrná zátěž spotřeby energie,
- nerovnoměrný rozvoj lokálních zdrojů, zejména fotovoltanických zdrojů.

Pro zajištění dlouhodobého úspěchu společnosti v silné konkurenci je nutné:

- poskytovat komplexní služby,
- pružně se přizpůsobovat legislativním změnám,
- modernizovat přenosovou soustavu,
- využívat moderní technologie a nové energetické zdroje.

4.2.2. Prohlášení o aplikovatelnosti modelových organizací

Dokument Prohlášení o aplikovatelnosti (POA) vychází z přílohy A normy ISO 27001. Jeho prostřednictvím organizace specifikuje rozsah aplikace této normy, tj. které prvky normy budou v organizaci aplikovány. Organizace má možnost některé prvky normy vynechat, pokud tato oblast není relevantní vůči kontextu organizace, tj. zpravidla pokud je mimo předmět činnosti organizace. V případě vynechání prvku je potřeba uvést důvod. Jednotlivé položky POA jsou číslovány shodně s položkami přílohy A normy ve znění z roku 2014 (pozor, ve starším znění přílohy je označení některých položek odlišné).

Níže v textu bude pro každou modelovou organizaci jako příklad uvedena jedna položka, která bude ze seznamu vyloučena a to způsobem, jak takové vyloučení vypadá ve skutečném dokumentu (výňatek z dokumentu). Nemá smysl uvádět zde celý dokument, protože většina položek bývá zpravidla do implementace zahrnuta (zejména u větších organizací) a dokumenty si jsou tedy velice podobné. Celé dokumenty tak, jak mohou vypadat v praxi, jsou jako přílohy 4 – POA – státní správa, 5 – POA – zdravotnictví a 6 – POA – soukromá organizace.

Stručný popis obsahu jednotlivých položek dokumentu POA

Politiky bezpečnosti informací (A.5)

Politika bezpečnosti informací představuje základní strategii a principy, které říkají zaměstnancům a zainteresovaným stranám, jakým způsobem organizace chce plnit bezpečnostní požadavky v jednotlivých oblastech.

Základní politiky je obvykle výhodné rozpracovat do sad konkrétních pravidel určených pro jednotlivé skupiny zaměstnanců, např. manažeři organizace, vedoucí pracovníci, vlastníci aktiv, správci aktiv, ostatní zaměstnanci atd.

Organizace bezpečnosti informací (A.6)

Cílem je ustavit rámec řízení pro zahájení, řízení a provozování bezpečnosti řízení v organizaci a zajistit bezpečnost při použití mobilních zařízení pro práci na dálku. Bezpečnost informací musí být zohledněna v řízení projektů a to nezávisle na typu projektu.

Nástroje pro dosažení cíle jsou následující:

- definice a přidělení odpovědností,
- oddělení povinností pro snížení příležitostí k neoprávněné nebo neúmyslné modifikaci nebo zneužití aktiv,
- udržování přiměřených vztahů s příslušnými orgány a autoritami, s odbornými zájmovými skupinami nebo odbornými fóry na bezpečnost nebo s profesními sdruženími.

Bezpečnost lidských zdrojů (A.7)

Cílem je zajistit:

- srozumění zaměstnanců a smluvních stran se svými povinnostmi,
- vybrání vhodných kandidátů pro jednotlivé role,
- ochranu zájmů organizace při změně nebo ukončení pracovního poměru se zaměstnanci nebo smluvního poměru se smluvní stranou.

Všichni uchazeči musí být prověřeni podle platných zákonů a předpisů na základě požadavků týkajících se předmětu činnosti organizace a s ohledem na klasifikaci informací, ke kterým by měli získat přístup.

Pracovní smlouvy uzavřené se zaměstnanci musí obsahovat ustanovení o jejich odpovědnosti za bezpečnost informací.

Všichni zaměstnanci musí s ohledem na svou pracovní pozici dostávat odpovídající vzdělání a školení pro zvyšování povědomí o bezpečnosti informací a musí být plně a včas informování o změnách v politikách a postupech organizace.

Vedení musí implementovat proces disciplinárního řízení a přijetí opatření vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací.

Řízení aktiv (A.8)

Cílem je identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně. Seznam a klasifikaci aktiv provádí IT specialisté. Klasifikujeme informační systémy (IS) a informační zařízení (IZ), určujeme jejich vlastníky, správce (osoby odpovědné za nákup, licence apod.), oprávněné pracovníky a pracovníky zodpovědné za vedení dokumentace.

Informační systémy (software) třídíme mezi:

- systémový (operační systémy serverů a jiných zařízení, bezpečnostní software, komunikační programy atd.),
- aplikační sdílený (systémy pracující se sdílenými daty, obvykle typu klient-server),
- aplikační lokální (zahrnuje lokální aplikace, např. kancelářský software).

Informační zařízení (hardware) třídíme mezi:

- páteřní infrastrukturu,
- podpůrné technologie a zařízení,
- pracovní stanice a periferie,
- neobsluhovaná zařízení,
- mobilní zařízení.

Řízení přístupu (A.9)

Cílem je:

- omezit přístup k informacím a vybavení pro zprostředkování informací pouze pro osoby, které mají k těmto informacím oprávněný přístup,

- zajistit dostupnost informací osobám s oprávněným přístupem a předcházet neoprávněným přístupům k systémům, službám a aplikacím.

Management společnosti definuje obecné politiky pro zaměstnance, dodavatele a zákazníky. IT specialisté definují přístupy k sítím, síťovým službám, operačním systémům, databázím apod.

Kryptografie (A.10)

Cílem je zajistit řádné a efektivní užívání kryptografie (nauka o ochraně informací za použití šifrování) k ochraně důvěrnosti, autentičnosti a integrity informací. Řeší se softwarové klíče, problematika certifikátů, vymezují se osoby zodpovědné za jejich vydávání a aktuálnost, osoby zodpovědné za vydávání a udržování dokumentace apod.

Fyzická bezpečnost a bezpečnost prostředí (A.11)

Cílem je:

- předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace,
- předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a předcházet přerušení činnosti organizace z uvedených příčin.

Musí být definovány bezpečnostní perimetry k ochraně oblastí obsahujících citlivé nebo kritické informace nebo vybavení pro zpracování těchto informací. Tyto perimetry je nutné zajisti vhodným systémem vstupních kontrol pro zajištění přístupu pouze oprávněných osob a systémem fyzické ochrany proti přírodním katastrofám, haváriím nebo úmyslnému útoku. Je nutné navrhnout a aplikovat postupy pro práci v jednotlivých perimetrech a přístupové body pro nakládku a vykládku materiálu.

Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím i neoprávněným přístupem, což zahrnuje ochranu před

selháním napájení a dalších klíčových služeb a ochranu komunikačních rozvodů před odposlechem, rušením či poškozením. Musí být zajištěná správná údržba zařízení a zajištění jeho stálé dostupnosti a zamezení jeho přemisťování mimo příslušné perimetry bez schválení odpovědnou osobou. Aktiva nacházející se mimo prostory organizace je nutné zabezpečit s přihlédnutím k rizikům vyplývajících z použití mimo bezpečnostní perimetry organizace.

Nosiče dat musí být kontrolovány před likvidací tak, aby se zajistilo bezpečné odstranění citlivých dat z těchto zařízení a předešlo se tak možnosti zjištění celku nebo části citlivých dat z fyzicky znehodnoceného nosiče. Dále je nutné zajistit přiměřenou ochranu všech zařízení bez obsluhy a zajištění zásad prázdného stolu a prázdné obrazovky u sdíleného vybavení pro zpracování informací.

Bezpečnost provozu (A.12)

Cílem je zajistit správný a bezpečný provoz vybavení pro zpracování informací.

Řeší se:

- zajištění tohoto vybavení proti ztrátě a škodám na informacích způsobených škodlivými kódy,
- integrita více systémů,
- nástroje k obraně proti zneužití technických zranitelností,
- minimalizace dopadů auditních činností na provozní systémy,
- postupy tvorby a správy záznamů o událostech.

Bezpečnost komunikací (A.13)

Cílem je zajistit ochranu informací v sítích a přidružených prostředích pro zpracování informací.

Norma se zde zaměřuje na bezpečnost informací při jejich přenosu v rámci organizace i s externími subjekty. V tomto kontextu se řeší kapacity sítě, bezpečnostní

nastavení bezdrátových sítí, monitorování provozu v sítích, oddělení jednotlivých částí sítě apod.

Akvizice, vývoj a údržba informačních systémů (A.14)

Cílem je zajistit aktualizace softwarových komponent v potřebném rozsahu a bez nežádoucích vlivů na bezpečnost informačních systémů.

Řeší se:

- správa, aktualizace a evidence operačních a databázových systémů,
- správa testovacích systémů a dat,
- správa a údržba programového vybavení,
- nastavení doménových politik ve vztahu k aktualizacím a správa licencí.

Dodavatelské vztahy (A.15)

Cílem je zajištění ochrany aktiv organizace, ke kterým mají dodavatelé přístup, a údržba dohodnuté úrovně bezpečnosti informací pro dodávky služeb ve shodě s dodavatelskými dohodami.

Těchto cílů se dosahuje jasnými a oboustranně odsouhlasenými dohodami a dokumenty s dodavateli, které řeší bezpečnost, přístup, zpracování a komunikaci dat mezi zúčastněnými stranami.

Organizace je povinna pravidelně monitorovat, přezkoumávat a auditovat dodávky a vést řízení změn v udržování a zlepšování existujících politik, postupů a opatření bezpečnosti informací.

Řízení incidentů bezpečnosti informací (A.16)

Cílem je zajistit efektivní přístup ke zvládání incidentů bezpečnosti a komunikace ohledně bezpečnostních událostí a slabých míst.

Pro zajištění efektivní a rychlé reakce na incident bezpečnosti informací je nutné, aby:

- byly ustanoveny postupy a odpovědnosti pro zvládání incidentů,
- byly události co nejrychleji hlášeny příslušnými komunikačními kanály,
- po zaměstnancích a dalších osobách ve vztahu k organizaci bylo požadováno všímat si a hlásit jakákoliv slabá místa v systémech.

Nahlášené události musí být posouzeny a následně musí být rozhodnuto o jejich klasifikaci. Organizace musí reagovat na incidenty v souladu s dokumentovanými postupy, provádět analýzy řešení incidentů k zavádění opatření ke snižování pravděpodobnosti nebo dopadu podobných incidentů v budoucnosti a definovat a aplikovat postupy pro identifikaci, sběr a uchování informací sloužících jako důkazy k proběhlým incidentům.

Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací (A.17)

Cílem je zajištění kontinuity činnosti organizace v případě výskytu incidentu.

V první řadě musí organizace určit požadavky na kontinuitu řízení bezpečnosti informací za nepříznivých situací, např. během havárií nebo katastrof. Dalším krokem je zdokumentování a implementování procesů a postupů k zajištění požadované úrovně kontinuity a jejich následné udržování. Implementovaná opatření se musí v pravidelných intervalech verifikovat.

Soulad s požadavky (A.18)

Cílem je vyvarovat se porušení zákonných, předpisových nebo smluvních povinností týkajících se bezpečnosti informací a bezpečnostních požadavků.

Pro každý informační systém musí být identifikovány, dokumentovány a udržovány aktuální zákonné a smluvní požadavky. Jejich dodržování zajišťuje

implementace a správa vhodných postupů. Záznamy musí být chráněny proti ztrátě, zničení, padělání, odcizení a zveřejnění.

Státní správa

Tabulka 9: výňatek z tabulky POA pro organizaci státní správy

Kapitola normy	Název kapitoly normy	Opatření je zahrnuto	Důvod vyloučení prvku normy
A.6.2	Mobilní zařízení a práce na dálku	-	-
A.6.2.1	Politika mobilních zařízení	ANO	
A.6.2.2	Práce na dálku	NE	Organizace neumožňuje zaměstnancům ani dodavatelům vzdálený přístup.

Zdravotnictví

Tabulka 10: výňatek z tabulky POA pro zdravotnickou organizaci

Kapitola normy	Název kapitoly normy	Opatření je zahrnuto	Důvod vyloučení prvku normy
A.9.4	Řízení přístupu k systému a aplikacím	-	-
A.9.4.1	Omezení přístupu k informacím	ANO	
A.9.4.2	Bezpečné postupy přihlášení	ANO	
A.9.4.3	Systém správy hesel	ANO	

A.9.4.4	Používání privilegovaných programových nástrojů	ANO	
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	NE	Organizace neprovádí vývoj vlastního SW.

Soukromá organizace

Tabulka 11: výňatek z tabulky POA pro soukromou organizaci

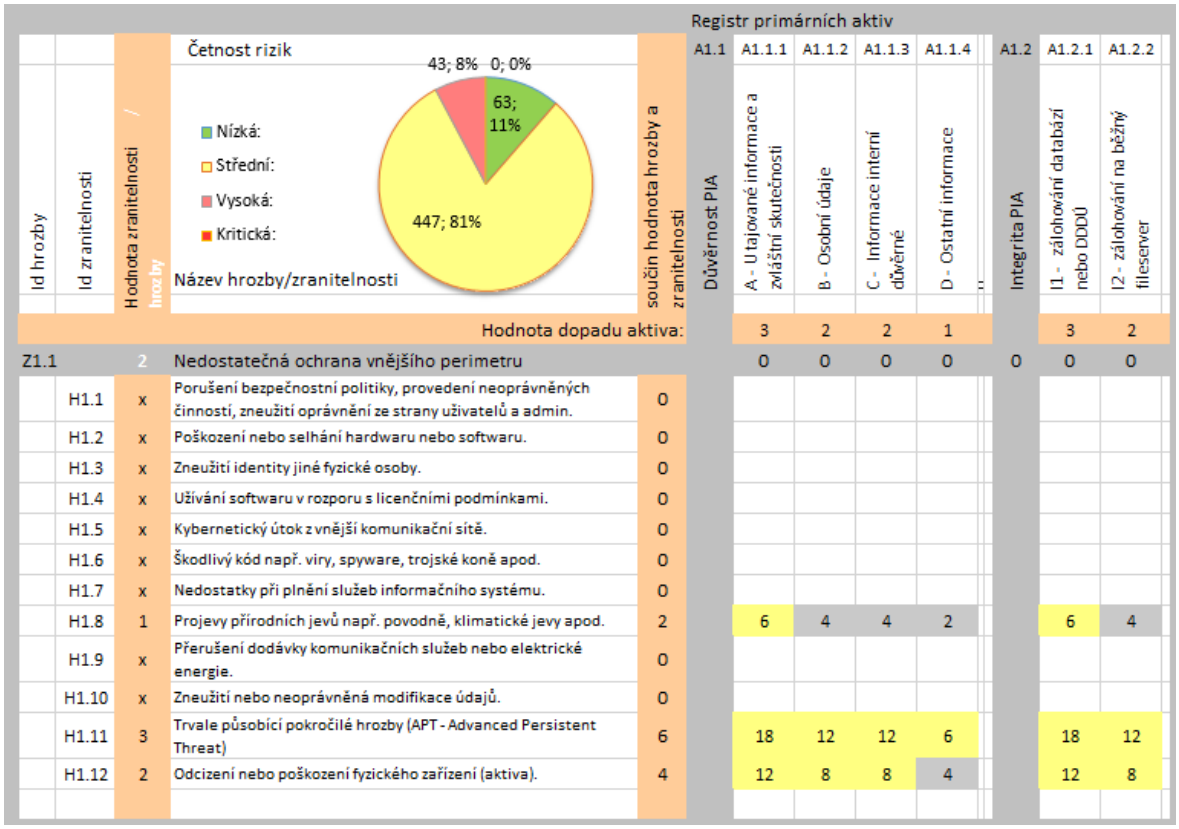
Kapitola normy	Název kapitoly normy	Opatření je zahrnuto	Důvod vyloučení prvku normy
A.11.2	Zařízení	-	-
A.11.2.1	Umístění zařízení a jeho ochrana	ANO	
A.11.2.2	Podpůrné služby	ANO	
A.11.2.3	Bezpečnost kabelových rozvodů	ANO	
A.11.2.4	Údržba zařízení	ANO	
A.11.2.5	Přemístění aktiv	ANO	
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	NE	Organizace nemá žádná odloučená pracoviště ani žádná stálá aktiva mimo vlastní prostory.
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	ANO	
A.11.2.8	Uživatelská zařízení bez obsluhy	ANO	

A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	ANO	

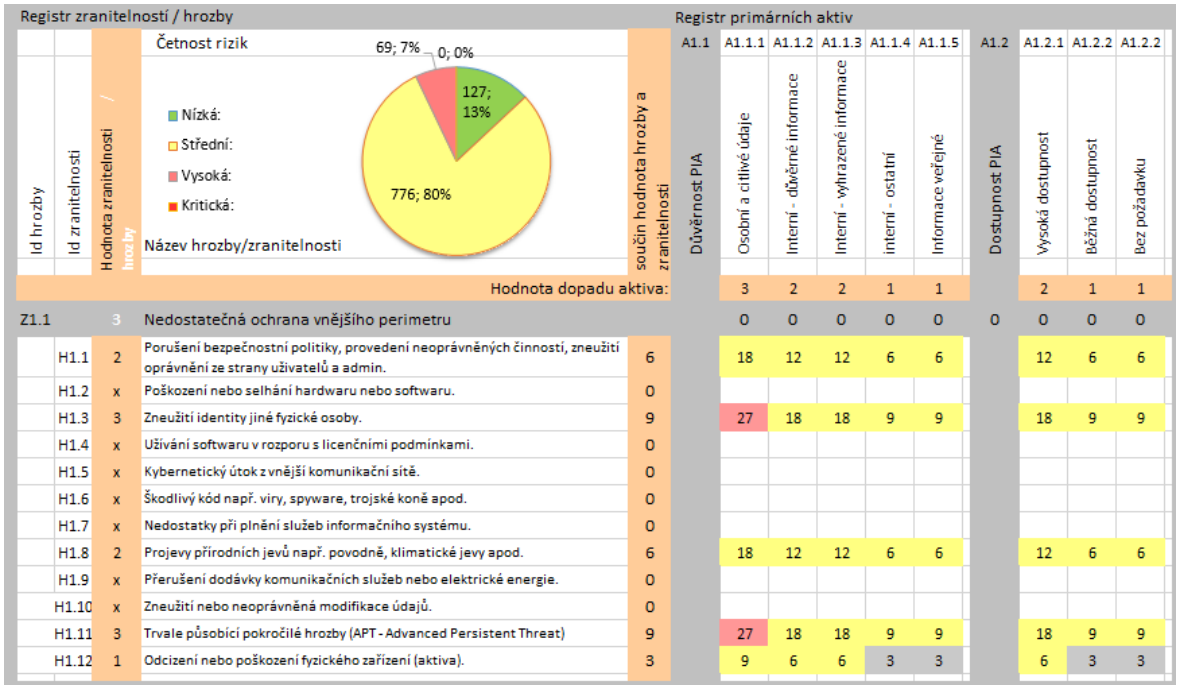
4.2.3. Analýza rizik modelových organizací

Analýza rizik modelových organizací je provedena podle metodiky a metrik stanovených přílohami 1 - Hodnocení úrovně důležitosti aktiv a 2 - Hodnocení rizik vyhlášky Národního bezpečnostního úřadu č. 316/2014 Sb., o kybernetické bezpečnosti, viz kapitoly 3.3.2 a 3.3.3.

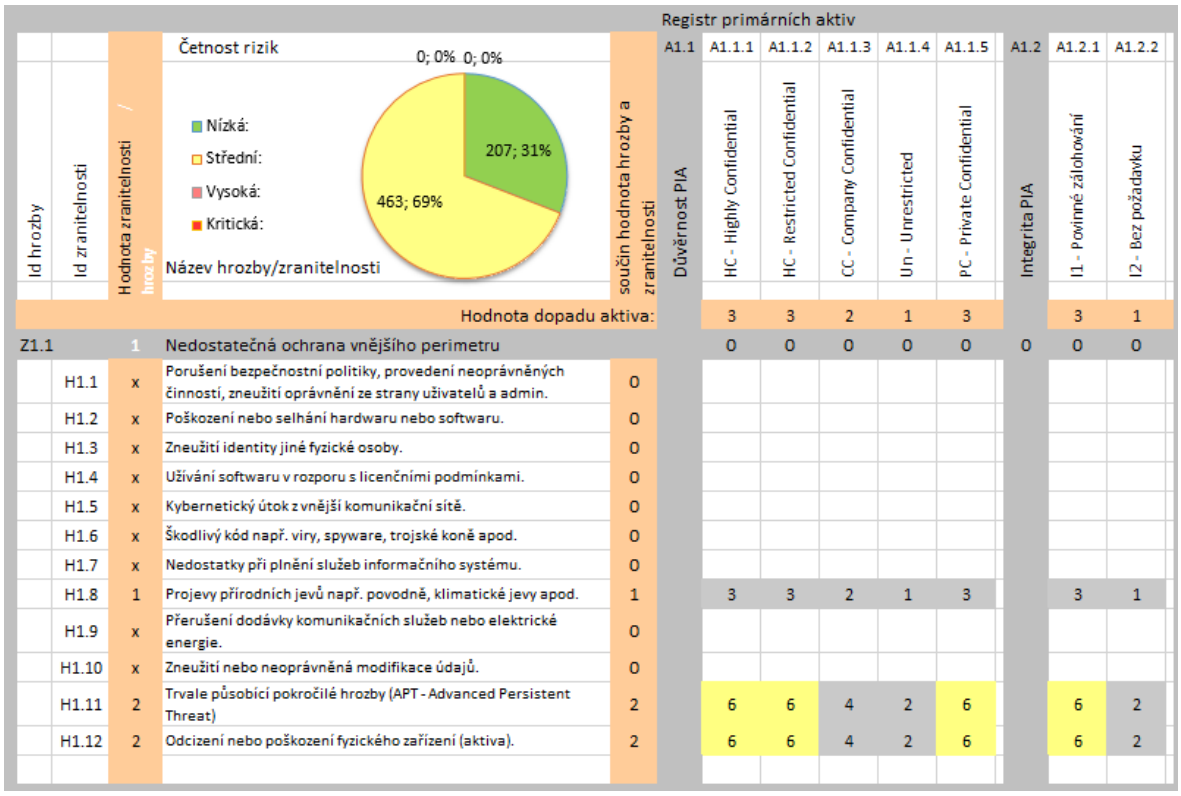
Vlastní analýzu rizik pro každou modelovou organizaci obsahují přílohy 7 – AR – státní správa, 8 – AR – zdravotnictví a 9 – AR – soukromá organizace. Zde jsou výňatky z těchto příloh, které budou popsány v následující kapitole.



Obrázek 5: analýza rizik státní správy



Obrázek 6: analýza rizik nemocnice



Obrázek 7: analýza rizik soukromé organizace

Popis tabulek analýzy rizik

Řádky tabulky obsahují hrozby H1.1 až H1.12 pro každou zranitelnost Z1.1 až Z1.7 a Z2.1 až Z2.4. Sloupce tabulky obsahují primární informační aktiva klasifikovaná dle požadavků na stupeň důvěrnosti, dostupnosti a integrity. V případě zdravotnické organizace jsou primární informační aktiva doplněna o klasifikaci dle požadavků na spolehlivost informací. Pro soukromé organizace a státní správu nejsou požadavky na spolehlivost informací strukturovány do více skupin, tj. soubor těchto požadavků je společný pro všechna primární informační aktiva.

Pro každou zranitelnost je ve sloupci „Hodnota zranitelnosti" určena míra zranitelnosti souvisejících podpůrných aktiv (řádky Zx). Pro každou relevantní hrozbu vůči zranitelnosti je ve stejném sloupci určena hodnota pravděpodobnosti vzniku hrozby (řádky Hx). Pro irelevantní hrozby je použit křížek, který znamená, že hrozba je z hodnocení vyloučena. Sloupec „Součin hodnoty hrozby a zranitelnosti" obsahuje součin hodnoty zranitelnosti a pravděpodobnosti vzniku hrozby. Pro každé relevantní primární informační aktivum je v řádku „Hodnota dopadu aktiva" stanovena hodnota škody, která vznikne jako důsledek porušení důvěrnosti, dostupnosti, integrity nebo spolehlivosti primárního informačního aktiva. Irelevantní informační aktiva jsou vyloučena křížkem.

Výsledná matice rizik je dána oblastmi „Registr zranitelností" a „Registr primárních aktiv". Každá buňka registru primárních aktiv, která obsahuje číselnou hodnotu, představuje relevantní riziko. Číslo v buňce vyjadřuje hodnotu rizika, která je výsledkem součinu hodnoty zranitelnosti, pravděpodobnosti rizika a hodnoty dopadu aktiva.

Uvedenou metodikou hodnotu rizika posuzujeme podle hodnoty pravděpodobnosti vzniku hrozby, hodnoty zranitelnosti souvisejících podpůrných aktiv a hodnoty dopadů (škod) při porušení důvěrnosti, dostupnosti, integrity nebo spolehlivosti primárních informačních aktiv. Kombinací registru zranitelností, registru hrozeb a registru primárních informačních aktiv vzniká třírozměrná matice, která je

relativně velká, např. pro zdravotnickou organizaci vzniká 972 relevantních rizik. 3D tabulku lze rozložit do 2D tabulky tak, že jednotlivé tabulky pro každou zranitelnost zařadíme pod sebe do dalších řádků (jak je vidět v přílohách). Takové tabulky jsou přehledné. Pro další zvýšení přehlednosti je použito podmíněné formátování buněk. Buňky nízkých rizik mají barvu zelenou, střední rizika mají barvu žlutou, vysoká rizika oranžovou a kritická rizika červenou.

Tabulku lze dále analyzovat. Je možné určit nejvyšší hodnotu rizika pro každou hrozbu v rámci každé zranitelnosti. Stejně tak lze určit maxima rizik pro každou zranitelnost. Pro tzv. „manažerský souhrn“ je vhodné stanovit četnost rizik nízkých, středních, vysokých a kritických. K tomu slouží pomocné výpočty na konci přehledu a koláčový diagram.

Srovnání modelových organizací

Pro každou sledovanou oblast bezpečnosti informací (státní správa, zdravotnictví a soukromá sféra) byly vytvořeny modelové organizace, které slouží jako případové studie zastupující danou oblast, viz kapitola 4.1. Protože pro všechny modelové organizace je použita stejná metodika analýzy rizik a jsou také použity stejné metriky, tj. parametry hodnocení rizik, je možné provést srovnání výstupů z analýzy rizik.

Státní správa

Dle kontextu organizace v příloze „1 – KO – státní správa“ se jedná o magistrát města, který v samostatné působnosti plní úkoly uložené zastupitelstvem a radou města a dále zajišťuje výkon přenesené působnosti státu v rozsahu stanoveném příslušnými zákony. Ve své působnosti a podle příslušné legislativy město spravuje velké množství agend.

Magistrát pro všechny oblasti zranitelností (Z1.1 – Z1.7 a Z2.1 – Z2.4) identifikoval celkem 553 rizik, které ohodnotil a zařadil do čtyř skupin takto: počet rizik nízkých 63, středních 447, vysokých 43, kritických 0.

Z analýzy rizik je zřejmé, že magistrát města implementoval základní resp. běžná organizační i technická opatření pro většinu informačních aktiv a oblastí bezpečnosti informací. Organizace proto nemá žádná kritická rizika. Existují však i vysoká rizika. Největší četnost je v oblasti rizik středních. Tento stav je důsledkem skutečnosti, že magistrát města spravuje velké množství agend, z nichž mnohé obsahují důvěrné a cenné informace.

Město tedy musí implementovat soubor dalších ochranných opatření pro ošetření zejména vysokých rizik. V případě středních rizik, kterých je nejvíce, je potřeba zvážit, zda náklady na zavedení ochranných opatření jsou efektivní vůči případným škodám. Po implementaci opatření musí město provést opakovanou analýzu rizik, která umožní porovnat účinnost provedených ochranných opatření.

Zdravotnictví

Podle kontextu organizace v příloze „2 – KO - zdravotnictví“ se jedná o středně velkou nemocnici okresního typu. Nemocnice spravuje množství agend včetně pacientské dokumentace, která obsahuje informace s vysokými požadavky na důvěrnost, ale také klade mimořádné požadavky na dostupnost, integritu a spolehlivost obsahu informací. Incidenty v oblasti informační bezpečnosti mohou mít dopady na zdraví a životy lidí. Hodnocení dopadů a škod na primární informační aktiva v oblasti hrozeb souvisejících s poskytováním zdravotní péče má proto zpravidla vyšší hodnoty.

Z výše uvedených důvodů není překvapením, že nemocnice identifikovala celkem 776 rizik. Pro oblast zdravotnictví jsou některá základní pravidla nakládání s pacientskou dokumentací přesně stanovena příslušnou legislativou. Také nemocnice si sama dobře uvědomuje potřebu ochrany informačních technologií a informací samotných. Některé oblasti jsou proto zabezpečeny dobře, čemuž odpovídá 127

nízkých rizik. Není však věnována dostatečná pozornost zejména oblasti sociálního inženýrství a pokročilých hrozeb (ATP). Proto bylo identifikováno nezanedbatelné množství vysokých rizik, celkem 69.

Nemocnice musí ošetřit slabá místa v bezpečnosti informací pomocí souboru dodatečných organizačních a technických opatření a poté provést novou analýzu rizik pro identifikaci tzv. zbytkových rizik. Také by měla věnovat pozornost středním rizikům, kterých je nevětší četnost, celkem 776. Protože její rozpočet je velmi omezený a účinná technická opatření bývají finančně náročná, měla by se nejdříve soustředit na nízkonákladová opatření, do kterých patří zejména organizační opatření, zavedení monitoringu a pravidelných kontrol, školení zaměstnanců v oblasti bezpečnosti informací apod.

Soukromá sféra

Podle kontextu organizace v příloze „3 – KO – soukromá organizace“ se jedná o velkou společnosti působící v oblasti energetiky. Organizace spadá do působnosti kybernetického zákona a má již několik let zaveden systém ISŘ (integrovaný systém řízení), který zahrnuje také normu ISO 27001. Prostřednictvím platného certifikátu této normy, metodiky analýzy rizik a dalších dokumentů požadovaných § 29 vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti, organizace dokládá plnění požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

Organizace již rutinním způsobem umí řídit rizika. Proto není překvapením, že aktuální analýza rizik identifikovala pouze rizika v oblastech středních a nízkých hodnot. Svědčí to o tom, že byly již opakovaně instalovány soubory organizačních a účinných technických ochranných opatření a prováděny opakované analýzy rizik pro zjištění efektivity těchto opatření. Skutečnost, že i přesto existuje velké množství středních rizik, je výsledkem skutečnosti, že organizace působí v oblasti energetiky, kde existují velmi závažné hrozby s vysokými možnými dopady.

V oblasti působnosti organizace probíhá rychlý technický rozvoj a vznikají stále nové hrozby a rizika. Proto musí organizace vytrvat a neustále hodnotit a zlepšovat svůj bezpečnostní systém.

4.2.4. Ošetření rizik modelových organizací

Proces ošetření rizik musí být řízen, tj. plánován. Proto organizace vytvářejí tzv. plán ošetření rizik. Pro jednotlivé modelové organizace jsou vytvořeny příklady plánu ošetření rizik jako přílohy 10 – POR – státní správa, 11 – POR – zdravotnictví a 12 – POR – soukromá organizace. Výňatky z těchto příloh jsou u jednotlivých typů organizací uvedeny níže v podobě zjednodušených tabulek pro představu a porovnání.

Organizace musí prioritně řešit rizika kritická, následně vysoká a případně i střední. Nízká rizika může naopak akceptovat, protože pro taková rizika jsou realizována již dostatečně účinná opatření, mají malou pravděpodobnost vzniku nebo případné dopady a možné škody jsou relativně nízké.

Při stanovení způsobu ošetření rizik je třeba hledat významné zranitelnosti podpůrných aktiv. To lze provést zpětnou analýzou tabulky analýzy rizik, tzv. obráceným postupem. Pro červeně označené buňky (kritická rizika) hledáme související zranitelnosti, hrozby a primární aktiva. Podobným způsobem můžeme postupovat i pro vysoká rizika.

Postup výběru opatření je blíže popsán v kapitole 3.3.4. Podstatné je umět identifikovat všechna chybějící opatření a posoudit možnosti a vhodnost jejich implementace.

Státní správa

Tabulka 12: výňatek z tabulky POR pro státní správu

Označení zranitelnosti	Popis opatření	Odpovědná osoba	Předpokládané náklady (Kč)
Z1.7 Z1.4	Provádět monitoring a pravidelnou kontrolu připojených chytrých telefonů.	Vedoucí odboru IT	-
Z1.7	Určit pravidla pro oddělení povinností IT techniků a outsourcera při přístupu k zálohám a archivům dat.	Vedoucí odboru IT	-
Z1.2 Z2.1	Instalovat plynové automatické hasicí zařízení v prostoru serveru a centrální spisovny.	Vedoucí odboru vnitřní správy	350 000 – 400 000
Z1.2	Proškolit zaměstnance v oblasti sociálního inženýrství a hrozeb kybernetických útoků, školení ISMS a penetrační testy.	Vedoucí odboru IT	5 000 – 10 000
-	Zakoupit systém Mobile Device Management.	Vedoucí odboru IT	15 000

Magistrát města vytvořil a schválil v pořadí již druhý plán ošetření rizik. Opatření z prvního plánu byla realizována a na základě identifikace zbytkových rizik z následné analýzy jsou doporučena další dodatečná opatření. Organizace navrhuje jak technická, tak i organizační opatření, která by měla odstranit zbývající slabá místa bezpečnostního systému, která byla zjištěna nezávislým auditem.

Zdravotnictví

Tabulka 13: výňatek z tabulky POR pro zdravotnickou organizaci

Označení zranitelnosti	Popis opatření	Odpovědná osoba	Předpokládané náklady (Kč)
Z2.1 Z1.3	Vyřadit platformu operačních systémů Windows SRV 2000 a 2003 z důvodů ukončení podpory.	Vedoucí oddělení ICT	270 000
Z2.1 Z1.3	Realizovat redundanci hlavního internetového připojení od koncového bodu poskytovatele a uzlového bodu počítačové sítě v nemocnici.	Vedoucí oddělení ICT	80 000
Z1.3	Přemístit centrální spisovnu do vhodných prostor pro splnění legislativních bezpečnostních požadavků.	Provozně technický náměstek	350 000
Z2.1 Z1.5 Z1.3	Realizovat virtualizaci páteřní infrastruktury - zakoupit nový server a provést migraci dat.	Vedoucí oddělení ICT	800 000
Z2.2 Z1.5	Vyřadit všechny zastaralé počítačové stanice s nepodporovanou verzí operačního systému.	Vedoucí oddělení ICT	200 000

Je zřejmé, že se organizace dlouhodobě potýká s nedostatkem finančních zdrojů, Plán ošetření rizik proto zahrnuje požadavky na výměnu starých IT technologií a dále opatření pro zvýšení bezpečnosti prostor, v nichž jsou důležité technologie umístěny. Organizace musí rovněž přemístit centrální spisovnu ze zcela nevyhovujících prostor, kde způsob uložení spisů je v rozporu s legislativními požadavky. Všechna navržená opatření mají technický charakter, jsou nezbytná, ale také nákladná. Organizace proto musí stanovit priority a soubor technických opatření řešit postupně v rámci plánování svých rozpočtů.

Zjevným nedostatkem tohoto plánu je absence organizačních opatření, která jsou zpravidla nízkonákladová a proto je lze realizovat bezodkladně. Některá technická opatření mohou být neúčinná, pokud nejsou doplněna vhodnými organizačními opatřeními. Nemocnice by tedy svůj plán ošetření rizik měla přizpůsobit možnostem svého rozpočtu, doplnit jej o harmonogram implementace opatření (drahá opatření rozdělit do více etap) a zejména doplnit o související organizační opatření.

Soukromá organizace

Tabulka 14: výňatek z tabulky POR pro soukromou organizaci

Instalov.	Plánov.	KII	VIS	§	Popis opatření
I. Organizační opatření					
X		X		3	Stanovení rozsahu a hranic systému řízení bezpečnosti informací a určení, kterých organizačních částí a technických prvků se systém řízení bezpečnosti informací týká.
X	X		X	4	Určení metodiky pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik.
X			X	5	Stanoví bezpečnostní politiky v oblastech a) až n) (14 oblastí).
II. Technická opatření					
X		X	X	16	Nezbytná technická opatření k zamezení neoprávněnému vstupu do vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva.
	X	X		17	Využití nástrojů pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.

	X	X	X	18	Nástroj pro ověření identity uživatelů a administrátorů informačního systému, který zajišťuje ověření jejich identity před zahájením jejich aktivit v informačním systému.

Zde se jedná se o velkou organizaci působící v oblasti energetiky, která má již víceleté zkušenosti s ISŘ (integrovaný systém řízení). Má tedy i zkušenosti s řízením rizik včetně jejich plánování a ošetřování. Nyní tato organizace stojí před náročným úkolem, a to zajistit soulad s požadavky kybernetického zákona v oblasti kritické infrastruktury.

Protože v rámci ISŘ má organizace také implementovaný a certifikovaný systém podle ISO 27001, je zřejmé, že organizace již dříve zavedla ochranná opatření pro všechny relevantní oblasti podle přílohy A normy a v rozsahu prohlášení o aplikovatelnosti v souladu se svým kontextem organizace.

Cílem nového plánu ošetření rizik je tedy porovnat a zajistit soulad s požadavky kybernetického zákona. Organizace musí určit chybějící technická a organizační opatření a stanovit priority pro jejich zavedení. Protože z výsledků analýzy rizik vyplynulo, že organizace nemá žádná kritická ani vysoká rizika, nehrozí prodlení při implementaci opatření ani žádné sankce ze strany Národního bezpečnostního úřadu.

Plán ošetření rizik je součástí registru opatření podle vyhlášky o kybernetické bezpečnosti. Organizace provedla porovnání již implementovaných opatření s tímto registrem. Chybějící opatření jsou označena ve sloupci „Zahrnout do plánu implementace“. Pomocí příslušných filtrů lze vybrat ochranná opatření, která jsou určena k implementaci.

4.3. Implementace a certifikace normy ISO 27001

4.3.1. Postup implementace krok za krokem

Pro úspěšnou implementaci normy ISO 27001 je třeba postupně realizovat všechny požadavky její požadavky. Vhodné pořadí činností zajistí plynulost celého procesu, což šetří čas i náklady.

Následuje postup implementace tak, jak jej doporučuje společnost MANA Consulting s.r.o., zabývající se poradenstvím v oblasti řízení procesů, bezpečnosti informací, informačních systému aj.

1. Situační audit v organizaci
   - zjištění výchozího stavu,
   - zpracování úvodní analýzy.
2. Stanovení kontextu organizace
   - porozumění organizaci,
   - porozumění prostředí, v němž organizace vykonává svojí činnost,
   - porozumění požadavkům jejich zainteresovaných stran.
3. Stanovení rozsahu aplikovatelnosti normy (POA)
   - určení rozsahu aplikace normy v rámci přílohy A, a to v souladu s kontextem organizace.
4. Analýza rizik
   - identifikace informačních aktiv a jejich hodnocení,
   - identifikace hrozeb, zranitelností a jejich hodnocení,
   - identifikace rizik a jejich hodnocení.
5. Ošetření rizik
   - plánování technických i organizačních opatření,
   - porovnání plánovaných opatření s přílohou A normy pro kontrolu, zda nebyla některá opatření opomenuta,
   - stanovení základních politik,
   - stanovení odpovědností.
6. Vytvoření tzv. dokumentovaných informací

- určení základních zásad a pravidel pro odborné pracovníky, vedoucí pracovníky, vlastníky aktiv a ostatní zaměstnance,
- vedení záznamů o procesech a činnostech,
- stanovení rozsahu monitoringu a kontrol.

7. Řízení incidentů
   - stanovení kritérií pro nedostatky, incidenty a havárie,
   - určení způsobu vypořádání se s incidenty,
   - stanovení procesu řízení neshod,
   - řízení stížností a námětů pro zlepšování,
   - plánování preventivních opatření.
8. Výcvik zaměstnanců
   - školení odborných pracovníků, vedoucích zaměstnanců a ostatních zaměstnanců v oblasti bezpečnosti informací,
   - vytvoření plánu vzdělávání a rozvoje všech zaměstnanců,
   - určení adaptačního procesu pro nové zaměstnance,
   - hodnocení zaměstnanců.
9. Přezkoumání systému
   - zainteresování (informovanost a rozhodovaní) vedení organizace,
   - interní audity,
   - nezávislé audity,
   - nezávislé přezkoumání a certifikace.

4.3.2. Certifikace

Společnost ISO normy pouze vyvíjí, jejich certifikací se nezabývá. Tento úkol spadá pod tzv. certifikační autority, tj. externí organizace oprávněné vydávat příslušné certifikáty. Jedná se o orgány, které by svojí nezávislostí měly zaručit nezaujatost při udělování certifikátů. Jsou sdruženy pod hlavičkou asociace známé pod označením IQNet – The International Certification Network.

Mezi členy patří např. německá organizace DQS (Deutsche Gesellschaft zur Zertifizierung von Managementsystemen), francouzká AFNOR (Association Française de Normalisation), japonská JQA (Japan Quality Assurance Organization) a další. Kompletní seznam členů je možné získat na této internetové adrese: http://www.iqnet-certification.com/index.php?page=homecontent&ID=128 (odkaz ze dne 2. 10. 2015). V České republice jsou zdejší členové IQNetu sdruženi ve skupině CQS (Association for Quality System Certification).

Všichni tito členové jsou vázáni společnou dohodou MLA (Multi-Lateral Agreement), která zajišťuje, že certifikát jednoho člena má stejnou váhu, jako by jej vydal jakýkoliv jiný člen asociace. Díky tomu mohou být tyto certifikace uznávány na mezinárodní úrovni.

Certifikace ISMS se provádí podle normy ISO 27002. Zjednodušeně se někdy říká, že ISO 27001 je normou pro organizace a ISO 27002 je normou pro auditory.

Udělení certifikátu

Při udělování certifikátu se obvykle postupuje následujícími kroky:

1. Poptávka po certifikátu
2. Informativní schůzka
3. Písemná žádost
4. Registrace a projednání žádosti ve skupině CQS
5. Delegace pravomocí na člena skupiny CQS
6. Jmenování auditního týmu
7. Certifikační audit 1. stupně
8. Nápravná opatření (jsou-li potřeba) a případné opakování předchozího bodu
9. Certifikační audit 2. stupně
10. Nápravná opatření (jsou-li potřeba) a případné opakování předchozího bodu
11. Návrh certifikátu

12. Vydání certifikátu

Společnost se při zobrazování certifikátu nemůže prokázat formou „ISO certified“, ale musí být vždy uvedeno označení normy a rok úpravy. Správný tvar je tedy např. "ISO 27001:2013 certified".

Obnova certifikátu

Platnost certifikátu je tři roky. Pokud si chce organizace certifikát udržet, musí se průběžně podrobovat nezávislým auditům. Dílčí audity, které kontrolují pouze klíčové prvky normy, se provádí jednou ročně nebo každých šest měsíců. Frekvenci dílčích auditů si může organizace zvolit sama podle svých potřeb. Některým organizacím může tento způsob častějších, ale kratších auditů vyhovovat více. Každé tři roky se provádí velký re-certifikační audit, který je svým rozsahem shodný s certifikačním auditem při udělování certifikátu.

4.4. Zhodnocení rozdílů pro různé typy organizací

Různé organizace mají odlišnou motivaci pro zavádění systémů bezpečnosti informací.

Aby autor nevycházel pouze z teoretické roviny a zkušeností někoho dalšího, rozhodl se se provést svůj vlastní průzkum. Formou dotazníku oslovil několik zástupců vybraných společností a zjišťoval informace související s důvody, náročností, dopadů a zpětným hodnocením procesu zavádění normy ISO 27001. Výsledky průzkumu budou prezentovány dále v této kapitole.

Pro pochopení rozdílů při zavádění normy ISO 27001 do různých typů organizací jsou důležité zejména kontexty těchto organizací. Kontext organizace umožňuje pochopit podstatu organizace, jejich cíle a očekávání zainteresovaných stran.

Obecně lze říci, že hlavní motivací pro zavedení normy v případě státních orgánů a zdravotnických zařízení je snaha plnit legislativní požadavky. Nemocnice potřebují plnit zákon o ochraně osobních údajů. Úřadů se tento zákon také dotýká významně a navíc musí plnit požadavky zákona o svobodném přístupu k informacím, což klade vysoké nároky na členění informací. U soukromých organizací bývá častým motivem účast na veřejných zakázkách, ochrana svého know-how, požadavky zainteresovaných stran, konkurenční výhoda nebo prestiž.

Klíčový je tedy cíl a okolnosti zavádění normy. Organizace se primárně zaměřují na ty části normy, které jim pomáhají plnit jejich cíle. Některé organizace plní pouze část požadavků normy, protože certifikace není jejich cílem. Jiné, které mají o certifikaci zájem, plní sice všechny požadavky, ale některé z nich jen v minimálním stanoveném rozsahu, zatímco požadavky vztahující se k jejich cílům řeší komplexněji (např. klasifikace a třídění informačních aktiv).

Oslovený jednatel poradenské firmy MANA Consulting s.r.o. Jaromír Novotný podle svých zkušeností dělí motivy soukromých firem na snahu o zlepšení situace informační bezpečnosti (20 % případů) a požadavky jejich zákazníků nebo dodavatelů (80 % případů). Uvádí, že soukromé organizace více než ty státní doceňují hodnotu vložených investic a zavedené bezpečnostní systémy lépe a pečlivěji udržují.

V případě zdravotnických zařízení a organizací veřejné správy pan Novotný uvádí jako největší problém pochopení vztahu řízení bezpečnosti informací a legislativních požadavků České republiky. Bývá složité přesvědčit vedení těchto organizací o potřebě zavádění řízených postupů. Pokud se tento krok povede zvládnout, pak vlastní příprava těchto organizací na plnění požadavků normy není více problematická než u soukromých organizací. Komplikovaná je spíše následná edukace zaměstnanců a údržba nastavených systémů a postupů.

Pan Novotný dále upozorňuje, že ve státních organizacích často chybí průběžná údržba a organizace se pak vše snaží dohnat na poslední chvíli krátce před plánovaným auditem. Často zde chybí tlak ze strany vedení na zaměstnance, který by je nutil zavedené postupy a systémy dodržovat, používat a udržovat. Absence tohoto tlaku souvisí s již zmíněným nepochopením důležitosti zavedených opatření vedením.

Naštěstí se však podle názoru pana Novotného situace v průběhu let od zavedení normy zlepšuje, jak si zaměstnanci na zavedené změny začínají pomalu zvykat.

4.4.1. Zjištění na základě dotazníku

Na základě získaných kontaktů bylo osloveno několik osob v různých organizacích na pozicích souvisejících se správou ICT. Oslovováni byli pouze zástupci takových organizací, u kterých byl předpoklad, že se otázkou zavádění normy ISO 27001 zabývají nebo se jí zabývaly v minulosti. Nejedná se tedy o výběr, který má za cíl reprezentovat kompletní spektrum organizací působících na území České republiky. Dotazník autor koncipoval jako neanonymní, aby zvýšil důvěryhodnost získaných informací, nicméně někteří zúčastnění vyjádřili požadavek, aby v textu nebyly spojovány konkrétní odpovědi se společností, jejíž jménem vystupují. Z řady oslovených se nakonec o své zkušenosti rozhodli podělit zástupci jedenácti organizací.

7 z oslovených společností uvedlo, že již jsou držitelem certifikátu normy ISO 27001. 1 organizace se o certifikát uchází a 1 plánuje zavádět normu v budoucnosti. Zbylé 2 organizace normu aplikovat neplánují. Tyto 2 organizace v dalších otázkách týkajících se normy nefigurují.

Z takto redukovaného seznamu 9 respondentů jich 6 uvedlo, že se významně podíleli na procesu zavádění normy do jejich společnosti, a zbývající 3 uvedli jen okrajovou účast. V souboru není nikdo, kdo by se nepodílel na zavádění normy do své společnosti a tak můžeme prohlásit tento soubor za oprávněný vyjadřovat se k dalším otázkám.

Mezi organizacemi, které poskytly své zkušenosti a názory níže prezentované, jsou např. tyto: Pardubická nemocnice, Chrudimská nemocnice, město Zábřeh, Krajský úřad Pardubice, ABB s.r.o., Remak a.s. a další. Je tedy pokryt sektor státní správy, zdravotnických zařízení i soukromých organizací.

Na otázku, z jakého důvodu se organizace rozhodla zavádět normu ISO 27001, byla nejčastější odpověď potřeba chránit informace partnerů nebo zákazníků (8 hlasů).

Se shodným množstvím odpovědí následuje plnění legislativních požadavků České republiky a potřeba lepší ochrany vlastních informačních aktiv (7 hlasů). 1 respondent uvedl jako důvod potřebu vyhovět kybernetickému zákonu. V této otázce mohl každý zvolit více vyhovujících odpovědí.

Otázka na posouzení obtížnosti a nákladnosti procesů spojených s uvedením věcí do souladu s požadavky normy ISO 27001 má poměrně zajímavý výsledek. Ukazuje, že alespoň některé požadavky normy před začátkem její aplikace splňovalo 7 organizací. 4 z nich dokonce uvedly, že splňovaly již většinu požadavků a vyhovět normě proto neznamenalo žádné velké úsilí a náklady.

Následoval dotaz, zda zástupci pozorují zlepšení úrovně bezpečnosti informací po zavedení normy. Shodně 2 společnosti uvedly výrazné a mírné zlepšení. Další 4 odpověděly, že už před zavedením normy byla úroveň bezpečnosti informací na vysoké úrovni. Tato skutečnost odráží odpověď na otázku z předešlého odstavce, kdy 4 respondenti uvádí plnění většiny požadavků normy ještě před jejím zavedením.

8 zástupců organizací uvedlo, že by podpořilo zavedení normy znovu a to ve stejném rozsahu. Zbývající 1 by normu znovu zavedl také, ale v jiném rozsahu. Nikdo neuvedl, že přínos normy nebyl takový, aby obhájil náklady na její zavedení.

Na otázku, zda organizace plánují plnit požadavky kybernetického zákona, většina respondentů (4 odpovědi) uvedla, že se budou požadavky kybernetického zákona zabývat tehdy, až se jich bude týkat. Další 2 se domnívají, že se na jejich organizaci kybernetický zákon nikdy vztahovat nebude. Společně tedy tvoří většinu 6 hlasů, která se kybernetickým zákonem v současné době nezabývá. 2 hlasy získala kladná odpověď s odůvodněním, že se očekává nutnost plnit požadavky kybernetického zákona v blízké budoucnosti. 1 organizace je plní již nyní. Zbylí 2 zástupci nedokáží na tuto otázku odpovědět.

Z odpovědí na volitelné otázky lze vyčíst další zajímavé informace. Proces od začátku prací na k připravenosti na certifikaci normy trvá zpravidla od 6 do 12 měsíců. Je běžnou praxí, že se zaváděním normy organizacím pomáhají poradenské firmy, které se na tuto problematiku zaměřují. Mezi nejnáročnějšími požadavky normy jasně vede

analýza rizik, následuje zpracovávání dokumentací, rozdělování a značení aktiv a řízení incidentů bezpečnosti informací. U otázky, zda se v průběhu zavádění normy organizace setkaly s neočekávanými komplikacemi, se odpovědi shodovaly, že nikoliv, protože příprava byla dobře zvládnutá. V jednom případě bylo uvedeno, že byl překročen finanční rozpočet. Tato skutečnost způsobila komplikaci, protože navýšení muselo být schváleno zastupitelstvem města a zde bylo složité přimět zastupitele k pochopení důležitosti bezpečnosti informací v kontrastu s dalšími investicemi.

Konkrétní znění otázek v dotazníku je obsahem přílohy 14 - Dotazník k zavádění normy ISO 27001 v praxi.

5. Zákon č. 181/20014 Sb. o kybernetické bezpečnosti

„Aby zůstal kybernetický prostor otevřený a svobodný, měly by online fungovat tytéž normy, zásady a hodnoty, které EU podporuje offline. Základní práva, demokracie a zásady právního státu je třeba chránit i v kybernetickém prostoru. Na celosvětové podpoře těchto práv spolupracuje EU se svými mezinárodními partnery, jakož i s občanskou společností a soukromým sektorem."

Catherine Ashtonová, místopředsedkyně Evropské komise a představitelka Evropské unie pro zahraniční věci a bezpečnostní politiku, k příležitosti představení plánu kybernetické bezpečnosti Evropské unie, 2013.

5.1. Události vedoucí ke vzniku kybernetického zákona

S příchodem digitální éry na přelomu tisíciletí začínají vyspělé země čelit novým hrozbám. Stále více služeb a systémů je řešeno elektronickou formou a jejich uživatelé si na nově vznikající prostředí začínají rychle zvykat. Přicházející digitální věk čelí novým výzvám a musí začít řešit problémy, které v takovém měřítku nikdy dříve řešit nemusel.

Rozšíření elektronických služeb a zejména internetu prakticky vymazalo většinu státních hranic a jednotlivé země začaly zjišťovat, že jejich vlastní legislativa, často nedokonalá a narychlo chaoticky vznikající, není s to zabezpečit celý digitální sektor. Přestože státy samy mohou mít kybernetickou bezpečnost na vysoké úrovni, jsou zranitelné, pokud jsou zranitelné další místa infrastruktury lokalizovaná za jejich hranicemi, kde jejich vlastní legislativa neplatí. Zranitelnost přichází z míst, kde poskytovatelé určitých informačních systémů nejsou právně nuceni k přijetí dostatečně silných opatření proti zneužití.

Evropa si pomalu začínala uvědomovat, že bude-li chtít zajistit kybernetickou bezpečnost jednotlivých zemí, bude potřeba sjednotit jejich legislativu a vytvořit strategii pro boj proti kybernetickému zločinu, rozvoje infrastruktury a bezpečnostní politiky do budoucna.

Dny, kdy byla tato otázka veřejně a globálně nadnesena k diskusi, byly 19. a 20. listopad roku 2010. V portugalském Lisabonu právě probíhal summit Severoatlantické aliance (NATO). Zde byla zdůrazněna globální povaha kybernetických hrozeb a nutnost jejich řešení na mezinárodní úrovni. Padla výzva k vytvoření mezinárodního konceptu pro zvýšení kybernetické bezpečnosti.

Dne 19. října roku 2011 vláda České republiky ve svém usnesení č. 781 nařizuje vybudování Národního centra pro kybernetickou bezpečnost (NCKB) jako součásti Národního bezpečnostního úřadu (NBÚ). Jedná se o organizaci typově spadající pod mezinárodní označení CERT (Computer Emergency Response Team).

CERT vznikl v listopadu roku 1988 jako reakce na první velký problém, kterému musel čelit celosvětový internet. Tehdy, v aféře známé jako Morrisův červ (Morris Worm), byla vyřazena z provozu velká část této sítě. Cílem organizace CERT se stala zejména prevence a včasná výstraha uživatelům v případě zjištění kybernetických hrozeb. Od té doby vzniklo mnoho podobných organizací na vnitrostátní úrovni, které zpravidla ve své zkratce výraz CERT obsahují (MOCERT – Čína, US-CERT – Spojené Státy Americké, CERT-UK – Velká Británie, DKCERT – Dánsko, atd.). V České republice se můžeme setkat s alternativním označením pro NCKB, které tuto zkratku také obsahuje – GovCERT (www.govcert.cz).

O šest měsíců později, 30. května roku 2012, vláda vydala usnesení č. 382, které schvaluje záměr vytvoření zákona o kybernetické bezpečnosti a ukládá Národnímu bezpečnostnímu úřadu povinnost zpracovat návrh tohoto zákona do 31. července roku 2013.

Ve stejný rok představila Evropská komise návrh nařízení o obecné ochraně údajů (GDPR – General Data Protection), jehož cílem je napříč celou Evropskou unií sjednotit pravidla pro ochranu osobních údajů, které nyní v České republice řeší zákon č. 101/2000 Sb., o ochraně osobních údajů, a který má úzkou souvislost s problematikou kybernetické bezpečnosti. Začátek platnosti tohoto nařízení se odhaduje na začátek roku 2016. Zda je současná legislativa České republiky dostačující, nebo bude po přijetí nařízení nutná jeho revize, zatím není známo. Jisté je zatím pouze to, že nařízení bude závazné pro všechny organizace působící v zemích Evropské unie,

a že jejím porušením se organizace budou vystavovat finančnímu postihu. Ten je zatím navržen na 5% z celosvětového ročního obratu.

7. února 2013 zveřejnila Evropská komise evropskou strategii kybernetické bezpečnosti nazvanou Otevřený, bezpečný a spolehlivý kybernetický prostor (An Open, Safe and Secure Cyberspace). Ta představuje vizi, jak co nejlépe předcházet narušení kybernetického prostoru, předcházet útokům na něj a jak na tyto útoky reagovat. Nově představená strategie obsahovala především tyto body:

- rozvoj Společné bezpečnostní a obranné politiky (SBOP, z roku 1999),
- rozvoj průmyslových a technologických zdrojů pro počítačovou bezpečnost,
- ucelenou mezinárodní kybernetickou politiku pro Evropskou unii,
- vytvoření evropského centra pro boj proti kriminalitě (EC3),
- návrh právních předpisů o útocích proti informačním systémům,
- program pro financování a rozvoj národních center pro boj proti kybernetické kriminalitě,
- návrh Směrnice o bezpečnosti sítí a informací (NIS – Network and Information Security).

Zejména poslední bod, tedy tzv. směrnice NIS, je pro další vývoj legislativy (nejen v České republice) týkající se kybernetické bezpečnosti velmi zásadní. Tato směrnice vznáší požadavek vůči všem členským státům Evropské unie, aby přijaly národní strategii pro bezpečnost sítí a informací. V České republice tuto strategii vypracovalo Národní centrum pro kybernetickou bezpečnost a je veřejně přístupná na jeho internetovém portálu (http://www.govcert.cz/cs/informacni-servis/strategie-a-akcni-plan/).

Směrnice dále požaduje jmenování vnitrostátního orgánu odpovědného za bezpečnost sítí a informací (který v České republice již od roku 2011 zastává Národní centrum pro kybernetickou bezpečnost) a další konkrétní opatření pro zvýšení kybernetické bezpečnosti. Např. definuje povinnosti pro poskytovatele vybraných informačních systémů (tzv. platformy digitální služby, jako jsou internetové obchody nebo provozovatelé DNS serverů) a rozděluje je do různých kategorií, podle kterých

přiděluje různé závazky. Směrnice také pracuje s pojmy kritická infrastruktura nebo významný informační systém, které můžeme znát z (v době zveřejnění návrhu směrnice ještě neexistujícího) českého kybernetického zákona. V roce 2015 byla nalezena shoda mezi Evropskou komisí a Evropským parlamentem na podobě směrnice a její schválení se očekává v průběhu roku 2016.

Národní centrum pro kybernetickou bezpečnost, které v roce 2012 dostalo od vlády za úkol do poloviny roku 2013 předložit návrh kybernetického zákona, se v mnohém inspirovalo právě v textech směrnice NIS a především reflektovalo její požadavky. Díky tomu je nově vznikající zákon již ve značném souladu s budoucí závaznou legislativou Evropské unie.

Návrh zákona o kybernetické bezpečnosti obsahuje také tzv. důvodovou zprávu, která detailně rozebírá problematiku kybernetické bezpečnosti, nezbytnost právních úprav, popis existujícího právního stavu České republiky, identifikaci dotčených subjektů, popis cílového stavu, návrhy řešení, rizika, vyhodnocení nákladů a přínosů a velké množství dalšího textu zahrnujícího také různé analýzy, na základě kterých se tvůrci zákonů rozhodovali o jeho podobě a formulaci. Některé z těchto částí důvodové zprávy budou probrány v další kapitole.

V konečné podobě nabyl zákon č. 181/2014 Sb., o kybernetické bezpečnosti, platnost 29. srpna roku 2014 a účinný je od 1. ledna roku 2015.

5.2. Legislativa před kybernetickým zákonem

V důvodové zprávě k návrhu zákona je oblast věnovaná existující legislativě, která v menší nebo větší míře řešila problémy kybernetické bezpečnosti před vznikem kybernetického zákona. Seznam této legislativy zabírá ve zprávě místo o velikosti osmi stran formátu A4. Vzhledem k tomu, že jde pouze o výčet, nikoliv o konkrétní pasáže, je jasné, že situace v této oblasti v období před kybernetickým zákonem byla přinejmenším velmi nepřehledná. Chyběla jakákoliv koordinovaná koncepce na celostátní úrovni, což důvodová zpráva uvádí jako jeden z hlavních důvodů pro potřebu nového zákona. Dalším klíčovým faktorem byla skutečnost, že stát neměl pravomoc

k přijetí opatření proti kybernetickým útokům vedeným proti osobám soukromého práva, které provozují kritickou infrastrukturu státem využívanou.

Zde jsou uvedeny některé z hlavních zákonů, které před kybernetickým zákonem řešily kybernetickou bezpečnost (Důvodová zpráva k vládnímu návrhu zákona o kybernetické bezpečnosti, 2014, s. 21-29):

- zákon č. 101/2000 Sb., o ochraně osobních údajů,
- zákon č. 240/2000 Sb., o krizovém řízení,
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy,
- zákon č. 480/2004 Sb., o některých službách informační společnosti,
- zákon č. 127/2005 Sb., o elektronických komunikacích,
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti,
- zákon č. 111/2009 Sb., o základních registrech.

5.3. Návrh zákona o kybernetické bezpečnosti

Důvodová zpráva v odůvodnění pro vznik zákona v podstatě přebírá argumentaci ze summitu Severoatlantické aliance a strategie pro kybernetickou bezpečnost prezentovanou Evropskou unií. Nejdůležitější body lze shrnout takto (Důvodová zpráva k vládnímu návrhu zákona o kybernetické bezpečnosti, 2014, s. 17-20):

- výrazný nárůst používání informačních technologií organizacemi, státem i jednotlivci,
- nárůst závislosti společnosti na informačních technologiích,
- z toho plynoucí nárůst motivace a tedy i rizika zneužití informačních technologií,
- zvýšení komplexnosti, sofistikovanosti i četnosti útoků na informační technologie,
- rozšíření kriminality páchané na informačních technologií z převážně jednotlivců do sféry organizovaného zločinu,

- cílem se stávají stále častěji prvky kritické infrastruktury a systémy veřejné správy,
- výrazné zvýšení rizika špionáže vedené prostředky informačních technologií.

Tvůrci důvodové zprávy uvádění nutnost vytvořit právní úpravu pro řešení zejména těchto problémů (Důvodová zpráva k vládnímu návrhu zákona o kybernetické bezpečnosti, 2014, s. 20):

- Ochrana existence a funkčnosti prostředí tvořeného informačními systémy, službami a sítěmi elektronických komunikací tak, aby v něm mohly subjekty pod jurisdikcí České republiky realizovat své právo na informační sebeurčení.
- Ochrana existence a funkčnosti prostředí tvořeného informačními systémy, službami a sítěmi elektronických komunikací tak, aby kybernetické bezpečnostní incidenty nemohly ohrozit fungování základních společenských funkcionalit chráněných nedistributivními právy České republiky.
- Ochrana existence funkčnosti prostředí tvořeného informačními systémy, službami a sítěmi elektronických komunikací tak, aby nebyla národní kybernetická infrastruktura zneužitelná k útokům mimo Českou republiku.

Vzhledem ke smyslu a účelu zákona, což má být ochrana vybraných informačních a komunikačních systémů před kybernetickými bezpečnostními incidenty, se zákon nedotýká uživatelů ani poskytovatelů obsahu. Orgány a osoby v navrhované právní úpravě jsou subjekty spravující specifické informační a komunikační systémy. Tyto systémy zákon rozpoznává pod pojmem kritická infrastruktura a významný informační systém.

Navrhovaná úprava částečně přebírá definice z již existujících právních předpisů, a to zejména ze zákona č. 365/2000 Sb., o informačních systémech veřejné správy a ze zákona č. 127/2005 Sb., o elektronických komunikacích.

Důvodová zpráva uvádí jako výchozí dokumenty pro vznik zákona normy ISO 27001 a ISO 27002. Důvodem k tomuto kroku byla související analýza současné situace mezi organizacemi v České republice, na které by se zákon měl vztahovat.

„Velmi pozitivním zjištěním je skutečnost, že metodika norem pro řízení informační bezpečnosti ISO/IEC 27001, 27002, z níž vychází návrh zákona, je již nyní využívána pro řízení informační bezpečnosti u 80% subjektů spravujících důležité informační a komunikační technologie státu, 98% subjektů spravujících důležité informační a komunikační systémy a technologie státu má již zcela nebo částečně zaveden systém evidence a zvládání bezpečnostních incidentů, a že 21% subjektů spravujících důležité informační a komunikační systémy a technologie státu má zavedeno certifikované řízení informační bezpečnosti. Z uvedeného je zřejmé, že vzhledem k rozšířenosti používání bezpečnostního standardu rodiny norem ISO IEC 27000 u subjektů spravujících důležité informační a komunikační systémy a technologie státu, je výběr této metodologie pro návrh zákona správným rozhodnutím.“ (Důvodová zpráva k vládnímu návrhu zákona o kybernetické bezpečnosti, 2014, s. 55-56)

Vzhledem k výše uvedenému byla volba vzoru pro nový zákon poměrně jednoduchá. Jeho tvůrci se snažili, aby zákonem postižené organizace musely vyvinout co nejmenší úsilí a investice pro splnění jeho požadavků. Pokud velká část dotčených organizací již využívá systémy kompatibilní s budoucími legislativními požadavky Evropské unie (a tedy i České republiky), proč nepostavit zákon právě na těchto základech.

5.4. Struktura kybernetického zákona

5.4.1. Zákon č. 181/2014 Sb.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, stanoví, koho se týká a jaké má dotyčný povinnosti. Všechny prvky jsou však psány maximálně obecně a v podstatě se dá říci, že se ze samotného zákona nic konkrétního vyčíst nedá. Zákon je takto

koncipován z toho důvodu, aby po svém přijetí pokud možno již nemusel být měněn. Změny zákonů totiž podléhají složitému schvalovacímu procesu, kdy se k návrhům vyjadřuje vláda, poslanecká sněmovna, senát a stvrdit je svým podpisem musí také prezident republiky. Z pohledu velkého množství dotčených osob, které se k zákonu vyjadřují, vyplívá riziko určitého lobbistického tlaku různých zákonem dotčených subjektů. Pro eliminaci těchto tlaků je vhodné zákon sepsat tak, aby se v něm dotčené subjekty neviděly a neměly proto potřebu lobbistické tlaky vytvářet. Maximální zobecnění zákona je účinná metoda.

V takovém případě se konkrétní vymezení přesouvají do vyhlášek nebo vládních nařízení. Správa vyhlášek je v kompetenci příslušných úřadů nebo ministerstev (stanoví zákon) a vládní nařízení přísluší vydávat aktuální vládě. Kromě značné eliminace nechtěných externích tlaků na podobu právní úpravy je přínosem také rychlejší proces schvalování a vydávání. Je tak možné rychleji reagovat na aktuální situaci.

Zákon ve svém znění v § 3 stanoví, kterých subjektů se týká:

- poskytovatelů služeb elektronických komunikací a subjektů zajišťujících sítě elektronických komunikací (poskytovatele konkrétně vymezuje zákon č. 127/2005 Sb., o elektronických komunikacích),
- osoby nebo orgány zajišťující významné sítě,
- správců informačních systémů kritické informační infrastruktury,
- správců komunikačních systémů kritické informační infrastruktury,
- správců významných informačních systémů.

Zákon dále:

- určuje kontaktní údaje a subjekty, které jsou povinné je oznámit Národnímu bezpečnostnímu úřadu (§ 16)
- řeší bezpečnostní opatření, která jsou dotčené subjekty povinné zavádět (§ 5),
- vymezuje pojmy kybernetickou bezpečnostní událost a kybernetický bezpečnostní incident (§ 7),

- stanoví povinnost evidovat a hlásit tyto události (§ 8 a 9),
- stanoví výčet opatření k ochraně informačních systémů (§ 11 - 13),
- vymezuje organizace CERT a jejich povinnosti (§ 17 – 20),
- definuje stav kybernetického nebezpečí (§ 21),
- stanovuje úlohu Národního bezpečnostního úřadu v oblasti státní správy kybernetické bezpečnosti (§ 22),
- stanovuje kontroly, nápravná opatření a sankce (§ 25 – 27),
- zmocňuje jiné orgány k vydávání a aktualizaci upřesňujících právních dokumentů (§ 28).

V posledním bodě získává Národní bezpečnostní úřad a Ministerstvo vnitra pravomoc stanovit vyhláškou významné informační systémy a jejich kritéria. Touto vyhláškou, která je konkretizací § 3 (viz výše), přesně určuje, koho se zákon o kybernetické bezpečnosti týká.

5.4.2. Vyhláška č. 316/2014 Sb.

Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti, konkrétně stanoví některé obecné pojmy uvedené v kybernetickém zákoně. Obsahuje výčet konkrétních opatření, které jsou dotčené organizace povinny učinit, aby splnily jednotlivé body uvedené v zákoně. Obsahem vyhlášky jsou mj. tyto body:

- systém řízení bezpečnosti informací (§ 3),
- řízení rizik (§ 4)
- bezpečnostní politika (§ 5),
- organizační bezpečnosti (§ 6),
- řízení aktiv (§ 8),
- bezpečnost lidských zdrojů (§ 9),
- řízení provozu a komunikací (§ 10),
- zvládání kybernetických bezpečnostních událostí a incidentů (§ 13),
- řízení kontinuity činnosti (§ 14),
- fyzická bezpečnost (§ 16).

Jednotlivé body v seznamu výše byly vybrány záměrně a čtenáři by již měly být povědomé. Jedná se totiž o oblasti, které byly již řešeny v kapitole 4. Hlavně v těchto paragrafech je nejlépe vidět míra inspirace normou ISO 27001 při tvorbě kybernetického zákona.

Vyhláška jde ale ještě dále nad rámec normy a poskytuje také konkrétní opatření, jak stanovených cílů dosáhnout. Jedná se např. o tyto části vyhlášky:

- nástroj pro ochranu integrity komunikačních sítí (§ 17),
- nástroj pro ověřování identity uživatelů (§ 18),
- nástroj pro řízení přístupových oprávnění (§ 19),
- nástroj pro ochranu před škodlivým kódem (§ 20),
- a další.

Podoba této vyhlášky podle znění kybernetického zákona spadá pod správu Národního bezpečnostního úřadu.

5.4.3. Vyhláška č. 317/2014 Sb.

Z kapitoly 5.4.1 je patrné, že vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, konkrétně stanoví, na koho se kybernetický zákon vztahuje. Jak již bylo řečeno, úprava vyhlášky je v kompetenci Národního bezpečnostního úřadu a Ministerstva vnitra.

Významný informační systém je zde uveden buď seznamem konkrétních systémů a jejich správců nebo seznamem určujících kritérií.

V prvním případě se tedy jedná o konkrétní výčet organizací, které spadají do působnosti kybernetického zákona. Tyto organizace jsou povinny zajistit bezpečnost vybraného informačního systému podle znění zákona. Výčet je uveden v příloze 1 vyhlášky a k dnešnímu dni obsahuje celkem 92 položek. Zde je příklad několika z nich:

Tabulka 15: příklad organizací spravující významné informační systémy

PČ	Správce	Název
2	Český statistický úřad	Integrovaný agendový informační systém registru osob (IAIS – ROS)
9	Energetický regulační úřad	Jednotný informační systém ERÚ
17	Ministerstvo dopravy	Centrální registr vozidel (CRV)
25	Ministerstvo financí	Integrovaný informační systém státní pokladny (IISSP)
52	Policie České republiky	Informační systém ZBRANĚ

V druhém případě vyhláška rozlišuje mezi dopadovým a oblastním určujícím kritériem, přičemž jako zodpovědného za správné určení, zda systém spadá do těchto kritérií, určuje správce informačního systému. Organizace samotná tedy rozhoduje, zda její informační systémy jsou klasifikovány jako významný informační systém. Pokud se při kontrole ukáže, že systém neklasifikovala jako významný informační systém, ačkoliv tak učinit měla, vystavuje se sankcím popsaným v zákoně.

Dopadová kritéria jsou kritéria na základě dopadu, který může mít úplná nebo částečná nefunkčnost systému způsobená narušením bezpečnosti. Jedním z kritérií je např. „zásah do osobního života nebo do práv fyzických nebo právnických osob postihující nejméně 50 000 osob“ nebo „poskytování služeb nebo informací orgánem veřejné moci veřejnosti“. Konkrétní výčet obsahuje § 4 vyhlášky.

Oblastní určující kritéria jsou kritéria na základě oblasti, které se informační systémy věnují. Jedná se o orgány veřejné moci, které poskytují např. státní dozor, tvorbu státních předpisů, zabývají se mezinárodní spoluprací atd. Konkrétní výčet obsahuje příloha 2 vyhlášky.

5.4.4. Nařízení vlády č. 315/2014 Sb.

Kybernetický zákon zavádí pojmy významný informační systém a prvek kritické infrastruktury. Konkrétní definici prvního pojmu se věnuje vyhláška č. 317/2014 Sb., viz kapitola 5.4.3. Druhý pojem upřesňuje právě toto nařízení vlády č. 315/2014 Sb., o kritériích pro určení prvku kritické infrastruktury. Prvky kritické infrastruktury jsou zde děleny podle odvětví na 9 částí, např. energetika, zdravotnictví, doprava atd.

Pro každou část jsou určena kritéria, která pokud jsou splněna, pak správce daného předmětu provozuje prvek kritické infrastruktury a musí se řídit zákonem o kybernetické bezpečnosti. Zde jsou příklady několika kritérií z vybraných odvětví, která popisují oblasti vztahující se k vybraných modelových organizací popsaných v kapitole 4:

- I. Energetika
    - A. Elektřina
        - A. 3 Distribuční soustava
            - elektrická stanice distribuční soustavy a vedení napětí 110 kV.
- IV. Zdravotnictví
    - zdravotnické zařízení, jehož celkový počet aktuálních lůžek je nejméně 2 500.
- IX. Veřejná správa
    - B. Sociální ochrana a zaměstnanost
        - B. 3 Sociální pomoc
            - informační systém pro zajištění realizace dávek sociálních služeb, který obsahuje údaje o více než 125 000 osobách.

Vládní nařízení vydává aktuální vláda České republiky.

5.5. Očekávaný vývoj kybernetického zákona v budoucnosti

Vývoj kybernetického zákona lze očekávat ze dvou směrů, externího a interního. Z externího pohledu se bude jednat o nutnost vyhovět evropské směrnici o bezpečnosti sítí a informací (NIS), jejíž schválení Evropským parlamentem se očekává během letošního roku.

Interní směr má dvě roviny. V té první je zde snaha o odstranění nedostatků, které byly identifikovány za dobu existence kybernetického zákona. Ve druhé je snaha rozšířit působnost zákona podle představ a potřeb prezentovaných v důvodové zprávě (viz kapitola 5.3).

Lze tedy předpokládat, že kromě drobných změn týkajících se odstraňování nepřesností, nejasností a úprav pro soulad legislativy s evropskou směrnicí, budou změny především formátu rozšiřování záběru pojmů významný informační systém (viz kapitola 5.4.3) a kritická infrastruktura (viz kapitola 5.4.4).

Konkrétně lze např. očekávat úpravu bodu IV (zdravotnictví) v nařízení vlády o kritériích pro určení prvku kritické infrastruktury (viz kapitola 5.4.4). Současnému jedinému kritériu na počet lůžek v České republice nevyhovuje žádné zdravotnické zařízení, a tedy žádné zdravotnické zařízení není k dnešnímu dni vázáno kybernetickým zákonem. Důvodem je zejména notoricky špatná finanční situace zdravotnických zařízení v České republice a potenciálně nákladná opatření, která je nutné zavést pro soulad se zákonem. Jde tedy o to, dát těmto organizacím čas se na změnu připravit a umožnit jim rozdělit náklady na nová opatření do delšího časového období. Je však nutné upozornit, že již dnes některé nemocnice splňují požadavky normy ISO 27001 a jsou tedy jen krůček od plnění požadavků kybernetického zákona. Jmenovitě jsou to např. Všeobecná fakultní nemocnice v Praze, Ústeckoorlická nemocnice, Chrudimská nemocnice, Fakultní nemocnice v Hradci Králové, Pardubická nemocnice nebo Litomyšlská nemocnice.

"Co se vývoje ZKB do budoucna týče, lze určitě uvést možnou úpravu ZKB v rámci transpozice (nyní stále připravované) evropské směrnice o informační a síťové

bezpečnosti (tzv. NIS směrnice). … Pravděpodobně bude ZKB se souvisejícími předpisy částečně upravován i v rámci odstraňování některých bílých míst a nedostatků, které byly identifikovány v prvním roce účinnosti ZKB. Základní systematika ZKB a dané pojetí zajišťování kybernetické bezpečnosti však s největší pravděpodobností zůstane zachováno." Z osobní korespondence autora a pana Václava Borovičky z Národního bezpečnostního úřadu a Národního centra kybernetické bezpečnosti, 2016.

6. Další nástroje pro zvýšení informační bezpečnosti

Norma ISO 27001 ukazuje, jak by jednotlivé procesy měly vypadat, a jak by jednotlivé systémy měly být nastavené. Říká, že je potřeba řídit bezpečnost informací. Co už neuvádí je způsob, kterým má být cílů dosaženo. Těchto způsobů je celá řada.

Samotná rodina norem ISO 27000 obsahuje normy, které uvádí, jak těchto cílů dosáhnout. Např. norma ISO 27005 vysvětluje, jak provádět analýzu rizik. Výčet těchto prováděcích norem obsahuje Tabulka 1: rodina norem ISO 27000 v kapitole 2.2.2.

V České republice platný zákon o kybernetické bezpečnosti rovněž obsahuje konkrétní pokyny, jak dosáhnout cílů stanovených normou, resp. zákonem. Zabývá se jimi vyhláška č. 316/2014 Sb., probraná v kapitole 5.4.2.

Kromě těchto dokumentů existuje celá řada dalších, které vyvíjejí specializované společnosti zpravidla na základě dlouholetých praktických zkušeností. Jejich zaměření bývá různé a s požadavky normy ISO 27001 se mohou různě překrývat. Některé nástroje řeší jen část jejího obsahu, jiné mnohem více než požaduje.

Tyto nástroje nastíním pouze okrajově. Pro více informací doporučuji prostudovat tyto zdroje:

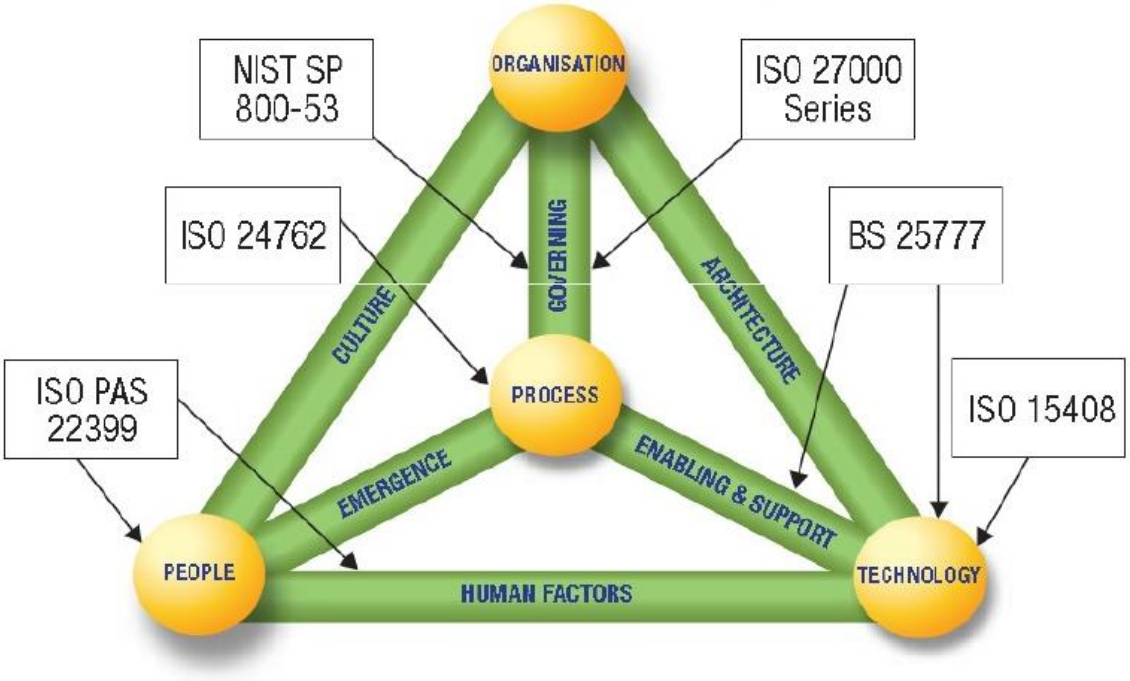
- ISACA (Information Systems Audit and Control Association): Trust in, and value from, information systems. Dostupné online z webové adresy https://www.isaca.org/Pages/default.aspx. Získáte zde informace o těchto modelech:
    - COBIT 4.1 (IT Governance & Control),
    - Risk IT,
    - Val IT (IT Value Delivery),
    - BMIS (Business Model For Information Security).
- Přístup k řízení informační bezpečnosti ve standardech ITIL, COBIT, ISO 27002. Bakalářská práce Luďka Veselého z katedry matematiky, statistiky a informačních technologií, Bankovního institut vysoká škola v Praha. Tato práce se detailně zabývá a porovnává modely:
    - ITIL V2 a V3,

    - COBIT 4.1,
    - ISO 27002:2005
- BMC: Global leader in inovative software solutions. Dostupné online z webové adresy http://www.bmc.com/guides/itil-introduction.html. Zde lze získat v elektronické podobě všechny knihy z knihovny ITIL.

6.1. BMIS

BMIS (Business Model For Information Security) prezentuje komplexní přístup na řízení ICT systémů z pohledu celé organizace, nikoliv pouze z pohledu samotné ICT části organizace. Model dokumentu je určen pro vedoucí pracovníky, manažerům informační bezpečnosti, osobám odpovědných za řízení obchodních rizik a osobám odpovídajícím za návrh, implementaci a monitorování systémů řízení bezpečnosti informací.

Model v sobě obsahuje celou řadu norem a řeší vztahy mezi jednotlivými aspekty organizace. Ve zjednodušené formě jej lze prezentovat následujícím diagramem.

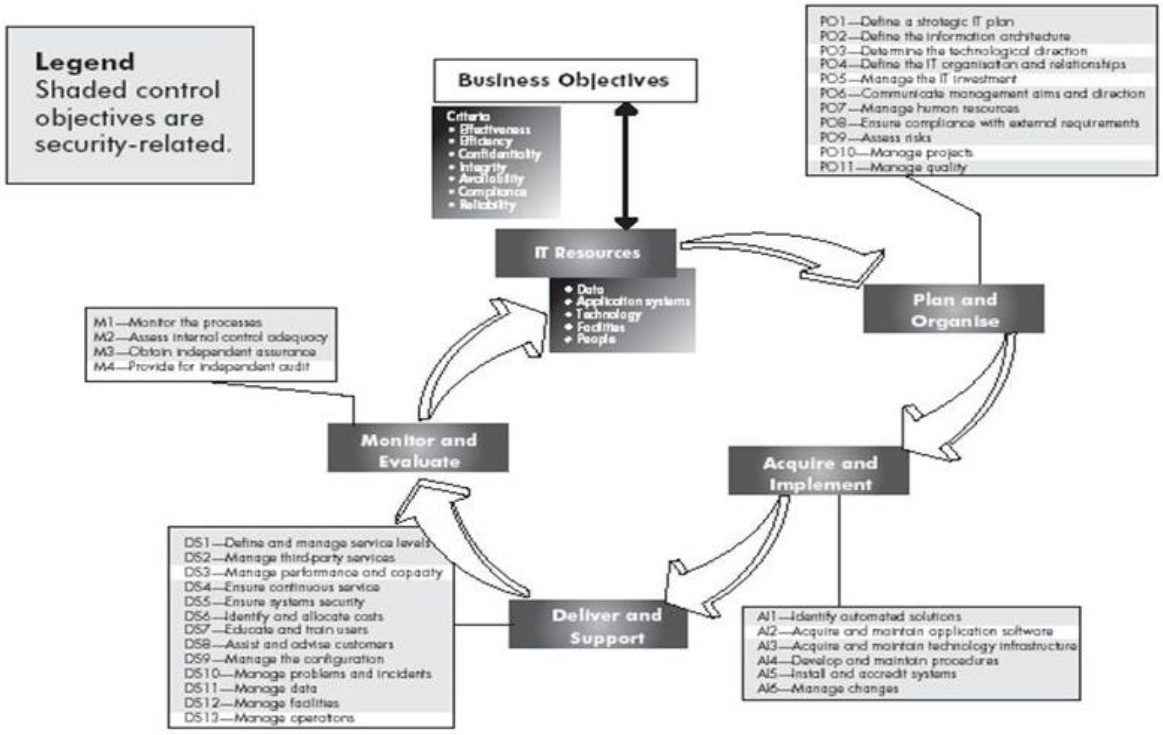


Obrázek 8: schéma modelu BMIS [31]

6.2. CSB

CSB (COBIT Security Baseline) popisuje rizika specifická pro oblast informační bezpečnosti. Snaží se tak činit jednoduchou a srozumitelnou formou, kterou cílí zejména na prostředí malých a středně velkých společností.

Rozděluje rizika do tří kategorií (záměrného zneužití ICT zařízení, porušení pravidel nebo norem a havárie) a obsahuje řadu bezpečnostních procesů a kontrolních kroků pro domácí i profesionální uživatele, manažery a výkonné ředitele. Vychází z pokročilé metodiky COBIT 4.1 a obsahuje vazby na normu ISO/IEC 27002.



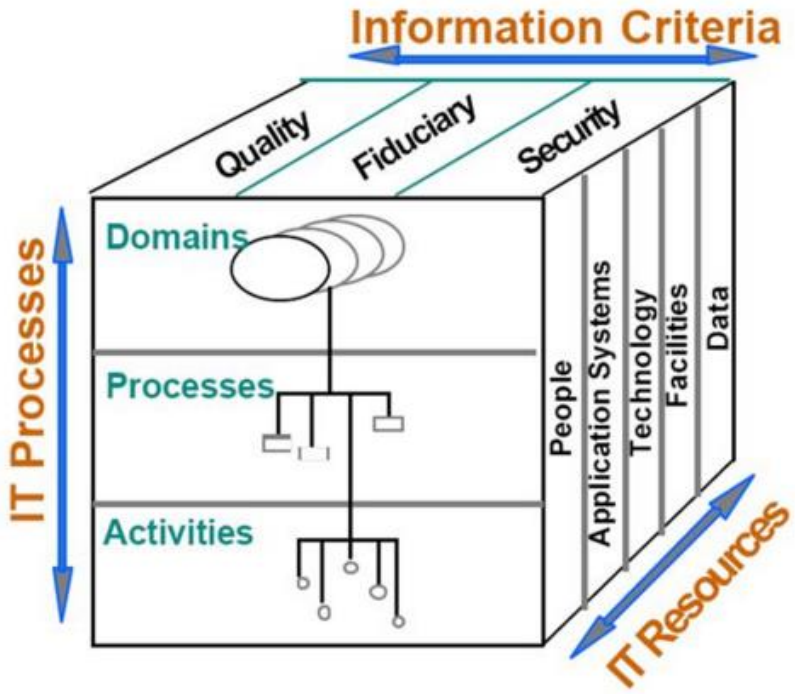
Obrázek 9: schéma modelu Cobit Security Baseline [17]

6.3. COBIT

Poslední verze metodiky COBIT (Control Objectives for Information and Related Technology) nese označení 4.1. Jedná se o soubor všeobecně přijímaných procesů, návodů a ukazatelů, které se vyznačují nejlepšími výsledky z praxe.

Setkáváme se zde s variací na známý PDCA (Plan, Do, Check, Act) cyklus, v tomto případě označený PO-AI-DS-MI (Plan and Organize, Acquire and Implement, Deliver and Support, Monitor and Evaluate).

Princip metodiky COBIT je zobrazován pomocí multidimenzionální kostky:



Obrázek 10: schéma modelu COBIT [18]

Pro tento způsob řízení ICT procesů existuje několik rozšíření. Některá z nich jsou popsána v kapitole 6.5.

6.4. ITIL

ITIL (Information Technology Infrastructure Library) je knihovnou nejlepších praktik pro správu ICT služeb. Zaměřuje se zejména na problematiku služeb, jejich dodávek a kvality, z pohledu poskytovatele i zákazníka.

První známá verze těchto knihoven nese označení V2 a přestože dnes již je k dispozici V3, předchozí verze se stále hojně využívá. Třetí verze se zabývá již pouze řízením IT služeb, kdežto předchozí verze řešila IT prostředí komplexněji. Nicméně třetí verze zase nabízí detailnější přístup.

Druhá verze knihovny ITIL se skládá ze sedmi samostatných knih (Service Support, Service Delivery, Planning to Implement Service Management, ICT Infrastructure Management, Applications Management, Security Management, The

Business Perspective), třetí verze pak z dalších pěti knih (Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvment).

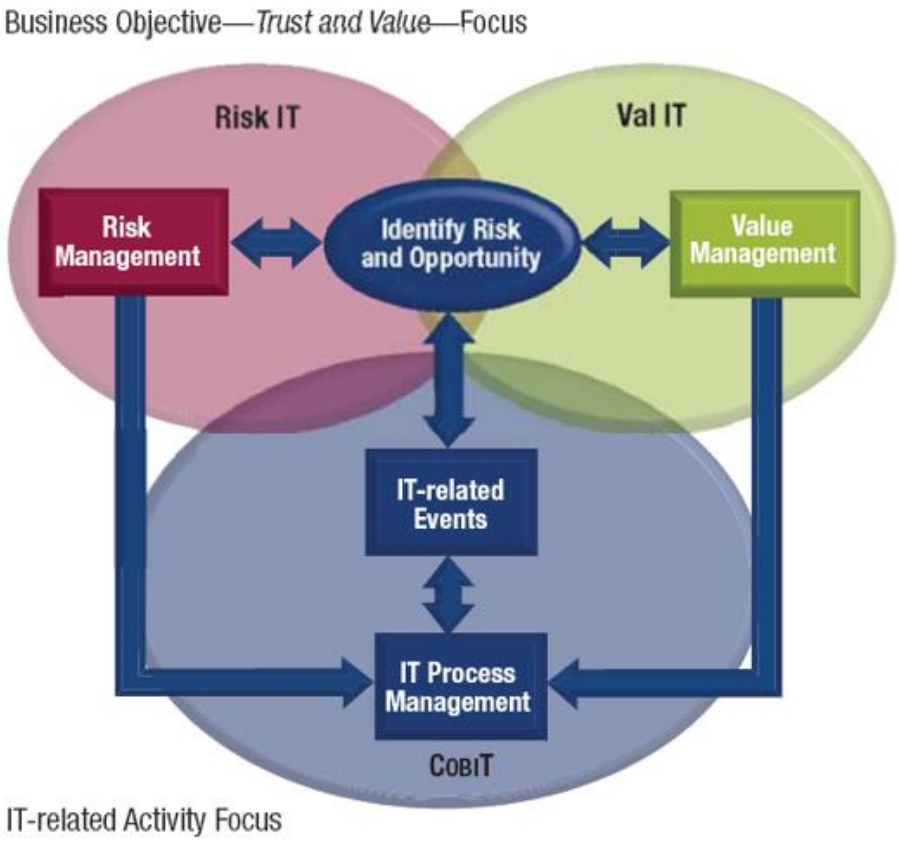
Obrázek 11: schéma modelu ITIL [16]

6.5. Val IT a Risk IT

Jedná se o dokumenty rozšiřující metodiku COBIT.

Val IT se zaměřuje na pochopení hodnoty ICT technologií a investicí do nich. Společnost ISACA (tvůrce COBIT, Val IT a Risk IT) demonstruje hodnotu těchto informací statistikou, kde v průměru končí dva z deseti velkých ICT projektů naprostým selháním. Dokument se snaží naučit management společnosti jak vytvářet spolehlivé investice.

Risk IT se zaměřuje na pochopení vztahu rizika a hodnoty v oblasti ICT. Upozorňuje na skutečnost, že riziko a hodnota jsou pouze dvě strany stejné mince a snaží se naučit management, jak správně postupovat při zvládání rizik.



Obrázek 12: schéma vztahu metodik COBIT, Val IT a Risk IT [32]

6.6. Shrnutí

Ukázali jsme si, že cíle normy ISO 27001 lze splnit různými přístupy. Většina z nich v nějaké formě aplikuje PDCA (Plan Do Chech Act) cyklus, kterým se zajišťuje neustálé zlepšování systémů. Je vidět, že přístupy jsou podobné.

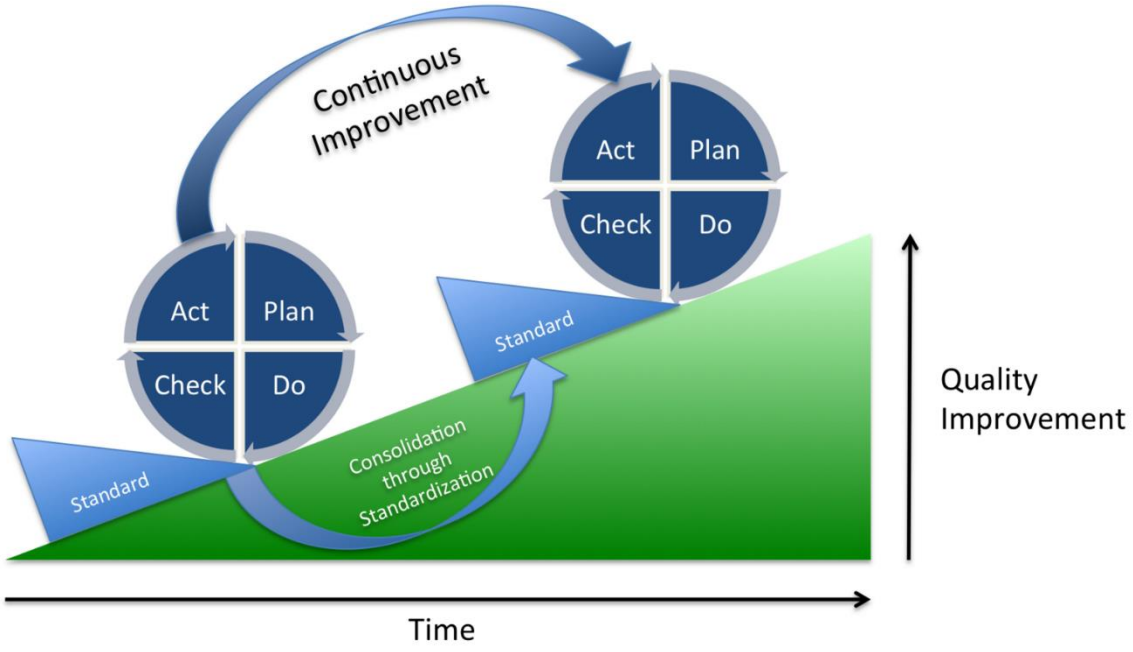
Jaký konkrétní přístup ke zvýšení informační bezpečnosti si organizace zvolí, je pochopitelně zcela její volba. Norma ISO 27001 neřeší, jak bylo jejich cílů dosaženo, ale zda byly dosaženy. Organizace by měla volit nástroje v souladu se svým zaměřením a dalšími požadavky, které jsou na ní kladeny. Pokud se zaměřuje na služby, nejspíše ji

dobře poslouží knihovna ITIL. CSB může být zase dobrým nástrojem pro malé společnosti. Univerzální řešení neexistuje a je na managementu organizace, aby prostudoval dostupné možnosti a zvolil z nich tu nejvhodnější.

Přestože některé ze zmíněných nástrojů jsou dostatečně komplexní na to, že by byly schopné nahradit celou samotnou rodinu norem ISO 27000, pro normu ISO 27001 hovoří jedna důležitá skutečnost. Je možné ji certifikovat, certifikátem je možné se prokázat a navíc je uznáván na mezinárodní úrovni.

Kromě toho umožňuje rozšiřování pomocí tzv. integrovaném systému řízení (ISŘ) o další certifikáty norem, jako např. ISO 9001 (řízení jakosti), ISO 14001 (řízení životního prostředí) nebo ISO 18001 (ochrana zdraví při práci). Za certifikaci více norem současně jsou vydávány tzv. stříbrné nebo zlaté certifikáty, které jsou pro organizace velmi prestižní záležitostí.

V neposlední řadě pouze certifikát ISO 27001 je uznáván jako automatické splnění většiny podmínek kybernetického zákona v České republice.



Obrázek 13: neustálé zlepšování pomocí cyklů PDCA [27]

7. Závěr

Cílem práce bylo představit normu ISO 27001 nejen z pohledu jejího obsahu, významu pro organizace a její role při formování legislativy České republiky. Autor se snažil, aby čtenář pochopil normu nejen jako dokument říkající co je potřeba dělat, ale aby chápal její význam z pohledu historického, současného a budoucího, aby chápal vztahy mezi normou, domácí legislativou a požadavky vznášené evropskými kolegy a spojenci. Normu se pokusil zasadit do souvislostí, které ukazují její místo a význam ve světě státních a soukromých společností s různými cíli a zaměřením.

Základy normy ISO 27001 vznikaly ve Velké Británii od devadesátých let jako reakce na první bezpečnostní incidenty v nově vznikajícím digitálním světě. Od té doby uběhlo mnoho času a z tehdejší normy jediné země vznikl celosvětově uznávaný standard, který se stal inspirací pro legislativní úpravy dalších států a v určité míře i celé Evropské unie.

Jak bylo v práci ukázáno, kybernetický zákon České republiky je touto normou velmi silně inspirován. Lze říci, že některé jeho části jsou z normy téměř bez úpravy převzaty. Národní bezpečnostní úřad zdůvodnil tento krok skutečností, že mnoho organizací, kterých se nově vzniklý zákon měl dotýkat, již podle této normy bezpečnost informací řídí.

Právě toto spojení normy ISO 27001 a legislativy je důvod, kvůli kterému autor v této práci věnoval tolik prostoru také kybernetickému zákonu. Český stát chce, aby pro stát důležité organizace řídily bezpečnost informací klíčových systémů, a to způsobem, který předkládá právě norma ISO 27001.

Samotný zákon vznikal rychle. Od záměru k jeho vytvoření z roku 2012 do začátku účinnosti z roku 2015 uplynuly pouze tři roky. To je velmi krátká doba na zajištění souladu s obrovským množstvím povinností, které zákon nařizuje. Zejména pokud jste organizace, která doposud řízení bezpečnosti informací vůbec neřešila. Zákonodárci museli být velmi opatrní, koho se zákonem dotknou, aby se jeho požadavky nestaly pro některé společnosti likvidační. Bylo jasné, že seznam organizací, které by se zákonem měly řídit, je značný. Zároveň bylo jasné, že většina z nich

potřebuje více času. V opačném případě by se dalo předpokládat silné lobby při tvorbě zákona, což by pravděpodobně vyústilo ve snížení jeho kvality.

Zákon tedy cílovou skupinu označil neurčitě a určující pravomoc udělil Národnímu bezpečnostnímu úřadu, Ministerstvu vnitra a vládě. Výchozí stav z roku 2015 je však tristní. Např. ani jedno jediné zdravotnické zařízení není dnes povinno řídit informace a tedy minimalizovat rizika jejich zneužití, poškození apod. Jak nebezpečný je tento stav u organizací spravující lékařské dokumenty podléhající zákonu o ochraně osobních údajů je nejspíše zřejmé. Pro mnohá zařízení by však nutnost okamžitého zavedení těchto systémů znamenala výdaje, které si nemohou dovolit. Hrozilo by snížení úrovně péče o pacienty. V jiných odvětvích situace není o mnoho lepší. Osobně se však domnívám, že kritéria se budou průběžně měnit a jejich zpřísnění povede ke stále většímu množství organizací, které do působnosti zákona budou spadat. Norma ISO 27001 tak, alespoň v České republice, bude nabývat na významu.

Kromě plnění požadavků kybernetického zákona má zavádění normy i jiný důvod. Je to dobře postavená norma, která se osvědčila v praxi. Jak je patrné ze zkušeností auditorů i odpovědí zástupců samotných organizací, norma opravdu pomáhá snižovat rizika hrozící informačním aktivům. Zejména soukromé společnosti vidí její nesporný přínos a s odstupem času hodnotí její zavedení jako správný krok, který by udělaly znovu. Právě tato skutečnost svědčí o kvalitách normy asi ze všeho nejvíce.

Smutnou realitou je, že zejména státní organizace si důležitost řízení informací stále plně neuvědomují a normu chápou jako další nutné zlo, kterým se jim někdo snaží zkomplikovat již tak složitý život. Naštěstí se ukazuje, že i čas hraje ve prospěch normy a i tyto organizace ji po více či méně letech od zavedení oceňují.

Na závěr práce byl vysvětlen vztah normy a dalších nástrojů pro zvyšování kybernetické bezpečnosti. Bylo ukázáno, že existuje více přístupů jak vyhovět požadavkům normy ISO 27001. Organizace si dnes mohou zvolit mezi velkou škálou mezinárodně uznávaných a v praxi ověřených nástrojů. Většina velkých organizací oslovuje poradenské firmy, které jim pomáhají při výběru vhodných nástrojů, jejich

samotné implementaci i následných auditech. Tato sféra se v posledních letech stala velkým podnikatelským hřištěm pro množství specializovaných společností. V zemích Evropské unie vznikají nové legislativy, normy a nástroje a situace se pro nespecializované organizace stává rychle velmi nepřehlednou. Blíží se doba, kdy k organizacím bude neodmyslitelně patřit oddělení zabývající se touto problematikou stejně, jako k nim již dnes neodmyslitelně patří např. právní oddělení. Lze tak očekávat, že sektor s těmito službami bude v budoucnosti pouze růst.

8. Seznam informačních zdrojů

1. *A Short History of the ISO 27000 Standards* [online]. Corwen: The ISO 27000 Directory, 2015 [cit. 2015-09-30]. Dostupné z: http://www.27000.org/thepast.htm
2. Akvizice. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2014 [cit. 2016-04-24]. Dostupné z: https://cs.wikipedia.org/wiki/Akvizice
3. *Bezpečnostní Incident* [online]. Wilmington: Management Mania, 2016 [cit. 2016-01-16]. Dostupné z: https://managementmania.com/cs/bezpecnostni-incident
4. *Business Model for Information Security (BMIS)* [online]. New York: Information Systems Audit and Control Association, 2016 [cit. 2016-04-13]. Dostupné z: http://www.isaca.org/Knowledge-Center/bMIs/Pages/business-Model-for-Information-security.aspx
5. *Certification* [online]. Geneva: International Organization for Standardization, 2016 [cit. 2016-04-12]. Dostupné z: http://www.iso.org/iso/home/standards/certification.htm
6. *Certifikace systému podle ISO/IEC 27001* [online]. Zábřeh: Město Zábřeh, 2015 [cit. 2016-04-12]. Dostupné z: http://www.muzabreh.cz/mestsky-urad/system-rizeni-bezpecnosti-informaci/2485-certifikace-systemu-podle-isoiec-27001
7. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* [online]. Brussels: European Commission, 2013 [cit. 2016-03-22]. Dostupné z: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
8. *Členové CQS* [online]. Praha: Sdružení pro certifikaci systémů jakosti, 2015 [cit. 2015-09-30]. Dostupné z: http://www.cqs.cz/O-nas/Clenove-CQS/
9. *ČSN ISO/IEC 27000 (36 9790) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.

10. *Databáze národní knihovny ČR* [online]. Praha: Česká terminologická databáze knihovnictví a informační vědy (TDKIV), 2014 [cit. 2015-09-25]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000456&local_base=KTD
11. GOGELA, Robert. Standardy a definice pojmů bezpečnosti informací. In: *CyberSecurity.cz: Kybernetická bezpečnost* [online]. 2015 [cit. 2015-09-25]. Dostupné z: http://www.cybersecurity.cz/data/gogela.pdf
12. *IQNet Association: Our Partners* [online]. Bern: The International Certification Network, 2015 [cit. 2015-09-30]. Dostupné z: http://www.iqnet-certification.com/index.php?page=homecontent&ID=128
13. *ISMS - Seriál o řízení bezpečnosti* [online]. Brno: Gity, 2015 [cit. 2015-10-01]. Dostupné z: http://www.chrantesidata.cz/cs/art/472-isms-serial-o-rizeni-bezpecnosti
14. *ISO 27001 Security: ISO 27K timeline* [online]. Hastings: IsecT, 2015 [cit. 2015-09-30]. Dostupné z: http://www.iso27001security.com/html/timeline.html
15. *ISO 9001: Zavedení a certifikace normy ISO 9001* [online]. Český Těšín: Info-ISO.cz, 2016 [cit. 2016-04-12]. Dostupné z: http://www.info-iso.cz/iso_9001_zavedeni_a_certifikace/
16. *ITIL® Processes & Best Practices: Introduction: Everything you need to know about ITIL and IT Service Management* [online]. Houston: BMC Software, 2016 [cit. 2016-04-13]. Dostupné z: http://www.bmc.com/guides/itil-introduction.html
17. IZQUIERDO, Fernando a Fernando Ferrer OLIVARES. V Jornada Nacional de Seguridad Informática: COBIT Security Baseline. In: *SlidePlayer* [online]. Španělské království: SlidePlayer.es Inc., 2005 [cit. 2016-04-13]. Dostupné z: http://slideplayer.es/slide/1701233/
18. JELÍNEK, Petr. Efektivnost informačních systémů. In: *SlidePlayer* [online]. Česká republika: SlidePlayer.cz Inc., 2005 [cit. 2016-04-13]. Dostupné z: http://slideplayer.cz/slide/3646308/

19. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0.
20. *Komise posiluje obranná opatření proti kybernetickým útokům* [online]. Praha: Zastoupení Evropské komise v České republice, 2013 [cit. 2016-03-22]. Dostupné z: http://europa.eu/rapid/press-release_IP-10-1239_cs.htm
21. *Kybernetická bezpečnost* [online]. CyberSecurity.cz, 2015 [cit. 2015-09-29]. Dostupné z: http://www.cybersecurity.cz/basic.html
22. MADAR, Zdeněk. *Slovník českého práva.* 1. vyd. Praha: Linde, 1995. ISBN 80-85647-62-1.
23. *Národní centrum kybernetické bezpečnosti: Co je NCKB* [online]. Praha: Národní centrum kybernetické bezpečnosti, 2015 [cit. 2015-09-30]. Dostupné z: http://www.govcert.cz/cs/
24. *Národní centrum kybernetické bezpečnosti: Strategie / akční plán* [online]. Praha: Národní centrum kybernetické bezpečnosti, 2016 [cit. 2016-03-22]. Dostupné z: http://www.govcert.cz/cs/informacni-servis/strategie-a-akcni-plan/
25. Nařízení vlády č. 315/2014 Sb., o kritériích pro určení prvku kritické infrastruktury. In: *Sbírka zákonů*. Praha: Vláda České republiky, 2014.
26. *Nová legislativa EU o kyberbezpečnosti a ochraně dat* [online]. Brno: SystemOnLine, 2016 [cit. 2016-03-22]. Dostupné z: http://www.systemonline.cz/clanky/nova-legislativa-eu-o-kyberbezpecnosti-a-ochrane-dat.htm
27. PDCA. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2014 [cit. 2016-04-24]. Dostupné z: https://en.wikipedia.org/wiki/PDCA
28. *Plán počítačové bezpečnosti v EU má chránit otevřený internet a svobodu a příležitosti v on-line prostředí* [online]. Praha: Zastoupení Evropské komise v České republice, 2013 [cit. 2016-03-22]. Dostupné z: http://ec.europa.eu/ceskarepublika/press/press_releases/13_94_cs.htm

29. *Pojmy: Bezpečnost* [online]. Praha: Ministerstvo vnitra České republiky, 2015 [cit. 2015-09-29]. Dostupné z: http://www.mvcr.cz/clanek/pojmy-bezpecnost.aspx

30. Politika. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2014 [cit. 2016-04-24]. Dostupné z: https://cs.wikipedia.org/wiki/Politika

31. *Prinya acis slide for swpark - it & information security human resource development plan for aec* [online]. Bangkok: ACIS Professional Center, 2011 [cit. 2016-04-13]. Dostupné z: http://www.slideshare.net/TISAProTalk/prinya-acis-slide-for-swpark-it-information-security-human-resource-development-plan-for-aec-2015tisa-ptotalk-22554

32. *Risk IT Framework for Management of IT Related Business Risks* [online]. New York: Information Systems Audit and Control Association, 2016 [cit. 2016-04-13]. Dostupné z: http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/default.aspx

33. *Řada norem ISO/IEC 27000* [online]. Praha: Risk Analysis Consultants, 2015 [cit. 2015-09-30]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/ISO27000

34. *SpreadsheetZONE* [online]. Cambridge: Pagos Inc., 2016 [cit. 2016-04-24]. Dostupné z: http://www.spreadsheetzone.com/ScreenShots/1/80/1.JPG

35. *V pátek 11. ledna zahajuje činnost Evropské centrum pro boj proti kyberkriminalitě (EC3)* [online]. Praha: Zastoupení Evropské komise v České republice, 2013 [cit. 2016-03-22]. Dostupné z: http://europa.eu/rapid/press-release_IP-13-13_cs.htm

36. *Val IT Framework for Business Technology Management* [online]. New York: Information Systems Audit and Control Association, 2016 [cit. 2016-04-13]. Dostupné z: http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx

37. VESELÝ, Luděk. *Přístup k řízení informační bezpečnosti ve standardech ITIL, COBIT, ISO 27002*. Praha, 2012. Bakalářská práce. Bankovní institut vysoká škola

Praha. Katedra matematiky, statistiky a informačních technologií. Vedoucí práce Doc. Ing. Vlasta Svatá, CSc.

38. Vládní návrh zákona o kybernetické bezpečnosti: Důvodová zpráva. In: *Návrhy zákonů*. Praha: Národní bezpečnostní úřad, 2014.
39. Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů*. Praha: Národní bezpečnostní úřad, 2014.
40. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. In: *Sbírka zákonů*. Praha: Národní bezpečnostní úřad, 2014.
41. *World distribution of ISO27001 certifications displayed graphically* [online]. Cambridge: IT Governance Ltd, 2014 [cit. 2015-09-30]. Dostupné z: http://www.iso270012013.info/news-articles/latest-news/april-2014/world-distribution-of-iso27001-certifications.aspx
42. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů*. Praha: Parlament České republiky, 2014.

9. Seznam obrázků

10. Seznam tabulek

11. Seznam příloh

Příloha č. 1	KO – státní správa
Příloha č. 2	KO – zdravotnictví
Příloha č. 3	KO – soukromá organizace
Příloha č. 4	POA – státní správa
Příloha č. 5	POA – zdravotnictví
Příloha č. 6	POA – soukromá organizace
Příloha č. 7	AR – státní správa
Příloha č. 8	AR – zdravotnictví
Příloha č. 9	AR – soukromá organizace
Příloha č. 10	POR – státní správa
Příloha č. 11	POR – zdravotnictví
Příloha č. 12	POR – soukromá organizace
Příloha č. 13	Registr agend
Příloha č. 14	Dotazník k zavádění normy ISO 27001 v praxi

12. Seznam výrazů

Agenda	Informace sdružené do celků podle účelu jejich zpracování nebo využití (Mana Consulting, 2015).
Aktivum	Cokoliv, co má hodnotu pro jednotlivce, organizace nebo veřejnou správu (Výkladový slovník kybernetické bezpečnosti, 2013).
Akvizice	Proces získávání či nabytí nějakého aktiva (předmětu, věci, osoby) nebo cíl tohoto procesu (Wikipedia: the free encyclopedia, 2014).
Audit	Systematický proces objektivního získávání a vyhodnocování auditních záznamů, jehož cílem je stanovit, zda činnosti systému jsou v souladu se stanovenou bezpečnostní politikou a provozními procedurami (Výkladový slovník kybernetické bezpečnosti, 2013).
Autenticita	Vlastnost, že entita je tím, za co se prohlašuje (Výkladový slovník kybernetické bezpečnosti, 2013).
Bezpečnost informací	Zajištění (ochrana) důvěrnosti, integrity a dostupnosti informací (Výkladový slovník kybernetické bezpečnosti, 2013).
Bezpečnostní hrozba	Je potenciální příčina nežádoucí události, která může mít za následek poškození informačního systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb (Výkladový slovník kybernetické bezpečnosti, 2013).
Bezpečnostní incident	Porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu Informační a komunikační technologie (Výkladový slovník kybernetické bezpečnosti, 2013).
Data	Informace ve snadno čitelné formě a pochopitelné pro subjekt, kterému jsou určeny (CyberSecurity.cz, 2015),
Dostupnost	Vlastnost přístupnosti a použitelnosti na žádost autorizované entity (Výkladový slovník kybernetické bezpečnosti, 2013).
Důvěrnost	Vlastnost, že informace není dostupná nebo není odhalena neautorizovaným jednotlivcům, entitám nebo procesům (Výkladový slovník kybernetické bezpečnosti, 2013).
Hardware	Fyzické součásti systému (zařízení) nebo jejich část (např. počítač, tiskárna, periferní zařízení) (Výkladový slovník kybernetické bezpečnosti, 2013).
Hodnocení rizik	Proces porovnání výsledků analýzy rizik s kritérii rizik k určení, zda je míra rizika přijatelná (akceptovatelná) (Výkladový slovník kybernetické bezpečnosti, 2013).

Hrozba	Potencionální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva (Vyhláška o kybernetické bezpečnosti č. 316/2014 Sb., 2014).
Informace	Každý znakový projev, který má smysl pro komunikátora i příjemce (Výkladový slovník kybernetické bezpečnosti, 2013).
Informační aktivum	Znalosti a data, která mají pro organizaci hodnotu (význam) (Výkladový slovník kybernetické bezpečnosti, 2013).
Informační bezpečnost	Viz bezpečnost informací.
Informační systém	(1) Je funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací a dat. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky; (2) komplex prvků, nacházejících se ve vzájemné interakci (L. von Bertallanfy, 1956) (Výkladový slovník kybernetické bezpečnosti, 2013).
Integrita	Vlastnost ochrany přesnosti a úplnosti aktiv (Výkladový slovník kybernetické bezpečnosti, 2013).
Kritická infrastruktura	Systémy a služby, jejichž nefunkčnost nebo špatná funkčnost by měla závažný dopad na bezpečnost státu, jeho ekonomiku, veřejnou správu a v důsledku na zabezpečení základních životních potřeb obyvatelstva (Výkladový slovník kybernetické bezpečnosti, 2013).
Kryptografie	Nauka o šifrování – disciplína, která zahrnuje zásady, prostředky a metody pro transformaci dat aby byl ukryt jejich sémantický obsah, zabráněno jejich neautorizovanému použití nebo zabráněno jejich nezjištěné modifikaci (Výkladový slovník kybernetické bezpečnosti, 2013).
Kybernetická bezpečnost	Viz bezpečnost informací.
Nepopiratelnost	Schopnost prokázat výskyt údajné události nebo činnosti a vznikajících entit s cílem řešit spory o výskytu nebo absence výskytu události nebo činnosti a zapojení entit do události (Výkladový slovník kybernetické bezpečnosti, 2013).
Ošetření rizik	Proces pro modifikování (změnu) rizika (Výkladový slovník kybernetické bezpečnosti, 2013).
Plán řízení rizik	Schéma v rámci managementu rizik specifikující přístup, dílčí části managementu a zdroje, které se mají použít k managementu rizik (Výkladový slovník kybernetické bezpečnosti, 2013).

Podpůrné aktivum	Zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému (Vyhláška o kybernetické bezpečnosti č. 316/2014 Sb., 2014).
Politika	Pojem obvykle označující proces a metodu rozhodování určité skupiny lidí (Wikipedia: the free encyclopedia, 2014).
Primární aktivum	Informace nebo služba, kterou zpracovává nebo poskytuje informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém (Vyhláška o kybernetické bezpečnosti č. 316/2014 Sb., 2014).
Registr opatření	Soubor opatření k dosažení požadované úrovně důvěry v ochranu komunikačních, informačních a jiných elektronických i ne-elektronických systémů a informací ukládaných, zpracovávaných nebo přenášených v těchto systémech s ohledem na důvěrnost, integritu, dostupnost, neodmítnutelnost a autentičnost (Výkladový slovník kybernetické bezpečnosti, 2013).
Riziko	(1) Nebezpečí, možnost škody, ztráty, nezdaru. (2) Účinek nejistoty na dosažení cílů. (3) Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu (Výkladový slovník kybernetické bezpečnosti, 2013).
Řízení rizik	Koordinované činnosti pro vedení a řízení organizace s ohledem na rizika (Výkladový slovník kybernetické bezpečnosti, 2013).
Software	Sada programů používaných v počítači, které vykonávají zpracování dat, či konkrétních úloh. Software lze dále rozdělit na: a) systémový software – vstupně/výstupní systémy, operační systémy nebo grafické operační systémy; b) aplikační software – aplikace, jednoduché utility nebo komplexní programové systémy; c) firmware – ovládací program hardwaru (Výkladový slovník kybernetické bezpečnosti, 2013).
Spolehlivost	Vlastnost konzistentního zamýšleného chování nebo výsledků (Výkladový slovník kybernetické bezpečnosti, 2013).
Významný informační systém	Informační systém naplňující určující kritéria uvedená v § 3 (Vyhláška o významných informačních systémech a určujících kritériích č. 317/2014 Sb., 2014).
Zranitelnost	Slabé místo aktiva nebo řízení, které může být využito hrozbou (Výkladový slovník kybernetické bezpečnosti, 2013).

13. Seznam zkratek

APT	Advanced Persistent Thread
AFNOR	Association Française de Normalisation
AR	Analýza rizik
BMC	Americká společnost zabývající se managementem služeb. Písmena zkratky jsou počáteční písmena příjmení zakladatelů.
BMIS	Business Model For Information Security
BS	British Standard
BSI	British Standards Insitution
CERT	Computer Emergency Response Team
COBIT	Control Objectives for Information and Related Technology
CQS	Certification of Quality Systems
CSB	COBIT Security Baseline
ČIA	Český institut pro akreditaci
ČSN	Česká státní norma
DISC	Delivering Information Solutions to Customers
DQS	Deutsche Gesellschaft zur Zertifizierung von Managementsystemen
EMS	Environmental Management System
ERÚ	Energetický regulační úřad
EU	Evropská unie
FIPS	Federal Information Processing Standards
GDPR	General Data Protection
ICT	Informační a komunikační technologie
IEC	International Electotechnical Commision
IS	Informační systém
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management Systems
ISO	International Organization for Standardization

ISŘ	Integrovaný systém řízení
IT	Informační technologie
ITIL	Information Technology Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria
ITSM	Information Technology Service Management
IZ	Informační zařízení
JQA	Japan Quality Assurance Organization
KI	Kritická infrastruktura
KII	Kritická informační infrastruktura
KO	Kontext organizace
MLA	Multi-Lateral Agreement
NATO	North Atlantic Treaty Organization
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
PD	Public Document
PDCA	Plan Do Check Act
POA	Prohlášení o aplikovatelnosti
POAIDSMI	Plan and Organize, Acquire and Implement, Deliver and Support, Monitor and Evaluate
POR	Plán ošetření rizik
QMS	Quality Management Systém
SBOP	Společná bezpečnostní a obranná politka
SP	Special Publication
VIS	Významný informační systém
ZKB	Zákon o kybernetické bezpečnosti

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2016/2017

Studijní program: Aplikovaná informatika
Forma: Kombinovaná
Obor/komb.: Aplikovaná informatika (ai2-k)

Podklad pro zadání DIPLOMOVÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Bc. Škeřík Ondřej	Voděrady 23, Voděrady	I1301590

TÉMA ČESKY:

Systém řízení bezpečnosti informací prostřednictvím normy ČSN/EN ISO/IEC 27001

TÉMA ANGLICKY:

Information Security Management System Standard and IEC / EN ISO / IEC 27001

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce je provést analýzu a posouzení specifických podmínek informační bezpečnosti v odlišných typech organizací s ohledem na související legislativní požadavky a požadavky normy ČSN/EN ISO/IEC 27001. Dále bude v práci pojednáno o vztazích normy ČSN/EN ISO/IEC 27001 a platné legislativy, zejména zákona 181/2014 Sb. o kybernetické bezpečnosti a souvisejících prováděcích právních předpisů (vyhláška o kybernetické bezpečnosti, vyhláška o stanovení významných informačních systémů a jejich určujících kritériích).
V praktické části autor ukáže některé z důležitých dokumentů normy ČSN/EN ISO/IEC 27001 na třech modelových organizacích různého typu a zhodnotí rozdíly při zavádění normy mezi různé typy organizací. Součástí této části bude také získávání informací pomocí průzkumu dotazníkovou formou.

SEZNAM DOPORUČENÉ LITERATURY:

ČSN ISO/IEC 27000. Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník. 1. Praha: normy.cz, 2014.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. In: 2014. Praha, 2015.

TRIM, Peter R a Yang-Im LEE. Cyber security management: a governance, risk and compliance framework. xxii, 240 pages. ISBN 978-147-2432-094.

Podpis studenta: ..... **Datum:** .....

Podpis vedoucího práce: ..... **Datum:** .....