Mendelova univerzita v Brně
Provozně ekonomická fakulta

Bezpečnostní audit síťové infrastruktury podniku

Diplomová práce

Vedoucí práce:
Ing. Jiří Balej

Bc. Čeněk Janza

Brno 2017

Poděkování

Rád bych poděkoval panu Ing. Jiřímu Balejovi, vedoucímu mé diplomové práce, za jeho pomocnou ruku, ochotu spolupracovat a cenné rady.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Bezpečnostní audit síťové infrastruktury podniku**
vypracoval samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*

Jsem si vědom, že se na moji práci vztahuje zákon č. 121/2000 Sb. Autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.

Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 14. května 2017 _____

Abstract

Bc. Čeněk Janza, Security audit of network infrastructure for company. Brno: Mendel University, 2017.

This thesis deals with security audit and its methods for finding gaps in safety and subsequently draft measures to eliminate or minimalize this gaps. This work also describes the standards and legislation of information security. There is carried out a safety audit of the business and the analysis results together with the subsequent design of security measures. Further it describes the important issues and points during audit process.

Keywords

Security audit, standards, legislative, information security management system, ISO/IEC 27000.

Abstrakt

Bc. Čeněk Janza, Bezpečnostní audit síťové infrastruktury podniku. Brno: Mendelova Univerzita, 2017.

Diplomová práce je zaměřena na bezpečnostní audit a jeho metody pro nalezení nedostatků v bezpečnosti a následný návrh opatření k jejich odstranění či minimalizaci. V práci jsou dále popsány normy a legislativa týkající se bezpečnosti informací. Je zde proveden bezpečnostní audit podniku a provedena analýza výsledků spolu s následným návrhem bezpečnostních opatření. Dále popisuje důležité otázky a body postupu při auditu.

Klíčová slova

Bezpečnostní audit, norma, legislativa, řízení informační bezpečnosti, ISO/IEC 27000.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Význam informačních a komunikačních technologií v organizaci roste ruku v ruce s objemem zpracovaných dat v informačních systémech. V posledních letech právě informace získaly pro většinu organizací velkou hodnotu a jejich ztráta by mohla znamenat problémy v činnosti, případně finanční ztrátu. Je tedy potřeba zajistit jejich dostatečnou ochranu, čímž se dostáváme do oblasti informační bezpečnosti. Ani použití nejrůznějších technických zařízení ovšem nemusí zajistit stoprocentní bezpečnost. Mnoho organizací si stále neuvědomuje, že předcházení bezpečnostním incidentům je efektivnější a z dlouhodobějšího hlediska výhodnější, než řešit až jeho následky. Čím větší jsou požadavky na bezpečnost informací, tím větší jsou i náklady vynaložené na implementaci potřebných opatření. Rozhodnutí je na každé organizaci, jak velké finanční prostředky je ochotna do zabezpečení investovat a posoudit, zda vynaložené prostředky na bezpečnostní opatření nepřesáhnou výšku potencionální škody. Často však chybí dostatečně kvalifikovaní zaměstnanci, kteří by toho byli schopni, a je nutné se obrátit na externí firmu zaměstnávající bezpečnostní experty. Tito experti mohou provést komplexní bezpečnostní audit, který odhalí nedostatky v informační bezpečnosti a následně navrhnout opatření pro jejich eliminaci či minimalizaci. Podobná kontrola, ať už interní nebo externí by měla být prováděna alespoň jednou ročně, aby bylo možné předejít bezpečnostním incidentům.

1.1 Cíl práce

Cílem práce je přiblížit problematiku informační bezpečnosti a metody pro vytvoření bezpečnostního auditu. Následně vybrat metodiku vhodnou pro využití ve středně velkém podniku se zaměřením na strojírenskou výrobu. Dále se seznámit s normami, o které se tato metodika opírá, a s legislativou České republiky týkající se bezpečnosti informací. Poté s vybranou metodikou stanovit postup a provést bezpečnostní audit v organizaci. Na základě vyhodnocení výsledků auditu navrhnout možná opatření, která odstraní nebo minimalizují nalezené zranitelnosti. Následně sestavit důležité otázky, které by si měly podobné organizace pokládat, pokud o bezpečnostním auditu uvažují a stanovit důležité body, na které by se měly zaměřit.

1.2 Základní pojmy

1. Aktiva

   Představují důležitý hmotný i nehmotný majetek a lidské zdroje organizace. Mezi hmotný můžeme zařadit různá hardwarová zařízení a jiné fyzické prostředky. Jako nehmotné se většinou považují podniková data. Lidské zdroje představují zaměstnance organizace a smluvní třetí strany. Každé aktivum má svého vlastníka, který za něj zodpovídá.

2. Hrozba

   Hrozbou rozumíme událost, která negativním způsobem ovlivňuje bezpečnost, působí na zranitelné místo aktiva a může mít za následek způsobení škody na tomto aktivu. Můžeme je rozdělit na úmyslné (krádež, útok na síťovou infrastrukturu apod.) a neúmyslné, které jsou způsobené lidskou chybou či neznalostí popř. přírodního charakteru.

3. Riziko

   Pravděpodobnost, s jakou hrozba využije zranitelnost a způsobí narušení důvěrnosti, integrity nebo dostupnosti.

4. Zranitelnost

   Zranitelnost je vlastnost aktiva. Jedná se o slabinu na fyzické, logické nebo administrativní úrovni, která může být zneužita hrozbou.

5. Opatření

   Opatřením rozumíme aktivitu, která nám umožnuje snižovat míru rizika hrozby. (Požár, 2005)

1.3 Bezpečnost IT

Oblasti bezpečnosti informačních systémů se v posledních letech dostává stále více pozornosti v důsledku zpracování narůstajícího množství informací. Pro organizace představují tyto informace často nezanedbatelnou hodnotu. Jedná se hlavně o osobní údaje, daňová přiznání, elektronické komunikace či bankovní výpisy, které musí být odpovídajícím způsobem chráněny. Zároveň s jejich ochranou musíme zaručit:

- Přístup pouze oprávněným osobám.
- Zpracování nefalšovaných informací.
- Možnost dohledat, kdo je vytvořil, změnil či odstranil.
- Dostupnost informací.
- Zamezení jejich vyzrazení.

Jedním z nejdůležitějších dokumentů řešících informační bezpečnost v organizaci je bezpečnostní politika. Jedná se o základní dokument, který jednoznačně definuje bezpečnostní zásady, předpisy, rozsah, hranice a bezpečnostní požadavky. Politika by měla určit klíčové osoby spolu s jejich pravomocemi a odpovědností za informační bezpečnost a postup v případě bezpečnostních incidentů.

1.3.1 Bezpečnostní mechanismy

Implementaci bezpečnostních funkcí můžeme rozdělit do několika základních bezpečnostních mechanismů.

1. Softwarové

   Softwarové či logické bezpečnostní mechanismy se zabývají řízením přístupu, při němž využívají různá kryptografická opatření jako hesla a práva v rámci autentizace a autorizace do systému.

2. Hardwarové

   Hardwarové neboli technické mechanismy představující šifrovací zařízení nebo autentizační a identifikační karty k přístupu do prostor s omezeným přístupem.

3. Fyzické

   Mezi tyto mechanismy řadíme stínění vyzařovaných signálů, trezory a zámky, protipožární ochranu, záložní generátory v případě výpadku elektrické energie.

4. Administrativní

   Bezpečnostním incidentům je možné předejít i výběrem důvěryhodné osoby, dostatečně silného hesla či dodržováním právních norem, zákonů, vyhlášek a předpisů. (Hanáček, Staudek, 2000)

1.3.2 Nejčastější hrozby

Zde si zmíníme skupiny nejčastějších hrozeb, které v dnešní době mohou narušit informační bezpečnost organizace.

1. Lidská chyba

   Největší počet bezpečnostních incidentů je způsoben právě lidskou chybou. Mohou být neúmyslné, kdy je zaměstnanec nedostatečně proškolen, jak se zařízením či systémem zacházet, nebo úmyslné za účelem poškození organizace, při kterém dojde k prozrazení interních informací či zničení majetku.

2. Nedostatečné zabezpečení

   K ochraně informací je potřeba přistupovat systematicky. Organizace však často zanedbávají své povinnosti, neprovádějí dostatečné kontroly a infor-

mační bezpečnosti nevěnují potřebnou pozornost, dokud nedojde k bezpečnostnímu incidentu.

3. Fyzická bezpečnost

   Zranitelnost fyzického prostředí vyplývá z nevhodně umístěných informačních technologií, jako jsou směrovače, přepínače či servery. Často jsou tato zařízení provozována v prostorech, kde je umožněn přístup neautorizovaným osobám.

4. Chybné nastavení procesů

   Organizace často zanedbávají dokumentaci popisující informační toky a procesy, které by měly odpovídat požadovaným normám, směrnicím a podobným dokumentům. Správci informační bezpečnosti nemají většinou k dispozici dostatek pravomocí pro uplatňování potřebných bezpečnostních postupů, aby mohli bezpečnostním incidentům předcházet. Zde je nutné zmínit nevhodné nastavení přístupů, kdy uživatel má k dispozici informace, které nejsou pro jeho práci potřeba. (Čermák, 2015)

2 Normy a legislativa

V této kapitole budou popsány nejdůležitější normy z oblasti informační bezpečnosti, které obsahují doporučení pro zavedení systému řízení bezpečnosti informací a platná legislativa České republiky, kterou se musí každý subjekt realizující informační bezpečnost řídit.

Pokud vytváříme návrh nebo provádíme kontrolu zabezpečení, není možné se spoléhat jen na osobní zkušenost. Existuje mnoho specifických požadavků a doporučení, které je nutné vzít za své. Normy také představují metriku, zaručující srovnatelnost implementace a stejný pohled nezávislých auditorů na informační bezpečnost organizace.

2.1 Normy řady ISO/IEC 27000

Pro oblast bezpečnosti informací rezervovala organizace ISO (International Organization for Standardization) sérii ISO/IEC 27000. Jedná se o mezinárodní normu použitelnou pro všechny typy a velikosti organizací, která poskytuje přehled termínů a definic systémů řízení informační bezpečnosti (ISMS). V České republice bývají normy ISO přebírány jako ČSN. Obsahuje především následující normy:

1. ČSN ISO/IEC 27000 - Přehled a slovník

   Zde jsou uvedeny definice pojmů a terminologický slovník týkající se norem z této série. Bezpečnost informací jako technický obor obsahuje rozsáhlou a komplexní terminologickou síť, aby nedocházelo k nedorozuměním, která by mohla znehodnotit formální hodnocení, audity nebo certifikace.

2. ČSN ISO/IEC 27001 Systémy řízení bezpečnosti informací – Požadavky

   Jedná se o klíčovou normu obsahující soubor formálních specifikací, která si klade za cíl aplikovat ISO/IEC 27002 v rámci procesu ustanovení, provozu, údržby a zlepšování systému řízení informační bezpečnosti v souladu se systémy řízení kvality a bezpečnosti prostředí. Na základě hodnocení rizik mohou organizace následně aplikovat vhodná opatření dle ISO/IEC 27002. Norma představuje model PDCA (Plan-Do-Check-Act) pro vývoj, implementaci a zdokonalování systému řízení informační bezpečnosti v organizaci.

3. ČSN ISO/IEC 27002 Soubor postupů pro opatření bezpečnosti informací

   Tato norma představuje sbírku nejlepších bezpečnostních opatření, která je vhodné implementovat pro bezpečnost informací v rámci organizace. Je zde obsaženo 114 základních opatření, která se dále rozšiřují do specifických bezpečnostních patření. Opatření vhodná pro implementaci jsou doporučena dle výsledků hodnocení rizik. Rozhodnutí, zda jednotlivá opatření implementovat, jsou však ponechána na samotné organizaci a konkrétní situaci. Tímto přístupem je zajištěno, že normu je možné aplikovat na nejrůznější organizace a poskytuje dostatečnou flexibilitu při její implementaci.

4. ČSN ISO/IEC 27003 Směrnice pro implementaci systému řízení bezpečnosti informací

   Obsahem této normy je návod k úspěšnému návrhu a implementaci systému řízení informační bezpečnosti v organizaci v souladu s požadavky normy ISO/IEC 27001. Je zde popsán proces plánování implementace, která slouží k realizaci projektu a zavedení ISMS. Tento proces obsahuje několik etap:

   - Souhlas organizace a zahájení projektu.
   - Definice cíle a rozsahu.
   - Identifikace a ohodnoceni aktiv.
   - Provedení analýzy rizik a návrh opatření.
   - Návrh ISMS.

5. ČSN ISO/IEC 27004 Řízení bezpečnosti informací - Měření

   Norma slouží jako pomůcka pro měření a prezentaci efektivity systému řízení informační bezpečnosti v organizaci a zároveň zahrnuje řídící procesy definované v rámci ISO/IEC 27001 a opatření normy ISO/IEC 27002. Obsahem je vývoj, používání a definice jednotlivých metrik pro měření informační bezpečnosti, odpovědnost za řízení, analýza dat a závěrečné vyhodnocení výsledků měření.

6. ČSN ISO/IEC 27005 Řízení rizik bezpečnosti informací

   Tato norma poskytuje doporučení pro řízení rizik bezpečnosti informací s ohledem na požadavky ISO/IEC 27001 a techniky pro analýzu informačních rizik. Vychází z revizí dříve vydaných norem ISO/IEC TR 13335-3:1998 a ISO/IEC TR 13335-4:2000. Normou definované činnosti pro řízení rizik jsou:

   - Stanovení kontextu.
   - Hodnocení rizik.
   - Zvládání rizik.
   - Přijetí rizik.
   - Seznámení s riziky.
   - Monitorování a přezkoumávání rizik.

7. ČSN ISO/IEC 27006 Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

   Norma blíže specifikuje jednotlivé požadavky a následně poskytuje doporučení pro orgány, které provádějí audit a certifikaci systému řízení informační bezpečnosti v organizaci. Zaměřuje se převážně na průběh certifikace ISMS a doplňuje požadavky norem ISO/IEC 17021 a ISO/IEC 27001.

8. ČSN ISO/IEC 27007 Směrnice pro audit systémů řízení bezpečnosti informací

   Obsahem je doporučení k provádění bezpečnostních auditů systému řízení informační bezpečnosti dle normy ISO/IEC 27001 a způsobilosti auditorů. Čerpá zejména z normy ISO/IEC 19011:2002 Směrnice pro auditování systému ma-

nagementu jakosti a/nebo systému environmentálního managementu. (Ondrák, Sedlák, Mazálek, 2013)

2.2 Legislativa v České republice

Celá řada zákonů a vyhlášek se opírá o normy vydané normalizačními organizacemi. Zde budou zmíněny některé z důležitých zákonů České republiky, které se týkají bezpečnosti informací.

1. Zákon o svobodném přístupu k informacím

   Zákon č. 106/1999 Sb. ukládá orgánům a organizacím povinnost poskytovat a zpřístupňovat veškeré informace týkající se své činnosti. Rovněž stanovuje způsob poskytování informací, potřebné lhůty, podávání a vyřizování žádostí.

2. Zákon o elektronickém podpisu

   Zákon č. 227/2000 Sb. upravuje používání elektronického podpisu, značky a certifikačních služeb. Stanovuje také sankce za porušení tohoto zákona. Je také povinnost vést a zveřejňovat seznam důvěryhodných certifikačních služeb.

3. Zákon o archivnictví a spisové službě

   Zákon č. 499/2004 Sb. se zabývá úpravou výběru, evidence, kategorizace a ochranou archivů. Následně pak právy a povinnostmi držitelů, vlastníků či správců těchto archivů a i zpracováním osobních údajů pro účely archivnictví. Vyhláškou č. 645/2004 Sb. byly definovány pojmy dokument a archiválie, kde dokumentem se rozumí písemný, obrazový, zvukový, elektronický nebo jiný záznam, který vznikl z činnosti původce. Archiválií chápeme záznam vybraný k trvalému uchování.

4. Zákon o ochraně osobních údajů

   Zákon č. 101/2000 Sb. v souladu s právem na ochranu před neoprávněným zasahováním do soukromí a zneužívání osobních údajů upravuje povinnosti i práva při zpracování osobních údajů.

5. Zákon o ochraně utajovaných informací

   Zákon č. 412/2005 Sb. stanovuje zásady, zda se jedná o utajované informace. Definuje podmínky přístupu k utajovaným informacím a požadavky na jejich ochranu, dále také upravuje zásady pro stanovení citlivých činností a vymezuje činnost Národního bezpečnostního úřadu. (Douček, 2011)

6. Zákon o kybernetické bezpečnosti

   Zákon č. 181/2014 Sb., jehož předmětem je úprava práv a povinností osob, působností a pravomocí orgánů státní správy v oblasti kybernetické bezpečnosti. Tento zákon se nevztahuje na informační či komunikační systémy, které nakládají s utajovanými informacemi. (Peterka, 2014)

7. Usnesení vlády ČR č. 624/2001 ze dne 20. 6. 2001

   Orgány státní správy a jimi řízené organizace jsou vázány pravidly, zásadami a způsoby zabezpečování kontroly užívání počítačových programů. Cílem je stanovit jednotné, komplexní a transparentní postupy pro pořizování, používání, evidenci a kontrolu aplikací v souladu s příslušnými licenčními smlouvami. (Douček, 2011)

3 Výběr metodiky

Kontrola bezpečnosti informací je náročná a komplexní činnost, při které je potřeba dodržovat mnoho specifických požadavků a lokální legislativu.

V rámci bezpečnostního auditu je nutné stanovit metodiku, podle které se bude postupovat. Existuje mnoho nejrůznějších metod a postupů aplikovatelných na různé cíle a požadavky organizací. Mezi nejpoužívanější metodiky pro provedení bezpečnostního auditu můžeme zařadit COBIT, ITIL, ISMS, BS7799 a PCIDSS. Více se seznámíme s metodikami COBIT, ITIL a ISMS, které můžeme využít pro malé, střední i velké organizace. Před započetím samotného auditu je potřeba si vybrat metodiku, podle které se bude postupovat. Je důležité si stanovit, co by hledaná metodika měla splňovat, aby vyhovovala požadavkům a potřebám pro provedení auditu. Metodika použitá v této práci by měla splňovat následující:

- Využitelnost pro malé a střední organizace.
- Dostupné nástroje.
- Aktuálnost.
- Přizpůsobitelnost.

3.1 COBIT

COBIT (Control Objectives for Information and Related Technology) je mezinárodně uznávaným standardem pro správu a řízení informatiky. Slouží jako podpůrný nástroj pro nejvyšší manažery, který umožňuje překlenutí zásadních rozdílů mezi technickými otázkami, obchodními riziky a požadovanou kontrolou.

První verze metodiky COBIT byla vydána v roce 1996 a obsahovala pouze základní rámec metodiky. Vytvořena byla asociací ISACA (Information Systems Audit and Control Association) a měla sloužit jako sada nástrojů pro správu IT v organizaci. V druhé verzi, která vyšla roku 1998, byla metodika rozšířena o kontrolní principy (Audit guidelines), rozpracované procesy a detailnější cíle (Control objectives) a implementační nástroje (Implementation toolset). V roce 2000 byla vydána třetí verze, která obsahovala již manažerské postupy (Management guidelines) a byl inovován rámec metodiky. Čtvrtá verze vyšla koncem roku 2005 a následně její aktualizace na verzi COBIT 4.1 v roce 2007. Nejnovější verze metodiky je nyní COBIT 5, jež byla představena v červnu roku 2012. (Bukovský, 2008)

COBIT 5

COBIT 5 se zakládá na 5 principech, které jsou společné pro organizace bez rozdílu velikosti. Tyto principy se navzájem doplňují a navazují na sebe. COBIT 5 v sobě rovněž zahrnuje různé standardy jako např. technické (ISO, EDIFACT), kvalitativní (ITSEC, TCSEC, TickIT) a průmyslové (ESF, I4) či kodex vydávaný asociací ISACA. Je patrné, že COBIT 5 je obecnější metodikou, jelikož má velice široký záběr a pokrývá různé oblasti. Aktuální verze se skládá z těchto dokumentů:

- Framework
  Představuje základní rámec metodiky, který obsahuje principy, předpoklady a vazby na další rámce.
- Enablers Guides (Enabling Processes, Enabling Information)
  Jedná se o obecnější návody umožňující efektivní správu IT.
- Professional Guides (Implemention, Information Security, Assurance, Risk)
  Tyto dokumenty jsou určeny pro specialisty v oblastech implementace, informační bezpečnosti, pojištění a hrozeb.
- Online Collaborative Enviroment
  On-line dokumenty, které obsahují zkušenosti sdílené uživateli s předchozími dokumenty.

Jak již bylo zmíněno výše, COBIT 5 se skládá z pěti principů. Tyto principy napomáhají organizacím k uživatelské spokojenosti, dodržování zásad a pravidel, zlepšování vztahů mezi businessem a IT. Jedná se o následující principy:

- Zajištění potřeb zainteresovaných stran (Meeting Stakeholder Needs).
- Pokrytí celé organizace (Covering the Enterprise End-to-end).
- Použití jednoho integrovaného rámce (Applying a Single Integrated Frameword).
- Povolení celistvého přístupu (Enabling a Holistic Approach).
- Oddělení vedení společnosti od každodenního řízení (Separatin Governance From Management).

Zajištění potřeb zainteresovaných stran

Každá organizace má nějakého majitele, pracují v ní zaměstnanci, poskytuje služby či vytváří produkty. S organizací vždy někdo spolupracuje, ať už dodavatel, partner nebo banka. Organizace také musí dodržovat určitá pravidla a právní normy. Všechny tyto zainteresované strany (majitel, zaměstnanci, zákazník, dodavatel, partner a bankovní ústavy) jsou tzv. stakeholdery a mohou existovat uvnitř i mimo organizaci.

Zájmy těchto zainteresovaných stran mohou být shodné ale i protichůdné s těmi, které má organizace a tyto zájmy mají pro každou stranu vlastní hodnotu. Tato hodnota je odvozena od získaných přínosů pro danou organizaci. Každá strana přitom do určité míry očekává zajištění jejich potřeb a zájmů.

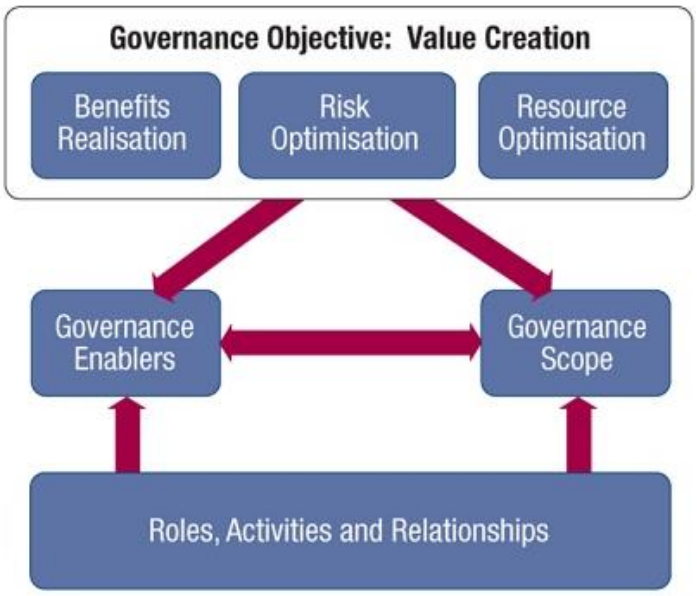
Pro zajištění přínosů je však potřeba vynaložit optimální prostředky a zdroje, abychom dosáhli co nejvyšší hodnoty. Vynaložení určité míry prostředků a zdrojů s sebou však přináší rizika a je potřeba zajistit, aby potenciální riziko bylo přiměřené získané hodnotě.

Tento vztah mezi zainteresovanými stranami je zobrazen na obrázku níže (Obr. 1), kde pomocí této definice COBIT 5 následně identifikuje obecné potřeby a transformuje je do podoby jednotlivých pilířů IT, cílů organizace a IT.

Obr. 1 Vytvoření hodnoty (Vitouš, 2013)

Pokrytí celé organizace

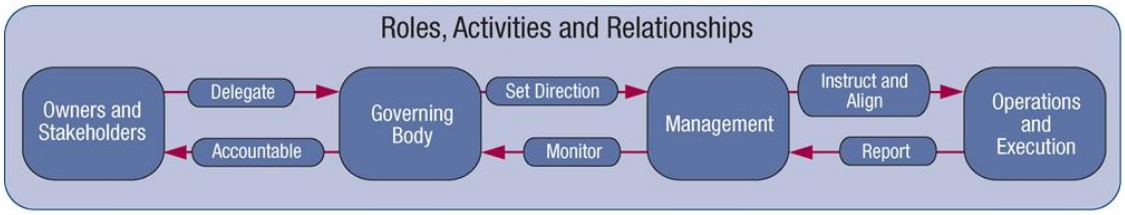
Jedná se o pokrytí všech funkcí a procesů v rámci celé organizace, kde IT oddělení nesmí být oddělováno od ostatních a mělo by se zapojovat i v ne-IT procesech. Je potřeba zajistit zdroje (Enablers), stanovit rozsah (Scope) a přiřadit odpovědnosti (Roles, Activities and Relationships), aby bylo možné definovat směr pro organizaci jako celek.



Obr. 2 Pokrytí organizace (Vitouš, 2013)

I proces přiřazení odpovědností začíná zainteresovanými stranami a hlavně majitelem organizace. Majitel specifikuje požadavky a následně deleguje odpovědnost

za vytvoření směru organizace na vrcholové vedení (Governing Body). To ovšem neznamená, že by se odpovědnosti (Accountability) sám zbavil. Vrcholové vedení poté vytvoří směr organizace podle, kterého střední vedení (Management) instruuje operační složky (Operations and Execution). Operační složky následně zpětně reportují výsledky střednímu vedení, které je kontrolováno vrcholovým vedením. Na obrázku (Obr. 3) je zobrazen celkový proces a vztahy.



Obr. 3 Odpovědnosti a vztahy (Vitouš, 2013)

Použití jednoho integrovaného rámce

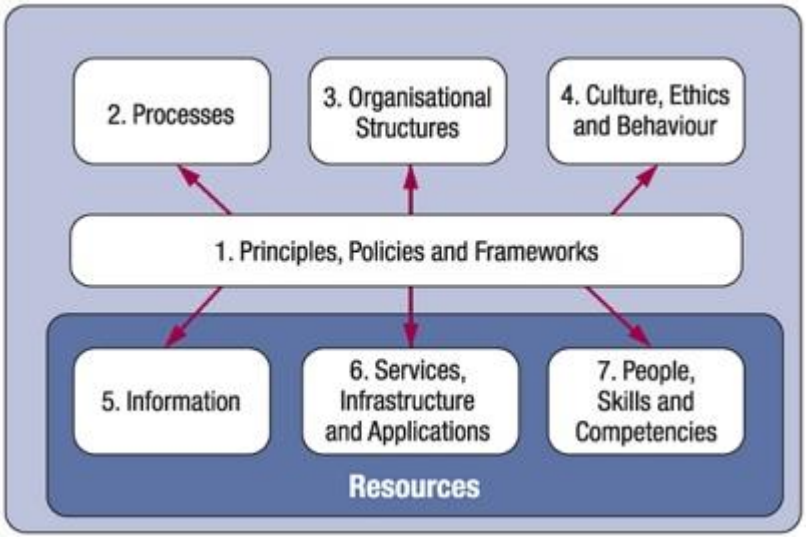
Existuje mnoho standardů, metodik a rámců využívaných v oblasti IT, které se navzájem doplňují či překrývají. Využívají různé přístupy, terminologii a byly vytvořeny různými organizacemi. V rámci zjednodušení a sjednocení by však bylo vhodné využít pouze jeden. COBIT 5 sjednocuje rámce COBIT 4, VAlIT a RiskIT, které byly vydány v různém období, a pokrývali odlišné oblasti. Tímto byla rozšířena funkcionalita a pokryta větší oblast působnosti.

Povolení celistvého přístupu

COBIT 5 definuje principy pro efektivní správu IT a řízení podniku, které jsou vyváženy dle následujících sedmi bodů:

- Principy, politiky a rámce (Principles, policies and frameworks)
  Definuje pravidla pro každodenní činnost.
- Procesy (Processes)
  Definuje principy a činnosti, které určují jak dosahovat potřebných výsledků.
- Organizační struktury (Organization structure)
  Definuje strukturu a způsob organizování lidí do týmů.
- Kultura, etika a chování (culture, ethics and behaviour)
  Jedná se o předvídání chování a komunikace v organizaci.
- Informace (Information)
  Definuje, jak a kde informace vznikají a také kdo s nimi může pracovat.
- Služby, infrastruktura a aplikace (Services, infrastructure and applications)
  Specifikuje technické prostředky, které jsou potřeba pro zajištění informací a jejich propojení.

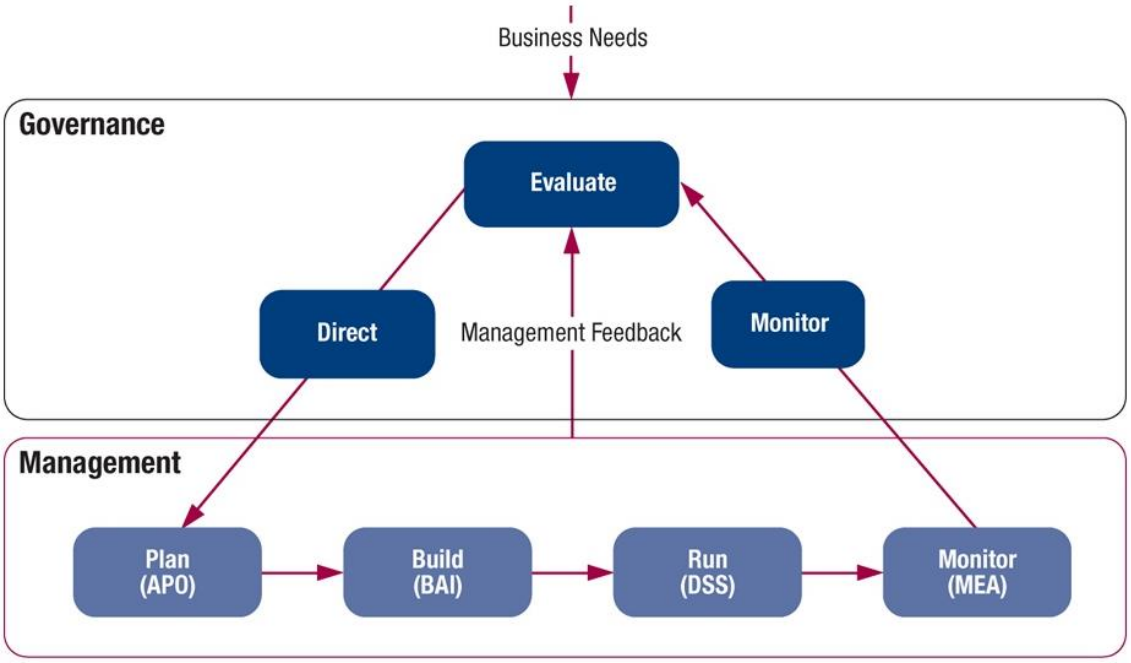
- Lidé, znalosti a kompetence (People, skills and competencies)
  Popisuje, jaké schopnosti a znalosti jsou u lidí potřeba, aby mohli splnit zadané cíle.



Obr. 4 Body celistvého přístupu (Vitouš, 2013)

Oddělení vedení společnosti od každodenního řízení

Přesto, že pracovníci mají své úkoly přiděleny svým nadřízeným, tak všechny úkoly musí směřovat ke společnému cíli, stanoveným vedením organizace. COBIT 5 rozlišuje mezi vedením (Governance) a řízením (Management) organizace, kdy vedení stanoví konečný cíl a řízení má za úkol tohoto cíle dosáhnout každodenní činností. Toto rozlišení je zobrazeno na obrázku (Obr. 5). (Vitouš, 2013)



Obr. 5 Vedení a řízení (Vitouš, 2013)

Zhodnocení využití

Z výše uvedeného popisu metodiky COBIT je patrné, že je využívána primárně pro větší organizace s vícevrstvým vedením a je určena zejména pro nejvyšší manažery a auditory. Z toho vyplývá výhoda této metodiky, kterou je právě její široký záběr v rámci v celé organizace, nejen IT či oblasti auditu. Metodika se zabývá otázkou, co je potřeba udělat, ale již neřeší, jakým způsobem. COBIT lze považovat za nástroj pro audit informatiky a strategického řízení. Nevýhodou metodiky COBIT je, že přesně nedefinuje, jak designovat a implementovat procesy, aktivity, role a funkce, které vedou k zajištění a splnění principu řízení.

V malých a středních podnicích by bylo potřeba metodiku COBIT značně přizpůsobit, jelikož je zde méně pracovníků, jednodušší struktura, sdílené role a méně prostředků. Management zde představuje hlavně majitel organizace a několik administrativních pracovníků. Využití této rozsáhlé a komplexní metodiky ve středním podniku se strojírenskou výrobou by mohlo být dojít ke špatnému uchopení metodiky a audit by mohl poskytnout zkreslené výsledky. Tudíž si nemyslím, že by bylo vhodné v tomto případě použít COBIT jako samostatný rámec.

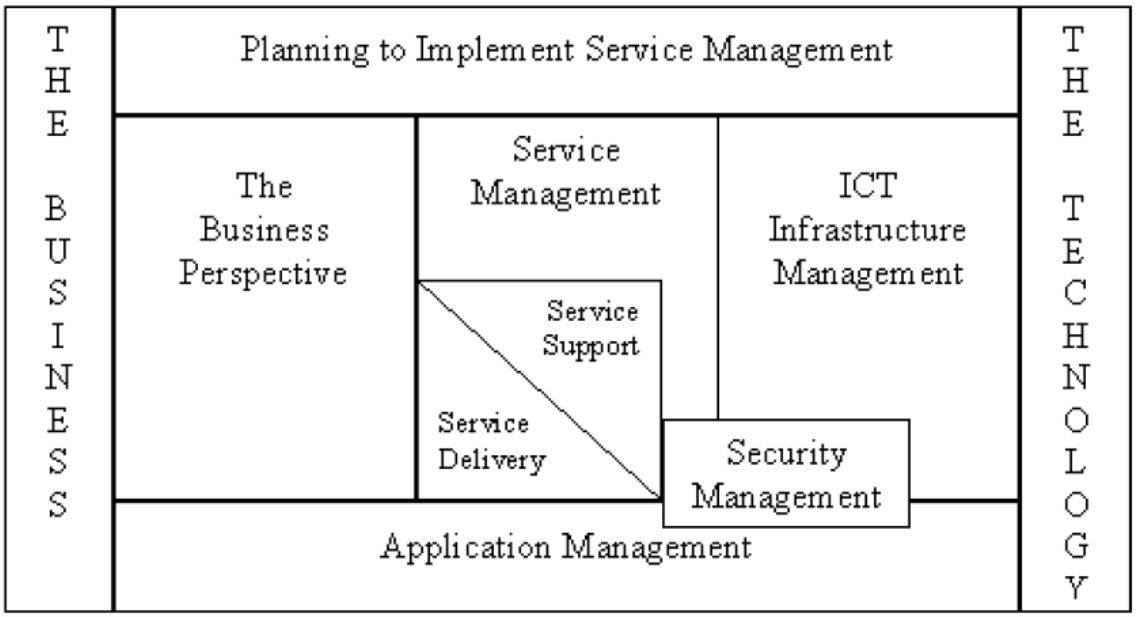
3.2 ITIL

Metodika ITIL (Information Technology Infrastructure Library) je mezinárodně rozšířenou a uznávanou knihovnou doporučení pro řízení a správu IT služeb. Jde tedy o tzv. „Best practice“ v rámci řízení integrovaných a procesně orientovaných IT služeb.

ITIL byl publikován během 80. let ve 20. století britskou vládní agenturou OGC (Office of Goverment Commerce), dříve CCTA (Central Communications and Telecommunications Agency), kdy britská agentura přišla s koncepcí pro řízení a správu provozu IT, kterou později pojmenovala ITIL. Cílem tehdy bylo v hlavních britských úřadech zlepšit IT služby.

Později k tomuto základu přidávaly nové knihy s poznatky a zkušenostmi další organizace a takto vznikla metodika ITIL, jak ji známe dnes. Právě díky zapojení ostatních organizací nemá nyní metodika ITIL soukromou podstatu, ale odpovídá spíše normám podobným ISO. Základ metodiky ITIL tvoří těchto sedm knih, které jsou zobrazeny na obrázku (Obr. 6):

- Podpora služeb (Service Support).
- Dodávka Služeb (Service Delivery).
- Obchodní dohled (The Business Perspective).
- Správa aplikace (Application Management).
- Řízení komunikační infrastruktury (ICT Infrastructure Management).
- Plánování zavedení řízení služeb (Planning to Implement Service Management).
- Řízení bezpečnosti (Security Management).



Obr. 6 Knihy ITIL (Svatá, 2016)

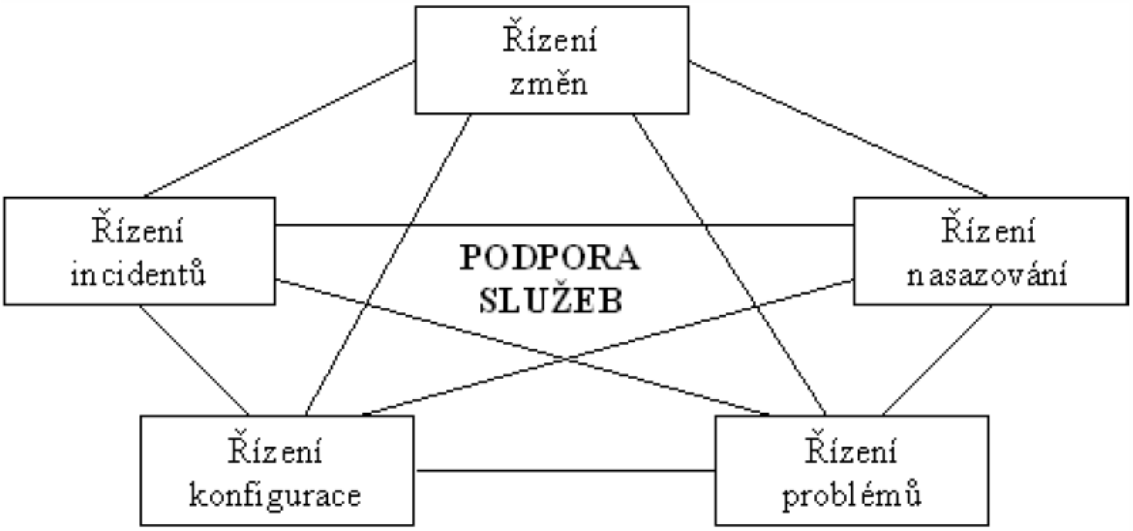
Nejčastěji používané jsou však tyto čtyři:

- Podpora služeb (Service Support).
- Dodávka Služeb (Service Delivery).
- Řízení komunikační infrastruktury (ICT Infrastructure Management).

- Plánování zavedení řízení služeb (Planning to Implement Service Management).

Podpora služeb

Tato kniha se věnuje každodenním provozním aktivitám, které mají na starosti pracovníci IT oddělení. Jedná se o podporu funkcí IT pro uživatele, kde tuto podporu zajišťuje převážně Service Desk jakožto centrum pro kontakt se zákazníky. Kniha obsahuje pět procesů, které jsou znázorněny na obrázku níže (Obr. 7).

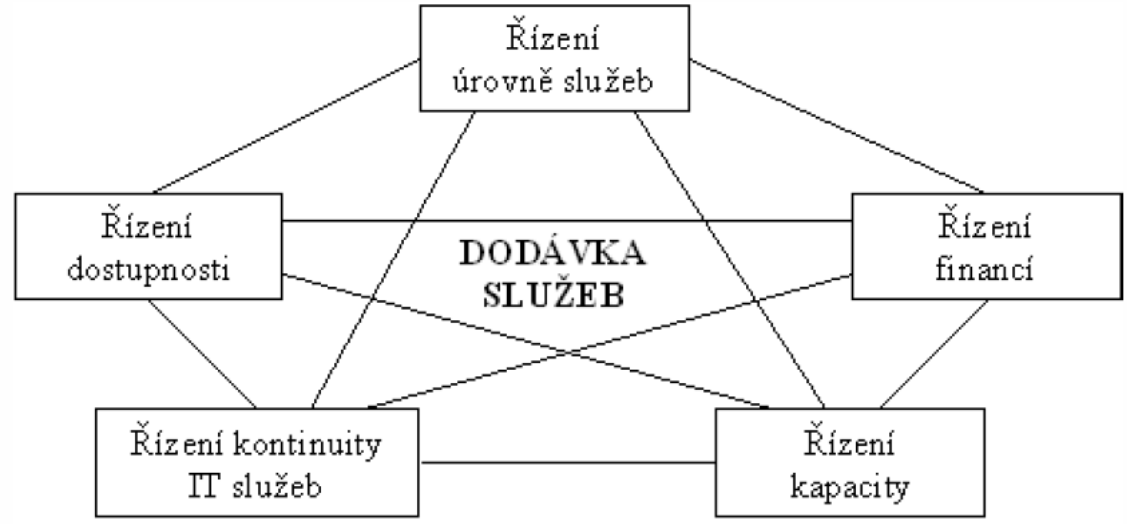


Obr. 7 Podpora služeb – procesy (Svatá, 2016)

- Řízení změn
  Každá změna je zpracovávána podle stanovených postupů a standardů. Cílem je snížit negativní dopad zamýšlených změn na kvalitu služeb.
- Řízení incidentů
  Incident je zpracováván nejrychlejším možným řešením bez ohledu na příčiny tzv. „quick and dirty“. Cílem je nejrychlejší možná obnova fungování služeb v původní kvalitě po incidentu.
- Řízení nasazování
  Jedná se o řízení zdrojů spolu s plánováním pro distribuci a nasazení nových služeb pro zákazníka. Cílem je zajistit dodržení technických i netechnických částí během nasazení.
- Řízení konfigurace
  Řízení služeb a infrastruktury pomocí konfiguračních složek.
- Řízení problémů
  Snaha najít původní příčinu problému a implementace opravy. Je zde také snaha dosáhnout v poskytování služeb maximální stability.

Dodávka služeb

Jedná se o knihu, která se zabývá procesy dodávky efektivních a kvalitních IT služeb. Obsahuje pět procesů, které jsou znázorněny na obrázku níže (Obr. 8).



Obr. 8 Dodávka služeb – procesy (Svatá, 2016)

- Řízení úrovně služeb
  Jedná se o stálé hlášení a monitorování kvality služeb za účelem udržování a zlepšování kvality IT služby.
- Řízení dostupnosti
  Zde je cílem rozšířit schopnosti IT infrastruktury, která má za úkol zajistit dodávku a dostupnost služeb tak, aby byly podporovány cíle organizace. Tato infrastruktura musí zajistit spolehlivost, udržovatelnost, provozuschopnost a bezpečnost.
- Řízení financí
  Převážně se jedná o účetnictví, rozpočet a platební systémy. Stanovují se zde vazby mezi IT a finančními zdroji.
- Řízení kontinuity IT služeb
  Cílem je poskytovat IT služby i přes přerušení jakoukoliv příčinou.
- Řízení kapacity
  Popis postupů od plánování, zavedení až po provoz procesů, které umožňují předpovídat potřebu jednotlivých zdrojů.

Řízení komunikační infrastruktury

V této knize jsou řešeny technologie ICT a zabývá se problémy týkající se:

- Řízení síťových služeb.
- Řízení provozu.

- Řízení lokálních procesorů.
- Řízení systémů.
- Instalace počítače.

Plánování zavedení řízení služeb

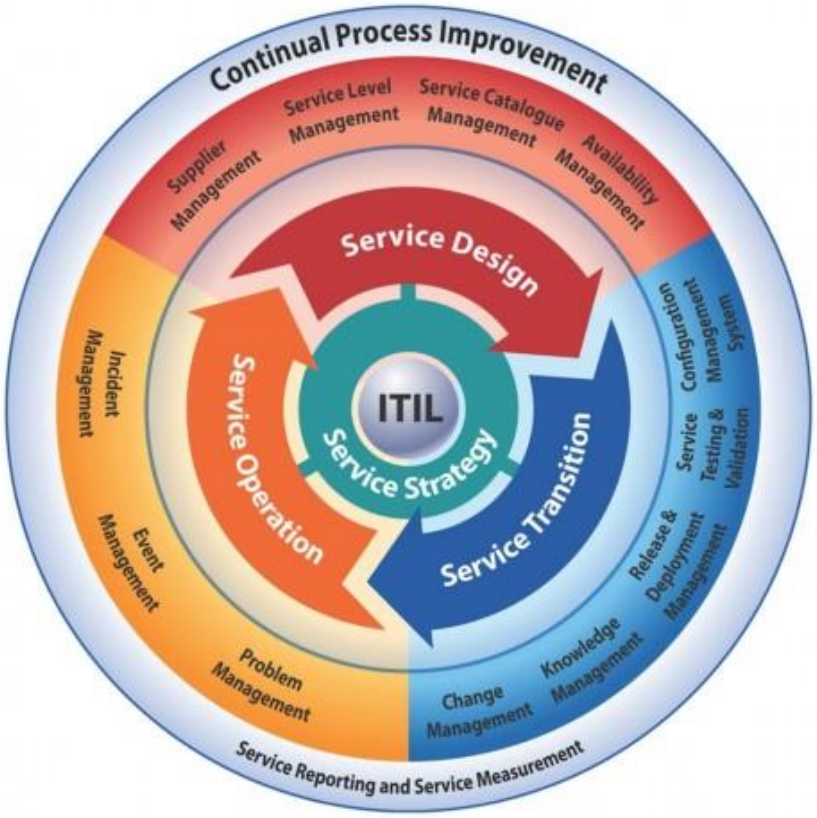
Tato kniha pojednává o problémech při implementaci řízení služeb. Obsahuje doporučené strategie pro implementaci, průběžné zlepšování a výhody procesů, které vyplývají z metodiky ITIL a klade důraz převážně na:

- Časové milníky.
- Kritické faktory úspěchu.
- Klíčové indikátory výkonosti.

ITIL V3

Následující verzí metodiky je ITIL V3, která vyšla v roce 2007. Využívá stejných základů „Best practice" jako původní verze. Změna oproti původní verzi je ta, že jádrem metodiky je nyní IT služba a její životní cyklus, tedy vývoj, implementace, změna a dodání. ITIL V3 je knihovna rozdělena těchto čtyř oblastí:

- První oblast
  Zaměřuje se převážně na „web-based products", jejíž účel je podporovat jádro metodiky. Obsahuje hlavně procesní mapy a definice ITIL jako např. případové studie, typy formulářů, osnovy agend či popis rolí.
- Druhá oblast
  Jedná se o jádro knihovny „set of core books", jenž obsahuje neměnné základy a „best practice". Jádro je tvořeno pěti knihami, jež sleduje model životní cyklu služby (Obr. 9):
    - Service Strategy.
    - Service Design.
    - Service Transition.
    - Service Operation.
    - Continual Service Improvement.
- Třetí a čtvrtá oblast
  Tyto části obsahují hlavně publikace, jež reflektují aktuální vývoj, jednotlivé potřeby odvětví a dílčí aspekty jako např.:
    - Brožury pro nejvyšší management.
    - Studijní pomůcky pro kvalifikační schéma.
    - Strategickou publikaci pro manažery.
    - Doplňující tituly jako „ITIL Practices in small IT units", které se věnují dílčím aspektům. (Svatá, 2016)



Obr. 9 ITIL V3 cyklus (ITIL V3)

Zhodnocení využití

Knihovna ITIL se na rozdíl od metodiky COBIT více zaměřuje na IT, služby poskytované prostřednictvím ICT a každodenní řízení infrastruktury. Obsahuje podrobnější popisy a definice nebo také ukázky šablon, diagramů a modelů. Je mířená především na IT management a řeší převážně otázku „Jak by se to mělo udělat?“. Výhoda knihovny ITIL spočívá v tom, že není nezbytně nutné doslovně uplatňovat všechny „Best practice“ k efektivnímu řízení IT služeb. Organizace si může zvolit, do jaké míry bude doporučení následovat a případně si vše upravit dle vlastních požadavků a potřeb. Možnou nevýhodou knihovny ITIL jsou náklady spojené s využitím mnoha knih „Best practice“ bez dostatečného posouzení přínosů, jelikož se jedná ve své podstatě o komplexní řešení.

Využít knihovnu ITIL je možné v malém, středním i velkém podniku. Nicméně malé a střední podniky nemají zdaleka dostatečné finanční prostředky pro zavedení většího rozsahu změn, které knihovna ITIL přináší. V menší a střední organizaci se zaměřením na strojírenskou výrobu rovněž v podstatě neexistuje nijak rozsáhlá struktura, z čehož následně vyvstává otázka skutečného přínosu ITIL pro podobné organizace. Knihovnu ITIL jsem rozhodl nepoužít, jelikož organizace se zaměřuje

na strojírenskou výrobu a nikoli na poskytování služeb, na které je z větší části ITIL využíván.

3.3 ISMS

Metodika ISMS (Information Security Management System) je založena na mezinárodně uznávané skupině standardů ISO/IEC 27000 pro zavádění, řízení a kontrolu informační bezpečnosti. Vytvořena byla mezinárodní organizací pro standardizaci ISO (International Organization for Standardization) v roce 2005.

ISMS zavádí řízení informační bezpečnosti pomocí modelu PDCA (Plan, Do, Check, Act), jehož obsahem jsou čtyři kroky pro postupné zavádění či zlepšování systému řízení bezpečnosti informací pro organizace jakékoliv velikosti.

Norma, kterou ISMS využívá pro návrh opatření je ISO/IEC 27002, která vznikla původně z normy ISO 17799 a obsahuje soubor doporučených opatření pro zajištění bezpečnosti informací. Tato opatření jsou rozdělena do 11 hlavních oblastí, které se následně dělí na 39 kategorií. Tyto kategorie dohromady obsahují 133 bezpečnostních opatření, jež se dále rozpadají na mnoho specifických bezpečnostních opatření. Hlavních 11 oblastí obsahuje následující:

- Bezpečnostní politika.
- Organizace bezpečnosti informací.
- Řízení aktiv.
- Bezpečnost lidských zdrojů.
- Fyzická bezpečnost a bezpečnost prostředí.
- Řízení komunikací a řízení provozu.
- Řízení přístupu.
- Akvizice, vývoj a údržba informačních systémů.
- Zvládání bezpečnostních incidentů.
- Řízení kontinuity činností organizace.
- Soulad s požadavky.

Vhodná opatření jsou zvolena na základě výstupu hodnocení rizik a jejich implementace na potřebách a požadavcích konkrétní organizace. Rozhodnutí, která opatření by měla být implementována je ponecháno na organizaci, jelikož norma zavedení těchto opatření nepřikazuje, ale pouze doporučuje.

Detailnější popis hlavních oblastí, příslušných kategorií a doporučených opatření normy ISO/IEC 27002 je k dispozici v části *Přílohy*.

Bezpečnostní politika

Bezpečnostní politika je základním dokumentem, jenž obsahuje soubor směrnic a pravidel, podle kterých je řízena informační bezpečnost v organizaci. Jednoznačně definuje požadavky, postupy a principy určující způsob správy, ochrany a distribuce informací či zdrojů v rámci celé organizace. Bezpečností politika se

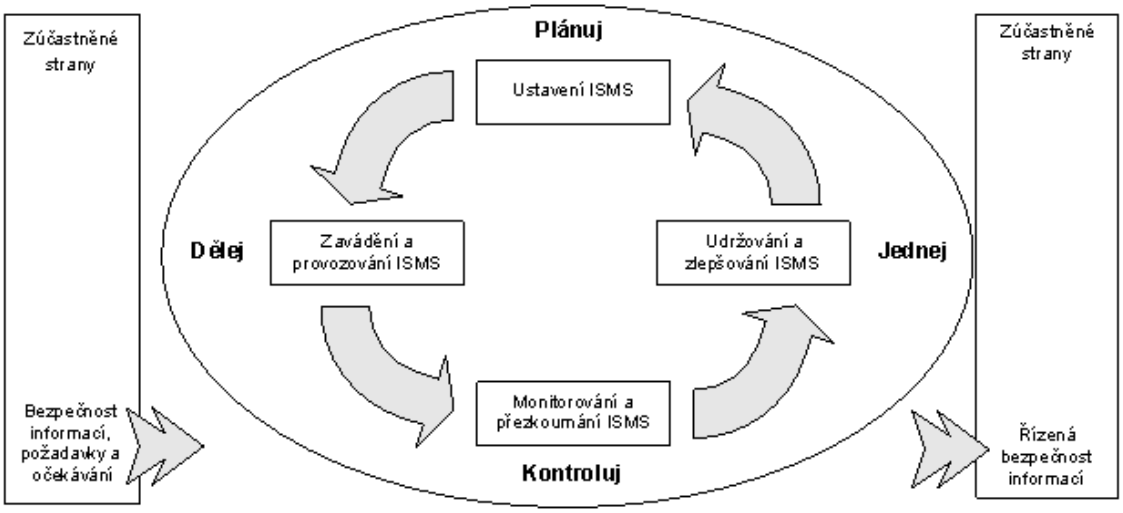
zakládá na porozumění procesům v organizaci a podpoře strategických cílů. Rovněž by měla vyjadřovat význam a cíle bezpečnosti informací, zájem managementu na řešení incidentů a přiřazovat pravomoci a odpovědnosti za jednotlivá aktiva. Uplatňuje se v rámci celého podniku a všemi externími subjekty. Bezpečnostní politiky můžeme rozdělit do čtyř kategorií:

- Promiskuitní

  Úkolem tohoto typu bezpečnostní politiky je zajistit alespoň minimální úroveň zabezpečení. Výhodou jsou zde velice nízké náklady na zavedení.
- Liberální
  Zajišťuje nízkou úroveň zabezpečení. Vhodné především pro malé organizace s minimálním rizikem nebezpečí a nízkou hodnotou uchovávaných informací. Provozní náklady jsou zde jen minimální.
- Racionální
  Bezpečnostní politika poskytuje vyšší úroveň zabezpečení. Zavádí klasifikaci aktiv, řízení přístupu k informacím a vyzývá k opatrnosti. Nevýhodou jsou již vyšší provozní náklady.
- Paranoidní
  Je zavedena velice striktní politika. Výhodou je vysoká úroveň zabezpečení, naopak nevýhodou je omezení přístupu a větší izolace.

Model PDCA

Právě norma ISO/IEC 27001 zavádí model PDCA (Plan-Do-Check-Act), česky plánuj-dělej-kontroluj-jednej, který je označován také jako Demingův cyklus. Tento model formuluje zásady pro vymezení systému řízení, jeho realizaci a neustálého zlepšování. Dříve se tento koncept využíval pro průmyslovou inovaci a implementaci systému řízení, ale dnes je již rozšířen o řízení informační bezpečnosti a je integrován také do mezinárodních standardů.



Obr. 10 Model PDCA (ČSN ISO/IEC 27001)

Tento model specifikuje požadavky pro postupné zlepšování kvality systému řízení informační bezpečnosti opakováním čtyř činností. Mezi tyto činnosti patří:

- Ustanovení.
- Zavedení a provoz.
- Monitorování a přezkoumávání.
- Udržování a zlepšování.

1. Ustanovení (Plánuj)

   V této etapě se definuje rozsah ISMS, tedy systémy a oddělení, které budou zahrnuty do systému řízení informační bezpečnosti. Výsledkem této definice je pak dokument bezpečnostní politiky, který se dále využívá v následujících etapách. Je tedy velice důležité promyslet všechny souvislosti dříve, než postoupíme do další etapy, jelikož zpětné úpravy politiky mohou být náročné. Důležitou součástí dokumentu je i identifikace a klasifikace aktiv, analýza rizik a následný návrh opatření pro nalezené hrozby. V posledním kroku je pak nutný souhlas vedení, které se tímto zavazuje k podpoře informační bezpečnosti v organizaci. Ustanovení ISMS lze tedy rozdělit do následujících skupin:

   - Definice rozsahu, hranice a vazeb ISMS.
   - Definice a odsouhlasení Prohlášení o politice ISMS.
   - Analýza a zvládání rizik.
   - Příprava Prohlášení o aplikovatelnosti.

2. Zavedení a provoz (Dělej)

   Druhá etapa řeší zavedení a provoz opatření, procesů a postupů, které byly stanoveny v předcházející části. Důležité je seznámit uživatele, správce, manažery a ostatní zainteresované osoby s bezpečnostní politikou a dané principy důkladně vysvětlit. Nejsnadnějším způsobem, jak tohoto dosáhnout, je prová-

dět v organizaci bezpečnostní školení, na kterém jsou ujasněny postupy měření účinnosti zavedených opatření a postup při bezpečnostních incidentech. Všechny tyto informace by také měly být dostupné v dokumentu o bezpečnosti informací a zvládání rizik. Během této etapy jsou prováděny tyto činnosti:

- Formulovat dokument Plán zvládání rizik a započít jeho zavádění.
- Zavést plánování bezpečnostních opatření dle ISO/IEC 27002.
- Definovat program budování bezpečnostního povědomí.
- Upřesnit způsoby měření účinnosti opatření.
- Zavést postupy pro bezpečnostní incidenty.
- Řídit zdroje, dokumenty a záznamy ISMS.

3. Monitorování a přezkoumávání (Kontroluj)

   Abychom mohli vyhodnotit, zda zavedení systému řízení informační bezpečnosti splnilo požadavky, je nutné provádět opakované kontroly. Tyto kontroly je možné provádět interně v rámci organizace či externími auditory. Vyhodnocení má ověřit, zda je zavedený ISMS implementován dle původních cílů a v souladu s potřebami organizace. Rovněž by měl obsahovat informace o oblastech, které je možné dále rozvíjet. Následně je vypracována zpráva hodnotící stav ISMS a přezkoumána vedením. Takováto přezkoumání by měla být prováděna na základě podnětů z interních a externích auditů alespoň jednou ročně. V rámci etapy je nutné provést následující úkony:

   - Monitorovat a ověřit účinnost prosazení bezpečnostních opatření.
   - Provést interní audit.
   - Připravit zprávu o stavu ISMS.

4. Udržování a zlepšování (Jednej)

   Poslední etapou je udržování a zlepšování ISMS, při které dochází ke sběru informací z výsledků auditů a kontrol implementovaných opatření pro možné zlepšení systému řízení informační bezpečnosti, které může dát podnět k začátku nového cyklu PDCA. V tomto novém cyklu budou opět naplánovány, implementovány, zkontrolovány a vyhodnoceny všechny možnosti zdokonalení ISMS. Během etapy bude provedeno:

   - Zavádění identifikovaných možností pro zdokonalení ISMS.
   - Provádění opatření k odstranění nedostatků. (Doucek, 2011)

Havarijní plán a plán obnovy

Havarijní plán a plán obnovy jsou tzv. DRP (Disaster Recovery Plans), které mají zajistit kontinuitu ICT v případě havárie. Jedná se o dokumenty vytvářené v rámci řízení kontinuity činností v organizaci (Business Continuity Management), jejichž cílem je zajistit co nejrychlejší obnovu provozu informačních systémů, aniž by došlo k negativnímu dopadu na plnění požadavků a potřeb organizace.

Vypracování havarijního plánu by mělo poskytovat odpovědi na otázky, jak zvládat technické selhání, výpadek dodávek elektrické energie, selhání technického či programového vybavení. Rovněž by se měly brát v úvahu přírodní katastrofy jako požár či povodeň. K dalším aspektům patří i selhání lidského faktoru, kde se jedná o úmyslné zavinění jako podvod či krádež nebo neúmyslná zavinění způsobená chybou uživatelů. Havarijní plán rovněž popisuje činnosti, které jsou potřeba provést v okamžiku zjištění havárie. Uvádí také, kdo ho spouští, kdo má co dělat a v jakém pořadí, dále pak účel a cílový stav plánu.

Plán obnovy zajišťuje nastavení RTO a RPO parametrů. RTO (Recovery Time Objective) reprezentuje maximální přípustnou dobu výpadku podnikového procesu a RPO (Recovery Point Objective) určuje v časových jednotkách maximální přístupnou dobu ztráty dat od poslední zálohy.

Oba parametry jsou definovány podle výstupu analýzy dopadů a analýzy rizik. Nejsou však na sobě závislé a mohou se lišit. Využívají se zde standardy BS 25999 (Code of Practice for Business Continuity Management a BS 25777 (Information and Communications Technology Continuity Management). (Doucek, 2011)

Zhodnocení využití

Z výše uvedeného popisu vyplývá, že ISMS neboli systém řízení bezpečnosti informací je metodikou a zároveň standardem pro úspěšné zvládnutí zavedení, kontroly a neustálého zlepšování informační bezpečnosti. Existuje celá řada nástrojů, které tuto metodiku podporují. Jedním z nich je online ISM-Benchmark od společnosti IPA, jenž je možné využít pro zjištění silných a slabých stránek zabezpečení v organizaci.

ISMS poskytuje přímější definice navrhovaných opatření oproti knihovně ITIL, která využívá více tzv. „Best practices“ využívaných v různých organizacích. Na rozdíl od metodiky COBIT a knihovny ITIL, které umožňují certifikovat pouze konkrétní osoby, ISMS umožnuje certifikaci v rámci celé organizace. Tato certifikace se provádí pomocí standardu ISO/IEC 27001, čemuž předchází samotné zavedení systému řízení bezpečnosti informací na základě doporučených opatření dle standardu ISO/IEC 27002. Metodiku ISMS je možné využít jak v malých, středních, tak i velkých organizacích s nejrůznějším zaměřením, jelikož se nezaměřuje na žádné konkrétní oblasti, ale věnuje se bezpečnosti celkově.

Výhodou metodiky ISMS je, že samotná implementace doporučených opatření je pouze volitelná a je možné implementovat pouze určitou část. Rovněž jako opatření, tak i certifikace organizace je volitelná a záleží tedy na potřebách společnosti. Nicméně certifikace by měla pozitivní vliv na vnímání společnosti ze strany potencionálních zákazníků. Možnou nevýhodou by bylo, že pokud by organizace zavedla jen minimum opatření, mohlo by to mít negativní vliv pro následnou certifikaci. Rovněž implementace mnoha opatření najednou by mohlo být finančně náročné pro menší podniky.

Na základě zhodnocení jednotlivých metodik se domnívám, že ISMS je vhodnou metodikou pro využití v této práci, jelikož má podporu celé řady nástrojů, nevynucuje zavedení všech opatření a nespecifikuje se jen na určité oblasti.

3.4 Souhrn metodik

Stále více organizací začíná integrovat informační technologie a systémy do svých procesů za účelem zvýšení kvality a spolehlivosti řízení. To však s sebou přináší i možná úskalí jako např. zvyšující se úroveň nákladů na IT či povinnost splňovat standardy a příslušnou legislativu. Za účelem této integrace je k dispozici množství postupů, které jsou sjednoceny do sbírek neboli metodik, které umožnují její úspěšné zvládnutí. Faktory, které mohou přispívat k důležitosti zavedení a kontrole informační bezpečnosti, jsou např.:

- Požadavky zákazníků.
- Povinnost splňovat zákonné požadavky.
- Snížení rizik.
- Optimalizace nákladů.

Infomační bezpečnost v organizacích lze také zavádět či kontrolovat podle mnoha standardů či metodik. Z uvedených příkladů a jejich popisů, které jsou zmíněny výše, je zřejmé, že každá metodika obsahuje svůj specifický pohled na problematiku a poskytuje vlastní postupy řešení. Z tohoto vyplývají jejich různá zaměření, výhody a nevýhody použití v organizacích s nejrůznější specializací.

COBIT je metodikou, jejíž cílovou skupinou jsou jednotlivci, kteří již chápou problematiku řízení bezpečnosti IT v podnikových procesech. Jedná se především o IT manažery, auditory a vlastníky procesů. Využívána je především ve velkých organizacích, neboť je většinou považována za zbytečně robustní a byrokratickou pro malé a střední podniky.

ITIL je knihovnou převážně určenou pro organizace se středním a vyšším managementem. Využita může být jak u malých, středních, tak i velkých organizací. Můžeme říci, že pro menší podnik představuje ITIL menší výhody s menšími náklady oproti větší organizaci, kde jsou výhody a náklady vyšší. Hlavní přínos knihovny ITIL spočívá v oblasti správy a řízení služeb.

ISMS neboli Systém řízení bezpečnosti informací obsahuje doporučený postup pro zavedení, rozvoj a zlepšování řízení bezpečnosti informací pomocí modelu PDCA. ISMS rovněž umožňuje certifikaci, která se provádí dle normy ISO/IEC 27001 a lze ji využít v malých, střeních i velkých organizacích. Pro návrh bezpečnostních opatření využívá standard ISO/IEC 27002.

Nelze však označit jeden konkrétní standard či metodiku a prohlásit, že je nejlepší. Nicméně můžeme říci, že v některých případech je využití určitého standardu vhodnější pro danou oblast než použití jiného a naopak. Je zcela běžné, že organizace působící ve stejném sektoru, využívají odlišné standardy pro řízení bezpečnosti informací.

4 Bezpečnostní audit

V této kapitole se budeme věnovat samotnému postupu při bezpečnostním auditu podniku.

4.1 Popis podniku

Firma, na které bude prováděn bezpečnostní audit, se řadí mezi malé až středně velké podniky. Zabývá se strojírenskou výrobou turbínových lopatek do vodních elektráren a podobných zařízení. Jedná se o podnik, kde většinu zaměstnanců tvoří dělníci. Dále pak zaměstnává několik programátorů a konstruktérů starajících se o nákresy a programování CNC strojů. V neposlední řadě také několik členů vedení podniku, jako jsou pracovníci personalistiky, účetnictví a obchodu.

Podnik nemá vlastní IT oddělení, které by obstarávalo údržbu a správu sítě, ale zaměstnává externí firmu, která se stará o zabezpečení a správu celé podnikové sítě.

4.2 Oddělení

Ve firmě se momentálně nachází 39 zaměstnanců rozdělených do několika oddělení.

1. Vedení

   Mezi vedení podniku patří jeho majitel, personalista, ekonom a účetní. V tomto oddělení se rozhoduje o budoucím vývoji, vyřizují se nové objednávky a platy zaměstnanců. Rovněž se zařizují smlouvy s dodavateli materiálu a ostatních služeb třetích stran. V kancelářích se na většinu práce využívá Microsoft Office.

2. Konstruktéři

   Na základě specifikací dodaných od zákazníka vytvoří nákres v programu AutoCad.

3. Programátoři

   Vytvářejí modely výrobku pro obrábění v programech SolidWorks a SolidCam podle výkresů poskytovaných konstruktéry. Poté model nahrají do konzole obráběcího stroje CNC a odladí hodnoty.

4. Výroba

   Oddělení tvoří většinu zaměstnanců podniku. Výroba je rozdělena do třísměnného provozu, kde každá směna má svého vedoucího a technika provozu. Vedoucí kontroluje dodržování postupů a stanovených kvót pro výrobu. Technik provádí kontrolu, údržbu a základní opravy obráběcích strojů.

4.3 Rozsah a cíl auditu

Pro stanovení rozsahu a cíle auditu byla potřeba konzultace s vedením a správcem IT podniku, při níž bylo domluveno, že bude udělen přístup k interní síti a bude k dispozici dostupná dokumentace. V rámci auditu bude provedena kontrola okolí podniku, fyzické bezpečnosti a analýza rizik.

Cílem bezpečnostního auditu je zjistit aktuální stav informační bezpečnosti podniku a porovnat míru shody s akceptovatelnou praxí. Následně zdokumentovat nalezené rozdíly, upozornit na potencionální rizika a navrhnout opatření, která odstraní nebo minimalizují rizika kritických části.

4.4 Okolí podniku a fyzická bezpečnost

Firma se nachází ve starší industriální budově rozdělené do několika částí. Samotné umístění budovy se nachází mimo jakékoliv vodní toky, riziko zaplavení je tedy velice nízké. Rovněž není pravděpodobné poškození kvůli zemětřesení, jelikož oblast je seismologicky klidná. Hlavním přístupem do prostoru budovy jsou zamřížované dveře, které využívají zaměstnanci, a brána pro vozidla přepravující materiál a výrobky. Vstupní dveře i brána jdou otevřít pouze zevnitř a tedy do prostoru se nedostanou neautorizované osoby.

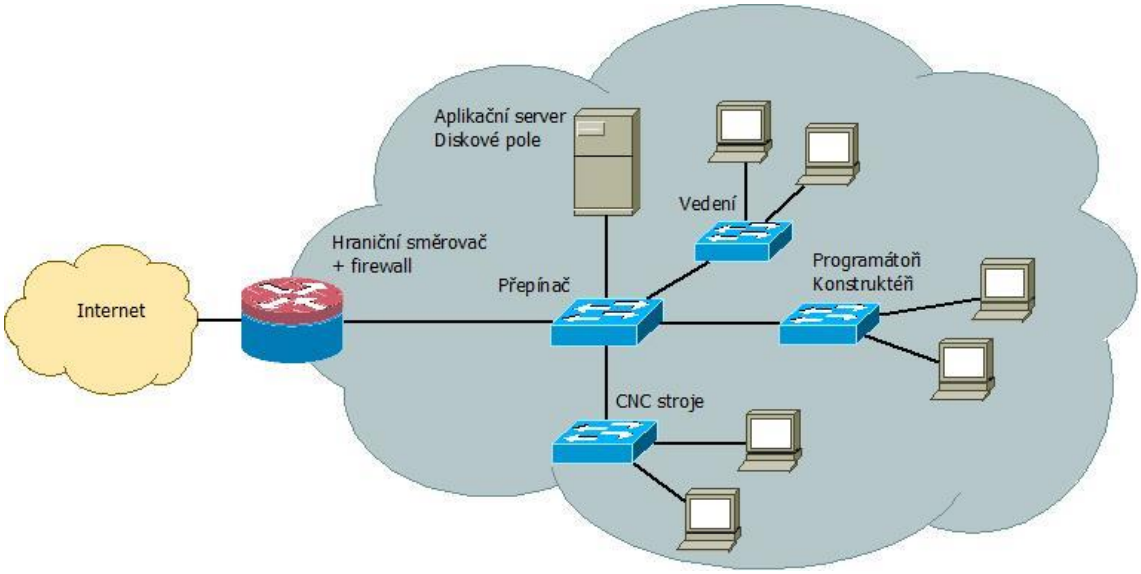
Po vstupu do prostor budovy se nachází nádvoří, kde je uskladněna většina materiálu pro zpracování a výrobu. Dále z nádvoří je pak vstup do různých oddělení podniku.

Zabezpečení přístupu do kanceláří a dalších oddělení je tvořeno pouze dveřmi s mechanickým zámkem. Přístupové klíče k zámku kanceláře vlastní pouze zaměstnanci vedení, kteří zde pracují. Přístupové body k jednotlivým oddělením se nezamykají z důvodu přepravy materiálů a výrobků mezi nimi. V případě potřeby jsou klíče umístěny u vedoucích pracovníků. Firma má zavedený třísměnný provoz, není teda potřeba najímat bezpečnostní pracovníky na hlídání přístupu do budovy.

4.5 Aktuální stav

Před započetím samotného auditu je potřeba znát, v jakém stavu se informační bezpečnost aktuálně nachází. Organizace neprovozuje vlastní IT oddělení. Správa IT a sítové infrastruktury je tedy obstarávána externí firmou. Veškeré dotazy týkající se aktuálního stavu ICT byly tedy směřovány na pověřenou osobu.

Infrastrukturu tvoří poměrně jednoduchá síť, která neosahuje redundanci ani loadbalancing. Je tvořena jen několika přepínači spojující síť do jednoho celku a hraničním směrovačem, který slouží pro propojení s externím prostředím a zároveň poskytuje firewallovou ochranu. Interní síť používá adresy z rozsahu 192.168.0.0/24, kde nejsou vytvořeny ani podsítě pro jednotlivá oddělení. Schéma sítové infrastruktury je k dipozici na obrázku níže (Obr. 11).



Obr. 11 Síťová infrastruktura

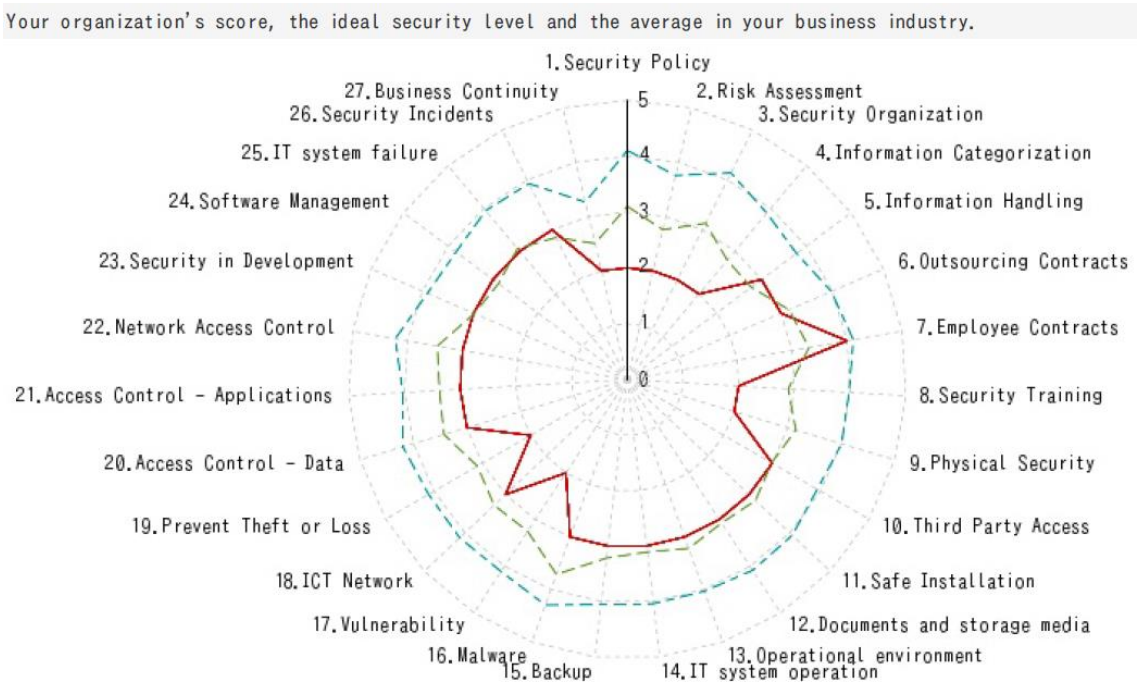
Organizace nemá vytvořenou bezpečnostní politiku či analýzu rizik. Informační bezpečnost je řešena jen v rámci nutného minima, např. se zde ani nemění cyklicky hesla uživatelů. Na zařízeních je povoleno připojování vlastních médií a instalace programového vybavení. Vedení podniku má jen pasivní postoj k řízení informační bezpečnosti, přičemž nemá povědomí o možných hrozbách a iniciativu přenechává externí firmě.

Úvodní průzkum

Pro zjištění aktuálního stavu informační bezpečnosti v podniku je potřeba nejdříve provést úvodní průzkum. K tomu je možné využít bezplatný online nástroj „*Information Security Management Benchmark*“ od agentury IPA.

Jedná se o sérii šestačtyřiceti otázek rozdělených do dvou hlavních částí. První část obsahuje sedmadvacet otázek, které jsou zaměřeny na informační bezpečnost a opatření. Druhá část a zbylých devatenáct se týká profilu samotné společnosti. Na každou z těchto otázek je možno odpovědět jednou z pěti možností, které jsou bodově ohodnoceny od jedné do pěti, kde jedna znamená nejhorší výsledek a pět nejlepší.

Dle poskytnutých odpovědí je následně vytvořen graf, který reprezentuje zvolené možnosti v grafické podobě. V tomto grafu je na první pohled viditelné, které oblasti informační bezpečnosti poskytují dostatečnou ochranu nebo naopak představují největší slabiny. Na základě těchto znalostí následně získáme potřebné informace o aktuálním stavu a představu, na které části se bude potřeba více zaměřit.



Obr. 12 Aktuální stav

Na výše uvedeném grafu (Obr. 12) jsou znázorněny jednotlivé body s jejich ohodnocením. Červená linie znázorňuje výsledek testované organizace. Následuje zelená, která reprezentuje průměrnou hodnotu, a jako poslední modrá linie označující ideální stav. Z grafu lze vyčíst, že organizace má nastavenou informační bezpečnost vcelku podprůměrně. Existuje tedy mnoho prostoru pro rozšíření stávajících a zavedení nových bezpečnostních opatření tak, aby se dosáhlo uspokojivého výsledku s ohledem na zaměření a velikost organizace.

Dle odpovědí na otázky týkající se profilu společnosti v druhé části je výsledek zařazen do statistik a máme tedy možnost zjistit, jak si společnost vede v porovnání s ostatními. Na obrázku níže (Obr. 13) je zobrazen počet bodů, které organizace získala, body potřebné k dosažení průměrného a ideálního ohodnocení. Rovněž je zde vidět i počet podniků podobného typu, které byly do statistik zařazeny pro srovnání, jež celkově činí 1416 organizací. Toto hodnocení odpovídá barevným liniím pro ideální, průměrný a aktuální stav z výše uvedeného grafu (Obr. 12).

Obr. 13 Ohodnocení bezpečnosti

Nalezené nedostatky

Zde si uvedeme nalezené nedostatky, které odhalil úvodní průzkum pomocí ISM Benchmark (Obr. 12):

- Security Policy (Bezpečnostní politika)
  - Není vypracován oficiální dokument Bezpečnostní politiky.
  - Jsou zavedena pouze obecná bezpečnostní pravidla a principy.
  - Chybí zde potřebná ICT dokumentace.
  - Nejsou vypracovány Havarijní plány a Plán obnovy.
  - Doposud nebyl proveden audit ICT.
  - Nepravidelné kontroly pravidel a postupů.
- Risk Assessment (Ohodnoceni rizik)
  - Chybí ohodnocení aktiv a analýza rizik.
  - Nejsou naplánovány pravidelné kontroly platnosti ohodnocení rizik.

- Security Organization (Bezpečnost organizace)
    - ICT je řešeno pouze svépomocí externím správcem, který bezpečnost IS řeší pouze na základě vlastního uvážení.
    - Pasivní postoj vedení k bezpečnosti IT.
    - Nejsou definovány plány pro kontrolu a rozvoj ICT.
    - Není zavedena cyklická změna hesel.
- Information Categorization (Kategorizace informací)
    - Informace nejsou kategorizovány podle důležitosti.
    - Externí osoba spravující ICT má přístup ke všem informacím.
    - Není zavedena politika pro klasifikaci a manipulaci informací.
- Information Handling (Manipulace s informacemi)
    - Nejsou stanoveny postupy pro správu a uchovávání informací.
    - Uživatelé mohou libovolně upravovat data, bez možnosti zpětného dohledání odpovědnosti.
    - Nejsou stanoveny role a pravidla pro přístup k informacím a jejich manipulaci.
- Security Training (Bezpečnostní trénink)
    - Zaměstnanci nejsou dostatečně školeni, co se týče informační bezpečnosti a manipulace s informacemi.
    - Není zavedeno pravidelné přeškolování.
    - Materiály využívané pro školení jsou pouze obecnými předlohami.
- Physical Security (Fyzická bezpečnost)
    - Přístupy jsou řešeny pouze mechanickými zámky.
    - Neautorizované osoby mohou volně vstoupit do prostor organizace.
    - Nejsou zavedeny identifikační karty, které by umožnovaly kontrolu osob.
    - Nejsou zde zaznamenávány přístupy návštěvníků.
    - Chybí vymezený prostor, kde se mohou návštěvy pohybovat.
- Third Party Access (Přístup třetích stran)
    - Není zavedená dokumentace definující postupy pro přístup třetích stran do kanceláří, místností a jiných prostor organizace.
    - Návštěvníci a uklízečky se mohou dostat k podnikovým zařízením.
    - Návštěvy mohou spatřit citlivé informace v kancelářích, jelikož neexistuje separátní místnost pro jejich přijetí.
    - Přístup třetích stran do sítě není zrušen okamžitě po ukončení smluvního vztahu.
- Safe Installation (Bezpečnost instalací)
    - Důležitá zařízení jako server, diskové pole a router jsou umístěny v prostoru kanceláře.
    - Organizace nemá definována pravidla v případě odchodu od počítače.
    - Není vynucováno zamykání obrazovek.
    - Je možné se dostat ke kabelům síťových zařízení.

- Documents and Storage media (Dokumenty a datová úložiště)
    - Nejsou stanovena pravidla pro využívání vlastních zařízení.
    - Uživatelé mohou volně zapojovat vlastní zařízení (DVD, USB, nootebook apod).
    - Nejsou stanoveny postupy a metody pro nahrazování starých zařízení (odstraňování citlivých informací, ničení dokumentů apod.).
    - Není zavedena politika čistého stolu, čímž může dojít k úniku informací.
- Operational enviroment
    - Není oddělena kancelářská síť od výrobní.
    - Nejsou definovány postupy a dokumentace pro provoz systémů.
- System operation (Operační systém)
    - Nejsou zavedeny pravidelné audity IS.
    - Nejsou definovány požadavky na informační systémy.
    - Není zavedena dokumentace a postupy pro správu IS (update, zálohování).
    - Nejsou v pravidelných intervalech přezkoumávány logy událostí.
- Backup (Zálohy)
    - Existuje pouze jedno diskové pole uchovávající data.
    - Nejsou definována pravidla pro správu záloh (kontroly, mazání starých dat apod.).
- Malware
    - Nepravidelné aktualizace programového vybavení.
    - Nejsou zavedeny pravidelné kontroly serveru a klientů.
    - Nejsou kontrolována osobní zařízení před připojením do podnikové sítě.
- Vulnerability (Zranitelnost)
    - Neexistuje seznam zranitelností a hrozeb.
    - Nejsou naplánovány pravidelné kontroly a aktualizace.
    - Uživatelé si mohou instalovat vlastní programy.
- ICT Network (Síťová infrastruktura)
    - Sít není segmentována.
    - Neexistují redundantní spoje.
    - Nepravidelné aktualizace firmwaru zařízení.
- Prevent Theft or Loss (Prevence krádeže nebo ztráty)
    - Nejsou definovány postupy zacházení se zařízeními mimo prostory organizace.
    - Data v zařízeních použitých mimo organizaci nejsou kryptograficky chráněna.
- Access Control – Data (Kontrola přístupu k datům)
    - Uživatelské účty nejsou smazány ihned v okamžiku, kdy již nejsou potřeba.
    - Není stanovena doba platnosti hesla uživatelů.
    - Není vynucována dostatečná síla hesel.

- Access Control – Applications (Kontrola přístupu k aplikacím)
    - Nejsou v pravidelných intervalech přezkoumávána přístupová práva uživatelů.
    - Není plně definována politika přístupových práv.
- Network Access Control (Kontrola přístupu k síti)
    - Podniková síť není segmentována, je tak možné odposlouchávat veškerou komunikaci.
    - K portům serveru, diskového pole a routeru je možný přístup neautorizovaným osobám.
- Software Management (Správa aplikací)
    - Nejsou definovány postupy pro instalace či změny programového vybavení a systémů.
    - Před implementací nových systémů a softwaru nejsou definované postupy pro kontrolu stability.
- Systém Failure (Selhání systému)
    - Nejsou definovány požadavky na dostupnost IS.
    - Výpadkem síťového zařízení může dojít k nedostupnosti síťových služeb kvůli neexistujícímu redundantnímu spojení či záložních zařízení.
    - Nejsou zavedené postupy a pravidla v případě výpadku IS.
- Security Incidents (Bezpečnostní incidenty)
    - Nejsou definovány postupy pro případ bezpečnostního incidentu.
    - V případě živelné katastrofy (požár, povodeň, zemětřesení) nejsou připravena záložní zařízení pro rychlou obnovu.
- Business Continuity (Podniková kontinuita)
    - Chybí analýza dopadu v případě výpadku systému.
    - Nejsou vytvořeny plány kontinuity.
    - Nejsou připraveny plány pro případ delšího výpadku (záložní prostory a zařízení pro základní činnost podniku).

4.6 Identifikace a klasifikace aktiv

Prvním krokem bezpečnostního auditu je identifikovat důležitá aktiva, která jsou nezbytná pro činnost podniku. U těchto aktiv rozlišujeme jejich důvěrnost, integritu a dostupnost. Podle těchto atributů klasifikujeme aktivum v závislosti na tom, jaký dopad má jejich porušení. Pro výpočet hodnoty aktiva je potřeba si tento dopad ohodnotit. V tabulce (Tab. 1) si ukážeme příklad, jak může vypadat ohodnocení dopadu pro jednotlivé atributy.

Jako nejdůležitější aktivum je možné označit CNC a ostatní stroje, které slouží pro samotnou výrobu produktů, jenž představuje hlavní činnost v organizaci. Nicméně audit je věnován bezpečnosti IT, takže tyto stroje nebudou uvedeny v seznamku aktiv.

Tab. 1 Dopad ztráty důvěrnosti, integrity a dostupnosti

Hod.	Dopad	Důvěrnost (C)	Integrita (I)	Dostupnost (A)
1	Nízký	Porušení důvěrnosti aktiva nepředstavuje žádnou nebo minimální škodu. Přístup k aktivu veřejný.	Modifikace způsobí jen minimální nebo žádný dopad na fungování organizace.	Přerušení dostupnosti má minimální nebo žádný dopad na činnost organizace.
2	Střední	Únik informací k neoprávněným osobám může mít výrazný dopad. Přístup je umožněn jen vybraným osobám.	Úprava aktiva zde představuje výrazný dopad na organizaci a její činnost. Škoda se pohybuje v řádech desítek tisíc Kč.	Nedostupnost po delší časový úsek představuje problémy v činnosti. Může způsobit finanční sankce ze strany zákazníka.
4	Vysoký	Ztráta důvěrnosti může závažným způsobem poškodit organizaci. Jen speciálně přeškolené osoby mají přístup k aktivu.	Porušení integrity aktiva znamená pro podnik závažné problémy. Škody se mohou dostat až do stovek tisíc Kč.	Nedostupnost aktiva je závažný problém a finanční ztráty, sankce ze strany zákazníka nebo pozastavení činnosti.

V další kroku si určíme kritický čas obnovy, tedy RTO (recovery time objective). Jedná se o parametr, který stanovuje maximální dobu, po které musí být aktivum dostupné v případě jeho výpadku. I zde si určíme hodnotu pro jednotlivé časové úseky.

Tab. 2 Hodnota RTO

Hodnota	RTO
1	24 hodin
2	72 hodin
4	1 týden

Nyní známe všechny potřebné hodnoty, které potřebujeme pro klasifikaci aktiva. Tu provedeme pomocí vzorce:

$$K = \frac{C \cdot I \cdot A}{RTO} \tag{1}$$

Dosazením do vzorce dostaneme různé hodnoty. Abychom věděli, jestli je aktivum pro podnik normální, důležité nebo kritické, musíme si stanovit rozmezí hodnot. Toto rozmezí si definujeme v následující tabulce (Tab. 3).

Tab. 3 Kategorie aktiv

Hodnota K	Aktivum	Dopad
K < 4	Normální	Nedostupnost aktiva neznamená žádné větší problémy pro činnost podniku.
4 ≤ K < 12	Důležité	Nedostupností aktiva může dojít k závažnějším problémům v činnosti.
K ≥ 12	Kritické	Nedostupnost znamená velké problémy a možné finanční ztráty.

Po stanovení metody, jakou budeme aktiva klasifikovat, můžeme přistoupit k samotné identifikaci. Abychom zjistili, jaká aktiva jsou pro podnik relevantní a jaký by byl na ně dopad v rámci ztráty důvěrnosti, integrity a dostupnosti, byla potřeba konzultace s majitelem a správcem IT podniku, na kterém je prováděn bezpečnostní audit.

Touto konzultací jsme získali všechny potřebné informace a mohli začít s identifikací důležitých aktiv pro činnost podniku. Výsledkem identifikace jsou následující aktiva.

1. Osobní počítače

   Osobní počítače a notebooky jsou základními prostředky pro práci v organizaci. Pokud dojde k nenávratnému poškození, je do několika pracovních dní zařízena výměna.

2. Diskové pole a aplikační server

   Diskové pole slouží jako hlavní úložný prostor pro firemní data. Kompletní zálohy jsou zde ukládány jednou denně. Aplikační server slouží pro provoz služby elektronické pošty, účetního a docházkového systému. Zařízení jsou umístěna v prostoru kanceláří.

3. Síťová zařízení a kabeláž

   Jedná se o zařízení jako přepínače, směrovače, tiskárny, telefony, poplašné systémy a veškerá s nimi spojená kabeláž, která vytváří síťovou infrastrukturu organizace.

4. Podniková data

   Podniková data představují nehmotný majetek podniku. Může se jednat o citlivé údaje jako účetní výkazy, osobní informace, korespondence se zákazníky nebo i běžnou komunikaci v interní síti mezi jednotlivými odděleními.

5. Služba webové stránky

   Webová stránka podniku slouží k distribuci informací o organizaci a její činnosti. Obsahuje seznam produktů, reference a kontakt v případě zájmu o spolupráci.

6. Konstruktérské programy

   AutoCad, SolidWorks a SolidCam patří mezi hlavní programové vybavení nutné pro činnost podniku. Konstruktéři a programátoři je využívají k vytvoření výkresů a modelů pro CNC stroje.

7. Dokumentace podniku

   Dokumenty velmi důležité pro úspěšnost podniku můžeme rozdělit na následující typy:

   - Základní dokumenty (pracovní a organizační řád).
   - Systémové dokumenty (příručka kvality, normy a směrnice, odpovědnosti a pravomoci).
   - Operativní (sdělení vedení, zápisy z porad).
   - Pracovní (návody, pravidla a instrukce).
   - Korespondence (externí dokumentace pro komunikaci se zákazníky, dodavateli a státními orgány).

8. Externí dodavatelé

Aktivum reprezentuje všechny smluvní třetí strany spolupracující s podnikem na dodávkách materiálu nebo služeb. Tyto služby mohou poskytovat internetové připojení, dodávky elektrické energie, konzultace či správu informačních technologií.

V následující tabulce (Tab. 4) jsou zobrazena aktiva a jejich důvěrnost, integrita, dostupnost a kritický čas obnovy (RTO) s výslednou klasifikací, kterou reprezentuje hodnota (K).

Tab. 4 Klasifikace aktiv

Aktiva	Dův.	Int.	Dos.	RTO	Klasifikace
Osobní počítače	2	2	2	1	Důležité
Diskové pole a aplikační server	4	2	4	1	Kritické
Síťová zařízení a kabeláž	4	2	4	1	Kritické
Služba webové stránky	1	2	2	2	Normální
Podniková data	4	4	2	1	Kritické
Konstruktérské programy	4	2	4	1	Kritické
Dokumentace podniku	2	4	1	2	Důležité
Externí dodavatelé	2	4	4	1	Kritické

4.7 Analýza rizik a hrozeb

Analýza rizik představuje další krok po klasifikaci aktiv. V této kapitole si představíme potencionální hrozby, které mohou zasáhnout aktiva podniku. To nám umožní zjistit rizika, která by mohla ohrozit důvěrnost, integritu nebo dostupnost aktiv.

Dalším úkonem bude určit, jaký dopad na podnik tyto hrozby budou představovat. Různý dopad označíme jinou hodnotou, kterou využijeme při výpočtu míry rizika.

Tab. 5 Popis dopadu

Hodnota	Dopad (D)	Popis
1	Minimální	Žádný nebo zanedbatelný dopad na činnost podniku.
2	Střední	Hrozba může způsobit problémy v činnosti nebo finanční ztráty.
3	Kritický	Hrozí vážné problémy v činnosti nebo finanční ztráty, které by mohly působit jako likvidační.

Stejným způsobem si určíme hodnoty pro pravděpodobnost, s jakou různé hrozby mohou nastat.

Tab. 6 Hodnoty pravděpodobností

Hodnota	Pravděpodobnost (P)
1	Nepravděpodobné
2	Málo pravděpodobné
3	Pravděpodobné

Pro určení míry rizika R je potřeba si stanovit rozmezí hodnot, které dostaneme po dosazení hodnot P a D do následujícího vzorce:

$$R = P \cdot D \tag{2}$$

Tab. 7 Popis míry rizika

Hodnota	Míra rizika (R)	Popis
1,2	Zanedbatelná	Riziko není natolik velké, aby se jím podnik musel více zabývat.
3,4	Akceptovatelná	Míra rizika se nachází v takové míře, že dosavadní opatření jsou na hranici přijetí.
6,9	Kritická	Míra rizika je příliš vysoka a je potřeba zajistit odpovídající opatření.

4.7.1 Hrozby

Hrozby poškozující aktiva vycházejí z jejich zranitelností. Mohou způsobit ztrátu důvěrnosti, integrity nebo dostupnosti jednoho i několika aktiv.

Představíme si hrozby, které mohou v organizaci nastat, a zranitelnosti, kterých mohou využívat. Lze je rozdělit do několika základních skupin:

1. Přírodní

1.1. Vodní zdroje

Elektrické zařízení nesmí přijít do kontaktu se zdrojem vody. Výrobní prostor se z větší části nachází pod úrovní země a v blízkosti oken. V případě přívalového deště by mohlo nastat, že se voda dostane do elektrických panelů a zařízení poškodí nebo zničí.

1.2. Požár

Požár může zranit zaměstnance, poškodit budovu a zařízení. Může vzniknout úmyslným založením nebo nesprávným zacházením s elektrickými zařízeními. V prostorách organizace se nachází malá zařízení jako varná konvice, kávovar apod., která mohou způsobit vzplanutí okolních materiálů nedostatečnou izolací kabelů nebo nesprávným zapojením.

2. Technické

2.1. Selhání nebo přerušení dodávek elektrické energie

Stálá dostupnost dodávek elektrické energie je nutná pro správnou činnost podniku. Kolísání napětí v síti je člověkem nepostřehnutelné, ale může způsobit narušení činnosti elektrických zařízení. Proti tomuto kolísání je potřeba chránit hlavně servery a diskové pole podniku. Pokud by došlo k celkovému přerušení dodávek elektrické energie, může dojít ke ztrátě dat, která nejsou správně zálohovaná.

2.2. Selhání nebo přerušení síťové infrastruktury

Výpadek síťové infrastruktury se dotkne mnoha procesů pro správnou činnost organizace. Služby jako email či internet nebo podniková data, které využívají přístup k lokální nebo externí síti, se stanou nedostupnými. V podniku by to znamenalo pozastavení činnosti pro zaměstnance v kanceláři, jelikož není zavedena redundance spojení.

2.3. Selhání nebo závada zařízení a systému

Selhání výrobních zařízení nebo účetních či konstruktérských systémů může vést ke zpoždění zakázek v organizaci. Důvod závady nemusí být však pouze příčinou technického selhání. Často dochází ke špatnému nastavení nebo zacházením se zařízením vinou špatně informovaného zaměstnance.

2.4. Programové zranitelnosti a chyby

Tato hrozba se dá aplikovat na každé programové vybavení a riziko roste s komplexností aplikace. V organizaci se využívají kancelářské i specializované aplikace pro výkresy a modelování 3D objektů. Dále pak systémy pro účetnictví a docházku. V těchto aplikacích se mohou vyskytovat chyby a zranitelnosti, na které se potencionální útočníci mohou zaměřit.

3. Lidská chyba

3.1. Informace a produkty z nespolehlivých zdrojů

Informace, software nebo zařízení pocházející z nespolehlivých zdrojů nebo není ověřeno, odkud pocházejí, představují bezpečnostní riziko. Takové produkty mohou poskytovat nepřesné výsledky, na jejichž základě se pak provádí rozhodnutí. Mohou obsahovat škodlivé programy a ohrozit bezpečnost informačních technologií. Pořizování aktualizace a záplat programů by mělo též pocházet od vývojářů produktu, aby se snížilo riziko pro narušení bezpečnosti systémů.

3.2. Ztráta zařízení, přenosných médií nebo dokumentů

Existuje mnoho důvodů vedoucích ke ztrátě zařízení, přenosných médií nebo dokumentů. Ztráta zařízení znamená finanční ztrátu pro organizaci, jelikož je nutné toto zařízení nahradit a pořídit nové. V případě, že zaří-

zení nebo médium obsahovalo podnikové informace a nebylo dostatečně chráněné, mohou citlivé údaje skončit v nesprávných rukou.

3.3. Prozrazení citlivých informací

Důvěrná data a informace by měly být přístupné pouze osobám, kterým byla svěřena. Vedle integrity a dostupnosti patří důvěrnost k základním parametrům informační bezpečnosti. Pro důvěrné informace jako hesla, osobní údaje a obchodní tajemství existuje vysoké nebezpečí jejich zneužití. Mohou být využita k přístupu k zařízením nebo narušení obchodních plánů organizace.

3.4. Nedostatek zdrojů

Nedostatek zdrojů v jednom oddělení může způsobit problémy v celé organizaci. V každé oblasti se může jednat o jiné zdroje. Mohou chybět zaměstnanci, finance pro jednotlivá oddělení, výpočetní výkon nutný pro správnou funkčnost aplikace. V případě špatně nadimenzované infrastruktury sítě může docházet k výpadkům spojení a nedostupnosti služeb.

3.5. Porušení zákonů a směrnic

Každá organizace musí dodržovat řadu zákonů, směrnic a standardů. Porušení nebo nedodržování těchto nařízení je často pod velkými finančními tresty a může dojít k vynucení přerušení v činnosti. Ať se jedná o bezpečnost informací, nakládání s osobními údaji nebo dodržování kvality výrobku.

3.6. Ztráta dat

Ke ztrátě dat může dojít více způsoby, mohou být smazána omylem, při výpadku elektrické energie, působením škodlivého softwaru nebo mohou být ztracena kvůli poškození média, kde jsou zapsána. V organizaci by vedlo zničení diskového pole k velkému poškození, jelikož neexistuje sekundární pole, které by sloužilo jako klon.

4. Úmyslné

4.1. Krádež zařízení, přenosných médií nebo dokumentů

Krádež datových uložišť, IT systémů, softwaru nebo dat by mohla mít za cíl získání citlivých informací organizace nebo způsobit finanční újmu, jelikož je kradené zařízení nutné nahradit novým. Přenosná média v organizaci nejsou kryptograficky chráněná, zloděj by dostal plný přístup k informacím.

4.2. Manipulace s daty

Manipulovat s daty můžeme pomocí úpravy polí v databázích, změnou jejich obsahu nebo falšováním korespondence. Osoba však může manipulovat jen s daty, ke kterým má přístup. Čím více přístupových práv do slo-

žek a systému osoba má, tím více může dojít k manipulacím s daty. Změny mohou způsobit velkou škodu ve finančních výkazech organizace.

4.3. Neautorizovaný přístup do systému

Pro každý vstup do IT systému platí, že existuje riziko využití i k neautorizovanému vstupu. Login uživatelů mohl být prozrazen, a pokud se útočník dostane do systému, může měnit práva souboru a provádět škodlivou činnost. Datová uložiště jako USB mohou obsahovat škodlivý program, neboť uživatelé v domácí síti nedodržují dostatečná opatření a následně USB použijí v organizaci.

4.4. Zneužití osobních informací

Skoro všechny osobní informace jsou částečně citlivou informací. Pokud ochrana osobních údajů není dostatečně zaručena, existuje riziko, že osoba bude poškozena v sociálním postavení nebo ekonomických podmínkách.

4.5. Sociální inženýrství

Sociální inženýrství je metoda pro získání neautorizovaného přístupu k informacím nebo IT systémů skrze sociální akce. Využívají se vlastnosti jako důvěra, strach nebo respekt z autorit. Pomocí nich útočník dokáže získat požadované informace, pokud si oběť dostatečně rychle neuvědomí, že je manipulována.

4.6. Neautorizovaný vstup do budovy

Pokud neautorizované osoby vstoupí do budovy nebo jednotlivých oddělení, hrozí riziko krádeže, manipulace s informacemi nebo informačními systémy. Fyzická bezpečnost je v organizaci řešena pomocí zámků. Je zaveden tří směnný provoz, takže jsou vždy přítomni pracovníci výroby. Kanceláře jsou však bez dohledu chráněny jen mechanickým zámkem.

4.7.2 Míra rizika hrozeb

V následující tabulce (Tab. 8) jsou zobrazeny hodnoty pravděpodobnosti, dopadu hrozeb a míry rizika vypočtené dle vzorce zmíněného výše. Pro přehlednost a zjednodušení jsou zde hodnoty pravděpodobnosti označeny jako „P“, dopadu hrozby „D“, míra rizika „M“, hrozby „H“, zanedbatelná míra rizika „Z“, akceptující „A“ a kritická jako „K“.

Tab. 8 Analýza rizik aktiv

	Osobní počítače			Diskové pole a aplikační server			Síťová zařízení a kabeláž			Podniková data			Konstruktérské programy			Dokumentace podniku			Externí dodavatelé		
H	P	D	M	P	D	M	P	D	M	P	D	M	P	D	M	P	D	M	P	D	M
1.1.	2	2	A	2	3	K	2	3	K	2	2	A	1	2	Z	1	2	Z	1	2	Z
1.2.	1	3	A	1	3	A	1	3	A	1	3	A	1	2	Z	1	3	A	1	2	Z
2.1.	2	2	A	2	3	K	2	3	K	2	3	K	2	2	A	2	2	A	2	3	K
2.2.	2	3	K	2	3	K	2	3	K	2	3	K	2	3	K	2	2	A	2	3	K
2.3.	2	2	A	2	3	K	2	3	K	2	2	K	2	2	K	2	2	A	2	3	K
2.4.	2	2	A	2	2	A	2	2	A	2	2	A	2	3	K	1	2	Z	2	3	K
3.1.	2	3	K	2	2	K	1	3	A	2	3	K	2	2	A	2	2	A	2	2	A
3.2.	2	2	A	1	3	A	1	3	A	2	3	K	1	2	Z	2	3	K	2	2	A
3.3.	2	2	A	1	3	A	2	3	A	2	3	K	2	2	A	2	3	K	2	3	K
3.4.	2	2	A	1	2	Z	2	2	A	2	2	A	1	2	Z	2	2	A	2	2	A
3.5.	1	2	Z	1	2	Z	1	2	Z	2	3	K	2	2	A	2	2	A	2	3	K
3.6.	2	2	A	2	3	K	2	2	A	2	3	K	2	2	A	2	2	A	2	2	A
4.1.	2	2	A	2	2	A	2	2	A	2	3	K	1	2	Z	2	3	K	2	2	A
4.2.	2	3	K	2	3	K	2	3	K	2	3	K	2	2	A	2	3	K	2	3	K
4.3.	2	3	K	2	3	K	2	3	K	2	3	K	2	2	A	2	3	K	2	2	A
4.4.	1	3	A	2	2	A	1	3	A	2	3	K	1	2	Z	1	3	A	2	2	A
4.5.	1	2	Z	1	2	Z	1	2	Z	1	3	A	1	2	Z	1	2	Z	1	3	A
4.6.	2	2	A	1	3	A	1	3	A	1	3	A	1	2	Z	2	2	A	2	2	A

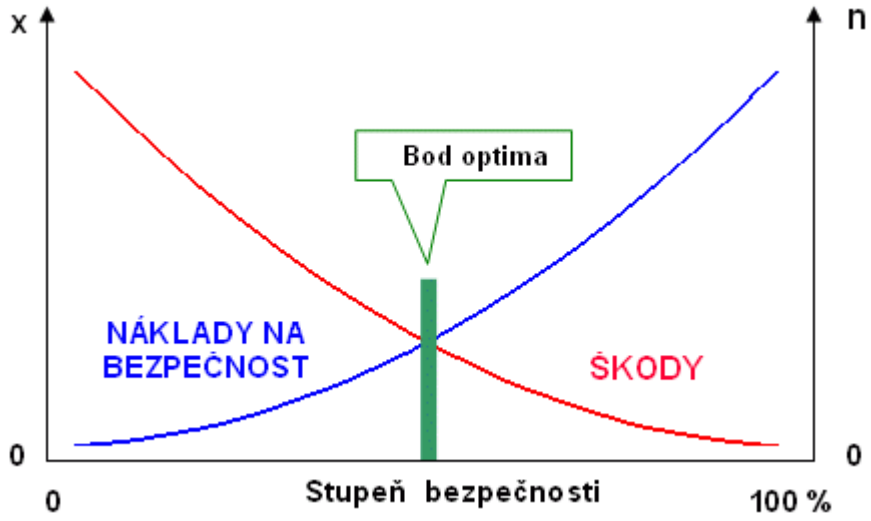
5 Návrh opatření

Podle výsledků analýzy rizik jsou navržena bezpečnostní opatření v souladu s přílohou A normy ISO/IEC 27002:2005 (dříve ISO/IEC 17799). Jedná se o soubor postupů pro řízení bezpečnosti informací.

Zde budou popsána opatření, která eliminují nebo minimalizují míru rizika pro všechna kritická aktiva. Při posuzování, jaká opatření zavést, je potřeba zvážit různé faktory. Pro malé a středně velké podniky je podstatná finanční náročnost implementace nového bezpečnostního opatření.

K efektivnímu zavedení nových opatření je potřeba zjistit optimální bod, do kterého se podniku stále vyplatí opatření zavést. Tento bod reprezentuje výšku nákladů na zavedení bezpečnostního opatření, která se rovná výšce potenciálně způsobené škody nedostupností aktiva. Od tohoto bodu by již cena přijatého opatření převyšovala výši způsobené škody a pro podnik by to znamenalo zbytečnou finanční zátěž, jak můžeme vidět v grafu (Obr. 14), kde „n“ reprezentuje náklady na opatření a „x“ výši způsobených škod.

V tabulce (Tab. 10), která je dostupná v kapitole *Přílohy*, budou tyto opatření označena jako „Ignorovat“. Opatření označena jako „Zavedeno“ jsou již v podniku implementována a není potřeba se jimi dále zabývat. Podle výsledků analýzy rizik jsou důležitá opatření pro implementaci a splňující bod optimální cenové dostupnosti označeny jako „Zavést“.



Obr. 14 Bod optima (Nádeníček, 2006)

Zde budou popsána navrhovaná opatření, která byla v tabulce (Tab. 10) označena jako „Zavést“. Tato opatření by měla odstranit či minimalizovat všechny hrozby pro aktiva s kritickou mírou rizika. U jednotlivých opatření jsou vypsány hrozby, na které se vztahují.

Bezpečnostní politika informací (A. 5.1)

Je doporučeno vytvoření oficiálního dokumentu bezpečnostní politiky, jenž je potřebný pro úspěšné řízení informační bezpečnosti v organizaci. Tento dokument by měl obsahovat následující:

- Definování účelu, cíle a záměru vedení organizace v oblasti bezpečnosti.
- Definování bezpečnostních pravidel, principů a politik.
- Definici požadavků a postupů pro řízení informací.
- Ustanovení rolí a zodpovědností za jednotlivá aktiva.

S vypracováním bezpečnostní politiky je také potřeba zajistit její opakované kontroly, aby se zaručila její aktuálnost a použitelnost. Tyto kontroly je nutné provádět pomocí externích auditů alespoň jednou ročně nebo při větší změně infrastruktury. Zavedením bezpečnostní politiky a její následováním se v organizaci zajistí:

- Soulad se zákony a předpisy.
- Porozumění cílům a potřebám organizace.
- Snížení rizik a zvýšení bezpečnosti informací.
- Zvýšení přehledu a povědomí o bezpečnosti mezi zaměstnanci.

Zavedení bezpečnostní politiky informací v organizaci bude mít pozitivní vliv na snížení rizika hrozeb H3.5, H4.2 a H4.4.

Odpovědnost za aktiva (A. 7.1)

Pro jednotlivá aktiva je nutné přiřadit konkrétního zaměstnance, který za něj bude mít zodpovědnost a stanoví pravidla ochrany a použití.

Každé aktivum tedy musí mít určeny a zdokumentovány pravidla pro přípustné použití, která musí dodržovat všichni zaměstnanci, smluvní strany a uživatelé třetích stran. Tato pravidla použití by měla obsahovat následující:

- Pravidla ochrany.
- Pravidla pro manipulaci a evidenci.
- Pravidla bezpečného elektronického sdílení.
- Pravidla fyzického přenášení aktiva.
- Pravidla správného mazání či ničení technických nosičů dat.

Přiřazením odpovědností a sepsáním pravidel přípustného použití by mělo přinést organizaci následující pozitiva:

- Menší poruchovost zařízení.

- Nižší náklady na zařízení.
- Zvýšení bezpečnosti informací.
- Zvýšení bezpečnosti na pracovišti.

Zavedení odpovědnosti za aktiva v organizaci bude mít pozitivní vliv na snížení rizika hrozeb H2.3, H3.1 a H4.1.

Klasifikace informací (A. 7.2)

Informace musí být klasifikovány podle citlivosti či kritičnosti, aby byla možná jejich kategorizace a mohli být distribuovány pouze uživatelům, kteří je potřebují pro svou pracovní činnost. Klasifikované informace budou rozděleny do následujících kategorií:

- Důvěrné.
- Soukromé.
- Citlivé.
- Veřejné.

Dále musí být vytvořena a zdokumentována pravidla pro manipulaci s informacemi podle jejich klasifikační kategorie. Klasifikace informací a jejich kategorizace by přinesla tyto výhody:

- Snížení rizika zneužití a úniku informací.
- Zvýšení úrovně bezpečnosti.
- Zvýšení bezpečnostního povědomí uživatelů.
- Vytvoření předpokladů pro implementaci DLP (Data Loss Prevention).

Zavedení klasifikace informací v organizaci bude mít pozitivní vliv na snížení rizika hrozeb H3.3, H3.5, H4.2 a H4.4.

Bezpečnost zařízení (A. 9.2)

Používání elektronických a elektrických zařízení v organizaci by mělo následovat určitá pravidla a postupy, které zajišťují jejich ochranu a bezpečnost. Mezi tyto důležité aspekty řešící bezpečnost zařízení, můžeme zařadit následující:

- Umístění zařízení a jeho ochrana

  Je doporučeno přemístění důležitých zařízení jako server, diskové pole a hraniční směrovač. Tato zařízení jsou momentálně umístěna v prostorech kanceláře a mají k nim tedy přístup administrativní pracovníci, kteří k tomu nemají oprávnění. Vhodné by bylo umístění do separátní místnosti, kde by byl umožněn přístup pouze správci IT a majiteli organizace.

- Podpůrná zařízení
  Implementace podpůrného zařízení jako je záložní zdroj pro ochranu před výpadkem elektrické energie, který tak poskytne čas pro uložení či zálohování důležitých dat.
- Bezpečnost kabelových rozvodů
  V rámci zvýšení přehlednosti síťové infrastruktury a bezpečnosti kabeláže by bylo vhodné:
    - Zřetelné označení kabeláže.
    - Zamezit přístupu ke kabeláži neoprávněným osobám.
    - Vedení kabeláže pomocí vodících trubek (husí krk).
    - Vytvoření seznamu připojení.
    - Vytvoření schématu infrastruktury organizace.

Zavedení výše zmíněných opatření přinesou organizaci následující výhody:

- Zvýšení úrovně bezpečnosti.
- Zvýšení přehlednosti o infrastruktuře.
- Nižší riziko ztráty dat.

Zavedení opatření pro bezpečnost zařízení v organizaci bude mít pozitivní vliv na snížení rizika hrozeb H1.1, H2.1, H2.2, H2.3 a H4.1.

Ochrana proti škodlivým programům a mobilním kódům (A. 10.4)

Narušení bezpečnosti a průnik do systému je velký problém i v malých a středních organizacích. Mnoho zaměstnanců vlastní přenosné zařízení, které využívají i uvnitř organizace, zapojují jej do firemní sítě. Jedná se především o mobilní telefony, notebooky, externí disky a jiná média. Pracovníci mají možnost instalovat vlastní programové vybavení z internetu do firemních počítačů. Z důvodu zvýšení bezpečnosti se doporučuje:

- Vytvořit seznam zařízení s povolením připojení do firemní sítě.
- Provést kontrolu externích zařízení správcem IT.
- Pravidelné školení zaměstnanců o bezpečnosti na internetu.
- Zavést pravidelné kontroly všech PC.
- Pravidelně provádět aktualizace systému a aplikací.

Implementace těchto opatření organizaci zajistí:

- Kontrolu nad externími zařízeními.
- Zvýšení úrovně bezpečnosti.
- Zvýšení povědomí zaměstnanců o bezpečnosti.
- Snížení rizika instalace škodlivých kódů.

Zavedení opatření na ochranu proti škodlivým programům a mobilním kódům v organizaci bude mít pozitivní vliv na snížení rizika hrozeb H2.4, H3.1 a H4.3.

Zálohování (A. 10.5)

Zálohování v organizaci je prováděno jednou denně na diskové pole, které se nachází v kancelářských prostorech. Neexistuje však sekundární pole pro případ, že by došlo k selhání primárního zařízení a to by mohlo způsobit ztrátu velkého množství dat. V rámci udržení provozu schopnosti a zvýšení kontinuity se doporučuje následující:

- Pořízení sekundárního diskového pole.
- Umístění sekundárního pole v jiné lokalitě.
- Provádět pravidelné kontroly funkčnosti záloh.
- Pravidelné zálohy zařízení a systémů.

Implementace výše uvedených opatření bude mít pro organizaci následující benefity:

- Zajištění kontinuity.
- Zkrácení doby obnovy.
- Zamezení ztráty velkého množství dat.

Zavedení opatření týkající se zálohování v organizaci bude mít pozitivní vliv na snížení rizika hrozeb H3.2 a H3.6.

Bezpečnost při zacházení s médii (A. 10.7)

Je potřeba vytvořit dokument, který bude řešit bezpečnost při zacházení s vyměnitelnými médii, jako jsou USB flash disky, externí disky či pevné disky. Tento dokument musí obsahovat postupy pro:

- Výměnu a likvidaci
  Principy a postupy pro odstranění informací uložených na médiu před jeho výměnou či zničením. Rovněž postup pro správnou likvidaci těchto zařízení.
- Ukládání informací
  Definovat způsob ukládání informací na vyměnitelných médiích.
- Modifikace
  Definovat postupy pro ochranu médií před neautorizovaným přístupem.
- Manipulace
  Definovat postupy příslušného použití vyměnitelných médií.

Vytvoření dokumentu řešící bezpečnost při zacházení s médii by organizaci přineslo následující:

- Snížení rizika úniku informací.
- Snížení rizika škodlivého softwaru.
- Zvýšení bezpečnosti.
- Předcházení ztrátě média.

Zavedení opatření týkající se zálohování v organizaci bude mít pozitivní vliv na snížení rizika hrozeb H3.1, H3.2, H4.1, H4.2 a H4.3.

Výměna informací (A. 10.8)

Je doporučeno zavést politiku pro výměnu informací, tedy stanovit pravidla pro jejich manipulaci mezi objekty. Obsahem této politiky musí být:

- Postupy pro přepravu médií a interních informací.
- Seznámení o technikách sociálního inženýrství.
- Kryptografická ochrana informací a médií.
- Ochrana proti neautorizovanému přístupu.

Implementace výše uvedených opatření pro výměnu informací zajistí organizaci výhody v podobě:

- Zvýšení bezpečnosti.
- Zvýšení povědomí zaměstnanců o praktikách sociálního inženýrství.
- Omezení možnosti neoprávněné manipulace s informacemi.
- Omezení přístupu k informacím neautorizovaným osobám.

Zavedení opatření týkající se zálohování v organizaci bude mít pozitivní vliv na snížení rizika hrozeb H3.3 a H4.2.

Kryptografická opatření (A. 12.3)

Je doporučeno vytvořit politiku pro používání kryptografických opatření na ochranu informací, která bude obsahovat:

- Požadavky na složitost hesla.
- Seznámení zaměstnanců s požadavky.
- Definování postupu pro generování a ukládání klíčů.
- Vytvoření postupů pro správu a ochranu kryptografických klíčů.
- Stanovení pravidelných intervalů kontroly.

Zavedení nových kryptografických opatření přináší organizaci následující pozitiva:

- Zvýšení bezpečnosti.
- Zvýšení povědomí zaměstnanců o bezpečnosti.
- Snížení rizika přístupu neautorizovaných osob.
- Snížení rizika úniku informací.

Zavedení opatření týkající se zálohování v organizaci bude mít pozitivní vliv na snížení rizika hrozeb H4.2, H4.3 a H4.4.

Zvládání bezpečnostních incidentů a kroky k nápravě (A. 13.2)

Je doporučeno vytvoření plánů pro úspěšné zvládání bezpečnostních incidentů. Tyto plány budou sloužit jako reakce na potencionální incident a měly by obsahovat:

- Odpovědnosti a postupy.
- Mechanizmy pro monitorování typu incidentů.
- Mechanizmy pro monitorování rozsahu a nákladů incidentů.
- Ponaučení z bezpečnostních incidentů.
- Shromažďování důkazů.

Mezi typické představitele bezpečnostních incidentů můžeme zařadit:

- Nechtěné změny v konfiguraci systému.
- Pokus o neoprávněný přístup k systémovým zdrojům.
- Neoprávněné použití systémových nástrojů ke zpracování dat.
- Přerušení poskytování služeb.

Vytvoření a následování plánů pro zvládání bezpečnostních incidentů organizaci zajistí:

- Prevenci proti bezpečnostním incidentům
- Zvýšení rychlosti obnovy.
- Zvýšení úrovně bezpečnosti.
- Snížení nákladů na bezpečnost.

Zavedení opatření týkající se zálohování v organizaci bude mít pozitivní vliv na snížení rizika hrozeb H3.1, H3.5, H4.1, H4.3 a H4.4.

Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací (A. 14.1)

Je potřeba vytvořit oficiální plány řízení kontinuity činností organizace za účelem minimalizace následků a zotavení ze ztráty informačních aktiv na akceptovatelnou úroveň. Do těchto plánů by mělo být zahrnuto:

- Opatření k identifikaci a minimalizaci rizik.
- Postupy omezení důsledků incidentů.
- Zajištění dostupnosti informací pro obnovení nezbytných činností.

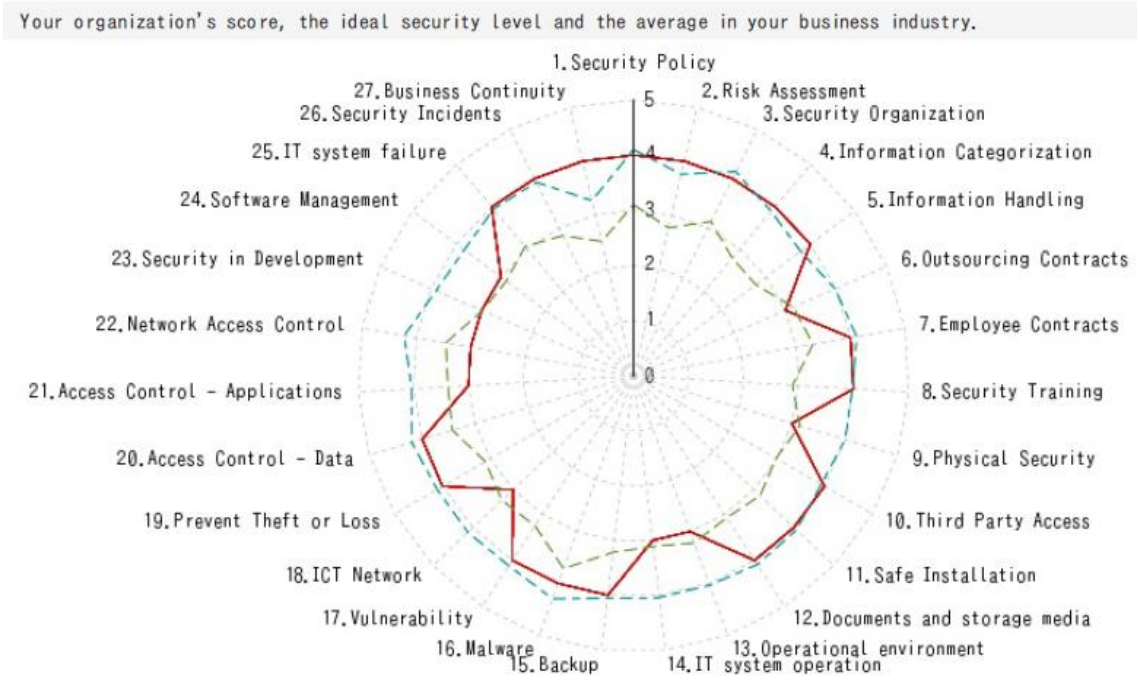
Výhody zavedení plánů pro řízení kontinuity činností organizace jsou:

- Snížení nákladů.
- Rychlejší obnova kritických činností organizace.
- Zvýšení bezpečnosti.

Součástí plánů pro řízení kontinuity činností je havarijní plán a plán obnovy, jenž jsou popsány výše v kapitole ISMS. Zavedení opatření týkající se řízení kontinuity činností organizace bude mít pozitivní vliv na snížení rizik pro skupiny hrozeb Přírodní, Technické, Lidská chyba a Úmyslné.

5.1 Souhrn

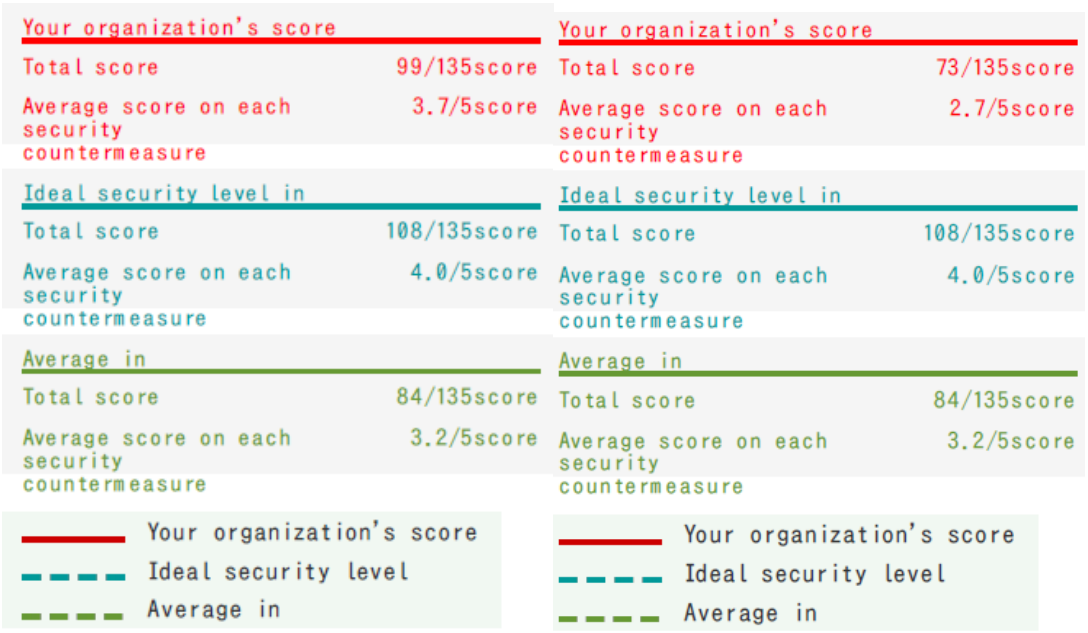
V případě, že by se vedení organizace rozhodlo následovat a implementovat doporučená opatření, která jsou uvedená výše, můžeme předpokládaný stav informační bezpečnosti vidět níže na grafu ISM-Benchmark.



Obr. 15 Předpokládaný stav

Z uvedeného grafu (Obr. 15) je viditelné zvýšení bezpečnosti oproti původnímu stavu (Aktuální stav), kdy porovnáním těchto dvou grafů můžeme vidět konkrétně, v jakých oblastech došlo ke zvýšení bezpečnosti. Zároveň se tímto zvýšilo i celkové hodnocení, které organizace obdržela, a bezpečnost se navýšila téměř k ideálnímu stavu, jak je možné vidět na obrázku níže (Obr. 16). Z obrázku je rovněž patrné, že klasifikace aktuálního stavu dosahuje pouze 73 bodů z celkových 135 a průměrné hodnocení jednotlivých opatření je 2,7 z 5 celkových. To však nedostačuje ani k dosažení průměrného ohodnocení bezpečnosti mezi všemi organizacemi, které se zúčastnily této statistiky.

Pokud dojde k implementaci všech navrhovaných opatření, tak se celková klasifikace zvedne na 99 bodů ze 135 celkových a průměrné ohodnocení pro jednotlivá opatření na 3,7 z 5 bodů. Tyto dosažené body již přesahují statistický průměr a blíží se k hranici 108 bodů, jenž reprezentuje ideální stav bezpečnosti organizace.



Obr. 16 Předpokládané a aktuální hodnocení

Z pohledu na doporučená opatření je patrné, že není potřeba investovat velké finanční částky pro nákup drahých zařízení. Samotné zařízení nezajistí nikdy stoprocentní bezpečnost. Organizace se tedy musí mít na pozoru především před vlastními zaměstnanci. Zavedení pravidel a postupů týkajících se informační bezpečnosti a manipulací s informacemi a následně jejich rozšíření pomocí školení často stačí k udržení dostatečné bezpečnosti v malých, středních, ale i velkých organizacích.

Řešení bezpečnosti informací v organizaci však není pouze jednorázovou záležitostí. Systém řízení informační bezpečnosti, jenž využívá modelu PDCA, pracuje na principu cyklů a je tedy nutné jednotlivé kroky opakovat v pravidelných intervalech či pří větších změnách infrastruktury v organizaci. Pro úspěšné řízení bezpečnosti informací v budoucnosti jsou nutné opakované kontroly, které by měly mít podobu bezpečnostních auditů a být prováděny alespoň jednou ročně.

Všechna výše uvedená opatření jsou pouze doporučením a je výhradně na majiteli organizace, zdali uzná za vhodné implementovat všechna nebo jen některá z nich, případně zda ponechá bezpečnost na úrovni, na jaké se nachází nyní.

6 Doporučení postupu při provádění auditu

V této kapitole si uvedeme důležité otázky bezpečnostního auditu, které si je potřeba položit při posuzování bezpečnosti informací u organizací podobných té, na níž je uveden příklad v této práci.

1. **Proč uvažovat o auditu?**

   Jedním z hlavních důvodů, proč by měla společnost uvažovat o bezpečnostním auditu, je nezávislé ujištění o tom, zda informační bezpečnost a bezpečnost informačních systémů organizace jsou v souladu s akceptovatelnou praxí a v souladu s platnou legislativou. Dalším důvodem může být, že si vedení chce ověřit informace, které dostává od zaměstnanců zodpovědných za podnikovou IT.

   Toto ujištění je možné získat pomocí nezávislých bezpečnostních firem, které disponují experty s mnohaletými zkušenostmi. Tito experti provedou externí kontrolu nastavení podnikových procesů nebo technologií, související s informační bezpečností a jejím řízením. Kontrola následně umožní zhodnotit, zda je bezpečnost informací řešena pravidelně a systematicky.

2. **Kdy se tedy začít bezpečnosti věnovat?**

   Začínající podniky mají zpravidla jen několik lidí, kteří všechny procesy a bezpečnost informací řídí samovolně a neformálně. Většina dat a informací je potřeba mezi sebou navzájem sdílet. Nejsou tedy implementovány role, odpovědnosti, data nejsou klasifikována a ani odpovídajícím způsobem chráněna.

   S růstem společnosti začínají narůstat i data a komplexnost údajů, která jsou pro činnost používána. Také se rozšiřuje počet pracovních pozic a rolí, přičemž nový zaměstnanci nemají povědomí o důležitosti informací a bezpečnostních požadavcích, které jsou s nimi spojené. Pokud by v tomto období nastal bezpečnostní incident, bylo by řešení bezpečnosti informací často již značně složité.

   Z tohoto důvodu by se společnosti měly věnovat informační bezpečnosti již v počátcích svého rozvoje, kdy je snadnější sledovat procesy, datové toky informací a určit jakým způsobem mají být chráněny z hlediska řízení přístupu.

3. **Proč a kdy by měly společnosti uvažovat o využití outsourcingu vzhledem k investicím do bezpečnosti firmy?**

   Využívání nových technologií nebo služeb nezávislých firem je stále u spousty organizací často opomíjené. Každá organizace provozuje množství softwaru a hardwaru, který je postupem času a na základě svých potřeb nutné aktualizovat nebo rozšiřovat. V tuto dobu se každá společnost musí rozhodnout, jak velké prostředky je ochotna do informační bezpečnosti investovat. Zde bude hrát největší roli velikost podniku.

Pro malé podniky, které mají často jen pár zaměstnanců, se nevyplatí zaměstnávat svého administrátora a bezpečnostního manažera. Bezpečnost informací je vhodné svěřit nezávislé firmě, která obstará všechny potřebné úkony týkající se informační bezpečnosti a jednoduché síťové infrastruktury. Pokud přistupuje systematicky k řízení bezpečnosti, tak i velice omezené prostředky jsou investovány jen do skutečně kritických oblastí.

U středně velkých podniků je otázka informační bezpečnosti již značně významná. Zpravidla mají malé oddělení, obsahující alespoň jednoho zaměstnance starajícího se o firemní IT. Toto malé oddělení často nemá dostatečné zkušenosti s řízením bezpečnosti informací podniku ani dostatečně potřebný prostor. Zde je na zvážení jednotlivých společností, zda chtějí investovat dostupné prostředky a rozšířit svá IT oddělení nebo bezpečnost svěřit nezávislé specializované firmě.

Velké společnosti zpravidla již řídí své vlastní technologie a mají vlastní IT oddělení starající se o bezpečnost informací a systémů. Tento tým však nemusí mít dostatečné znalosti v oblasti bezpečnosti. Služby, které tyto organizace vyhledávají, se týkají nezávislých posouzení bezpečnosti pomocí komplexních bezpečnostních auditů externích firem. Tento audit jim poskytne přehled o rizicích a určí priority pro implementaci bezpečnostních opatření.

6.1 Důležité body

Podniků podobných tomu z bezpečnostního auditu v této práci je celá řada. Tedy organizace do 50 zaměstnanců se zaměřením na výrobu. Probereme zde postup, který by bylo možné aplikovat na tyto podniky, na jaké části se zaměřit nebo jaké je možné vynechat.

Cíl a rozsah auditu

Před započetím auditu je potřeba si domluvit schůzku s majitelem, vedením a případně také s lidmi, kteří jsou zodpovědní za jednotlivá oddělení. Na tomto setkání by se měly určit jednotlivé cíle a požadavky, které jsou od auditu očekávány. Společně s cíli a požadavky je nutné stanovit i rozsah. V rámci stanovení rozsahu je potřeba vymezit hranice, tedy oblasti, kterých se bude audit týkat.

Nejčastějším cílem bývá porovnat a posoudit míru shody aktuálního stavu procesů a bezpečnosti vůči požadovaným kritériím, dále pak zdokumentovat nalezené rozdíly či nedostatky a navrhnout opatření proti potencionálním rizikům. Příklad je možné vidět v kapitole *Rozsah a cíl auditu*.

Metodika

V úvodu bezpečnostního auditu je potřeba vybrat metodiku, podle které se bude postupovat. Tu je nutné zvolit na základě předchozího kroku, kdy jsou již stanoveny požadavky a cíle auditu tak, aby zvolená metodika splnění těchto cílů plně pod-

porovala. Rovněž je potřeba si při výběru zvolit určitá kritéria, která by metodika měla splňovat. Tato kritéria však může splňovat více metodik, je tedy nutné zúžit výběr pomocí jejich srovnání, kde budou zdůrazněny jejich klady a zápory využití v dané organizaci. Následně na základě tohoto srovnání je již možné zvolit tu nejvhodnější z nich. Postup výběru je možné vidět v kapitole *Výběr metodiky*.

V této práci byla využita metodika ISMS normy ISO/IEC 27001, která dle výše uvedeného postupu byla vybrána jako nejvhodnější pro středně velkou organizaci se zaměřením na strojírenskou výrobu.

Jejím cílem je prověření aktuálního stavu bezpečnosti s požadavky pro řízení bezpečnosti informací a návrh opatření pro nalezené nedostatky podle normy ISO/IEC 27002:2013. Tímto se získá jistota, že bezpečnost je komplexně zvládána a umožní získat záruku pro klienty a orgány státní správy.

Aktuální stav

Prvním krokem samotného auditu by mělo být zjištění aktuálního stavu bezpečnosti v organizaci. V případě, že do dříve stanoveného rozsahu byla zařazena i fyzická bezpečnost, je vhodné začít audit z externího prostředí a pokračovat směrem dovnitř.

V rámci kontroly externího prostřední můžeme začít kontrolou nejbližšího okolí a fyzické bezpečnosti organizace, jež obsahuje kontrolu přístupů do prostorů objektu a přístupu ke kabeláži či rozvodným skříním. Příklad je k nahlédnutí v kapitole *Okolí podniku a fyzická bezpečnost*.

Po dokončení externího auditu, můžeme přejít ke kontrole v interním prostředí organizace. Zde se zaměříme na firemní postupy, procesy, dokumenty týkající se informační bezpečnosti a její řízení. Následně provedeme kontrolu interní zařízení a jejich nastavení, abychom zjistili zranitelnosti systémů, kterých by se dalo potencionálně využít.

K zjištění aktuálního stavu je možné využít různé nástroje, které podporují zvolenou metodiku. V práci bylo využito nástroje „*Information Security Management Benchmark*“ podporující metodiku ISMS, jenž je zobrazen na obrázku aktuálního stavu (Obr. 12). Samotný postup kontroly aktuálního stavu je popsán v kapitole *Aktuální stav*.

Identifikace a ohodnocení aktiv

Identifikace a ohodnocení aktiv organizace je dalším krokem při postupu auditem. Zde je nutné provést konzultaci s vedením, vedoucími jednotlivých oddělení a správci IT podniku. Na základě poznatků se poté sestaví seznam aktiv a jednotlivá aktiva ohodnotit z hlediska důvěrnosti, integrity a dostupnosti. Toto ohodnocení se činí na základě vlastního algoritmu nebo můžeme využít příkladu zmíněného výše v této práci (Tab. 1). Dále pak určit hodnoty RTO (Tab. 2) a využitím vzorce (1) vytvořit tabulku s klasifikací jednotlivých aktiv (Tab. 4). Kla-

sifikace aktiv je nutná pro následující krok, kterým je analýza rizik. Celkový postup je k nahlédnutí v kapitole *Identifikace a klasifikace aktiv*.

Analýza rizik

Na základě výsledků klasifikace aktiv z předchozího kroku vybereme ta aktiva, která se vyhodnotila jako důležitá či kritická pro každodenní činnost organizace. Pro tato aktiva identifikujeme potencionální hrozby využívající zranitelnosti vybraných aktiv. Příklad seznamu hrozeb s jejich popisem je dostupný výše v části *Hrozby*. Následně je stanovena hodnota dopadu hrozby (Tab. 5) a její pravděpodobnost výskytu (Tab. 6), podle vlastního algoritmu. Poté využijeme vzorce (2) pro určení rozsahu míry rizika (Tab. 7). Nyní můžeme určit míru rizika hrozeb pro jednotlivá aktiva (Tab. 8).

Dokument analýzy rizik je nejdůležitějším bodem bezpečnostního auditu organizace. Umožňuje určit hrozby, zranitelnosti, dopad a na jeho základě se vytváří všechna příslušná bezpečnostní opatření. Příklad postupu analýzy rizik je dostupný v kapitole *Analýza rizik a hrozeb*.

Návrh opatření

Pro návrh bezpečnostních opatření je možné využít normu ISO/IEC 27002:2005 či aktualizovanou verzi ISO/IEC 27002:2013. Tato norma představuje soubor postupů pro řízení bezpečnosti informací rozdělených do 11 oblastí. Celkem tyto oblasti obsahují 133 doporučených bezpečnostních opatření.

Pro každé opatření je vhodné uvést jeho pozitiva a rizika, která snižuje jeho implementace. Je vhodné také znázornit, jaký by byl předpokládaný stav bezpečnosti po zavedení všech opatření (Obr. 15). Toto znázornění můžeme provést znovu pomocí nástroje *ISM Benchmark*, jenž byl využit pro úvodní kontrolu (Obr. 12). Měla by být stanovena i doba, po které je potřeba kontrolu opět provést. Celkový postup návrhu opatření je dostupný v kapitole *Návrh opatření*.

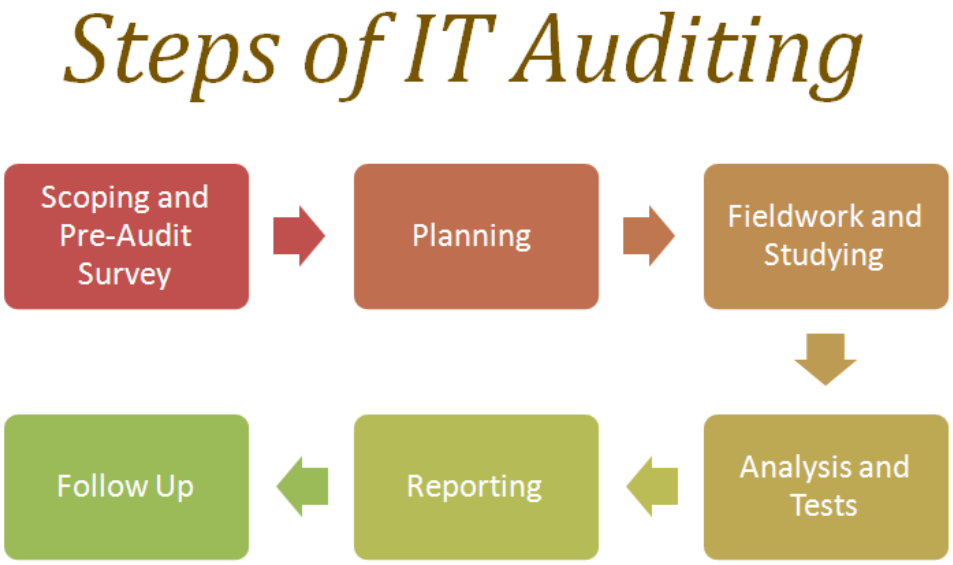
6.2 Délka auditu

Celková doba potřebná pro uskutečnění bezpečnostního auditu záleží převážně na dvou hlavních faktorech:

- Prvním faktorem je počet všech externích a interních zařízení připojených do podnikové sítě, jelikož každé zařízení je testováno a kontrolováno, což může být časově náročné.
- Druhým faktorem je množství nalezených chyb a nedostatků. Jelikož čím více nedostatků a chyb je nalezeno, tím více času je potřeba pro ověření, zda se nejedná o falešně pozitivní výsledky.

Je také důležité zmínit, že testy nenarušují podnikové služby každý den, ale jsou naplánovány tak, aby minimalizovaly zatížení pro organizaci při každodenních činnostech.

Odhad celkové délky se provádí na začátku auditu ve fázi plánování, nicméně konečný čas se může během auditu změnit v důsledku zdržení v jednotlivých fázích a v závislosti na počtu nalezených chyb. Jednotlivé fáze lze vidět na obrázku níže (Obr. 17).



Obr. 17 Fáze auditu (Kumar, 2014)

Od započetí auditu až po jeho ukončení a prezentaci výsledků může tedy uplynout doba jen několika málo dní, ale je možné se pohybovat i v řádech měsíců, jak uvádí autor článku „*Frequently Avoided Questions about IT auditing*“.

Na základě výše uvedených informací je vytvořen hrubý odhad a vypracována tabulka (Tab. 9), kde je zobrazena předpokládaná délka provedení bezpečnostního auditu v závislosti na počtu serverů, zařízení v síti a zaměstnanců. Jako počáteční bod použitý pro odhad slouží organizace zmíněná v diplomové práci.

Tento hrubý odhad však záleží na velikosti týmu a zkušenostech auditorů, kteří jsou pověřeni bezpečnostní audit provést, a slouží pouze jako příklad možných časových úseků, v jakých by se mohla délka auditu pohybovat.

Tab. 9 Časový odhad auditu

Počet serverů	Zařízení v síti	Počet zaměstnanců	Časový odhad
1 - 2	1 - 25	1 - 50	1 - 2 týdny
3 - 4	26 - 50	51 - 100	3 - 4 týdny
5 - 6	51 - 75	101 - 150	5 - 6 týdny
7 a víc	76 a víc	151 a víc	7 týdnů a víc

7 Závěr

Stále velká část malých až středně velkých organizací nepřikládá informační bezpečnosti dostatečný význam. Neprovádí pravidelné kontroly, nemají identifikovaná aktiva či zhotovenou analýzu rizik. Často je otázka bezpečnosti a správy síťové infrastruktury outsourcována na externí firmy, které však bezpečnost řeší jen sporadicky a veškeré prostředky jsou investovány jen do nejkritičtějších oblastí. Většina organizací si neuvědomuje, že pro zajištění dostatečné bezpečnosti informací není potřeba vynaložit přehnané finanční prostředky.

V práci jsme provedli bezpečnostní audit středně velkého podniku se zaměřením na strojírenskou výrobu, kde správa bezpečnosti a síťové infrastruktury je vedena externí firmou. Zjistili jsme, že organizace nikdy audit neprováděla a není si vědoma bezpečnostních hrozeb ani nedostatků. Identifikovali jsme aktiva, hrozby a provedli analýzu rizik, z jejichž výsledků byla navržena bezpečnostní opatření, která sníží či odstraní nalezená rizika. V síťové infrastruktuře není zavedena redundance ani loadbalancing. Nicméně s ohledem na celkovou složitost síťové infrastruktury organizace (Obr. 11), jejíž hlavní činností je strojírenská výroba, není nezbytně nutné implementovat tato opatření. Jak je vidět na obrázku, (Obr. 15) zvýšila se úroveň bezpečnosti v kritických a důležitých oblastech, které odhalila analýza rizik. Stále však existují oblasti, které mají prostor pro implementaci nových opatření. Na tyto oblasti je možné se více zaměřit v rámci dalšího auditu, jelikož momentálně nepředstavovaly taková rizika, aby bylo nutné se jim věnovat. Další audit by měl proběhnout v příštím roce.

Pro návrh bezpečnostních opatření byla použita norma ISO/IEC 27002:2005, z níž byla vybrána ta, jež poskytne dostatečnou ochranu vzhledem k potřebám podniku. Z výše uvedených opatření je patrné, že k dosažení požadované bezpečnosti není potřeba implementovat drahá technická zařízení, ale postačí definovat jasná pravidla či postupy při zacházení s informacemi. Dále je potřeba řídit přístup k těmto informacím stanovením rolí a odpovědností. Dokument bezpečnostní politiky obsahující všechny tyto pravidla a postupy je nezbytnou součástí pro úspěšné zvládnutí řízení informační bezpečnosti.

V neposlední řadě jsme stanovili důležité otázky, které by si měly podobné organizace pokládat, pokud uvažují o bezpečnostním auditu, a popsali jsme hlavní body, na které by se měly zaměřit. Tímto je vytvořena šablona či vzor, jenž poskytuje metody a postupy pro vytvoření bezpečnostního auditu. V rámci této šablony jsou vytvořeny odkazy, jež odkazují na konkrétní kapitoly této práce a mohou být využity jako příklad k provedení auditu v podobných organizacích.

Informační bezpečnost je vhodné řešit již od počátku a přistupovat k ní systematicky, aby se úspěšně předcházelo bezpečnostním incidentům, které by mohly organizacím způsobit vážné problémy.

8 Literatura

ALEXANDER, PAVEL. *Audit bezpečnosti informačních systémů: Klíčový krok k eliminaci zranitelností* [online]. 2016 [cit. 2017-01-02]. Dostupné z: http://www.itbiz.cz/clanky/audit-bezpecnosti-informacnich-systemu-klicovy-krok-k-eliminaci-zranitelnosti

ANTLOVÁ, K. *Informační a znalostní podpora malých a středních podniků.* Hradecké dny 2008. ISBN 978-80-7041-190-2.

BÉBR, R, DOUCEK, P. *Informační systémy pro podporu manažerské práce.* Professional publishing 2005. ISBN80-86419-79-7.

BROTHBY, W. K. *Information Security Governance: Guidance for Information Security Managers*. ISACA 2008. ISBN 978-1-933-284-73-6.

BROTBY, W. KRAG. *Information security governance: a practical development and implementation approach*. Hoboken, N.J.: John Wiley, c2009. Wiley series in systems engineering and management. ISBN 978-0470131183.

BRUCKNER, T., VOŘÍŠEK, J. *Outsourcing informačních systémů*, Ekopress 1998. ISBN 80-86119-07-6.

BUKOVSKÝ, RADIM. *Semestrální práce COBIT*. Http://deathless.cz/skola.html [online]. 2008 [cit. 2014-04-27]. Dostupné z: http://deathless.cz/documents/COBIT.pdf

CARTLIDGE, A. *An Introductory Overview of ITIL V3*. ItSMF. 2007. ISBN 0-9551245-8-1.

COBIT 4.1. *COBIT 4.1: Framework for IT Governance and Control* [online]. [cit. 2016-12-28]. Dostupné z: http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx.

Computer audit FAQ: *Frequently Avoided Questions about IT auditing*. Isect.com [online]. 2015 [cit. 2017-05-11]. Dostupné z: http://www.isect.com/html/ca_faq.html

ČERMÁK, MIROSLAV. *Jaké kybernetické hrozby můžeme očekávat v roce 2016* [online]. 2015 [cit. 2016-12-28]. Dostupné z: http://www.cleverandsmart.cz/jake-kyberneticke-hrozby-muzeme-ocekavat-v-roce-2016/.

ČERMÁK, M. *Řízení informačních rizik v praxi.* Tribun EU. s. 138. ISBN: 978-80-7399-731-1.

ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky*. Praha: Český normalizační institut, 2006.

DAVIS, CHRIS, MIKE. SCHILLER A KEVIN. WHEELER. *IT auditing: using controls to protect information assets*. 2nd ed. New York: McGraw-Hill, c2011. ISBN 978-0071742382.

DOUCEK, P. *Dokumentace, kontrola a audit bezpečnosti IS/ICT – Jak bezpečnost kontrolovat?*, In: AT&P Journal, 03/2005. ISSN 1335-2237.

DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací.* Professional Publishing. Praha 2008. ISBN 978-80-86946-88-7.

DOUCEK, P. et al. *Řízení bezpečnosti informací. 2*. Rozšířené vydání o BCM. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

GOLL, J. *Ustavení a řízení bezpečnosti informací*. Security World 6/2008. s. 44-45. ISSN 1802-4505.

HANÁČEK, PETR A JAN STAUDEK. *Bezpečnost informačních systémů: Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií.* [online]. Soubor ve formátu PDF. 2000 [cit. 2016-12-27].

CHLUP, MAREK. *BEZPEČNOST ICT* [online]. [cit. 2016-12-28]. Dostupné z: http://www.cimib.cz/ors/fileadmin/user_upload/dokumenty/CIMIB_Bezpecnost_ICT.pdf.

ITIL V3*. ITIL Set of Best Practices for IT Service Management* [online]. [cit. 2016-12-28]. Dostupné z: http://wildcatit.com/itil/.

JOHNSON, ROB. *Security policies and implementation issues. Second edition*. ISBN 978-1284055993.

KUMAR, VINOD. *How to Audit Information Technology* [online]. 2014 [cit. 2017-05-15]. Dostupné z: http://www.svtuition.org/2014/02/how-to-audit-information-technology.html

MOELLER, ROBERT R. *IT audit, control, and security*. Hoboken, N.J.: Wiley, c2010. ISBN 978-0471406761.

NÁDENÍČEK PETR. *Finance a bezpečnost, aneb peníze až na prvním místě* [online]. 2006 [cit. 2016-12-28]. Dostupné z: http://firmy.finance.cz/zpravy/finance/66819-finance-a-bezpecnost-aneb-penize-az-na-prvnim-miste/.

NOVÁK, L. *Měření účinnosti bezpečnostních opatření.* DSM 2/2008. s. 18-21. ISSN 1211-8737.

ONDRÁK, V., P. SEDLÁK A V. MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

PETERKA, J.: *Kdo (a co) bude spadat pod nový zákon o kybernetické bezpečnosti*? [online]. 2014 [cit. 2014-10-22]. Dostupné z: http://www.lupa.cz/clanky/kdo-a-co-bude-spadat-pod-novy-zakon-okyberneticke-bezpecnosti/

POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

SCARFONE, K., GRANCE, T., MASONE, K. *Computer Security Incident Hangling Guide*. NISTI. 2008. SP 800-61.

SUSANTO, HERU, MOHAMMAD NABIL ALMUNAWAR A YONG CHEE TUAN. *Information Security Management System Standards: A Comparative Study of the Big Five* [online]. 2011 [cit. 2016-12-28]. Dostupné z: http://ijens.org/Vol_11_I_05/113505-6969-IJECS-IJENS.pdf.

SVATÁ, VLASTA. *Audit informačního systému*. V Praze: Oeconomica, nakladatelství VŠE, 2016. ISBN 978-80-245-2168-8.

VITOUŠ, MARTIN. *COBIT 5 v malých a středních firmách.* [online]. 2013 [cit. 2017-05-14]. Dostupné z: https://www.systemonline.cz/sprava-it/cobit-5-v-malych-a-strednich-firmach.htm

What is the COBIT. *FAQ: What is the COBIT framework's approach to IT management?* [online]. [cit. 2016-12-28]. Dostupné z: http://searchcompliance.techtarget.com/guides/FAQ-What-is-the-COBIT-frameworks-approach-to-IT-management.

What is ITIL?. *What is ITIL?* [online]. [cit. 2016-12-28]. Dostupné z: https://www.axelos.com/best-practice-solutions/itil/what-is-itil.

9 Přílohy

Tab. 10 Opatření dle ISO/IEC 27002

Kapitola		
A. 5 Bezpečnostní politika		
A. 5.1 Bezpečnostní politika informací Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky organizace, příslušnými zákony a směrnicemi.		
A. 5.1.1	Dokument bezpečnostní politiky informací	**Zavést**
A. 5.1.2	Přezkoumání bezpečnostní politiky informací	**Zavést**
A. 6 Organizace bezpečnosti informací		
A. 6.1 Interní organizace Cíl: Řídit bezpečnost informací v organizaci.		
A. 6.1.1	Závazek vedení směrem k bezpečnosti informací	Zavedeno
A. 6.1.2	Koordinace bezpečnosti informací	Zavedeno
A. 6.1.3	Přidělení odpovědností v oblasti bezpečnosti informací	Zavedeno
A. 6.1.4	Schvalovací proces prostředků pro zpracování informací	Zavedeno
A. 6.1.5	Dohody o ochraně důvěrných informací	Zavedeno
A. 6.1.6	Kontakt s orgány veřejné správy	Zavedeno
A. 6.1.7	Kontakt se zájmovými skupinami	Ignorovat
A. 6.1.8	Nezávislá přezkoumání bezpečnosti informací	Ignorovat
A. 6.2 Externí subjekty Cíl: Zachovávat bezpečnost informací organizace a prostředků pro zpracování informací, které jsou přístupné, zpracované, sdělované nebo spravované externími subjekty.		
A. 6.2.1	Identifikace rizik plynoucích z přístupu externích subjektů	Ignorovat
A. 6.2.2	Bezpečnostní požadavky pro přístup klientů	Zavedeno
A. 6.2.3	Bezpečnostní požadavky v dohodách se třetí stranou	Zavedeno
A. 7 Řízení aktiv		
A. 7.1 Odpovědnost za aktiva Cíl: Nastavit a udržovat přiměřenou ochranu aktiv organizace.		
A. 7.1.1	Evidence Aktiv	**Zavést**
A. 7.1.2	Vlastnictví aktiv	**Zavést**
A. 7.1.3	Přístupné použití aktiv	**Zavést**
A. 7.2 Klasifikace informací Cíl: Zajistit, aby informace získaly odpovídající úroveň ochrany.		
A. 7.2.1	Doporučení pro klasifikaci	**Zavést**
A. 7.2.2	Označování a nakládání s informacemi	**Zavést**
A. 8 Bezpečnost lidských zdrojů		

A. 8.1 Před vznikem pracovního vztahu Cíl: Zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.		
A. 8.1.1	Role a odpovědnost	Zavedeno
A. 8.1.2	Prověřování	Zavedeno
A. 8.1.3	Podmínky výkonu pracovní činnosti	Zavedeno
A. 8.2 Během pracovního vztahu Cíl: Zajistit, aby si zaměstnanci, smluvní a třetí strany byli vědomi bezpečnostních hrozeb a problémů s nimi spojených, svých zodpovědností a povinností a aby byli připraveni podílet se na dodržování politiky bezpečnosti informací během své běžné práce a na snižování rizika lidské chyby.		
A. 8.2.1	Odpovědnost vedoucích zaměstnanců	Zavedeno
A. 8.2.2	Informovanost, vzdělávání a školení v oblasti bezpečnosti informací	Zavedeno
A. 8.2.3	Disciplinární řízení	Ignorovat
A. 8.3 Ukončení nebo změna pracovního vztahu Cíl: Zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců, smluvních a třetích stran proběhla řádným způsobem.		
A. 8.3.1	Odpovědnost při ukončení pracovního vztahu	Zavedeno
A. 8.3.2	Navrácení zapůjčených prostředků	Zavedeno
A. 8.3.2	Odebrání přístupových práv	Zavedeno
A. 9 Fyzická bezpečnost a bezpečnost prostředí		
A. 9.1 Zabezpečené oblasti Cíl: Předcházet neautorizovanému fyzickému přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací organizace.		
A. 9.1.1	Fyzický bezpečnostní perimetr	Zavedeno
A. 9.1.2	Fyzické kontroly vstupu osob	Ignorovat
A. 9.1.3	Zabezpečení kanceláří, místností a prostředků	Zavedeno
A. 9.1.4	Ochrana před hrozbami z vnějšího prostředí	Zavedeno
A. 9.1.5	Práce v zabezpečených oblastech	Zavedeno
A. 9.1.6	Veřejný přístup, prostory pro nakládku a vykládku	Zavedeno
A. 9.2 Bezpečnost zařízení Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činnosti organizace.		
A. 9.2.1	Umístění zařízení a jeho ochrana	**Zavést**
A. 9.2.2	Podpůrná zařízení	**Zavést**
A. 9.2.3	Bezpečnost kabelových rozvodů	**Zavést**
A. 9.2.4	Údržba zařízení	Zavedeno
A. 9.2.5	Bezpečnost zařízení mimo prostory organizace	Ignorovat
A. 9.2.6	Bezpečná likvidace nebo opakované použití zařízení	Zavedeno
A. 9.2.7	Přemístění majetku	Zavedeno

A. 10 Řízení komunikací a řízení provozu		
A. 10.1 Provozní postupy a odpovědnosti Cíl: Zajistit, správný a bezpečný provoz prostředků pro zpracování informací.		
A. 10.1.1	Dokumentace provozních postupů	Zavedeno
A. 10.1.2	Řízení změn	Zavedeno
A. 10.1.3	Oddělení povinností	Zavedeno
A. 10.1.4	Oddělení vývoje, testování a provozu	Ignorovat
A. 10.2 Řízení dodávek služeb třetích stran Cíl: Zavést a udržovat přiměřenou úroveň bezpečnosti informací a úroveň dodávání služeb ve shodě s uzavřenými dohodami.		
A. 10.2.1	Dodávky služeb	Zavedeno
A. 10.2.2	Monitorování a přezkoumávání služeb třetích stran	Ignorovat
A. 10.2.3	Řízení změn služeb poskytovaných třetími stranami	Zavedeno
A. 10.3 Plánování a přejímání systémů Cíl: Minimalizovat riziko selhání systémů.		
A. 10.3.1	Řízení kapacit	Zavedeno
A. 10.3.2	Přejímání systémů	Ignorovat
A. 10.4 Ochrana proti škodlivým programům a mobilním kódům Cíl: Chránit integritu programového vybavení a dat.		
A. 10.4.1	Opatření na ochranu proti škodlivým programům	Zavedeno
A. 10.4.2	Opatření na ochranu proti mobilním kódům	**Zavést**
A. 10.5 Zálohování Cíl: Udržet integritu a dostupnost informací a prostředků pro jejich zálohování.		
A. 10.5.1	Zálohování informací	**Zavést**
A. 10.6 Správa bezpečnosti sítě Cíl: Zajistit ochranu informací v počítačových sítích a ochranu podpůrné infrastruktury.		
A. 10.6.1	Síťová opatření	Zavedeno
A. 10.6.2	Bezpečnost síťových služeb	Zavedeno
A. 10.7 Bezpečnost při zacházení s médii Cíl: Předcházet neoprávněnému vyzrazení, modifikaci, ztrátě nebo poškození aktiv a přerušení činnosti organizace.		
A. 10.7.1	Správa výměnných počítačových médií	**Zavést**
A. 10.7.2	Likvidace médií	**Zavést**
A. 10.7.3	Postupy pro manipulaci s informacemi	**Zavést**
A. 10.7.4	Bezpečnost systémové dokumentace	Zavedeno
A. 10.8 Výměna informací Cíl: Zajistit bezpečnost informací a programů při jejich výměně v rámci organizace a při jejich výměně s externími subjekty.		
A. 10.8.1	Postupy a politiky při výměně informací	**Zavést**
A. 10.8.2	Dohody o výměně informací a programů	**Zavést**
A. 10.8.3	Bezpečnost medií při přepravě	**Zavést**

A. 10.8.4	Elektronické zasílání zpráv	Zavedeno
A. 10.8.5	Informační systémy organizace	Ignorovat
A. 10.9 Služby elektronického obchodu Cíl: Zajistit bezpečnost služeb elektronického obchodu a jejich bezpečné použití.		
A. 10.9.1	Elektronický obchod	Ignorovat
A. 10.9.2	On-line transakce	Zavedeno
A. 10.9.3	Veřejně přístupné informace	Zavedeno
A. 10.10 Monitorování Cíl: Detekovat neoprávněné zpracování informací.		
A. 10.10.1	Pořizování auditních záznamů	Ignorovat
A. 10.10.2	Monitorování používání systému	Ignorovat
A. 10.10.3	Ochrana vytvořených záznamů	Ignorovat
A. 10.10.4	Administrátorský a operátorský deník	Zavedeno
A. 10.10.5	Záznam selhání	Zavedeno
A. 10.10.6	Synchronizace hodin	Zavedeno
A. 11 Řízení přístupu		
A. 11.1 Požadavky na řízení přístupu Cíl: Řídit přistup k informacím.		
A. 11.1.1	Politika řízení přístupu	Zavedeno
A. 11.2 Řízení přístupu uživatelů Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k informačním systémům.		
A. 11.2.1	Registrace uživatele	Zavedeno
A. 11.2.2	Řízení privilegovaného přístupu	Zavedeno
A. 11.2.3	Správa uživatelských hesel	Ignorovat
A. 11.2.4	Přezkoumání přístupových práv uživatelů	Ignorovat
A. 11.3 Odpovědnosti uživatelů Cíl: Předcházet neoprávněnému přístupu, vyzrazení nebo krádeži informací a prostředků pro zpracování informací.		
A. 11.3.1	Používání hesel	Zavedeno
A. 11.3.2	Neobsluhovaná uživatelská zařízení	Zavedeno
A. 11.3.3	Zásada prázdného stolu a prázdné obrazovky monitoru	Ignorovat
A. 11.4 Řízení přístupu k síti Cíl: Předcházet neautorizovanému přístupu k síťovým službám.		
A. 11.4.1	Politika užívání síťových služeb	Zavedeno
A. 11.4.2	Autentizace uživatele pro externí připojení	Zavedeno
A. 11.4.3	Identifikace zařízení v sítích	Zavedeno
A. 11.4.4	Ochrana portů pro vzdálenou diagnostiku a konfiguraci	Zavedeno
A. 11.4.5	Princip oddělení v sítích	Ignorovat
A. 11.4.6	Řízení síťových spojení	Ignorovat
A. 11.4.7	Řízení směrování sítě	Zavedeno

A. 11.5 Řízení přístupu k operačnímu systému Cíl: Předcházet neautorizovanému přístupu k operačním systémům.		
A. 11.5.1	Bezpečné postupy přihlášení	Zavedeno
A. 11.5.2	Identifikace a autentizace uživatelů	Zavedeno
A. 11.5.3	Systém správy hesel	Ignorovat
A. 11.5.4	Použití systémových nástrojů	Ignorovat
A. 11.5.5	Časové omezení relace	zavedeno
A. 11.5.6	Časové omezení spojení	Zavedeno
A. 11.6 Řízení přístupu k aplikacím a informacím Cíl: Předcházet neoprávněnému přístupu k informacím uloženým v počítačovém systému.		
A. 11.6.1	Omezení přístupu k informacím	Zavedeno
A. 11.6.2	Oddělení citlivých systémů	Ignorovat
A. 11.7 Mobilní výpočetní zařízení a práce na dálku Cíl: Zajistit bezpečnost informací při použití mobilní výpočetní techniky a zařízení pro práci na dálku.		
A. 11.7.1	Mobilní výpočetní zařízení a sdělovací technika	Ignorovat
A. 11.7.2	Práce na dálku	Ignorovat
A. 12 Akvizice, vývoj a údržba informačních systémů		
A. 12.1 Bezpečnostní požadavky informačních systémů Cíl: Zajistit, aby se bezpečnost stala neoddělitelnou součástí informačních systémů.		
A. 12.1.1	Analýza a specifikace bezpečnostních požadavků	Ignorovat
A. 12.2 Správné zpracování v aplikacích Cíl: Předcházet chybám, ztrátě, neoprávněné modifikaci nebo zneužití informací v aplikacích.		
A. 12.2.1	Validace vstupních dat	Ignorovat
A. 12.2.2	Kontrola vnitřního zpracování	Ignorovat
A. 12.2.3	Integrita zpráv	Ignorovat
A. 12.2.4	Validace výstupních dat	Ignorovat
A. 12.3 Kryptografická opatření Cíl: Ochránit důvěrnost, autentičnost a integritu informací s pomocí kryptografických prostředků.		
A. 12.3.1	Politika pro použití kryptografických opatření	**Zavést**
A. 12.3.2	Správa klíčů	**Zavést**
A. 12.4 Bezpečnost systémových souborů Cíl: Zajistit bezpečnost systémových souborů.		
A. 12.4.1	Správa provozního programového vybavení	Zavedeno
A. 12.4.2	Ochrana systémových testovacích subjektů	Ignorovat
A. 12.4.3	Řízení přístupu ke knihovně zdrojových kódů	Ignorovat
A. 12.5 Bezpečnost procesů vývoje a podpory Cíl: Udržovat bezpečnost programového vybavení a informací aplikačních		

systémů.		
A. 12.5.1	Postupy řízení změn	Zavedeno
A. 12.5.2	Technické přezkoumání aplikací po změnách operačního systému	Ignorovat
A. 12.5.3	Omezení změn programových balíků	Zavedeno
A. 12.5.4	Únik informací	Zavedeno
A. 12.5.5	Programové vybavení vyvíjené externím dodavatelem	Ignorovat
A. 12.6 Řízení technických zranitelností Cíl: Snížit rizika vyplívající z využívání zveřejněných technických zranitelností.		
A. 12.6.1	Řízení, správa a kontrola technických zranitelností	Ignorovat
A. 13 Zvládání bezpečnostních incidentů		
A. 13.1 Hlášení bezpečnostních událostí a slabin Cíl: Zajistit nahlášení bezpečnostních událostí a slabin informačního systému způsobem, který umožní včasné zahájení kroků vedoucích k nápravě.		
A. 13.1.1	Hlášení bezpečnostních událostí	Zavedeno
A. 13.1.2	Hlášení bezpečnostních slabin	Zavedeno
A. 13.2 Zvládání bezpečnostních incidentů a kroky k nápravě Cíl: Zajistit odpovídající a účinný přístup ke zvládání bezpečnostních incidentů.		
A. 13.2.1	Odpovědnosti a postupy	**Zavést**
A. 13.2.2	Ponaučení z bezpečnostních incidentů	**Zavést**
A. 13.2.3	Shromažďování důkazů	**Zavést**
A. 14 Řízení kontinuity činností organizace		
A. 14.1 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací Cíl: Bránit přerušení provozních činností a chránit kritické procesy organizace před následky závažných selhání informačních systémů nebo katastrof a zajistit včasnou obnovu činnosti.		
A. 14.1.1	Zahrnutí bezpečnosti informací do procesu řízení kontinuity činností organizace	**Zavést**
A. 14.1.2	Kontinuita činností organizace a hodnocení rizik	**Zavést**
A. 14.1.3	Vytváření a implementace plánů kontinuity	**Zavést**
A. 14.1.4	Systém plánování kontinuity činností organizace	**Zavést**
A. 14.1.5	Testování, udržování a přezkoumávání plánů kontinuity	**Zavést**
A. 15 Soulad s požadavky		
A. 15.1 Soulad s právními normami Cíl: Vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.		
A. 15.1.1	Identifikace odpovídajících předpisů	Zavedeno
A. 15.1.2	Ochrana duševního vlastnictví	Zavedeno
A. 15.1.3	Ochrana záznamů organizace	Zavedeno
A. 15.1.4	Ochrana dat a soukromí osobních informací	Zavedeno
A. 15.1.5	Prevence zneužití prostředků pro zpracování informací	Zavedeno

A. 15.1.6	Regulace kryptografických opatření	Zavedeno
A. 15.2 Soulad s bezpečnostními politikami, normami a technická shoda Cíl: Zajistit shodu systémů s bezpečnostními politikami organizace a normami.		
A. 15.2.1	Shoda s bezpečnostními politikami a normami	Zavedeno
A. 15.2.2	Kontrola technické shody	Zavedeno
A. 15.3 Hlediska auditu informačních systémů Cíl: Maximalizovat účinnost auditu a minimalizovat zásahy do/z informačních systémů.		
A. 15.3.1	Opatření k auditu informačních systémů	Ignorovat
A. 15.3.2	Ochrana nástrojů pro audit informačních systémů	Ignorovat