Západočeská univerzita v Plzni
Fakulta aplikovaných věd
Katedra informatiky a výpočetní techniky

Diplomová práce

Příprava bezpečnostní dokumentace vyhovující zákonu o kybernetické bezpečnosti

Plzeň 2016 Bc. Milan Široký

Prohlášení

Prohlašuji, že jsem diplomovou práci vypracoval samostatně a výhradně s použitím citovaných pramenů.

V Plzni dne 3. května 2016

Bc. Milan Široký

Abstrakt

Tato diplomová práce se zabývá tvorbou návodu na vytvoření bezpečnostní dokumentace požadované zákonem č. 181/2014 Sb.. V první kapitole je uveden popis samotného zákona spolu se zajímavými paragrafy. Další kapitola se věnuje představení dvou interních systémů, které poslouží jako vzor pro vytvoření dokumentace. Třetí nejdůležitější kapitola se věnuje samotné tvorbě bezpečnostní dokumentace se všemi náležitostmi vyžadovanými zákonem. K diplomové práci jsou přiloženy dva soubory. První obsahuje veškerá identifikovaná aktiva, hrozby a rizika. Druhý soubor je vlastní návrh bezpečnostní dokumentace pro systém Webový HelpDesk.

Abstract

This thesis focused on making a tutorial for creating security documentation, which is required by law number 181/2014 collection. In the first chapter is describe of this law with interesting paragraphs. The next chapter is focused on presentation of two internal systems, which are used as example for creating a documentation. In the third the most important chapter is shown how is it possible to make a security documentation with all, what the law requires. The thesis contains two external files as an attachment. The first file contains all identified assets, threats and risks. The second file is a proposal of security documentation for Web HelpDesk.

Poděkování

Rád bych zde poděkoval paní Ing. Monice Loutocké za její skvělou pomoc při vedení mé diplomové práce, její čas, cenné rady a za pomoc při průběžných korekturách textu. Dále bych chtěl poděkovat panu Ing. Petru Přibylovi za jeho pomoc při analýze rizik a za poskytnutí velkého množství cenných informací o hodnocených firemních systémech.

Obsah

Kapitola 1

Úvod

Na zákonu o kybernetické bezpečnosti začal pracovat Národní bezpečnostní úřad (NBÚ) již v průběhu roku 2013. Od té doby bylo možné zákon připomínkovat a měnit jeho obsah. Tyto úpravy postupně trvaly až do 29. srpna roku 2014, kdy zákon vyšel ve Sbírce zákonů pod číslem 181/2014 Sb.. Tento zákon nabyl svojí účinnost 1. ledna roku 2015.

Zákon se zabývá zejména právy a povinnostmi osob a orgánů, které jsou v zákonu určené a spadají tudíž pod tento zákon. Dále uvádí pravomoci a působnost orgánů veřejné moci. Zákon je prováděn třemi prováděcími vyhláškami:

- 315/2014 Sb. - nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
- 316/2014 Sb. - vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
- 317/2014 Sb. - Vyhláška o významných informačních systémech a jejich určujících kritériích

V práci se nejprve zabývám popisem a vysvětlením samotného zákona o kybernetické bezpečnosti a jeho tří vyhlášek. Dále se věnuji popisu dvou firemních systémů, které sloužily jako testovací systémy, a to Webovému HelpDesku a systému ISZA (Informační systém zákaznické administrace). Na těchto systémech jsou ukázány jednotlivé požadavky zákona č. 181/2014 Sb.. Slouží tedy jako ukázkové systémy pro příklad, jak by měla vypadat bezpečnostní dokumentace.

Celá část práce věnující se bezpečnostní dokumentaci je tvořena tak, že je vždy nejprve uvedeno, jakým způsobem se přijde k hodnotám vyžadovaných zákonem, a až poté jsou uvedeny konkrétní hodnoty pro vzorový systém Webový HelpDesk. Tyto údaje jsou zde jen pro názornou ukázku a byly by v případě použití této diplomové

práce jako návodu pro tvorbu dokumentace jiného systému nahrazeny informacemi právě o tomto zkoumaném systému. Z tohoto tedy vyplývá účel této diplomové práce, ve které nebylo hlavním cílem vytvořit přesnou a úplnou bezpečnostní dokumentaci, ale spíše vytvořit návod pro firmu CCA, jak vypracovat bezpečnostní dokumentaci pro jiný systém nasazený u zákazníka.

Kapitola 2

Zákon o kybernetické bezpečnosti

Tento zákon číslo 181/2014 Sb. nabyl svoji účinnost 1. ledna 2015. Zákon se zaměřuje na úpravu práv a povinností osob a dále na míru působnosti a pravomocí orgánů veřejné správy v oblastech kybernetické bezpečnosti. Také je v zákonu zřetelně uvedeno, že se nevztahuje na informační a komunikační systémy, které přenášejí, ukládají či jinak pracují s tajnými informacemi. V zákonu se také často mluví o *systémech kritické infrastruktury*, ale již neříká, jaké systémy či sítě sem patří. To určuje až vyhláška číslo 315/2014 Sb. aktualizující současný zákon číslo 432/2010 Sb., který v sobě obsahuje kritéria pro určení prvků (řízení letového provozu, řídicí systém elektrárny), systémů či odvětví, která splňují tato zákonem stanovená kritéria a tudíž se zařadí mezi prvky kritické infrastruktury. Průřezovým kritériem je například hledisko, že v případě výpadku tohoto prvku se počet obětí na životech bude pohybovat okolo 250 mrtvých nebo bude více jak 2500 lidí zraněno a následně hospitalizováno po dobu minimálně jednoho dne.

Dále je v zákonu také používán pojem *významný informační systém*. Tímto pojmem se rozumí informační systém, který je spravován orgánem veřejné moci (např. Registr vozidel spravovaný Ministerstvem dopravy) a není zároveň kritickou informační infrastrukturou. U tohoto systému by případné narušení bezpečnosti v něm uložených dat mohlo způsobit omezení nebo téměř zastavení prováděných činností orgánu. Dalším pojmem je *významná síť*, kde se jedná o páteřní sítě zajišťující přenos dat do veřejných sítí v zahraničí anebo o sítě, které poskytují přímé připojení do kritických infrastruktur.

Zákon také uvádí osoby či orgány, kterým ukládá jejich povinnosti v oblasti kybernetické bezpečnosti. Tyto orgány dělí do pěti kategorií, přičemž na první dvě (pod čísly 1 a 2 ve výčtu níže) klade menší požadavky a zbývajícím třem (čísla 3, 4 a 5 ve výčtu níže) naopak stanovuje přísnější podmínky.

Kategorie orgánů, na které se vztahuje zákon číslo 181/2014 Sb:

1. poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací (nejedná se o internet, ale o televizní a rádiové vysílání a také o mobilní sítě), který ale nezajišťuje významnou síť

2. orgán nebo osoba zajišťující významnou síť, který ale zároveň není správcem komunikačního systému kritické informační infrastruktury
3. správce informačního systému kritické informační infrastruktury
4. správce komunikačního systému kritické informační infrastruktury
5. správce významného informačního systému

Dále bych uvedl části zákona, které mě při seznamování se zákonem zaujaly:

1. **Bezpečnostní opatření**

   Tímto opatřením je zde myšlen souhrn činností, které mají za svůj cíl zajistit bezpečí uložených informací v informačních systémech a také spolehlivost a dostupnost služeb a sítí elektronických komunikací. Dále zákon uvádí, že orgány uvedené v paragrafu 3) zákona číslo 181/2014 Sb. v odstavcích c) až e), mají povinnost zavést a provádět bezpečnostní opatření (tato opatření jsou uvedena v paragrafu 5), ve kterém jsou uvedeny také jednotlivé oblasti, které musí orgán splnit) alespoň v takovém rozsahu, aby byly schopné zajistit kybernetickou bezpečnost jejich systémů. Orgány musí mít také povinně bezpečnostní dokumentaci, jejíž obsah a strukturu stanoví příslušný prováděcí předpis. Zákon také uvádí, že tyto orgány musí vzít v potaz požadavky kladené tímto zákonem na nové systémy již při samotném výběru dodavatelů na realizaci těchto systémů.

   Bezpečnostní opatření zákon číslo 181/2014 Sb. rozděluje do dvou kategorií:

   - Organizační opatření

     Do této kategorie patří opatření týkající se firemních politik a interních směrnic. Mezi tato opatření patří např. systém řízení bezpečnosti informací, řízení rizik, organizační bezpečnost, zvládání kybernetických bezpečnostních událostí a incidentů a v neposlední řadě také řízení přístupu osob ke kritickým informačním infrastrukturám.

   - Technická opatření

     Mezi tato opatření patří již ryze technická opatření jako je např. fyzická bezpečnost, nástroj pro ověření identity uživatelů, nástroj pro řízení přístupových oprávnění a také nástroj pro ochranu před škodlivým kódem a kryptografické prostředky.

   Tato opatření se následně člení na jednotlivé složky, kterými jsou varování, reaktivní opatření a ochranné opatření.

- Varování

  Varování vydává úřad na základě informace zaslané národním bezpečnostním týmem nebo orgánem ze zahraničí, který se také zabývá činností v oblasti kybernetické bezpečnosti. Toto varování poté úřad zveřejní na svých internetových stránkách a kontaktuje orgány a správce (paragraf 3 a) až e)), jejichž kontaktní údaje má k dispozici.

- Reaktivní opatření

  Další složkou je reaktivní opatření (jsou to ta opatření, která se provádí, pokud již probíhá útok a slouží ke zmírnění následků tohoto útoku), které svým rozhodnutím pověří dotčený orgán, aby provedl tato opatření pro řešení kybernetického bezpečnostního incidentu.

- Ochranná opatření

  Poslední složkou je ochranné opatření, které úřad vydá k provedení všem orgánům v paragrafu 3 zákona č. 181/2014 Sb. odstavce c) až e) za tím účelem, aby zajistil zvýšení ochrany jejich informačních systémů. Rozsah tohoto opatření je dán především analýzou proběhlého útoku a slouží tedy pro ostatní orgány jako prevence, pokud by se tento útok u nich v budoucnosti objevil. Úřad vydá ochranné opatření formou obecné povahy, což znamená, že orgánům a správcům uvedeným v paragrafu 3 odstavce c) až e) stanoví způsob, jakým si mají zvýšit ochranu a tím pádem bezpečnost svých informačních systémů, a také lhůtu, do které musejí ochranná opatření zavést.

2. **Kybernetická bezpečnostní událost, incident a jejich hlášení**

   Bezpečnostní událostí rozumí zákon takový stav, který může vést k narušení bezpečnosti uložených dat v informačních systémech nebo k porušení integrity bezpečnosti v sítích elektronických komunikací. Pokud ale nastane *bezpečnostní incident*, jedná se již o narušení bezpečnosti informací uložených v informačních systémech nebo porušení bezpečnosti a integrity sítí, ve kterých probíhá elektronická komunikace. Toto narušení bezpečnosti je důsledkem kybernetické bezpečnostní události.

   Hlášení bezpečnostních incidentů je pro orgány uvedené v paragrafu 3 odstavce b) až e) (orgán zajišťující významnou síť; správce informační, komunikační kritické informační infrastruktury; správce významného informačního systému) povinné a musejí tak učinit neodkladně po detekci bezpečnostního incidentu. Orgán nebo osoba provozující významnou síť musí bezpečnostní incidenty hlásit národnímu bezpečnostnímu týmu. Správci informačních a komunikačních systémů kritických informač-ních infrastruktur a významných informačních systémů hlásí incidenty

v jimi spravovaných systémech vládnímu bezpečnostního týmu, který spadá pod Národní bezpeč-nostní úřad.

Zkratka CERT (Computer Emergency Response Team) označuje bezpečnostní tým starající se o koordinaci řešení nastalých bezpečnostních incidentů v počítačových sítích nacházejících se v České republice. Tuto činnost provádí podle zákona číslo 184/2014 Sb., o kybernetické bezpečnosti a jeho příslušných prováděcích předpisů. Mezi hlavní úkoly tohoto CERT týmu a potažmo dalších týmů patří zejména poskytování nejnovějších bezpečnostních informací o bezpečnostních incidentech a také poskytování pomoci orgánům uvedeným v paragrafu 3 zákona číslo 181/2014Sb.[2] Dále je zde ještě zkratka CSIRT (Computer Security Incident Response Team), který je ale v tomto zákonu označován jako "Národní CERT"tým, který se stará zejména o koordinaci při řešení bezpečnostních incidentů v počítačových sítích, které jsou provozované v České republice. Hlavním cílem českého CSIRT týmu je pomáhat firmám, které provozují síťovou infrastrukturu, zřizovat si svoje vlastní bezpečnostní týmy a také řešit bezpečnostní incidenty v jejich sítích, čímž se nejen zlepšuje bezpečnost jejich sítí, ale také i globálního internetu. Dále národní CERT tým může předávat hlášení o incidentech správcům těch sítí, ze kterých pocházejí tyto útoky, ale spíše jen tehdy, pokud nereagují na stížnosti od uživatelů nebo od jiných subjektů.

Národní CERT provozuje sdružení CZ.NIC, které je současně správcem národní domény .CZ.[3] Tento CERT tým může provozovat pouze právnická osoba, která splňuje požadavky dané zákonem[1]. Například nikdy neprováděla špionáž pro získání informací proti zájmům České republiky, provozuje nebo zajišťuje funkčnost informačních systémů nejméně 5 let a také má k dispozici odpovídající technické znalosti nejen z oboru kybernetické bezpečnosti. Následně se zájemce o provozování národního CERT týmu prokazuje čestným prohlášením, že splnil většinu požadavků, které na něj klade tento zákon. Zbývající podmínky prokáže výpisem z rejstříku trestů a potvrzením od finančního a celního úřadu, že nemá vůči těmto orgánům žádné závazky. Také je zde zajímavé, že národní CERT vykonává téměř všechny činnosti, které mu ukládá tento zákon, bezúplatně. CERT tým má ale možnost provozovat na svoji zodpovědnost vlastní hospodářskou činnost v oblasti kybernetické bezpečnosti, ale pouze tehdy, pokud tato činnost nenaruší plnění povinností, které mu ukládá zákon (paragraf 17 odstavec 2).

3. **Stav kybernetického ohrožení**

Tento stav je vyhlašován ředitelem Národního bezpečnostního úřadu a to tehdy, pokud dojde k výraznému ohrožení informací, které jsou uloženy v informačních systémech, nebo k ohrožení fungování sítí elektronické komunikace. Pokud se tak

stane, je zde vysoká pravděpodobnost, že může dojít nebo již došlo k ohrožení zájmu České republiky, tedy k vyzrazení tajných informací z těchto systémů ve smyslu zákona, který upravuje ochranu utajovaných informací. Pokud už dojde k vyhlášení stavu kybernetického nebezpečí, vysílá se tato informace v celoplošném rozhlasovém a televizním vysílání. Zajímavostí je, že toto vysílání musí provozovatel celoplošného vysílání zveřejnit neprodleně a bez jakékoliv změny obsahu zprávy, která je mu dodána bezpečnostním úřadem. Provozovatel také nesmí požadovat náhradu nákladů a ušlých zisků, které mu mohly vzniknout vysíláním zprávy o kybernetickém nebezpečí. Rozhodnutí o vyhlášení stavu nebezpečí se stává platné okamžikem, stanoveným v rozhodnutí. Toto rozhodnutí se vydává na nezbytně dlouhou dobu, maximálně na 7 dnů. Ředitel bezpečnostního úřadu ho také může zrušit dříve, než vyprší doba, na kterou bylo vydáno, nebo ho může opět prodloužit o maximálně 7 dnů. Je zde podmínka, že celková doba, po kterou je vyhlášen stav nebezpečí, nesmí překročit 30 dnů. Stav nebezpečí nemůže úřad vyhlásit, pokud je sám vykonáváním svých činností, stanovených tímto zákonem, schopen eliminovat vzniklé ohrožení bezpečnosti informací v informačních systémech.

Zákon ke svému fungování potřebuje ještě tři prováděcí předpisy, které stručně představím.

1. Novela nařízení vlády číslo 315/2014 Sb., kterou se mění zákon číslo 432/2010 Sb., o kritériích pro určení prvku (jedná se např. o elektrárny, leteckou dopravu a o komunikační a informační systémy) kritické infrastruktury

   Touto novelou se mění odvětvová kritéria pro určení, která firma nebo organizace se po splnění těchto podmínek stane kritickou infrastrukturou. Kritéria jsou nastavena vcelku rozumně, a proto je splní pouze velké podniky nebo systémy. Nestane se tak, že by se zákonem o kybernetické bezpečnosti musela řídit nějaká malá firma zabývající se např. registrací domén druhého řádu (webgarden.cz). Zákonem se už ale musí řídit registrátor národní domény nejvyšší úrovně .CZ.

2. Vyhláška číslo 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

   Zákon o kybernetické bezpečnosti neuvádí konkrétní postupy či metody, které musí subjekty, kterých se tento zákon týká, splnit a zavést za účelem vyhovění všem podmínkám, které na ně zákon klade. Z toho důvodu se zákon odkazuje na tuto vyhlášku, ve které již konkrétněji stanovuje obsah a strukturu bezpečnostní dokumentace a také stanovuje jednotlivé oblasti z bezpečnostních opatření, které subjekt musí zavést. Ale ani tato vyhláška přímo neříká, jaké konkrétní systémy

či nástroje se musí zavést, takže zůstává celkem velký prostor pro samotný orgán, jaký konkrétní systém zavede pro splnění požadavků.

Nejprve je potřeba vysvětlit několik pojmů, které se vyskytují v této vyhlášce.

První na řadě je *aktivum*, které se skládá z primárního a podpůrného aktiva. Primárním aktivem rozumíme službu nebo informaci, která je zpracovávána nebo také poskytována informačním nebo komunikačním systémem kritické infrastruktury. Podpůrné aktivum sestává z technického aktiva (patří sem technické vybavení, komunikační prostředky a také programové vybavení informačních, komunikačních systémů), zaměstnanců a dodavatelů, kteří se starají o provoz, správu a bezpečnost informačního a komunikačního systému.

Dalším pojmem je *riziko*, které znamená určitou možnost, že dojde ke zneužití zranitelnosti (jedná se o slabé místo, buďto ve službě poskytované informačním systémem, nebo v bezpečnostním opatření) informačního systému orgánu a poté k poškození aktiva systému.

Následujícím pojmem je *hrozba*, která je v tomto zákonu definována jako potencionální příčina bezpečnostní události nebo bezpečnostního incidentu, která může ve výsledku ohrozit nebo poškodit firemní aktiva. Uvedl bych zde pro lepší představu příklad jedné z možných hrozeb. Tato hrozba může vypadat například tak, že firma bude donucena propustit jednoho ze svých administrátorů firemních serverů z důvodu jeho nevhodného chování na pracovišti. Tento propuštěný zaměstnanec se s firmou nerozejde v dobrém a vzniká zde proto hrozba, že se bude chtít firmě pomstít nebo jí nějakým způsobem uškodit. Toho může docílit například tím, že zastaví některý ze serverů, čímž způsobí firmě finanční újmu a také je možné, že pošpiní dobré jméno firmy u zákazníků, kterým kvůli jeho zásahu nepůjdou jimi využívané služby. Příklad zranitelnosti související s hrozbou poškození serverů je neodebrání přístupových práv tomuto propuštěnému zaměstnanci, který má tak možnost se na servery připojit vzdáleným přístupem a jejich poškozením způsobit firmě škodu.

Vyhláška je členěna na organizační a technická opatření, kde jsou uvedeny informace o tom, jaké postupy a metody musí orgán zavést, ale ne nijak konkrétně. U *organizačních opatření* je např. sekce týkající se řízení rizik, ve které je orgánu řečeno, že musí stanovit metodiku pro identifikaci a hodnocení aktiv, rizik a také určit důležitost jím nalezených aktiv. V části týkající se *technických opatření* je například uvedena fyzická bezpečnost, kde jsou uváděny zejména prostředky (např. systémy pro kontrolu vstupu, kamerové systémy a mechanické zábranné prostředky), které má přijmout orgán podle paragrafu 3 odstavce c) až e) zákona o kybernetické bezpečnosti. Dále se zde nacházejí sekce věnující se nástrojům

pro řízení přístupových oprávnění, pro ochranu před škodlivým kódem a pro detekci kybernetických incidentů. V poslední části této vyhlášky jsou uvedeny zejména typy bezpečnostních incidentů, jejich kategorizace a také náležitosti, které použije orgán při hlášení těchto incidentů vládnímu CERT týmu, potažmo bezpečnostnímu úřadu.

Rád bych zde uvedl paragraf, který mi připadal zajímavý, a to paragraf týkající se organizační bezpečnosti. Tento odstavec uvádí povinnost pro orgány (paragraf 3 písmene c) až e) zákona 181/2014 Sb.) zavést organizaci řízení bezpečnosti informací, ve které musí určit bezpečnostní role.

Orgán (firma, státní organizace) má za povinnost stanovit následující role a to:

- manažera kybernetické bezpečnosti

  Tento manažer bude nést odpovědnost za systém řízení bezpečnosti informací a také bude náležitě proškolen, což prokáže minimálně tříletou praxí v řízení bezpečnosti informací.

- architekta kybernetické bezpečnosti

  Architekt se bude starat o návrh a o následnou implementaci bezpečnostních opatření a také bude mít minimálně tříletou praxi.

- auditora kybernetické bezpečnosti

  Auditor, jak je již patrné z názvu jeho funkce, bude vykonávat nestranně audit kybernetické bezpečnosti a bude disponovat nejméně tříletou praxí.

- garant aktiva

  Roli garanta aktiva bude vykonávat fyzická osoba z pověření orgánu a starat se zejména o rozvoj, použití a o zajištění bezpečnosti jemu přiděleného aktiva.

Jak je z předchozího výčtu potřebných rolí zřejmé, je nutné mít u všech osob vykonávající tyto role zajištěno, že budou disponovat praxí v délce nejméně tří let, což může být ale pro orgány státní správy problém (mít k dispozici tyto osoby s odpovídající praxí). Z tohoto důvodu je v zákonu uvedeno, že si tyto orgány mohou najmout osoby z externích firem pro zajištění zákonem požadovaných rolí (manažer, architekt, auditor a garant aktiva).

3. Vyhláška číslo 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

   V příloze číslo 1 k této vyhlášce je uveden seznam informačních systémů, které splňují určující kritéria dané touto vyhláškou. Správce nebo provozovatel těchto

systémů má zákonem danou povinnost vést pro tyto systémy bezpečnostní dokumentaci. Tato určující kritéria se skládají z dopadových určujících kritérií a oblastních určujících kritérií. Pokud nastane situace, že nějaký informační systém není uveden v seznamu v příloze číslo 1, tak o splnění určujících kritérií a tedy zařazení tohoto systému mezi významné informační systémy rozhoduje správce tohoto systému. Zákon definuje dopadové určující kritérium jako skutečnost, při které by úplná nebo částečná nefunkčnost sytému (jako důsledek narušení bezpečnosti informací v informačním systému) mohla mít negativní vliv na funkčnost orgánu veřejné správy nebo na narušení provozu prvku (např. elektrárny) kritické infrastruktury.

Dále se v určujících kritériích mluví také o tom, že informační systém provozovaný obcí nebo hlavním městem Praha není významný informační systém a proto tyto obce nemusejí vytvářet bezpečnostní dokumentaci.

Kapitola 3

Představení hodnocených systémů

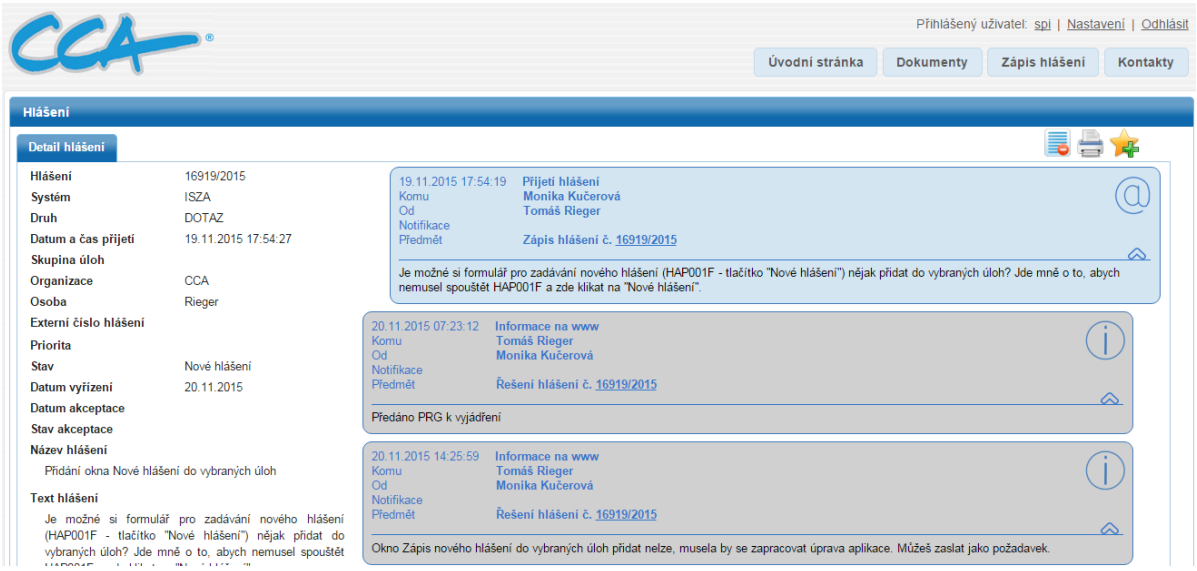
V této sekci bych rád přiblížil dva informační systémy firmy CCA Group a.s. (dále jen CCA), které slouží jako ilustrační příklady v této práci. Prvním systémem je Webový HelpDesk, přes který zákazníci hlásí svoje požadavky, připomínky, náměty i chyby programů. Druhým systémem je interní informační systém zákaznické administrace (ISZA), ve kterém jsou uložena veškerá hlášení, komunikace se zákazníkem i veškeré informace od přijetí hlášení přes vývoj až po samotnou distribuci zákazníkovi.

3.1 Webový HelpDesk

Tento Webový HelpDesk je určen jen pro zákazníky firmy CCA a umožňuje jim několik funkcionalit, a to podávat nová hlášení přes webové rozhraní, doplňovat k již zaslaným hlášením zprávy, prohlížet hlášení zaslaná jinými uživateli, avšak jen ty, ke kterým mají nastaven přístup v uživatelském účtu. Poslední funkcí je možnost prohlížet dokumenty, které byly vystaveny pro konkrétní systém poskytovaný firmou CCA.

Webový HelpDesk také zobrazuje pro zákazníky různá oznámení a probíhající změny, které na HelpDesk vkládají pracovníci Hotline CCA. Tyto informace jsou zde zejména pro informování zákazníka o aktuálních činnostech a událostech, které se týkají práce se systémy od firmy CCA.

Dále přiblížím jednotlivé části Webového HelpDesku, aby bylo zřejmé, co všechno HelpDesk nabízí a co všechno v něm může uživatel (zákazník) nastavit a přes něj odeslat.



Obrázek 3.1: Ukázka prostředí Webového HelpDesku

Začnu stránkou **Nastavení**, na které si zákazník může nastavit, jaké informace se mu budou zobrazovat na hlavní stránce (např. počet záznamů na stránce, jestli se mají zobrazit novinky, atp.). Dále si zde může nastavit svoje kontaktní údaje (jméno, příjmení, telefon, email) a určit, zda mu budou chodit na jím zadaný email informační emaily přímo z webového HelpDesku. Na tento email může zákazníka kontaktovat přímo CCA v případě řešení nějakého jeho požadavku.

Po úspěšném přihlášení (jméno a prvotní heslo je nastaveno pracovníky Hotline CCA) se zákazníkovi zobrazí **úvodní stránka** Webového HelpDesku, která se skládá ze čtyř částí a to z Hlavičky, bloku Novinky, bloku Hlášení a z bloku Sledovaný obsah.

Nyní bych uvedl krátký popis každé zmíněné části.

- V Hlavičce je uveden aktuálně přihlášený uživatel. Dále se zde nacházejí volby sloužící k přesunu na jednotlivé stránky:
  - volba pro přesun na domovskou stránku zastoupená tlačítkem Úvodní stránka
  - volba pro přesun na sekci Dokumenty
  - volba pro navigaci na stránku pro vložení (Zápis) nového hlášení
  - volba pro zobrazení kontaktních údajů na Hotline CCA a také na jeho provozní dobu.
- Blok Novinky obsahuje v záhlaví volbu pro Vyhledávání, která otevře stránku, na které je zákazníkovi umožněno vyhledávat ve zveřejněných novinkách. Pod záložkami Oznámení, Změny a Vše najde zákazník informace vystavené na Webovém

HelpDesku, dále pod záložkou Změny nalezne vystavené změnové balíčky (aktualizované balíčky) a pod záložku Vše najde zákazník jak novinky, tak i všechny zveřejněné aktualizace programů.

- V bloku Přehled hlášení jsou důležité zejména tyto tři záložky a to Sledovaná hlášení, Všechny hlášení a Nezpracovaná hlášení. V části Sledovaná hlášení vidí zákazník hlášení dané organizace pro systém, který si zákazník nastavil v sekci Nastavení. Dále jsou zde zobrazena ta hlášení, která si zákazník označil jako svoje oblíbené. V části Všechny hlášení se zobrazují hlášení všech organizací, které požívají stejný systém jako aktuálně přihlášený zákazník. Nastavení parametrů v nastavení pro zobrazení jednotlivých hlášení o všech organizacích pro daný systém provádí CCA podle smlouvy nebo dohody se zákazníkem.

- V sekci Sledovaný obsah se zákazníkovi zobrazuje obsah Webového HelpDesku, který je vystavován společností CCA. Každý zákazník si může v Nastavení v sekci Sledovaný obsah přizpůsobit zobrazení obsahu podle svých požadavků. Obsah se zde zobrazuje jen v malých náhledech, ve kterých je uveden jen nadpis a datum vystavení a prvních 150 znaků obsahu. Po rozkliknuti nadpisu zákazníkem se zobrazí celá zpráva se všemi informacemi.

Další částí Webového HelpDesku je část Dokumenty, která je uložena spolu s obsahem HelpDesku v adresářové struktuře. V ní se nachází seznam všech složek, který je tvořen názvy systémů, se kterými má zákazník možnost pracovat. Každá tato složka má určeny čtyři základní podsložky, jsou to:

- Distribuce

  Zde jsou umístěny distribuce systému a aktualizační balíčky (patche), které byly nahrány na Webový HelpDesk mimo termín řádné distribuce.

- Příručky

  Tato složka slouží pro ukládání uživatelských příruček a případně další uživatelské dokumentace. Pokud se vyskytnou dokumenty určené zákazníkovi, které nelze zařadit do žádné ze čtyř standardních kategorií, tyto dokumenty se umístí do podsložky Ostatní v této části (Příručky).

- Realizační týmy

  Složka slouží pro ukládání podkladů pro následné jednání realizačních týmů daného systému.

- Trvalé dokumenty

  Zde jsou uloženy dokumenty trvalého charakteru, které jsou neměnné pro daný systém.

- V další části adresářové struktury je umístěn archiv novinek vystavených na Webovém HelpDesku.

Další část Webového HelpDesku se věnuje Detailu hlášení. Pokud zákazník otevře stránku s detailem hlášení, zobrazí se úplné informace o tomto konkrétním hlášení. Zákazník jich samozřejmě může mít v jeden okamžik více. Na tuto stránku je možné se dostat ze všech míst Webového HelpDesku, kliknutím na číslo a ročník hlášení. V detailu hlášení je přehledně a zřetelně zobrazena probíhající komunikace mezi zákazníkem a HelpDeskem CCA.

Další sekce se věnuje vyhledávání a to jak v hlášeních, tak i v dokumentech. Zákazník má při vyhledávání hlášení k dispozici velmi podrobný filtr, ve kterém lze nastavit velké množství parametrů, které následně vytvoří omezující podmínky pro dotaz nad všemi hlášeními. Jen pro ukázku uvedu některé parametry, které lze nastavit: Číslo hlášení, Systém (pro jaký systém chce zákazník vidět hlášení), Organizace (pole pro výběr konkrétní organizace) a Priorita.

Posledními částmi HelpDesku jsou Zápis nového hlášení a Zpětná vazba od zákazníků. Zákazník vytvoří nové hlášení pomocí tlačítka Zápis hlášení, které je dostupné v hlavičce stránky. Podle typu přihlášeného zákazníka se zobrazí buďto webový formulář pro vytvoření nového hlášení nebo jen dvě tlačítka, která mu dají na výběr mezi odesláním formuláře ve formátu PDF nebo odesláním přes webový formulář. Jestliže se zákazník rozhodne pro tvorbu hlášení použít webový formulář, dojde k automatickému předvyplnění polí Firma a Kontaktní osoba podle aktuálně přihlášeného uživatele. Pokud dojde následně k odeslání hlášení prostřednictvím webového formuláře, je tomuto hlášení okamžitě přiděleno evidenční číslo hlášení a toto hlášení se zobrazí na HelpDesku. Když zákazník odešle hlášení přes PDF formulář, je nutné nejprve toto hlášení zaevidovat pracovníkem Hotline CCA.

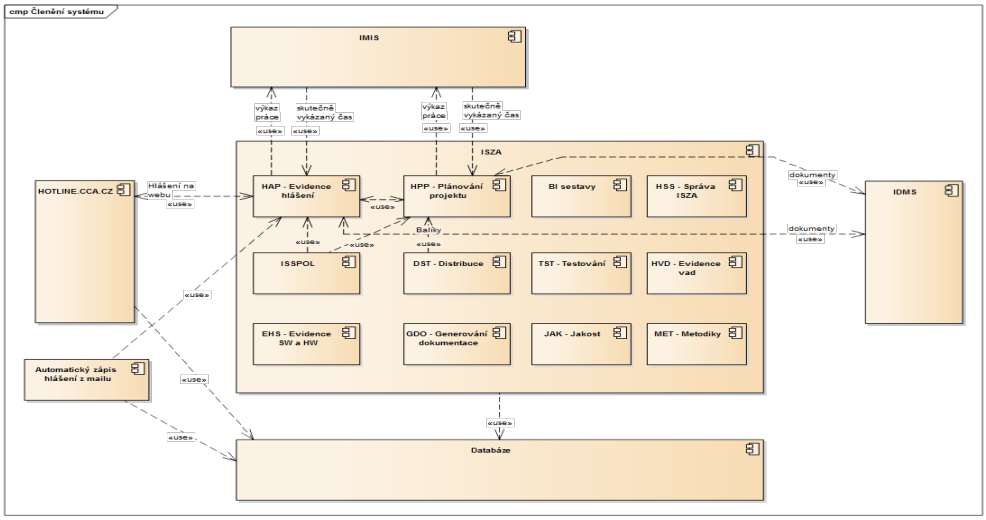
Automatický zápis hlášení usnadňuje práci operátorkám na HelpDesku tím, že převádí informace z přijatého hlášení ve formě emailu rovnou do ISZA do modulu starajícího se o správu hlášení a požadavků (modul HAP). Je ale nutné splnit základní předpoklady pro správné fungování převodu z emailu do modulu HAP. Prvním předpokladem je potřeba znalosti uživatele, potažmo zákazníka. Druhým předpokladem je dodržení správného formátu posílaného emailu s hlášením. V případě, že není formát emailu zcela správný, systém se alespoň pokusí převést část dat do modulu HAP, aby opět ulehčil práci operátorkám.

Část Zpětná vazba se zabývá automatickým zasláním emailu zákazníkovi po vyřešení jeho hlášení spolu se žádostí o poskytnutí zpětné vazby. Zákazník má v emailu na výběr ze tří možností a to, že byl s řešením spokojen bez výhrad, spokojen s výhradou anebo že nebyl spokojen vůbec. Po výběru některé ze tří možností se zákazníkovi otevře stránka s detailem tohoto hlášení, na které má možnost se ještě dodatečně vyjádřit k průběhu

řešení jeho hlášení.

3.2 ISZA - Informační systém zákaznické administrace

Tento interní informační systém slouží pro správu požadavků a hlášení od všech zákazníků firmy. Systém umožňuje uchovávat kompletní historii komunikace mezi firmou a zákazníkem. Telefonní ústředna firmy je také napojena na tento systém. Dále systém nabízí funkci umožňující sledovat průběh vyřizování jednotlivých hlášení. Je pak možné sdělit zákazníkovi, (pokud by kontaktoval firmu se žádostí o informaci o průběhu řešení jeho požadavku), ve které fázi se aktuálně nachází jeho požadavek, zda se testuje nebo už je připraven k distribuci. S tím souvisí také další možnost, kterou systém ISZA nabízí - je možné zákazníkovi sdělit, pokud by se o to zajímal, v jakém releasu (vydané verzi programu) mu firma dodala funkcionalitu, na kterou se ptal. Systém ISZA také umožňuje zjistit, alespoň přibližně, zda byl dodaný program ziskový nebo naopak.

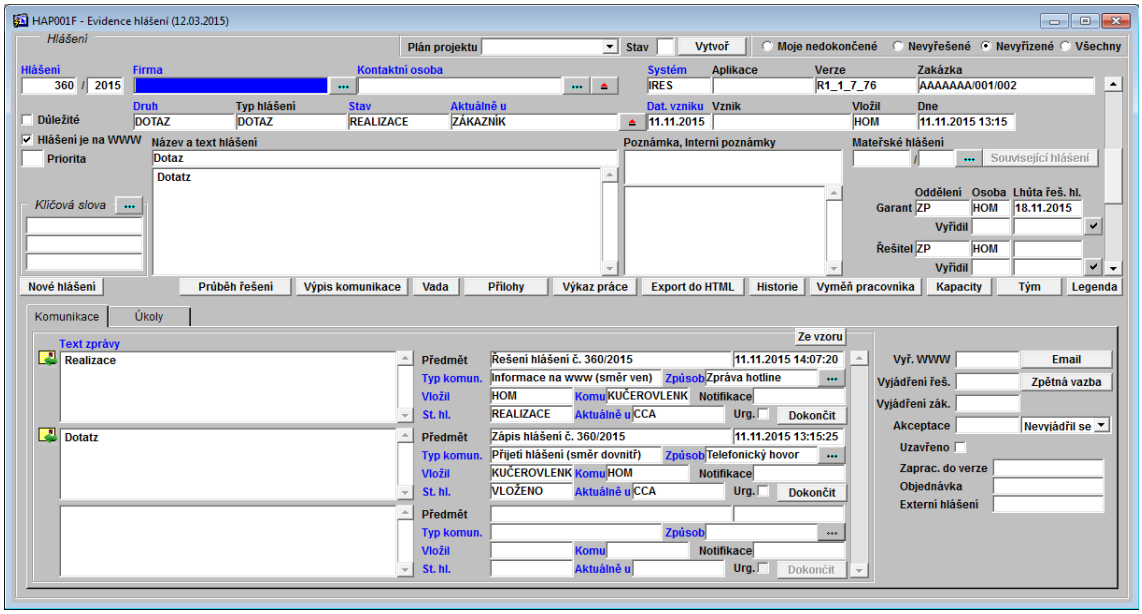


Obrázek 3.2: Přehled modulů systému ISZA

Systém ISZA se skládá z těchto modulů:

- Modul HAP - Hlášení a požadavky (Evidence hlášení)

  V modulu jsou uloženy kompletní informace o jednotlivých hlášeních, např. o garantovi a řešiteli. Garant hlášení ručí za to, že zákazník dostane to, co od firmy požadoval ve svém hlášení (požadavku) a že s tímto výsledkem bude spokojen. Řešitel hlášení zodpovídá za vyřešení hlášení, které může vyřešit sám nebo jeho řešení přidělit někomu jinému. Řešitel však nese zodpovědnost za to, že dojde k vyřešení hlášení a k dodání výsledku zákazníkovi včas a v požadované kvalitě. Hlavním (nejdůležitějším) formulářem tohoto modulu je Evidence hlášení (obrázek 3.3), ve které jsou uvedeny jak úplné údaje o zákazníkovi, textu hlášení, tak také o stavu řešení požadavku, o přiložených přílohách k hlášení a také o historii komunikace se zákazníkem k tomuto konkrétnímu hlášení.



Obrázek 3.3: Ukázka prostředí ISZA - formulář Evidence hlášení

- Modul HPP - Plánování požadavků

  Tento modul obsahuje zejména formuláře, přes které se zadávají úkoly, které je nutné splnit pro vyřešení hlášení, a také se zde evidují požadované výstupy. V oddělení výroby se naplánují jednotlivé kroky, které vedou ke splnění hlášení. Tyto kroky (činnosti, které je nutné vykonat) nejčastěji vedou k vytvoření potřebné dokumentace a k vytvoření programového kódu. Jednou z částí tohoto modulu je formulář Pracovní stůl, který slouží pracovníkům jako přehled úkolů, na kterých mají pracovat pro splnění konkrétního hlášení nebo požadavku. S prací

na úkolech také úzce souvisí plánování kapacit, které je řešeno samostatným formulářem umožňujícím pohled na vytíženost jednotlivých zaměstnanců. Formulář slouží ke zjištění, jací zaměstnanci jsou dostupní, a je možné jim přidělit práci na úkolech.

- Modul BI (Business Intelligence) sestavy

  Tento modul se stará o generování sestav nad Oracle BI, které obsahují reporty o tom, zda firma plní směrem k zákazníkovi. Dále se zde nacházejí sestavy zobrazující trendy a fungování testů, zda probíhají v pořádku nebo zda končí neúspěšně kvůli chybám v programovém kódu.

- Modul HSS - Správa ISZA

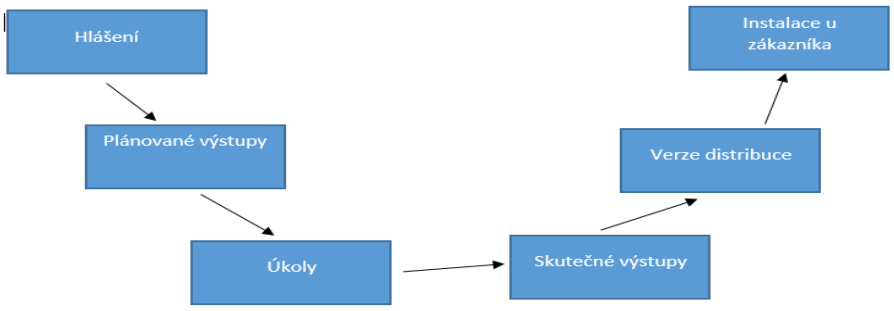
  Tento modul obsahuje veškerá nastavení, kterými lze měnit chování systému ISZA. Tento modul je menší než většina jiných modulů a sdružuje v sobě správcovské utility (nástroje). Modul obsahuje uložené dotazy SQL (dotazovací jazyk pro relační databáze) a nabízí každému zaměstnanci možnost, uložit si svoje často prováděné dotazy.

- Modul ISSPOL - Informační systém pro společnou část

  V modulu jsou uloženy všechny přístupové role k systému ISZA, dále jsou zde vedeny parametry nastavení jednotlivých aplikací. Jedná se tedy o centrální správu práv a nastavení. Nachází se zde formulář Seznam jmen, který obsahuje informace o zákaznících firmy (kontakty na zákazníky) a také o pracovnících firmy CCA.

- Modul DST - Distribuce

  Tento modul navazuje na předchozí modul pro evidenci hlášení a pro plánování projektů. Díky informacím v tomto modulu je firma schopná, po obdržení dotazu od zákazníka, předat zpět odpověď s vysvětlením, jak bylo jeho hlášení vyřešeno a případně v jaké verzi produktu byly jeho požadavky vyřešeny. Pokud ale zákazníkem navrhované změny ještě nebyly vyřešeny, firma mu sdělí, v jaké verzi produktu je může očekávat. Dále modul umožňuje zjistit, u konkrétní aplikace (ať už funkce nebo tabulka), kdy došlo k jejím změnám a také proč se tyto změny udály. Jsou zde také uloženy informace o všech podprogramech (existujících programech u zákazníka), které se nacházejí v celém projektu, který je nasazen u zákazníka. Díky těmto informacím dokáže firma zajistit, aby nedošlo u zákazníka k nějakým problémům, které by mohlo způsobit vzdálené nahrání např. opravy na zákazníkem nahlášenou závadu. Firmě jde tedy o zajištění funkčnosti systémů a také toho, aby nedošlo nahráním této opravy k narušení běhu programů u zákazníka.



Obrázek 3.4: Proces zpracování požadavku

- Modul TST - Testování

  Modul Testování eviduje všechny testy od jejich definic až po samotné provedení. V modulu existují 2 role: test analytik a samotný tester. Test analytik má za povinnost vymyslet, jak otestovat daný program, a připravit testovací scénáře (jak provádět příslušné testy). Naproti tomu tester provádí již samotné testování podle předpřipravených scénářů. Tester má možnost spustit testy přímo z úkolu. Testování se skládá z těchto činností:

  - testovací případ

    Udává, co se bude testovat (například vkládání různých hodnot do pole pro rodné číslo).

  - testovací scénář

    Obsahuje jednotlivé kroky nutné pro otestování produktu.

  - testovací plán

    Udává, kdy bude probíhat testování a co všechno bude součástí tohoto testování.

  Ještě je potřeba vysvětlit pojem testovací milník. Pojem označuje konkrétní datum, na které je naplánováno provedení připravených testů.

- Modul HVD - Evidence vad

  Modul obsahuje nalezené nebo nahlášené vady, které byly objeveny zejména při vývoji. Vady je nutné nejen znát, ale i se zabývat jejich odstraněním z výsledného produktu.

- Modul EHS - Evidence SW a HW

  Tento modul byl vytvořen administrátory firmy pro jejich vlastní účely, protože bylo pro ně důležité vědět o všech aplikacích, které běží jak ve firmě, tak i u zákazníků. Tito administrátoři se ve firmě starají o správný chod všech systémů,

databází a také telefonů. V této evidenci jsou uvedeny veškeré licence programů třetích stran a v jakých verzích se tyto programy aktuálně nachá-zejí (například databáze Oracle 12c relaese 1, Windows 7). Další částí evidence je pracovní deník. Do deníku mají pracovníci (administrátoři) povinnost zapisovat veškeré zásahy a popisy toho, co prováděli na firemních serverech, konkrétní situace na daném serveru, proč byl na něm nutný zásah a v neposlední řadě informaci o době výpadku tohoto serveru.

- Modul GDO - Generování dokumentace

  Modul vznikl pro potřeby generování sestav z Oracle Case nástroje a slouží pro generování projektové dokumentace.

- Modul JAK - Jakost

  Tento modul se věnuje měření kvality jak programu, tak i dokumentace. Firma měří kvalitu nejčastěji podle počtu chyb v programu. U dokumentace má firma potíž ohodnotit její kvalitu. Modul také obsahuje checklisty (seznamy otázek), které si čte akceptant (přejímá produkt) - může se jednat o zákazníka, tak i o programátora ve firmě, a odsouhlasí například zadání až ve chvíli, kdy mu plně rozumí. Pokud nerozumí jen jedné části, zadání úkolu nepřijme. Přijme ho ve chvíli, kdy odsouhlasí veškeré otázky v příslušném seznamu. Otázkami, které se nacházejí v těchto seznamech, udává vedení firmy to, co je pro ně důležité. V současné době má firma v tomto modulu k dispozici více než 3 500 otázek.

- Modul MET - Metodiky

  Modul vznikl za účelem potřeby spojit proces změn směrnic a metodik zároveň se změnami systému ISZA, protože docházelo k situacím, že se v systému ISZA objevily nové formuláře, ke kterým ale chyběly metodiky a popis, jak s nimi pracovat. Je také snaha postupně přesunout veškeré směrnice a metodiky do tohoto modulu, aby byly dostupné na jednom místě a bylo možné v nich vyhledávat. Metodiky jsou v tomto modulu členěny způsobem, že se nejprve odehraje nějaká událost a na ní navazují příslušné činnosti, které se mají následně provést pro vyřešení této události.

Nad systémem ISZA se nachází Webový HelpDesk (hotline.cca.cz), který čerpá data právě z ISZA.

Kapitola 4

Bezpečnostní dokumentace

4.1 Bezpečnostní politika

4.1.1 Systém řízení bezpečnosti informací

Vyhláška 316/2014 Sb. vyžaduje jako první věc řízení rizik, kterému je věnována samostatná kapitola Analýza rizik uvedená dále.

Vyhláška požaduje vytvoření a schválení bezpečnostní politiky, která bude obsahovat následující části: hlavní zásady, cíle, bezpečnostní potřeby a práva a povinnosti ve vztahu k řízení bezpečnosti informací. Následně je potřeba provádět aktualizace hodnocení aktiv a rizik, samotné bezpečnostní politiky, plánu zvládání rizik a plánu na rozvoj bezpečnostního povědomí uživatelů ve firmě. Maximální doba je stanovena vyhláškou na tři roky nebo je možné tuto dobu změnit a to v souvislosti s prováděnými nebo plánovanými změnami.

4.1.2 Organizační bezpečnost

V této sekci se hovoří o vytvoření výboru pro řízení kybernetické bezpečnosti a příslušných rolí s danými právy a povinnostmi, které souvisí s významným informačním systémem. Je nutné stanovit následující bezpečnostní role a to manažera, architekta, auditora kybernetické bezpečnosti a také garanta aktiva. Podle vyhlášky 316/2014 Sb. musejí mít všechny osoby vykonávající tyto role praxi po dobu nejméně tří let. Tyto pracovníci ve výboru i v jednotlivých rolích musí mít také zajištěna pravidelná odborná školení.

Pro firmu CCA tvoří výbor pro řízení kybernetických bezpečnostních událostí vedení firmy. Bezpečnostní role spolu s jejich popisem jsou následující:

- manažer kybernetické bezpečnosti

  osoba odpovědná za systémy řízení bezpečnosti informací

- architekt kybernetické bezpečnosti

  osoba zajišťující návrh a implementaci bezpečnostních opatření

- auditor kybernetické bezpečnosti

  osoba provádějící audit kybernetické bezpečnosti

- garant aktiv

  fyzická osoba pověřená firmou k zajištění rozvoje, použití a bezpečnosti aktiva

4.1.3 Klasifikace a řízení firemních aktiv

Metody identifikace a následné ohodnocení všech aktiv jsou již uvedeny v sekci týkající se řízení rizik (kapitola 5.3).

4.1.4 Bezpečnost lidských zdrojů

Cílem bezpečnosti lidských zdrojů je zejména snížení pravděpodobnosti rizika lidského selhání, také možné krádeže nebo zneužití zařízení poskytnuté zaměstnanci firmou. Je nutné stanovit plán na rozvoj bezpečnostního povědomí uživatelů, který bude obsahovat formu, obsah a rozsah školení, které jsou potřeba pro zvýšení informovanosti všech zaměstnanců. Dále je nutné stanovit osoby, které budou provádět tato školení a činnosti uvedené v plánu. Také je nutné v souladu s plánem zajistit pomocí vstupních a pravidelných školení poučení jednotlivých uživatelů, správců a osob zajišťujících bezpečnostní role o jejich povinnostech a o bezpečnostní politice. Dále je potřeba uvést jakým způsobem (potažmo jak často) je zajišťováno dodržování bezpečnostní politiky administrátory, uživateli a osobami zastávajícími bezpečnostní role. Také musí být uvedeno, že po ukončení pracovního poměru musí dojít k odebrání přístupových práv a k navrácení svěřených aktiv. V této sekci je nutné vést záznamy o proběhlých školeních, ve kterých budou informace o předmětu školení a seznamu osob, které tato školení absolvovaly.

Ve firmě je stanoven systém směrnic a metodik, které důkladně popisují pravidla pro chování uživatelů. Dále je stanoven systém školení, ve kterém jsou uvedeny další informace o tom, kteří zaměstnanci a jak často se musejí účastnit školení. Školení jsou prováděna formou průběžných školení jednou za rok a to prostřednictvím elektronických kurzů a testů. Proběhlá školení se zapisují do Evidence školení a také do systému pro řízení výuky, školení (LMS - Learning Management System). Veškeré informace o proběhlých školeních se společně se záznamy v LMS systémech zapisují do papírové evidence.

Pokud dojde k nějaké změně ve směrnici nebo v metodice, je samozřejmě potřeba neodkladně informovat zaměstnance (uživatele). K tomu se používá nejprve nejrychlejší

způsob - rozeslání informace o změně elektronickou zprávou (email) všem uživatelům. Další možností, jak informovat uživatele o změnách, je prezentace těchto změn na pravidelných firemních schůzkách.

Ve firmě je zabráněno uživatelům pomocí přístupových oprávnění v přístupu ke všem zdrojům (zejména datům) firmy. Je tedy zřejmé, že každý uživatel má přístup jen k omezené části zdrojů, které potřebuje pro vykonávání svojí práce.

Kontrolu (vizitu) plnění vybraných ukazatelů provádí ředitel zákaznické podpory pravidelně jednou za týden. Stejně často je prováděna kontrola toho, jak jsou plněny úkoly se vztahem k zákazníkovi, jestli jsou firmou dodržovány termíny (např. dodání nového produktu), které byly domluveny se zákazníkem.

Pokud dojde k odchodu nebo k přijetí nového zaměstnance, použijí se pravidla a postupy stanovené ve směrnici "Pravidla při nástupu a odchodu pracovníka". Tato směrnice udává přesné kroky, které je nutné podniknout při nástupu nebo odchodu pracovníka. Příkladem těchto kroků může být např.: při nástupu - přidělení přístupových oprávnění do systémů a ke zdrojům, při odchodu - odebrání veškerých práv a odebrání z Evidence zaměstnance. Nemůže se stát, aby zaměstnanec, který odešel sám nebo dostal výpověď, byl schopen nějakým způsobem poškodit firmu (vzdáleně se připojit k systému a poškodit v něm obsažená data).

4.1.5 Fyzická bezpečnost

Tato sekce pojednává o zajištění bezpečnosti samotné firmy a zejména o zamezení vstupu neoprávněných osob do vymezených prostor (místností). Je možné pro zjištění bezpečnostních opatření klást následující otázky:

Jaká se konkrétně používají opatření pro zabránění přístupu cizích osob do určených místností, ve kterých se zpracovávají informace a kde jsou umístěna technická aktiva informačního systému?

Jaká opatření se používají pro zabránění poškození a zásahům do určených (vymezených) prostor, kde jsou uložena data informačního systému a kde se nacházejí servery (technická aktiva)?

Jakým způsobem se předchází poškození, krádeži nebo zneužití aktiv?

Jak se zabrání tomu, aby někdo přerušil chod systému?

Firma CCA si nepřála uvádět žádné informace o způsobech zajištění fyzické bezpečnosti.

4.1.6 Řízení provozu a komunikací

V této sekci se hovoří především o tom, jaké nástroje je potřeba použít na detekci kybernetických událostí a následné vyhodnocování získaných informací.

Ve firmě jsou používány antivirové produkty pro ochranu počítačů uživatelů. Tento antivir je spravován centrálně a uživatelé nemají potřebná práva na jeho deaktivaci. Poštovní server spolu s firemní sítí je chráněn firewally. Je také nutné říci, že není umožněn veřejný přístup z vnějšího prostředí do sítě firmy CCA. Proto je nutné použít pro přístup do vnitřní sítě VPN.

Dále jsou stanovena následující pravidla pro zajištění bezpečného provozu informačního systému:

- Práva a povinnosti osob, které jsou v bezpečnostních rolích, administrátorů a také uživatelů.

  Veškerá práva a povinnosti osob jsou uvedeny ve směrnici "Katalog funkcí", kde jsou přesně specifikována. Další informace k právům a informacím jsou uvedeny v ostatních směrnicích a metodikách.

- Postupy pro spuštění a ukončení chodu systému, dále postupy pro restart a obnovení po pádu

  Pro firmu je nejdůležitější co nejdříve opravit a spustit vnitřní infrastrukturu. Z toho důvodu je ve firmě sepsaný postup udávající přesné kroky pro spuštění systémů (serverů) po pádu. Většina systémů je nastavena tak, že se dokáže zotavit sama.

- Zajištění sledování bezpečnostních událostí a přístupu k těmto zázna-mům?

  Pro sledování bezpečnostních incidentů nebo jen problémů v síti nebo v systému se používá ve firmě standardní systém logování. Pokud nastane nějaký problém, zaměstnanec má povinnost napsat záznam o tomto problému do bezpečnostního deníku. Firma následně provádí pravidelné (jednou za měsíc) vyhodnocování zpráv zapsaných v deníku a přijímá opatření podle závažnosti zjištěných incidentů.

- Možnosti kontaktu osob poskytujících podporu při řešení nepředvídatelných systémových nebo technických potíží.

  Firma má zavedenou technickou pohotovost, která stanovuje pravidla pro postup při zjištění nějakých technických problémů. Zejména jsou zde uvedena telefonní čísla na osoby, kterým má zaměstnanec v případě problému (typicky neběží server) volat. Tito lidé drží službu většinou od šesti hodin ráno až do jedenácti hodin večer a mají za tuto pohotovost příplatky.

- Sledování, plánování a řízení kapacit lidských a technických zdrojů.

  Ve firmě existuje oddělení lidských zdrojů, které se spolu s vedoucími středisek zabývá sledováním kapacit lidí. Funguje zde také systém vykazování, do kterého

zaměstnanci vykazují svoji práci. Díky tomuto přístupu má vedoucí oddělení přehled, jací lidé jsou přetížení nebo mají naopak práce málo. Následně se může rozhodovat, zda bude nutné přijmout další zaměstnance nebo těm, kteří mají málo práce, přidělit nějakou další práci.

4.1.7 Řízení přístupu k datům a bezpečné chování uživatelů

V této sekci je nutné stanovit pravidla pro přístup k informačním systémům a pravidla pro přidělování jednoznačného identifikátoru (uživatelského účtu) každému zaměstnanci. Dále je potřeba stanovit opatření, která zajistí bezpečné uložení přihlašovacích údajů jak zaměstnanců, tak i administrátorů a zajistí, že nedojde k jejich zneužití.

Ve firmě existuje směrnice "Pravidla chování uživatelů v prostředí CCA", která upravuje problematiku přihlašování a ukládání přihlašovacích údajů. Dále je zde systém zabezpečení, který se stará o přihlašování a také o přidělení práv jen k té části systému, ke které má mít uživatel přístup. Ověření identity uživatele probíhá běžným způsobem autentizací (je ověřena jeho identita - většinou jménem a heslem) a autorizací (dostane přidělen přístup jen k vybraným datům a k části systému).

4.1.8 Zálohování a obnova dat

V sekci Zálohování je potřeba uvést požadavky na zálohování a obnovu dat, dále stanovit pravidla a postupy pro samotné zálohování a pro bezpečné ukládání vytvořených záloh. Poté je vhodné stanovit pravidla a postupy pro obnovu záloh a pro testování funkčnosti zálohování a obnovy.

Zálohování probíhá v reálném čase replikou dvou úložišť mezi dvěma domy, avšak toto zálohování naráží na omezenou kapacitu úložišť vlastněnými firmou. Nejvíce kritická data se replikují okamžitě. Jednou denně se všechna data zálohují na magnetické pásky, které se jednou týdně odvážejí do banky. Zde se tyto pásky uchovávají v průměru půl roku, ale i zde záleží na povaze dat, jak dlouho zde zůstanou. Nejdůležitější data zůstávají uložené v bance nejméně deset let.

Pro následnou obnovu dat má firma stanoveny tři kategorie podle závažnosti a důležitosti dat, které udávají, za jak dlouho dojde k obnově dat:

- u nejvíce kritických dat - obnova do dvou hodin
- u méně důležitých dat - obnova do dvou dnů
- u zbývajících dat - obnova do dvou týdnů a déle

Firma také provádí recovery (obnovení) testy, kterými si chce ověřit především to, zda je vůbec schopná provést obnovu v jí stanoveném čase a zda se podaří obnovit všechna data z provedených záloh.

4.1.9 Poskytování a nabývání programových licencí

Do této sekce je potřeba uvést pravidla a postupy pro nasazení programového vybavení a pro kontrolu dodržování licenčních podmínek.

Nákup licencí a instalování programů na počítače uživatelů řídí opět směrnice udávající pravidla chování. Je v ní zejména uvedeno, za jakých podmínek si může uživatel nainstalovat různé programy na svůj pracovní počítač a také jaké postupy musí zaměstnanec dodržet, pokud by si chtěl koupit nějaký program.

4.1.10 Ochrana osobních údajů

Ochrana údajů i dat jak jednotlivých uživatelů, tak i dat celé firmy je realizována pomocí přístupových oprávnění (více kapitola 4.1.7).

4.1.11 Používání kryptografické ochrany

V této sekci by měla firma určit, jaké prostředky pro šifrování používá pro zabezpečení komunikace nebo uložených dat.

Šifrovací algoritmy se rozdělují do dvou skupin a to na symetrické a asymetrické (vysvětlení dále). Symetrické šifry se nejčastěji používají pro ochranu uložených dat na discích serverů a uživatelských stanic. U těchto šifer se používá pro proces šifrování i dešifrování jen jeden klíč. Nejznámější šifra z této skupiny je AES (Advanced Encryption Standard). Tuto šifru uvádí i příloha číslo 3 k vyhlášce 316/2014 Sb., která jí považuje za bezpečnou při použití klíčů délek 128, 192 a 256 bitů. V případě AES se jedná o blokovou šifru, kde se vždy šifruje celý blok o velikosti 128 bitů. Pokud se stane, že je dat méně než 128 bitů a tedy by některé bity byly prázdné, doplní se nulami do délky 128 bitů.

V kryptografii existují algoritmy zajišťující zároveň integritu i pravost zprávy (autenticitu). Mezi nejpoužívanější patří algoritmy HMAC (keyed-hash message authentification code), které spojují použití běžné hash (otisk vstupních dat získaný matematickou funkcí) funkce (MD5, SHA-1, SHA-2, SHA-256) spolu s tajným klíčem. Je možné použít jen samotné hash funkce pro kontrolu integrity (kontrolní součty, otisky zprávy) zpráv, zda nedošlo k nějaké nežádoucí změně v průběhu přenosu. To je možné díky tomu, že stejný obsah (text) dává pořád stejný hash, při použití stejné hash funkce. Tedy jinak řečeno, odesílatel si vytvoří ke svojí zprávě otisk pomocí hash funkce a odešle ho spolu s textem zprávy příjemci, který si vytvoří znovu hash přijaté zprávy a

pokud se jeho hash bude rovnat s tím, který mu poslal odesílatel, může si být jistý, že je zpráva v pořádku.

Vyhláška 316/2014 Sb. ve své příloze číslo 3 zřetelně uvádí seznam hash funkcí, které je možné použít. Mezi nejznámější funkce patří SHA-224, 256, 384 z rodiny SHA-2 a hash funkce z rodiny SHA-3, konkrétně SHA3-224, 256, 384 a SHA3-512.

Pro bezpečnou komunikaci s firmou je silně doporučeno používat zabezpečené spojení využívající HTTPS protokol. Protokol se skládá ze dvou částí: z běžného HTTP (Hypertext Transfer Protocol) protokolu a z části zajišťující šifrování a zabezpečení transportní vrstvy (TLS Transport Layer Security - v aktuální verzi 1.2). Použitím TLS se dostáváme k dalším oblastem šifer a to k asymetrickým šifrám, které jsou sice výpočetně náročnější, avšak zajistí bezpečné přenesení šifrovacího klíče (pro symetrickou šifru) přes nezabezpečený kanál. Slouží jen pro dohodnutí šifrovacího klíče a po jeho přenesení se celé následné spojení šifruje již rychlou symetrickou šifrou, nejčastěji AES s klíčem délky 256 bitů. Pro použití HTTPS je ale nutné mít na serveru validní certifikát (prokazuje pravost stránek i toho, že jsme opravdu majiteli domény nebo veřejného klíče uvedeného v certifikátu) vydaný důvěryhodnou certifikační autoritou. V protokolu TLS se používá více typů šifer, jak pro ověření digitálního podpisu, tak pro dohodnutí šifrovacího klíče.

Pro technologii digitálního podpisu se používají tyto algoritmy:

- DSA (Digital Signature Algorithm) s využitím klíčů o délce 2048 bitů

  Tento algoritmus je široce používaný pro digitální podpis. Na výběr máme tyto hašovací funkce: SHA-1 a SHA-2. Oproti ECDSA používá větší klíče (2048 bitů oproti 224 bitům), což ve výsledku znamená větší velikost samotných podpisů i přenášených dat.

- ECDSA (Elliptic Curve Digital Signature Algorithm) s klíči o délce 224 bitů

  ECDSA je novějším a méně náročnějším algoritmem než DSA. Umožňuje používat pro podpis kratší klíče a dosáhnout menší velikosti přenášených dat spolu s původními daty.

Je tedy zřejmé, že algoritmům založených na eliptických křivkách postačuje klíč s daleko menší velikostí (224 bitů oproti 2048 bitům), ale stále se stejnou úrovní bezpečnosti.

Pro dohodnutí se na šifrovacím klíči se nejvíce používal algoritmus DH (Diffie-Hellman) s klíči o délce nejméně 2048 bitů (existuje ještě DHe, kde písmeno e představuje dočasnost (Ephemeral), která udává povinnost vždy vygenerovat nový šifrovací klíč, tedy není možné v případě kompromitace serveru dešifrovat již proběhlou komunikaci), ale v dnešní době je často nahrazován modernějším algoritmem ECDHe (Elliptic Curve Diffie-Hellman), kde postačuje používat klíče o délce 224 bitů a delší. Tento protokol

je často provozován v kombinaci s asymetrickou šifrou RSA (Rivest Shamir Adleman), která je používaná pro podepsání výměny klíčů prostřednictvím ECDHE.

Šifra RSA jako zástupce asymetrických šifer funguje na principu dvou klíčů, z nichž je jeden veřejný a druhý tajný (soukromý). Soukromým klíčem dojde k podepsání vyměňovaných informací a následně veřejným klíčem si může každý klient zkontrolovat jejich pravost. Soukromý a veřejný klíč jsou spolu těsně svázány. Zprávu, kterou zašifruje odesílatel, je možné rozšifrovat jen veřejným klíčem (obvykle vystaven na důvěryhodném zdroji - např. webová stránka), který byl vytvořen současně se soukromým klíčem. Bezpečnost této šifry je založena na velmi složitém matematickém výpočtu (faktorizace velkého čísla vzniklá ze součinu dvou velkých prvočísel), který se ale pomalu stává řešitelným z důvodu neustálého zvyšování výpočetního výkonu počítačů. Proto není doporučováno používat šifru RSA s klíči o délce 1024 bitů (je velké riziko, že již byla prolomena), ale raději s klíči 2048 bitovými a delšími.

Všechny výše uvedené šifry splňují minimální požadavky na kryptografické algoritmy uvedené v příloze číslo 3 vyhlášky 316/2014 Sb.. Tato příloha obsahuje přehled šifrovacích algoritmů, které je možné použít pro zabezpečení komunikace a dat v systémech firmy. Já jsem zde uvedl pouze ty nejpoužívanější a nejznámější. Vyhláška také zcela jasně vymezuje případy použití hashovací funkce SHA-1 (není již považována za bezpečnou), a to pouze pro ověřování existujících digitálních podpisů a časových razítek. Dále je možné tuto hash funkci používat pro vytváření a ověřování HMAC-SHA-1 a také pro již existující pseudo náhodné generátory čísel.

Vyhláška uvádí rovněž případy, ve kterých se SHA-1 nesmí používat a to:

- pro generování nových digitálních podpisů a časových razítek
- pro použití v aplikacích vyžadující bezpečnou hash funkci

Hash funkce se obecně považuje za bezpečnou, pokud pro ni nejsou známy nalezené kolize (kolizní bloky). Ty znamenají možnost vytvořit pro dva různé zdrojové texty stejný hash (otisk). Pokud se toto provede, nelze již považovat zvolenou hash funkci za bezpečnou.

Jen pro příklad bych uvedl konkrétní podobu šifrovaného spojení používaného na stránkách hotline.cca.cz pro zajištění bezpečné komunikace zákazníků s Hotline firmy:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Veškerá firemní komunikace je standardně šifrovaná. Firma má svoji vlastní certifikační autoritu pro vnitřní záležitosti, která disponuje podrobnou politikou, ve které jsou popsány postupy pro vytvoření certifikátu a pro používání šifrování. Telefony zaměstnanců nejsou šifrované vůbec. Paměťové karty (ani flash disky uživatelů) v těchto telefonech nejsou šifrované zejména z důvodu, že v nich zaměstnanci nenosí

nic důležitého. Pokud by došlo ke krádeži telefonu zaměstnance za účelem připojit se do firmy a odcizit nějaká data, útočník by toho nebyl schopen z důvodu, že heslo vyžadované pro připojení přes VPN není nikdy uloženo přímo v telefonu. Přenášená data prostřednictvím VPN není možné po cestě jakkoliv odposlouchávat nebo s nimi manipulovat.

4.1.12 Ochrana před škodlivým kódem

Informace o používaných bezpečnostních opatřeních pro zajištění ochrany před škodlivým kódem jsou uvedeny v sekci 4.6 Řízení provozu a komunikací.

Firma provádí pravidelnou a účinnou aktualizaci antivirů (definic, signatur) a firewallu.

4.1.13 Nástroj pro detekci kybernetických událostí

Pro detekci bezpečnostních událostí v síťovém provozu se nejčastěji používají IDS systémy (Intrusion Detections Systems - systémy pro detekci narušení), které jsou v současné době nahrazovány systémy IDPS (Intrusion Detection and Prevention Systems - systémy pro detekci a případné zablokování škodlivé činnosti). Nejprve bych vysvětlil IDS systémy a poté IPS (IDPS) systémy.

Systém pro detekci narušení může existovat ve dvou podobách: jako samostatné zařízení nebo jako aplikace běžící na vybraném serveru. V obou případech systém provádí dohled nad síťovým provozem a nad aktivitami samotného systému, kde se snaží identifikovat škodlivé činnosti nebo možné porušení zásad. Pokud zjistí nějaký problém, podává hlášení administrátorům sítě. Je tedy možné pohlížet na IDS systém jako na systém, který běží nad všemi firewally, antivirovými programy, routery a servery a který dokáže vyhodnocovat informace získané z logů z těchto aplikací a serverů.[18]

Systémy pro detekci narušení se dělí:

- na síťově orientované (network-based IDS)

  Síťově orientované IDS se starají o sledování provozu v síťovém prostředí a snaží se v něm odhalit škodlivé aplikace nebo narušení sítě pomocí signatur chování (ukazatel špatného chování, se kterým se porovnávají zjištěné události). Tyto signatury mají uložené ve svých databázích a podle nich systém pozná, jaké chování lze považovat za správné a jaké již za špatné.[18]

- na ty, které provádějí ochranu koncových stanic (host-based IDS)

  Systémy na ochranu koncových stanic se starají o ochranu systému v síti a jejich působení je z toho důvodu na počítačích připojených do sítě nebo také na serverech. Obrana těchto stanic probíhá, podobně jako u síťově orientovaných

IDS, pomocí signatur, se kterými se porovnávají informace zjištěné při kontrole operací a souborového systému.[18]

- a na distribuované IDS

  Distribuovaný IDS funguje na principu rozmístění množství senzorů v rámci celé sítě, které pokud zjistí nějakou odchylku od normálu, tuto informaci předají svému řídícímu systému. Pro maximalizaci úspěšných detekcí narušení se vyplatí používat jak systémy síťově orientované (monitorující síťové prostředí), tak i systémy kontrolující narušení koncových stanic.[18]

V těchto systémech se používají pro detekci hrozeb narušujících síť dva různé způsoby: detekce signatur a detekce anomálií.

Detekce signatur zde funguje na stejném principu jako u antivirových programů, kde dochází k porovnání obsahu vstupujícím do sítě s již obsaženými signaturami (vzory špatného chování) v IDS systému. Pokud dojde k nalezení shody mezi vzorkem dat a signaturou, IDS systém tuto situaci neprodleně ohlásí odpovědným osobám. S tím však souvisí nevýhoda spočívající v tom, že systém není schopen rozeznat novou hrozbu či škodlivý kód, pokud ho nemá ve své databázi signatur.

Druhým způsobem je snaha o detekci anomálií v síťovém provozu, kde se systém IDS snaží identifikovat abnormální chování hlídaného systému. Pro svoji činnost systém používá pravidla, která určují normální a abnormální chování (heuristiky), za účelem odhalení odklonu systému od normálního stavu. Systém obsahuje sady pravidel říkající, jak vypadá normální provoz v síti, např. jaká je většinou využita šířka pásma, jaké protokoly se nejčastěji používají a jaké porty nebo zařízení jsou k sobě běžně připojeny. Pokud následně zjistí špatné chování systému (anomálii), tedy že došlo k výraznému odchýlení od normálního stavu, je systém sám schopen přijmout opatření pro zastavení tohoto narušení (např. zablokováním této přicházející komunikace ve firewallu nebo ohlásí zjištěný problém správci systému).[18]

Druhou velkou skupinou jsou IDPS (Intrusion Detection Prevention Systems - systémy na detekci a prevenci před narušeními), které jsou, opět jako IDS systémy, zařízeními pro zajišťování síťové bezpečnosti, jejichž úkolem je monitorovat síť a chování systémů a vyhledávat v nich podezřelé aktivity, které by mohly naznačovat probíhající útok na cílový systém. Mezi hlavní činnosti těchto IDPS systémů patří zejména identifikace podezřelé aktivity, následné ukládání informací o těchto aktivitách (logování), v případě potřeby zablokování příchozí komunikace způsobující narušení v síti a v neposlední řadě informování odpovědných osob. Na samotný systém IDPS lze pohlížet jako na rozšíření funkcionality systému IDS, protože se oba dva systémy zaměřují na monitorování síťového provozu, ve kterém se snaží nalézt podezřelou aktivitu. Hlavním rozdílem oproti normálním IDS systémům (které jen detekují podezřelé chování a

nahlásí ho správcům sítě) je to, že IPS systémy jsou schopny aktivně bránit případným narušením, které objeví v síťovém provozu, nebo je rovnou zablokovat. Blokaci narušení může IPS provést několika možnými způsoby: od poslání výstražné zprávy správcům sítě, přes zahazování škodlivých paketů, až po resetování nebo blokování příchozí komunikace z určitého rozsahu IP adres. Systémy IDPS také umí opravit chyby v kontrolních součtech (CRC - Cyclic Redundancy Check) a také odstranit nevyžádaný síťový provoz přicházející do kontrolované sítě.[19]

Systémy pro prevenci narušení (IPS - Intrusion Prevention System) je možné rozdělit do následujících kategorií:[19]

- Síťové IPS systémy (Network-based intrusion prevention system) - zabývají se monitorováním celé sítě a odhalováním podezřelé aktivity prostřednictvím analyzování protokolů síťové aktivity.
- IPS systémy pro bezdrátové sítě (Wireless intrusion prevention system) - provádějí monitorování bezdrátových sítí a hledání podezřelé aktivity pomocí analyzování protokolů používaných v bezdrátových sítích.
- Analýza síťového chování (Network behavior analysis) - hledá v síťovém provozu podezřelé datové toky (netypické chování), které by mohly způsobovat hrozby útočící na cílovou síť jako např. DDoS (zahlcení síťového prvku značným množstvím paketů z velkého počtu strojů (IP adres)) útok nebo malware (počítačový virus určený pro vniknutí do systému) v různých formách.
- IPS systém na koncové stanici (Host-based intrusion prevention system) - zde se jedná o samotný program nainstalovaný na koncové stanici (počítači), který se zabývá hledáním podezřelé aktivity pomoci analyzování událostí vzniklých na tomto stroji.

V této kapitole (4.1.13) se bude nacházet popis systémů (IDS nebo IDPS nebo jiných), které firma používá pro monitorování sítě a hledání podezřelé aktivity v této síti, aby zabránila nebo alespoň minimalizovala následky možných útoků na její síť. Tento nástroj, pokud je používán, by měl mít za úkol zajištění ověřování, kontroly a případného zablokování komunikace mezi vnitřní a vnější sítí.

Pro detekci bezpečnostních incidentů ve firmě CCA se kromě informací získaných z antivirových programů a firewallů, používají také záznamy systému Windows o proběhlých událostech.

Tato politika je pravidelně hodnocena z hlediska její účinnosti a aktualizována.

4.2 Analýza rizik

Analýzou rizik se rozumí kontrolní metoda zabývající se včasným odhalením možných rizik, které se týkají činnosti orgánu veřejné správy, identifikováním těchto rizik a určováním míry těchto rizik (zjištěním jak je nalezené riziko významné pro naše aktiva). Tato míra se určuje zejména podle velikosti nežádoucího dopadu na aktiva spolu s pravděpodobností, že se riziko projeví. Nalezená a ohodnocená aktiva by se měla následně předat k vyhodnocení příslušným lidem z vedení firmy, kteří poté na základě zjištěných informací o závažnosti rizik rozhodnou o tom, jakým způsobem se bude firmy snažit odstranit nebo alespoň zmírnit možný dopad těchto rizik. Firma se s nejvyšší prioritou zabývá riziky, která jsou pro firmu kritická nebo vysoká, protože by realizace těchto rizik vedla k velkým finančním ztrátám případně až k vážným existenčním potížím firmy.

V průběhu této analýzy si firma musí stanovit způsob přijetí rizika a také jeho stupeň významnosti. Tyto rozsahy významnosti jsou uvedeny v sekci Výpočet významnosti rizika, kde jsou uvedeny dvě běžně používané metody a jedna upravená pro potřeby firmy CCA. Dále je vhodné, podle zjištěných hodnot rizik, vytvořit taková opatření, která se budou snažit minimalizovat možné dopady rizik na firemní aktiva např. tím, že odstraní existující zranitelnosti umožňující vznik rizika.[7]

Na tomto místě bych uvedl pojmy, se kterými budu pracovat v analýze rizik. Mezi nejčastěji používané pojmy patří zejména tyto:[16]

- **Aktivum**

  Za aktivum je běžně považováno všechno ve firmě, co má nějakou hodnotu pro firmu, a může být sníženo nebo poškozeno právě působením hrozby na tato aktiva. Aktiva se rozdělují do dvou velkých skupin:

  - na aktiva hmotná - kam patří například domy vlastněné firmou, firemní servery s uloženými daty, počítačové vybavení kanceláří,
  - a nehmotná - kam patří např. informace o zákaznících, jejich hlášení, projektová dokumentace a informace o průběhu testování produktů firmy.

  Aktivem může být i firma sama, protože je možné, že hrozba bude působit přímo na existenci této firmy. Základní charakteristikou aktiva je jeho hodnota, kterou je možné získat objektivně pomocí vyjádření ceny, na kterou si ho firma cení, anebo subjektivně určením toho, jak je pro ni toto aktivum důležité. Při následném hodnocení aktiv firmy je dobré brát na zřetel zejména tato hlediska:[16]

  1. jak velké byly pořizovací náklady tohoto aktiva

2. jak je pro firmu toto aktivum důležité a zda jeho poškození neohrožuje existenci firmy
3. zda má firma dostatek finančních prostředků pro případ, že by došlo k poškození aktiva
4. za jakou dobu je firma schopná odstranit následky rizik na firemních aktivech

- **Hrozba**

  Příkladem hrozeb, které působí na aktiva firmy a mají na ně nežádoucí dopad, jsou zejména různé události, živelné pohromy, poruchy firemních serverů, výpadky elektrické energie, ale také možný odchod klíčového zaměstnance. Hrozby mohou být náhodné nebo úmyslné a pocházet mohou jak z vnějšího prostředí firmy, tak i přímo zevnitř firmy (např. chyba zaměstnance). Jako dopad hrozby na některé aktivum se označuje škoda, která je způsobena touto hrozbou při jejím vypuknutí a ohrožení aktiva. Velikost tohoto dopadu může být stanovena podle hodnoty ztrát, do kterých se započítávají náklady potřebné na opětovné obnovení funkčnosti postiženého aktiva. Nebo podle nákladů potřebných na likvidaci všech následků způsobených hrozbou.[16]

  V našem případě jsme si stanovily tyto faktory, podle kterých budeme hodnotit úroveň hrozby:

  – Pravděpodobnost hrozby - jak často se může hrozba stát skutečností a ohrozit naše aktiva
  – Dopad - jak velké následky způsobí hrozba našemu aktivu
  – Zranitelnost - jak rychle se dokážeme vzpamatovat z poškození aktiva hrozbou a opět obnovit funkčnost aktiva
  – Odhalení - tento faktor jsme si stanovili sami a udává, jak rychle a zda vůbec přijdeme na to, že na naše aktiva působí nějaká hrozba

- **Zranitelnost**

  Zranitelnost je možné definovat jako slabé místo aktiva nebo nedostatek v jeho ochraně, který může způsobit nežádoucí stav, kdy jedna nebo více hrozeb zneužije tuto slabinu a poškodí aktivum. Následně určíme hodnotu zranitelnosti, která nám bude udávat, jak je naše aktivum náchylné na působení konkrétní hrozby. To, že jsme odhalili nějakou zranitelnost našich aktiv, ještě neznamená, že existují hrozby, které by mohly tuto slabinu zneužít a způsobit škodu na našich aktivech. Pokud takové zranitelnosti, na které jsme neidentifikovali prozatím žádné hrozby, máme, není ihned nutné stanovovat opatření, ale stačí jen tyto slabiny monitorovat a hlídat, zda se v čase nemění. Slabinu mohou tvořit i špatně zavedená či

nefunkční opatření. Existuje zde také možnost, že nalezneme nějaké hrozby, pro které neidentifikujeme žádné zranitelnosti. Díky tomu nemusí být tato hrozba pro naše aktiva rizikem a není tak nutné se jí věnovat. Zranitelnost vznikne vždy tam, kde je možnost, že dojde ke vzájemnému působení aktiva a hrozby. Zranitelnost má opět svoji úroveň, která se získá z hodnot podle těchto faktorů:[16]

  - Citlivost - jak je jednotlivé aktivum náchylné na poškození danou hrozbou
  - Kritičnost - jak je pro naši firmu toto aktivum důležité

- **Protiopatření**

  Protiopatřením se rozumí postup nebo také proces, který byl účelně zřízen pro to, aby v případě expozice hrozby snížil její působení na aktivum, případně snížil její dopad. Tato opatření se navrhují zejména pro to, aby pomohla předejít možnému vzniku škody na aktivu nebo pro přežití doby potřebné pro vyřešení následků způsobených touto hrozbou.

  V analýze rizik je opatření definováno z hlediska efektivity a nákladů. Pod efektivitou se skrývá informace udávající, o kolik toto opatření sníží účinek příslušné hrozby. Tento ukazatel efektivity opatření se používá zejména ve fázi zvládání rizik jako jeden z podstatných parametrů používaných pro ohodnocení, jak je vhodné použít právě toto opatření. Opatření se používají ve více oblastech, zejména v oblasti starající se o snížení úrovně hrozby, zmenšení hodnoty zranitelnosti a následků po působení této hrozby. Opatření se také používají pro identifikování nežádoucího vlivu zejména proto, aby se rychle a včas přišlo na probíhající hrozbu a zabránilo se jejímu plnému spuštění. Poslední oblastí, kterou se opatření zabývají, je oblast starající se o obnovení aktiv po poškození hrozbou.

  Další složkou opatření používanou při analýze rizik jsou náklady, do kterých patří náklady vynaložené na pořízení, uvedení do provozu a následné používání těchto opatření.[16] Důležitá činnost prováděná v průběhu analýzy rizik je identifikace již implementovaných opatření. Slouží především k tomu, abychom nezaváděli znovu opatření, která už ve firmě máme, a také aby nedošlo k jejich nepříznivému ovlivňování s již zavedenými opatřeními. Může ale nastat situace, že dojde k selhání použitého opatření, a proto je potřebné mít stanovená dodatečná opatření k již určenému účinnému řešení námi nalezených rizik.

- **Riziko**

  Riziko je nejčastěji charakterizováno mírou ohrožení aktiva nebo mírou udávající nebezpečí, že se aktivuje hrozba a dojde tak k nežádoucímu efektu, který může vést až k poškození našeho aktiva nebo i více aktiv. Velikost námi nalezených

rizik (i obecně) je vyjadřována jeho úrovní získanou nejčastěji vynásobením hodnot příslušného aktiva a hrozby. Tyto výpočty spolu s ukázkovými výpočty budou analyzovány dále v části zabývající se výpočtem významnosti rizika. Riziko vznikne v ten okamžik, kdy na sebe vzájemně začne působit hrozba a aktivum. Při analýze rizik je zřejmé, že nemusíme brát vůbec v úvahu hrozby, které žádným způsobem neohrožují naše aktiva. Podle stejné logiky nemusíme při analýze rizik uvažovat aktiva, která nejsou ohrožena žádnou z identifikovaných hrozeb.

Celková úroveň rizika je poté stanovována hodnotou aktiva (jak je toto aktivum důležité a cenné pro firmu), hodnotou hrozby (ve vzorcích uvedených níže se pracuje s hodnotou pravděpodobnosti hrozby) a také hodnotou zranitelnosti.

Výslednou míru rizika ovlivňuje růst hodnot jak u aktiva, tak i u zranitelnosti a hrozby, ale pouze zavedení opatření může snížit výslednou míru rizika. Pokud budeme navrhovat nějaká opatření, je důležité si uvědomit, že má smysl zavádět jen ta opatření, jejichž velikost nákladů použitá na jejich zavedení a používání je přiměřená hodnotě aktiv, která se těmito opatřeními snažíme chránit. Tedy nemá smysl zavádět opatření např. v ceně sto tisíc korun, když aktivum, které má chránit, má pro nás hodnotu jen deseti tisíc korun. S tímto postupem (pravidlem) na tvorbu opatření souvisí potřeba určit referenční hodnotu rizika. Ta nám říká, že pokud se míra rizika (hodnota) ocitne pod touto hranicí, riziko se prohlásí za zbytkové a již proti němu nepodnikáme žádné kroky (nezavádíme žádná opatření).

Dále je zde ještě jeden pojem a tím je referenční úroveň udávající hranici, podle které je riziko zařazeno do skupiny zbytkových rizik anebo do skupiny ostatních rizik. V této skupině jsou již rizika závažnější (jejich úroveň se nachází nad stanovenou referenční hodnotou aktiva) a je potřeba proti nim zavést opatření. Jde tedy o stanovení míry rizika, která nám vytvoří oddělující hranici.

Pro ukázku: hranice má stanovenou hodnotu pět a nalezené riziko hodnotu šest. Riziko se tedy nachází nad touto hranicí a jedná se o riziko, které je potřeba řešit. Ale pokud bude mít jiné riziko hodnotu čtyři, bude se jednat o zbytkové riziko a proti němu nebudeme muset použít žádné opatření. Platí zde podmínka udávající, že zvolená referenční úroveň by měla mít takovou hodnotu, aby dopad rizik nacházejících se pod touto hranicí, měl téměř zanedbatelný dopad na naše aktiva. Neměli bychom automaticky dávat přednost při vytváření opatření jen rizikům s nejvyšší úrovní, ale také dát pozor na situaci, kdy vetší množství rizik se střední závažností může vytvořit za určitých okolností daleko větší celková rizika než několik nalezených rizik s vysokou závažností.

Obecná analýza rizik se skládá z těchto kroků:[12]

- **Seznam aktiv**

  V tomto počátečním kroku je nutné shromáždit a zapsat, nejlépe do tabulky, všechna identifikovaná aktiva našeho systému. Stejně jsem postupoval i já spolu s panem Ing. Přibylem a paní Ing. Loutockou při hledání aktiv.

- **Hodnocení aktiv**

  V tomto kroku je potřeba buďto kvantitativně nebo kvalitativně určit náklady, které vzniknou při narušení dostupnosti, důvěrnosti a integrity. Toto oceňování by měl provádět vlastník (garant) příslušného aktiva.[12]

  Zde jsme ke každému aktivu přidělili hodnocení pro každé ze tří kritérií (důvěrnost, dostupnost, integrita). Ohodnocení bylo získáno od osoby (pana Ing. Přibyla), která zná velmi dobře zkoumaný systém. Po ohodnocení byla výsledná hodnota aktiva získána vypočtením váženého aritmetického průměru z těchto tří kritérií (důvěrnost, dostupnost a integrita).

- **Seznam hrozeb**

  Zde je nutné identifikovat možné hrozby, které mohou napadnout firemní aktiva a tyto hrozby uchovat (např. ve formě seznamu) pro jejich pozdější ocenění. Hrozby se nejčastěji hledají formou brainstormingu s pracovníky firmy, kteří mají o daném systému největší přehled.

  Zde jsme opět s pomocí odpovědných osob (pan Ing. Přibyl, paní Ing. Loutocká) sestavili seznam všech možných hrozeb, které mohou působit na náš systém (Webový HelpDesk).

- **Ohodnocení hrozeb**

  Při ohodnocování hrozeb se provádí určení úrovně hrozby, tedy s jakou pravděpodobností může daná hrozba nastat a poškodit firemní aktivum.[12]

  V tomto kroku jsme nejprve stanovili kritéria, podle kterých budeme hodnotit námi identifikované hrozby. Tři kritéria jsme převzali z přílohy č. 2 k vyhlášce 316/2014 Sb. a to dopad na aktivum, zranitelnost (v našem případě však rychlost vzpamatování se z narušení aktiva) a pravděpodobnost hrozby. Čtvrté kritérium stanovil pan Ing. Přibyl a to rychlost odhalení hrozby, tedy jak rychle a zda vůbec přijdeme na narušení aktiva. Zde jsme si stanovili vlastní stupnici:

  - od nízké (přijdeme na narušení aktiva do jedné hodiny)
  - přes střední (do jednoho pracovního dne)
  - až po vysokou (nepřijdeme na narušení aktiva)

Výslednou hodnotu u každé hrozby jsme získali vypočtením váženého aritmetického průměru ze všech čtyř kritérií.

- **Určení míry rizik**

  V tomto kroku je potřeba určit hodnotu pravděpodobnosti (rizika), že daná hrozba zneužije jednu nebo více zranitelností a poškodí tak aktivum firmy. Riziko je nejčastěji reprezentováno kombinací dvou faktorů a to pravděpodobností výskytu bezpečnostní události a velikostí jejího dopadu na aktiva.[12]

  V posledním kroku jsem sestavil matici rizik (nachází se v přiloženém souboru: "DP_Siroky_Vyhodnocena_Rizika.xlsx"na listu "Rizika", k diplomové práci) skládající se na svislé ose z nalezených aktiv a na horizontální ose z identifikovaných hrozeb. Jedno aktivum může být ohroženo více hrozbami a jedna hrozba může ohrozit více aktiv. Poté jsem do příslušných buněk, které odpovídaly tomu, že dané aktivum je ohroženo danou konkrétní hrozbou, vkládal výslednou míru rizika. Danou míru rizika jsem určil vynásobením hodnoty příslušného aktiva s hodnotou příslušné hrozby. Tímto jsem dostal vyplněné buňky jen tam, kde hrozba ovlivňovala aktivum. Tam, kde hrozby neovlivní aktiva, zůstaly buňky v matici prázdné. Stanovili jsme posléze stupnici hodnot, která nám určovala, jak je pro nás konkrétní riziko vážné a jestli musíme ihned podniknout určitá opatření pro zmírnění nebo eliminaci tohoto rizika.

  Stupnice je následující:

  - nízké riziko - rozsah hodnot 1,00 - 3,50
  - střední riziko - rozsah hodnot 3,51 - 5,00
  - vysoké riziko - rozsah hodnot 5,01 - 9,00
  - kritické riziko - rozsah hodnot 9,01 - 16,00

  Tímto jsme získali v matici závažnost jednotlivých rizik. Pro přehlednější zobrazení hodnot rizik v matici jsem doplnil do tabulky podmíněné formátování buněk, které každou neprázdnou buňku zbarvilo příslušnou barvou podle bodového ohodnocení rizika, tedy jeho závažnosti. Vysvětlivky barevných hodnot se nacházejí přímo v matici "Rizika"v souboru ""DP_Siroky_Vyhodnocena_Rizika.xlsx".

Analýzu rizik můžeme nejčastěji zpracovat ve dvou základních krocích:[23]

- Orientační analýza rizik

  Tato analýza slouží jen pro rozhodnutí o použití a zvolení vhodné metody pro následnou analýzu rizik v konkrétní firmě. Orientační analýza se provádí proto, abychom jako firma zjistili, která naše aktiva jsou pro nás nejdůležitější, a jejich poškození by nás zasáhlo nejvíce.

- Detailní analýza rizik

  Provedeme ji pouze pro dříve nalezená a pro nás důležitá aktiva pomocí některé z výše uvedených metod nebo i jejich kombinací. Tato varianta je na jednu stranu nejvhodnější, na druhou stranu nejdražší a časově nejnáročnější.

4.2.1 Metody analýzy rizik

Tyto metody se dají rozdělit do dvou skupin podle toho, zda se pro určení hodnoty rizika použije matematický výpočet nebo ohodnocení hodnotami ze stupnice s rozsahem např. od 1 do 5 (nebo pravděpodobnostní hodnotou 0 až 1). V analýze rizik je možné použít buďto jen jednu z těchto oblastí, nebo jejich vzájemnou kombinaci (např. jednu kvantitativní a jednu kvalitativní metodu).[22]

Kvalitativní metody

Metody patřící do této skupiny se vyznačují tím, že vyjadřují míru (hodnotu) rizika v předem stanoveném rozsahu (např. stupnice nízká až kritická, obodování v intervalu 1 - 10, nebo pravděpodobnost výskytu rizika 0 až 1). Příslušná úroveň každého rizika je nejčastěji odhadována pomocí kvalifikovaného odhadu (např. osobou, která zná dobře systém). Díky tomu je tato metoda daleko jednodušší a rychlejší než metody kvantitativní. Avšak určování hodnot jednotlivých rizik je značně subjektivní. Metoda může způsobovat problémy v oblasti zvládání rizik, protože nedokáže přesněji určit množství finančních nákladů potřebných ke zneškodnění rizika, neboť riziko ohodnotí jako vysoké až kritické, ale neřekne nám přesnou částku, se kterou bychom mohli dále počítat při zvládání tohoto rizika. Z důvodu absence přesného finančního vyjádření (kolik peněz bude potřeba) nastává problém s kontrolou efektivního zacházení s náklady.[20]

Příklad kvalitativní metody

Metoda účelových interview (metoda Delphi)

Tato metoda je nejběžnější variantou používanou v kvalitativních metodách a spočívá v řízené komunikaci mezi experty, kteří provádějí analýzu, a představiteli organizace, kteří znají systém, na kterém je prováděna analýza rizik. Existují i další metody založené na strojovém vyhodnocování značného množství dotazníků. Na rozdíl od nich používá metoda Delphi analýzu rizik pomocí souboru otázek, které se projednávají na účelových pohovorech. Tyto otázky se skládají z:

- z předem připravených otázek a z proměnné části, která se přizpůsobuje podle toho, jak probíhá rozhovor a také podle postavení respondenta

Při rozhovorech je zapotřebí dodržet to, aby se respondenti navzájem nepotkali, čímž je zajištěno vzájemné neovlivňování. Tato metoda má velkou výhodu v menší

náročnosti ve spotřebě zdrojů a času, díky čemuž nezdržuje pracovníky firmy od jejich práce. Použití metody Delphi pro analýzu rizik je vhodné zejména proto, že metoda určuje, co všechno se může stát a za jakých podmínek.[21]

Metodě Delphi je často vytýkána absence finančního vyjádření u jednotlivých rizik, které by pro firmu mělo větší vypovídající hodnotu než konstatování, že riziko je střední až vysoké. Na druhou stranu metoda nabízí iterační postup, při kterém jsou výsledky z předchozího kola pohovorů po nezbytném statistickém vyhodnocení předloženy respondentům, kteří tak dostanou možnost se k těmto výsledkům vyjádřit a říci, zda by chtěli své původní sdělení upravit nebo ho nechat v původní podobě. Následně jsou tito respondenti požádáni, aby k těmto souhrnným výsledkům zaujali stanovisko. Díky tomu dojde k prosazení těch nejpodstatnějších hypotéz, aniž by hrozilo riziko, že tito respondenti budou ovlivněni některým z dominantních pracovníků z jejich skupiny. Obecně se doporučuje provést dvě až tři opakování rozhovorů, ne však více, protože by mohlo dojít ke zkreslení dat kvůli statistické chybě této metody.[21]

Kvantitativní metody

Tyto metody jsou na rozdíl od metod kvalitativních založeny na matematickém výpočtu rizika z pravděpodobnosti výskytu hrozby a jejím dopadu na aktiva. Metody vyjadřují dopad na aktiva většinou pomocí velikosti nákladů (finančních prostředků), které mohou rizika způsobit. Nejčastěji se hodnoty dopadů udávají pomocí roční předpokládané finanční ztráty. Kvantitativní metody jsou na rozdíl od kvalitativních více objektivní, avšak jejich zpracování vyžaduje daleko více času a úsilí. Naopak nám tyto metody poskytnou peněžní vyjádření nalezených rizik, které nám určí přesněji závažnost těchto rizik a umožní nám tak jejich následné zvládání.[20]

Tyto metody mají několik nevýhod. Mezi ně patří zejména větší časová náročnost na samotné provedení, určení výsledků a také příliš formální přístup. To může vést až k zahlcení osoby provádějící analýzu velkým objemem dat, který je důsledkem složitého a komplexního přístupu k analýze.

Shrnutí vlastností kvantitativních metod:[20]

- jsou založeny na matematickém výpočtu míry rizika
- jsou více exaktní, ale také náročnější na čas a úsilí
- na rozdíl od kvalitativních metod poskytují vyjádření rizika pomocí peněžních prostředků

Příklady kvantitativních metod

1. **Metodika CRAMM (CCTA Risk Analysis and Management Methodology)**

Tato metodika je zřejmě nejznámější a také hojně používaná jako uznávaný nástroj pro analýzu rizik pokud je potřeba, aby naše metoda byla v souladu s českou normou ČSN ISO/IEC 13335 a také s mezinárodní normou ISO/IEC 17799. Původně byla metoda vyvinuta jen pro potřeby vlády Velké Británie, ale dnes se již používá téměř ve všech státech. Analýza rizik prováděná pomocí CRAMM řeší následující činnosti:[22]

- ohodnocení aktiv systému
- rozdělení nalezených aktiv do logických skupin
- nalezení hrozeb působících na tato aktiva
- nalezení a prozkoumání zranitelností systému a také určení požadavků týkajících se bezpečnosti pro každou skupinu aktiv

Na základě nalezených rizik a identifikaci jejich stavu je navržena množina bezpečnostních opatření, která jsou upravena podle úrovně nalezených rizik a podle toho, jaká již existující systémová opatření máme k dispozici (jsou již implementována).[22]

Podstatným prvkem této metody je to, že se vždy zkoumá jen model určité části systému, a nikoliv přímo samotný systém. Pro metodiku CRAMM je klíčově důležité získat výsledky strukturovaných rozhovorů s klíčovými osobami z firmy, na kterých je prováděna analýza. Velkou nevýhodou této metodiky je bohužel její cena, která nepatří k nejnižším, a proto je používána především odborníky, kteří se zabývají bezpečností, a ne běžnými uživateli ze strany běžných firem či státních orgánů.[22]

Další metody jsou již obecné metodiky pro kvantitativní analýzu rizik:

2. **Metodika @Risk**

   Tato metodika používá pro analýzu rizik simulační metodu Monte Carlo. Metoda zpracovává celou problematiku prostřednictvím tabulek, ve kterých se následně zaměňují nepřesné hodnoty za funkce, které jsou zde pro reprezentaci rozsahu možných hodnot. Zvolené souhrnné hodnoty se poté následně používají jako nástroj pro další rozhodování. Rozhodujícím faktorem je vytvoření návrhu modelu, v podobě tabulek určuje danou situaci systému. Jde vlastně o metodu z kvantitativního přístupu určující pravděpodobnostní rozdělení hrozeb a rizik v systému.[22]

3. **Metodika RiskPAC**

   Nástroj RiskPAC pro automatizovanou analýzu rizik dokáže nalézt hrozby v systému a pomáhat při opravování zranitelností, které mohou být těmito hrozbami

zneužity. Dále nástroj umožňuje automaticky provádět hodnocení nalezených bezpečnostních hrozeb a tím napovídat firmě, jaké kroky by měla provést ke zmírnění těchto rizik. Výhodou nástroje je velmi přehledné uživatelské prostředí vypadající jen jako dotazník, a proto je pro uživatele velmi snadné rychle odpovědět na otázky položené RiskPAC nástrojem.[10]

4. **RiskWatch**

   Tento nástroj je již přímo aplikací přinášející metodický seznam pro nalezení, vyzkoušení (simulaci) a změnu parametrů u identifikovaných rizik umožňující spustit simulaci znovu s již upravenými hodnotami rizik. Nástroj (metoda) je postaven na tvorbě modelu, který je vytvořen buďto ze získaných dat, nebo z výstupu simulační metody Monte Carlo. Obě předchozí možnosti lze kombinovat a doplňovat je informacemi z obou přístupů. Mluvíme o automatickém zpracování výsledků, které jsme získali na základě seznamu otázek strukturovaném podle předem určených bezpečnostních oblastí.[22]

5. **Hazard Operation Process - HAZOP**

   Česky se tato metoda označuje jako analýza ohrožení a provozuschopnosti, což znamená, že se v ní uplatňuje systematický a ucelený přístup k predikci toho, jak četná mohou být rizika a také, jaký by mohl být jejich dopad na aktiva, potažmo na celou firmu.[14] Tato metodika je založena na principu určení pravděpodobnosti možných ohrožení souvisejících s hrozbami (pohromami) a následném stanovení příslušných rizik. Hlavní cíl celé analýzy prováděné pomocí metody HAZOP je nalezení scénářů, při kterých může dojít k ohrožení způsobenému havárií nebo poruchou. Hledání těchto scénářů probíhá na setkání expertů formou brainstormingu. V průběhu setkání se experti zaměřují převážně na posouzení možných ohrožení a na provozní schopnosti systému (operability problems), které jsou předurčující pro bezpečnost celého systému nebo podniku. Pracovním nástrojem expertů při analýze jsou pracovní výkazy ve formě tabulek a také předem dohodnuté vodící výrazy (guidewords), pomocí kterých experti postupně odhalují nové neplánované nebo nepřípustné dopady. Ty následně experti formulují v závěrečném doporučení za účelem zlepšení celého procesu. Z toho ovšem vyplývá zásadní nevýhoda metody HAZOP - její velká časová náročnost, zejména pokud se do celého procesu brainstormingu zapojí větší množství expertů.[17]

   Metoda HAZOP byla nejdříve vyvinuta pro nalezení hodnot rizik v procesním podniku a pro následné určení problému ohrožující provoz, který by mohl potencionálně snížit efektivitu procesu (např. nedosáhl by své plné kapacity). Hlavní účel této metody je v pozorném a komplexním prozkoumání celého procesu nebo jednotlivé činnosti. Dalším krokem je stanovení, zda nalezené procesní odchylky

mohou způsobit nežádoucí dopady. Poté celý tým provádějící analýzu prochází a dále prozkoumává seznam pravděpodobných příčin a dopadů odchylky spolu se seznamem existujících opatření, kterými se snaží zamezit vlivu odchylky na proces nebo činnost. Pokud tým při zkoumání již zavedených opatření zjistí, že používané opatření neposkytuje dostatečnou ochranu proti odchylce, kterou již firma zná, doporučí většinou přijetí vhodného opatření za účelem snížení rizika, které by mohlo ohrozit firemní procesy. Mít k dispozici trénované a zkušené vedoucí je jednou z prvních podmínek pro zajištění účinné a kvalitní analýzy. Pokud je potřeba analyzovat velké a složité procesy, musí podnik zajistit tým pěti až sedmi lidí s patřičnými zkušenostmi (technolog, projektant, provozní údržbář, atd.) Nejčastěji jeden člen týmu vede celou analýzu, přičemž má k dispozici zapisovatele, který zaznamenává veškeré úvahy a nápady týmu. Pro jednodušší procesy lze sestavit týmy ze čtyř lidí, mající patřičné zkušenosti a technické dovednosti.[17]

Ostatní metody používané pro analýzu rizik

Pro nalezení, analýzu a řízení rizik lze použít například tyto metody:

1. **Stromový (systematický) diagram**

   Tento diagram zobrazuje celý systém rozložený na jednotlivé části ve stromové struktuře. Tato metoda slouží převážně pro popis skladby analyzovaného systému a je jednou z mnoha základních metod používaných pro strukturovanou analýzu. Výhodou této metody je její grafická podoba, ve které je prostřednictvím stromových diagramů zachycen rozklad systému na jeho jednotlivé části a prvky. Díky této stromové struktuře jsou srozumitelně a přehledně zobrazeny vzájemné vazby mezi jednotlivými částmi systému a také jejich vzájemné vztahy, tj. která část systému je podřízena jiné části systému. Takto získaný popis, vyjádřený stromovým diagramem, je přehledný a jednoduchý a je proto vhodný pro získání základní představy o systému, na kterém je prováděna analýza rizik.[22]

2. **Expertní metody**

   - **FMEA (Failure Mode and Effect Analysis)**

     Tato metoda (česky „Analýza možnosti vzniku vad a jejich následků“) umožňuje analyzovat v týmu možnosti vzniku závad u posuzovaného návrhu, hodnotit rizika těchto závad a navrhovat a poté uskutečňovat opatření, která by vedla ke zlepšení kvality samotného návrhu. Za dobu používání této metody bylo zjištěno, že za pomoci této metody je možné odhalit 70 až 90 % všech nesrovnalostí v původním návrhu. Metoda byla vytvořena v 60. letech minulého století ve Spojených státech amerických a její původní účel,

pro který byla vytvořena, sestával z analyzování spolehlivosti u složitých systémů zejména v oblastech kosmonautiky a jaderné energetiky. Pokud nasadíme metodu FMEA do reálného použití, dosáhneme např. těchto výhod:[8]

- zlepšení jakosti produktů zavedením systémového přístupu
- zmenšení výsledných ztrát
- zkrácení doby potřebné pro vývoj produktu, optimalizaci návrhu produktu
- snížení počtu požadovaných změn při probíhajícím vývoji
- ohodnocení rizikovosti případných vad a podle zjištěných rizik stanovení příslušných opatření
- podporování správného využívání dostupných zdrojů
- zlepšení výsledné spokojenosti zákazníka

Kromě výše uvedených výhod, má tato metoda i pozitivní efekt na ostatní zaměstnance, který spočívá v jejich motivaci ke společné práci a zodpovědnosti za provedené úkoly.[8]

3. **Mapy nebezpečí a rizik**

   Z výstupu této metody se dozvíme priority (tedy jakým rizikům se především věnovat z důvodu velké hrozby pro naše aktiva) jednotlivých rizik z hlediska jejich možného dopadu na firmu. Tyto informace (přehled z hodnocení významnosti rizik) poskytuje metoda v přehledném grafickém nebo tabulkovém znázornění.

   Metoda se například používala při zkoumání a hodnocení možného ohrožení a rizik v záplavových územích. Výhodou metody je to, že není potřeba kvantitativní odhadování způsobených škod, ale jen rozdělení rizika povodně do čtyř kategorií. Výstupem této metody jsou v prvním kroku mapy zobrazující ohrožení pomocí čtyřbarevné škály ploch, které jsou ohroženy záplavami.[11]

4.2.2 Řízení rizik

Jedna z možných definic uvedená ve zdroji [6] říká, že pokud chceme řídit rizika, která by mohla potencionálně ohrozit aktiva v naší firmě, znamená to pro nás provádět soustavně a opakovaně množinu navzájem provázaných činností. Tím, že se budeme snažit rizika řídit, dosáhneme:[6]

- snížení pravděpodobnosti, že se vyskytnou a způsobí škodu na našich aktivech,
- snížení jejich možného dopadu na naši společnost.

Mezi hlavní funkce řízení rizik patří zejména snaha předejít možným problémům, které by nás jako firmu mohly postihnout a pokusit se vyhnout použití krizového řízení.

Proces řízení rizik sestává ze čtyř fází, které jsou navzájem propojeny. Jsou to:[6]

1. identifikování rizik (kvalifikovanými osobami z firmy, které znají daný systém nejlépe)
2. zhodnocení (určení významnosti pro naši firmu)
3. zvládnutí rizik (přesněji snaha o umírnění jejich dopadu na firmu)
4. monitorování rizik (zda nehrozí nějaké nové riziko nebo zda je už určité riziko irelevantní z důvodu nasazení nového opatření).

Dále je potřeba odhadnout,

1. jak jsou aktiva firmy náchylná na hrozby, zjištěné v průběhu této analýzy
2. jaké se vyskytují slabiny umožňující těmto hrozbám negativně ovlivnit naše aktiva,
3. velikost následků na naší firmě v případě, že nějaká hrozba poškodí firemní aktivum.

Samotné řízení rizik znamená použít správné nástroje a postupy, které nám umožní snížit míru rizika na námi akceptovatelnou přijatelnou úroveň. Jedná se tedy o standardní postup jak identifikovat a posléze ohodnotit nalezená rizika (zjistit jejich závažnost pro aktiva) a stanovit vhodná opatření pro zmírnění jejich dopadu. Řízení rizik se neskládá jen z jedné činnosti, ale z více na sebe navzájem navázaných činností. Mezi ně patří

- ohodnocení (další činnosti, které je nutné provést, jsou identifikace, analýza a rozdělení priorit)
- vyhýbání se riziku
- zvládání rizika (sem spadají činnosti jako plánování, řešení a sledování)

Firma má možnost se případnému riziku úplně vyhnout a nedovolit riziku ohrozit firemní aktiva. Příkladem může být volba dražšího a spolehlivějšího poskytovatele internetového připojení, který má na rozdíl od levného poskytovatele, daleko méně výpadků připojení. Vyhýbání se rizikům není v praxi příliš reálné a je mnohem častější nalezená závažná rizika nejenom identifikovat, ale i zvládat.

Plánování rizik znamená, že budeme hledat způsoby, jak by bylo možné alespoň částečně zmírnit následky rizika, vymýšlet krizové scénáře a také časové plány pro

případ, že riziko nastane. Máme také ještě možnost určit odpovědné osoby za jednotlivá rizika. Naším cílem je se pokusit zmírnit rizika takovým způsobem, že už pro nás nadále nebudou představovat problém. Pokud tato rizika nedokážeme eliminovat, je nutné snížit alespoň jejich míru závažnosti (není už pro nás tak nebezpečné). Musíme také pamatovat na to, že se případná rizika nedokáží vyřešit sama a proto je nutné po fázi plánování začít fázi řešení rizik. V této fázi začne firma stanovené plány používat v reálném nasazení.

Závěrečnou fází k úplnému pokrytí rizik je fáze sledování rizik, ve které sledujeme fungování našich opatření a snah na zmírnění dopadu rizika. Nezůstaneme jen u nalezených rizik, ale stále budeme hledat nová rizika, která by mohla potencionálně ohrozit naše aktiva. Dále je potřeba aktualizovat priority u již identifikovaných rizik. Nemusíme se také zabývat riziky, která se nám podařilo zavedením opatření eliminovat nebo alespoň výrazně snížit jejich možný dopad na naše aktiva.[13]

Při hodnocení rizik nemusíme být přesní, stačí, abychom oddělili ta nejzávažnější rizika od těch, kterým nemusíme okamžitě věnovat pozornost. Je také možné si práci s hodnocením pravděpodobnosti výskytu rizika a jeho dopadu ulehčit a hodnotit je pouze na stupnici nízké, střední a vysoké.

V našem případě jsme ale používali u aktiv stupnice o čtyřech kritériích (nízké, střední, vysoké, kritické) a u hrozeb ještě navíc jednu stupnici o třech kritériích (nízké, střední a vysoké) pro určení rychlosti odhalení napadení aktiva.

Pro firmu je přínosné vytvořit plán zmírnění, ve kterém bude uvedeno, jakým způsobem, bude chtít firma řídit rizika. Jednou z možných strategií řízení rizik, je snižování pravděpodobnosti výskytu rizik a s tím související snižování možných následků těchto rizik. Je důležité zohlednit při tvorbě opatření jeho finanční náročnost, aby se nestalo, že do opatření, které by pomohlo předcházet riziku, vložíme 30 000 Kč a nakonec zjistíme, že v případě problému by byly škody vyčísleny na 15 000 Kč. Je vhodné si stanovit nouzový plán, abychom věděli, co dělat v případě, že by se vyskytlo (i přes vynaloženou snahu) některé z nejzávažnějších rizik. Pro každé řízené riziko je potřeba stanovit zodpovědnou osobu, která se postará o to, aby došlo k zavedení všech zmírňujících opatření do určitého termínu.[13]

Měli bychom si také zvyknout na pravidelné kontrolování rizik, která nám hrozí. Také bychom měli neustále a pečlivě sledovat přibližně deset nejzávažnějších rizik a zjišťovat, zda jsou námi zavedená opatření stále efektivní. Pokud dokončíme zavedení některého z opatření, je potřeba znovu určit pravděpodobnost a dopad příslušného rizika a následně obnovit seznam rizik a příslušné plány na řízení těchto rizik.

I přesto, že se nám podařilo zavést některá opatření, nemůžeme se spoléhat na to, že je riziko již eliminováno, ale je nutné ještě zkontrolovat, zda došlo ke zmírnění rizika na přijatelnou úroveň nebo k eliminaci rizika.[13]

4.2.3 Identifikace, hodnocení aktiv a hrozeb

Za aktivum se považuje cokoli v dané firmě, co má pro tuto firmu nějakou cenu. Může se jednat o hmotné (disky, počítače) i nehmotné (know-how firmy, data na serverech a v informačním systému) formy aktiv viz kapitola 4.2. Identifikace těchto aktiv nejčastěji probíhá formou brainstormingu, kde se lidé snaží navrhnout a vyčlenit aktiva, která se týkají informačního systému a případně i jeho okolí. Jako další metoda pro identifikaci aktiv nebo k doplnění již známých aktiv, lze použít rozhovor s klíčovými pracovníky firmy nebo také použití vlastních zkušeností jednotlivých zaměstnanců.

Tento postup jsme použili i my pro nalezení aktiv, hrozeb a jejich následné ohodnocení. Aktiva i hrozby jsem získal rozhovorem (brainstormingem) se dvěma zaměstnanci firmy CCA a to s panem Ing. Přibylem, který zná velmi dobře zkoumaný systém, a s paní Ing. Loutockou, která také pomohla s nalezením a doplněním některých aktiv a hrozeb. S ohodnocením aktiv a hrozeb mi opět velmi pomohl pan Ing. Přibyl, který určil hodnoty u jednotlivých aktiv z hlediska, jak jsou pro firmu důležitá a to samé provedl i u hodnocení hrozeb, kde jsme je hodnotili z hlediska, jak často mohou nastat a jak rychle se z nich dokáže firma vzpamatovat.

Aktiva se také dají členit do skupin z důvodu, že nemusí být důležité hodnotit některá aktiva samostatně v případě, že by jich byl velký počet, ale je výhodnější je dát do jedné skupiny, která je bude zastřešovat.

Aktiva se dělí do následujících skupin[5]:

- informační aktiva (informace)
- hardwarová aktiva (technické prostředky - hardware)
- softwarová aktiva (technické prostředky - software)
- poskytované služby informačním systémem

Identifikace aktiv našeho systému

Nejprve jsme se pokusili nalézt všechna možná aktiva, která náš systém může obsahovat. Pro hodnocení aktiv použijeme tato tři kritéria, díky kterým je možné zjistit a ohodnotit aktiva zejména podle toho, jak jsou pro nás důležitá a potřebná:

- důvěrnost (pouze oprávněné osoby mají umožněn přístup k těmto datům či službám)
- dostupnost (zajišťuje, že oprávněné osoby budou moci přistoupit k těmto datům či službám v okamžiku jejich potřeby)
- integrita (zajišťuje, že nedošlo k poškození dat v systému nebo při jejich přenosu a také se stará o to, aby data byla správná a úplná)

Dále jsme si stanovili stupnice pro následné hodnocení aktiv. Pro každé kritérium u každého aktiva jsme určili podle stupnice dopad, pokud by došlo u aktiva k porušení důvěryhodnosti, integrity a dostupnosti. V našem případě jsme se shodli na použití stupnic z přílohy číslo 1 k vyhlášce 316/2014 Sb., ve kterých se nacházejí tři kritéria pro hodnocení důvěrnosti, dostupnosti a integrity. Zmíněné tabulky, se stupnicemi a popisem jednotlivých úrovní, se nacházejí v sekci Zdroje a přílohy v tabulkách č. 6.1, 6.2 a 6.3. Stupnice budou mít čtyři úrovně začínající na nízké, střední, pokračující na vysoké a končící na úrovni kritická.

Uvedu zde jen názvy aktiv, která jsme v našem systému identifikovali. Jejich ohodnocení a míra dopadu se nachází v přiloženém souboru k diplomové práci: "DP_Siroky_-Vyhodnocena_Rizika.xlsx"na listu "Aktiva". Námi nalezená aktiva jsou rozdělena do čtyř skupin:

Tabulka 4.1: Přehled aktiv identifikovaných v systému HelpDesk firmy CCA

Informace		**Hardware**
Seznam zákazníků		Databázový server
Hlášení zákazníků		Webový server
Ostatní data		File systém ISZA
Testy		Komunikační kanály
Projektová dokumentace		Vnitřní infrastruktura
		Klientské stanice
Software		**Lidské zdroje**
Databázový server		Znalosti patřičných systémů
ISZA		Pracovníci hotline
HelpDesk		Ostatní pracovníci
Oracle Designer		
Share point		
Telefonní ústředna		
Zdrojové kódy		

Pro pozdější ukázku výpočtu míry rizika uvedu tabulku identifikovaných aktiv jen s 5 aktivy a jejich hodnocením. Pro následný výpočet celkové hodnoty aktiva jsme se rozhodli použít vážený průměr s následujícími vahami:

- pro důvěrnost jsme stanovili váhu 0,2,

- pro dostupnost váhu 0,4,
- a pro integritu váhu 0,4.

Tyto váhy byly takto stanoveny z důvodu, že je pro firmu důležitější u jejich dat a systémů, aby byly dostupné a obsahovaly integritní (správná) data než aby byla zajištěna jejich ochrana před zcizením nebo kompromitací (narušením důvěrnosti). Po stanovení vah bylo již možné vypočítat celkový dopad jednotlivých aktiv následujícím vzorcem, který má tento obecný tvar:

(váha důvěrnosti)*(hodnota důvěrnosti) + (váha dostupnosti)*(hodnota dostupnosti) + (váha integrity)*(hodnota integrity) = celkový dopad (hodnota) aktiva.

Uvedl bych také konkrétní příklad výpočtu hodnoty u aktiva Seznam zákazníků. Vzorec pro výpočet dopadu u Seznamu zákazníků má tento tvar:

$$0,2 * 3 + 0,4 * 2 + 0,4 * 1 = 1,80 \tag{4.1}$$

Pro ukázku uvedu hodnoty a celkové dopady 5 aktiv (v tabulce č. 4.2).

Tabulka 4.2: Identifikovaná a ohodnocená aktiva - ukázka

Název aktiva	Důvěrnost	Dostupnost	Integrita	Celkový dopad
Seznam zákazníků	3	2	1	1,80
Hlášení zákazníků	1	3	3	2,60
Ostatní data	2	2	2	2,00
Testy	2	1	2	1,60
Projektová dokumentace	2	3	2	2,40

Identifikace hrozeb našeho systému

Dále jsme se zabývali nalezením hrozeb v systému HelpDesk. K jednotlivým hrozbám jsme stanovili hodnoty z hlediska čtyř kritérií, pro tři z nich platí stupnice o čtyřech úrovních (nízká, střední, vysoká a kritická), které jsou uvedeny v kapitole Přílohy v části č. 3. Tři kritéria (pravděpodobnost hrozby, dopad a zranitelnost udávající, jak snadno se vzpamatujeme z narušení aktiv) jsme převzali z přílohy č. 2 z vyhlášky 316/2014 Sb.. Poslední, tedy čtvrté kritérium, jsme si určili sami a jedná se o odhalení, které má pouze tři úrovně (1 - přijdeme na narušení hned, 2 - přijdeme na to během dne a 3 - nepřijdeme na to vůbec).

Při hledání hrozeb jsme využili pro inspiraci hrozby ze seznamu uveřejněného ve zdroji [15]. Seznam hrozeb vychází ze zprávy, která je sice již z roku 2005, ale domnívám se, že pro prvotní inspiraci je postačující.

- SPAM
- výpadek proudu
- porucha hardware
- počítačový virus
- chyba uživatele
- chyba programového vybavení
- selhání lokální sítě
- výpadek internetové přípojky
- chyba administrátora nebo obsluhy
- krádež zařízení
- nepovolený přístup k datům
- zneužití zařízení
- přírodní katastrofa

Je možné použít seznam hrozeb uvedený ve vyhlášce 316/2014 Sb. Příklad možných hrozeb uváděných vyhláškou je následující:

- porušení bezpečnostní politiky
- zneužití oprávnění uživatelem nebo administrátorem
- poškození nebo selhání technického vybavení
- zneužití identity fyzické osoby
- užívání SW v rozporu s licencí
- kybernetický útok z komunikační sítě
- škodlivý kód (viry, trojské koně)
- nedostatky při poskytování služeb systémem
- narušení fyzické bezpečnosti
- výpadek internetu nebo proudu
- zneužití nebo upravení údajů
- odcizení nebo poškození aktiva

Opět zde uvedu pouze seznam všech námi identifikovaných hrozeb. Jejich hodnocení se nachází v přiloženém souboru: "DP_Siroky_Vyhodnocena_Rizika.xlsx"na listu "Hrozby". Zde budou uvedeny jak hrozby, tak i hodnoty u všech čtyř kritérií pro každou hrozbu a výsledná hodnota hrozby, kterou určíme aritmetickým průměrem ze všech čtyř hodnot u každé hrozby.

Nalezené hrozby ve Webovém HelpDesku

- Porucha Hardwaru - Server
- Chyba uživatele
- Porucha klientské stanice
- Výpadek komunikační linky

- Virová nákaza
- DDoS útok
- Výpadek proudu
- Chyba programů
- Chyba administrátora
- Krádež zařízení
- Nepovolený přístup k datům zvenku
- Přírodní katastrofa
- Odchod klíčového zaměstnance
- Krádež dat
- Pošpinění dobrého jména firmy
- Riziko prodlení (nedodržení lhůt)

Pro potřeby následujícího výpočtu míry rizika (kapitola 4.2.4) opět uvedu na ukázku pět hrozeb i s jejich ohodnocením. Celkový dopad je určen váženým průměrem všech čtyř kritérií.

Váhy byly nastaveny takto:

- pro pravděpodobnost hrozby byla určena váha 0,2,
- pro dopad hrozby váha 0,4,
- pro zranitelnost byla zvolena váha 0,3,
- a pro odhalení rizika váha 0,1.

Výsledný vzorec vypadá následovně:

(váha pravděpodobnosti hrozby)*(pravděpodobnost hrozby) + (váha dopadu)*(dopad) + (váha zranitelnosti)*(slabina) + (váha odhalení rizika)*(odhalení) = celkový dopad (hodnota hrozby)

Uvedl bych opět pro ukázku konkrétní výpočet pro hrozbu Porucha HW - Server. Výpočet je obdobný pro zbývající hrozby jak uvedené v následující tabulce č. 4.3, tak v celkové tabulce všech hrozeb (v souboru "DP_Siroky_Vyhodnocena_Rizika.xlsx"na listu "Hrozby").

Příklad výpočtu pro Porucha HW - Server:

$$0,2 * 3 + 0,4 * 3 + 0,3 * 1 + 0,1 * 1 = 2,20 \tag{4.2}$$

Tabulka 4.3: Identifikované a ohodnocené hrozby - ukázka

Nalezené hrozby	Možnost hrozby	Dopad	Slabina	Odhalení	Celkový dopad
Porucha HW - Server	3	3	1	1	2,20
Porucha klientské stanice	3	1	2	1	1,70
Chyba uživatele	3	1	1	3	1,60
Výpadek komunikační linky	3	2	3	1	2,40
Virová nákaza	2	2	1	2	1,70

Výpočet významnosti rizika

1. **Analýza (výpočet) významnosti rizika z hodnoty aktiva, hrozby a zranitelnosti**

   Prvním způsobem analýzy rizik podle zdroje [9] je zjištění výsledné míry rizika použitím hodnoty příslušného aktiva, která se následně vynásobí s pravděpodobností hrozby a hodnotou zranitelnosti u této hrozby.

   Pro ukázku opět uvedu pět aktiv z tabulky č. 4.2 a pět hrozeb z tabulky č. 4.3. Ve výsledné matici budou vyplněné buňky pouze tam, kde daná hrozba ovlivňuje dané aktivum. Celý vzorec výpočtu bude tedy vypadat takto:

   $$R = T * A * V \tag{4.3}$$

   kde R nám udává výslednou míru rizika, T znamená pravděpodobnost hrozby (tedy jaká je šance, že hrozba naruší aktivum), A udává hodnotu aktiva (jak je pro nás důležité) a V určuje hodnotu zranitelnosti daného aktiva (v našem případě se jedná o ukazatel, jak rychle se vzpamatujeme z narušení aktiva). Výsledná matice s doplněnými hodnotami je uvedena jako tabulka č. 4.4 níže.

   Po této analýze jsme si stanovili rozsahy hodnot, které pro nás oddělí čtyři úrovně závažností:

   - nízká (1 - 16)
   - střední (17 - 32)
   - vysoká (33 - 48)
   - kritická (49 - 64)

Tyto hodnoty udávající rozptyl jsou použité jen pro výpočet touto metodou. Podle této metody výpočtu jsme objevili 13 rizik s nízkou úrovní a 1 riziko se střední úrovní. Výsledný vzorec tedy vypadá následovně:

Hodnota aktiva (vypočtena aritmetickým průměrem) x Hodnota možnosti hrozby x Hodnota zranitelnosti aktiva = Míra rizika

Pro představu bych uvedl názorný příklad pro aktivum Seznam zákazníků a pro hrozbu Porucha serveru. Hodnoty budou uvedeny v závorkách: Seznam zákazníků (2) * Porucha Server - pravděpodobnost hrozby (3) * Porucha Server - zranitelnost (1) = Míra rizika (6).[9]

Tabulka 4.4: Vypočtené hodnoty rizik - ukázka

Aktiva/Hrozby	Porucha Server	Porucha PC	Chyba uživatele	Výpadek spojení	Virová nákaza
Seznam zákazníků	6		6		4
Hlášení zákazníků	6			18	
Ostatní data	6		6		4
Testy	6		6		4
Projektová dokumentace	6		6		4

2. **Analýza (výpočet) významnosti rizika z pravděpodobnosti incidentu a z jeho dopadu na aktiva**

   Jako druhý přístup k analýze rizik je uváděna ve zdroji [9] analýza, která pouze vyhodnocuje pravděpodobnost incidentu (PL) a jeho dopad na aktiva (D). Jak je zřejmé, tato metoda oproti metodě v kapitole 4.2.3 používá pouze dva parametry místo tří pro určení míry rizika. Při použití této metody je stejně jako u předchozí nutné identifikovat a ocenit jednotlivá aktiva (výsledné číslo dostaneme použitím aritmetického průměru ze tří kritérií u každého aktiva) a také nalézt hrozby ovlivňující tato aktiva. Ke každé hrozbě je potom nutné určit pravděpodobnost, že tato hrozba využije některou ze zranitelností a poškodí tak naše aktivum. Pravděpodobnost incidentu může nabýt jedné ze čtyř hodnot (nízká, střední, vysoká, kritická) ze stupnice uvedené v sekci Přílohy v části Stupnice pod číslem 1. Pro použití vzorce na určení hodnoty rizika (R),

$$R = PL * D \tag{4.4}$$

   potřebujeme znát velikost dopadu na naše aktiva. Za velikost dopadu si stanovíme hodnotu aktiva.

Pro lepší pochopení uvedu konkrétní příklad: jako aktivum si zvolím Seznam zákazníků, které má svoji hodnotu 2 (důvěrnost - 3, integrita - 1, dostupnost - 2) vzniklou aritmetickým průměrem ze všech tří kritérií uvedených v závorce.

Jako hrozbu zvolím Porucha HW - server, která je již také uvedena výše v sekci týkající se nalezených hrozeb a také v předchozí metodě na výpočet míry rizika. U této konkrétní hrozby jsme stanovili pravděpodobnost výskytu na hodnotu 3 (vysokou).

Pro následné určení míry rizika použijeme již jednou uvedený vzorec a to tento:

Riziko (R) = Pravděpodobnost incidentu (PL) x Dopad (D)

Pro náš příklad to tedy bude vypadat následovně:

Seznam zákazníků - 2 (hodnota aktiva) x Porucha HW - server - 3 (pravděpodobnost hrozby) = míra rizika - 6

Stupnice pro určení, zda je nalezené riziko vážné či ne, použijeme následující rozdělení závažností:

- nízké riziko nabývá hodnot 1 a 2
- střední riziko 3 a 4
- vysoké riziko pak nabývá hodnot 6, 8, 9
- kritické riziko je určeno hodnotami 12 a 16

Podle této stupnice patří námi nalezené riziko z příkladu do skupiny rizik s vysokou závažností. Příslušné vypočtené míry rizik jsou uvedeny v následující tabulce číslo 4.5.

Tabulka 4.5: Výpočet rizika jen z hodnoty aktiva (dopadu) a pravděpodobnosti hrozby

Aktiva/Hrozby	Porucha Server	Porucha PC	Chyba uživatele	Výpadek spojení	Virová nákaza
Seznam zákazníků	6		6		4
Hlášení zákazníků	6			6	
Ostatní data	6		6		4
Testy	6		6		4
Projektová dokumentace	6		6		4

3. **Námi zvolený postup pro výpočet rizika**

   V našem případě jsme vycházeli ze vzorce pro výpočet rizika z kapitoly 4.2.3 z části 1. Vzorec jsme si následně upravili do podoby vzorce ze strany 58, kde je podrobně vysvětlen. Zde jen uvedu, že se ve vzorci vypočítává hodnota rizika z celkové hodnoty aktiva a hrozby.

   Z tabulky identifikovaných aktiv použijeme pro následující výpočet hodnotu každého aktiva. Stejným způsobem z tabulky nalezených hrozeb využijeme výslednou hodnotu hrozby. Následně jsme tyto zjištěné údaje uspořádali do matice, ve které jsem umístil všechna nalezená aktiva na svislou stranu matice a na rovnoběžnou stranu všechny nalezené hrozby. V každé odpovídající buňce (podle toho, zda příslušné riziko ovlivňuje aktivum) vynásobíme hodnotu aktiva s hodnotou hrozby, což nám určí výslednou míru rizika. Tu zařadíme podle stanovených hranic do jedné ze čtyř skupin (nízká závažnost, střední, vysoká a kritická.).

   Vzorec vypadá v každé buňce následovně:

   Riziko = Hodnota aktiva x Hodnota příslušné hrozby, která toto aktivum ovlivňuje

   Níže budu uvádět pro ukázku vždy matici s pěti aktivy a pěti hrozbami. Celá matice s vypočtenými míry rizik se nachází v souboru "DP_Siroky_Vyhodnocena_Rizika.xlsx"na listu "Rizika".

4.2.4 Způsoby vypočtení významnosti rizik pro systém HelpDesk

Metoda násobení hodnot parametrů u aktiv, hrozeb a rizik

Před tím, než jsem mohl určovat výsledné hodnoty rizik, jsem se zabýval výběrem vhodné metody na určení hodnoty aktiva a rizika. Jako první jsem zkoušel násobit mezi sebou hodnoty u všech parametrů aktiva (hodnotu důvěrnosti, dostupnosti a integrity).

Pro ukázku zde uvedu výpočet u aktiva Seznam zákazníků: důvěrnost (3) * dostupnost (2) * integrita (1), což nám dá hodnotu aktiva šest. Ale tento postup se ukázal jako nevhodný z důvodu, na který jsem přišel poté, co jsem zvýšil hodnotu jednoho parametru o jednotku. Pokud jsem to provedl, původní hodnota se (z předchozího příkladu hodnota šest) zvýšila o součin ostatních parametrů. Tedy k původní hodnotě šest se přičetl ještě součin hodnot důvěrnosti (3) a dostupnosti (2), pokud jsem zvýšil hodnotu integrity z 1 na 2. Zjistil jsem tedy, že výsledná hodnota aktiva nebo rizika je ovlivněna velikostí zbývajících parametrů a ne tím, že zvýšíme jeden parametr o jednotku. Proto jsem se rozhodl tuto metodu nepoužít, protože dochází k výrazným skokům výsledných hodnot aktiv.

Uvedu zde ještě pro lepší znázornění obecný příklad, který ukáže nevýhodu této metody a to závislost na ostatních hodnotách parametrů. U aktiva parametry vyjádřím proměnnými a, b, c. Tedy při násobení dostaneme $a*b*c = f$ (výsledná hodnota aktiva). Ale pokud zvýšíme hodnotu parametru c o jednotku, bude vzorec vypadat následovně: $a * b * (c + 1) = g$ (nová hodnota aktiva). Ale předchozí hodnota aktiva se změní o více než o jednotku, změní se o součin $a * b$. Vzorec vypadá takto:

$$(a * b * c) + a * b \tag{4.5}$$

Ze vzorce je patrné, že dojde-li ke zvýšení hodnoty parametru c o 1, zvětší se výsledná velikost aktiva o součin zbývajících dvou parametrů.

Mohu uvést ještě příklad: $(3 * 2 * 1) + (3 * 2) = 12$, dojde tedy ke zdvojnásobení původní hodnoty. Tato metoda proto není vypovídající a není vhodná pro určování hodnoty aktiv a rizik.

Tabulka 4.6: Ohodnocená aktiva vynásobením hodnot parametrů - ukázka

Název aktiva	Důvěrnost	Dostupnost	Integrita	Celkový dopad
Seznam zákazníků	3	2	1	6
Hlášení zákazníků	1	3	3	9
Ostatní data	2	2	2	8
Testy	2	1	2	4
Projektová dokumentace	2	3	2	12

Tabulka 4.7: Ohodnocené hrozby vynásobením hodnot parametrů - ukázka

Nalezené hrozby	Možnost hrozby	Dopad	Slabina	Odhalení	Celkový dopad
Porucha HW - Server	3	3	1	1	9
Porucha klientské stanice	3	1	2	1	6
Chyba uživatele	3	1	1	3	9
Výpadek komunikační linky	3	2	3	1	18
Virová nákaza	2	2	1	2	8

Tabulka 4.8: Výsledná matice rizik - ukázka

Aktiva/Hrozby	Porucha Server	Porucha PC	Chyba uživatele	Výpadek spojení	Virová nákaza
Seznam zákazníků	54		54		48
Hlášení zákazníků	81			162	
Ostatní data	72		72		64
Testy	36		36		32
Projektová dokumentace	108		108		96

Metoda použití aritmetického průměru pro stanovení hodnot aktiv a rizik

Poté, co jsem zjistil, že násobení hodnot u parametrů není správná cesta a že jeho výsledek není vypovídající, zkusil jsem použít pro určení hodnoty aktiva i rizika běžný aritmetický průměr. Aritmetický průměr již není závislý na ostatních hodnotách jednotlivých parametrů, ale zvyšuje se pouze o jednu entinu při zvýšení jednoho členu o jednotku. Uvedu pro názornost příklad.

Pokud máme hodnoty parametrů u aktiva následující: pro důvěrnost 3, pro dostupnost 2 a pro integritu 1, bude průměr následující: $\frac{3}{3} + \frac{2}{3} + \frac{1}{3} = 2,00$. Pokud následně zvýšíme hodnotu jednoho parametru (např. hodnotu integrity) o jednotku, výpočet a výsledek průměru se zvýší o jednu třetinu, viz příklad: $\frac{3}{3} + \frac{2}{3} + \frac{1}{3} + \frac{1}{3}$. Poslední člen součtu ($\frac{1}{3}$) je zde z důvodu zvýšení hodnoty parametru integrity o 1. Po tomto zvýšení vyjde průměr $2,33$, což je věrohodnější výsledek, než jakého jsme dosáhli při určování hodnoty aktiva použitím násobení jednotlivých hodnot parametrů.

Tabulka 4.9: Hodnoty aktiv získané použitím aritmetického průměru - ukázka

Název aktiva	Důvěrnost	Dostupnost	Integrita	Celkový dopad
Seznam zákazníků	3	2	1	2,00
Hlášení zákazníků	1	3	3	2,33
Ostatní data	2	2	2	2,00
Testy	2	1	2	1,67
Projektová dokumentace	2	3	2	2,33

Tabulka 4.10: Ohodnocené hrozby použitím aritmetického průměru - ukázka

Nalezené hrozby	Možnost hrozby	Dopad	Slabina	Odhalení	Celkový dopad
Porucha HW - Server	3	3	1	1	2,00
Porucha klientské stanice	3	1	2	1	1,75
Chyba uživatele	3	1	1	3	2,00
Výpadek komunikační linky	3	2	3	1	2,25
Virová nákaza	2	2	1	2	1,75

Tabulka 4.11: Výsledná matice vzniklá vynásobením průměrů hodnot aktiv a rizik - ukázka

Aktiva/Hrozby	Porucha Server	Porucha PC	Chyba uživatele	Výpadek spojení	Virová nákaza
Seznam zák.	4,00		4,00		3,50
Hlášení zákazníků	4,67			5,25	
Ostatní data	4,00		4,00		3,50
Testy	3,33		3,33		2,92
Projektová dok.	4,67		4,67		4.08

Metoda použití váženého průměru pro stanovení hodnot aktiv a rizik

Po získání hodnot použitím běžného průměru jsem se rozhodl použít vážený průměr, zda bych díky němu nedosáhl na lépe vypovídající celkové hodnoty rizika. Hodnoty aktiv a hrozeb jsou vypočítány pomocí váženého průměru. U aktiv jsem použil větší váhy u parametrů, u kterých jsem odhadl, že jsou pro firmu důležitější.

Odhadl jsem tyto váhy:

- u důvěrnosti jsem zvolil váhu 0,4,
- u dostupnosti váhu 0,4,
- u integrity váhu 0,2.

Po konzultaci s panem Ing. Přibylem jsme určili váhy trochu jinak z důvodu, že pro firmu je důležitější dostupnost a integrita služeb a dat než jejich důvěrnost.

Finální váhy jsou tedy následující:

- pro důvěrnost je váhu pouze 0,2,
- pro dostupnost váhu 0,4,
- pro integritu váhu 0,4.

Konkrétní příklad výpočtu hodnoty aktiva Seznam zákazníků je:

$$0,2 * 3 + 0,4 * 2 + 0,4 * 1 = 1,80 \tag{4.6}$$

Obdobným způsobem jsem postupoval při určování hodnot hrozeb s tím rozdílem, že váhy byly zvoleny rozdílně. U hrozeb jsem určil váhy následovně pro každý parametr a to takto:

- pro pravděpodobnost hrozby váhu 0,2 - zdála se mi méně důležitá než dopad hrozby,
- pro dopad hrozby váhu 0,4,
- pro zranitelnost váhu 0,3,
- pro rychlost odhalení váhu 0,1.

Tyto mnou navržené váhy odsouhlasil pan Ing. Přibyl. Pro následnou ukázku výpočtu váženého průměru je potřeba uvést konkrétní hodnoty parametrů např. hrozby Porucha HW - Server, pro kterou budeme počítat vážený průměr. U této hrozby má parametr pravděpodobnost hrozby hodnotu 3, parametr dopad na firmu hodnotu 3, parametr udávající rychlost vzpamatování (zranitelnost) hodnotu 1 a poslední parametr udávající rychlost odhalení rizika hodnotu 1.

Vzorec tedy bude vypadat takto:

$$0,2 * 3 + 0,4 * 3 + 0,3 * 1 + 0,1 * 1 \tag{4.7}$$

Jeho výsledek má hodnotu $2,20$. Tato hodnota se spolu s příslušnou hodnotou aktiva násobí ve výsledné matici rizik, kde tato výsledná hodnota určí, jak závažné je pro nás riziko.

Tabulka 4.12: Hodnoty aktiv získané použitím váženého aritmetického průměru - ukázka

Název aktiva	Důvěrnost	Dostupnost	Integrita	Celkový dopad
Seznam zákazníků	3	2	1	1,80
Hlášení zákazníků	1	3	3	2,60
Ostatní data	2	2	2	2,00
Testy	2	1	2	1,60
Projektová dokumentace	2	3	2	2,40

Tabulka 4.13: Ohodnocené hrozby použitím váženého aritmetického průměru - ukázka

Nalezené hrozby	Možnost hrozby	Dopad	Slabina	Odhalení	Celkový dopad
Porucha HW - Server	3	3	1	1	2,20
Porucha klientské stanice	3	1	2	1	1,70
Chyba uživatele	3	1	1	3	1,60
Výpadek komunikační linky	3	2	3	1	2,40
Virová nákaza	2	2	1	2	1,70

Tabulka 4.14: Výsledná matice vzniklá vynásobením vážených průměrů hodnot aktiv a rizik - ukázka

Aktiva/Hrozby	Porucha Server	Porucha PC	Chyba uživatele	Výpadek spojení	Virová nákaza
Seznam zák.	3,96		2,88		3,06
Hlášení zákazníků	5,72			6,24	
Ostatní data	4,40		3,20		3,40
Testy	3,52		2,56		2,72
Projektová dok.	5,28		3,84		4,08

Ve výsledné matici, nacházející se v přiloženém souboru "DP_Siroky_Vyhodnocena-_Rizika.xlsx", jsou stanovené míry rizika na listu "Rizika". Tyto míry rozdělí rizika do čtyř úrovní:

- nízké - obsahuje rizika s hodnotou 1,00 - 3,50,
- střední - rizika s hodnotou 3,51 až 5,00,
- vysoké - rizika s hodnotami v rozmezí 5,01 až 9,00,
- kritické - rizika s hodnotami 9,01 a 16,00

Výsledný vzorec tedy vypadá následovně:
Hodnota aktiva ((váha důvěrnosti)*(důvěrnost) + (váha dostupnosti)*(dostupnost) + (váha integrity)*(integrita)) **x Hodnota hrozby** ((váha pravděpodobnosti)*(pravděpodobnost hrozby) + (váha dopadu)*(dopad) + (váha zranitelnosti)*(zranitelnost) + (váha odhalení)*(odhalení)) **= Výsledná míra rizika**

4.3 Prohlášení o aplikovatelnosti

V této sekci je potřeba, na základě bezpečnostních potřeb a výsledků hodnocení rizik, vytvořit přehled vybraných a zavedených bezpečnostních opatření ve firmě.

Po vypočtení hodnot u všech rizik jsme získali několik rizik s vysokou závažností. Zbývající rizika byla s nízkou a střední závažností a není potřeba se jim věnovat. Jen je potřeba je monitorovat a zjišťovat, zda náhodou nevzrostla jejich úroveň. Dále uvedu jen rizika s vysokou závažností, ke kterým budou navržena opatření, která jsou použita proti poškození aktiv za účelem buď těmto rizikům zcela zabránit v narušení aktiva, nebo alespoň zmírnit škody způsobené těmito riziky.

Výpis bude vypadat následovně, vždy bude uvedeno jako první aktivum a k němu příslušné hrozby, které pro nás představují vysoké riziko.

Nalezená aktiva a k nim příslušné hrozby představující pro firmu závažné narušení bezpečnosti:

1. Hlášení zákazníků - aktivum
    - Porucha HW - server

      Proti zničení nebo částečnému poškození dat uložených na serveru se firma brání zejména zálohováním všech dat, přičemž tyto zálohy jsou umístěné na dvou fyzicky oddělených místech ve dvou budovách v jedné ulici. Obnova dat je velmi rychlá, protože na obou serverech jsou data stejná (dochází k replikaci dat) a je proto velmi rychlé přejít na druhý, nedotčený server, který bude používán jako primární pro všechny běžící aplikace.

- Výpadek komunikační linky

  Při poruše komunikační linky dojde k nedostupnosti systému pro příjem hlášení od zákazníků. V tomto případě má zákazník možnost pro nahlášení problému či požadavku použít pro kontaktování Hotline CCA mobilní telefonní číslo, které má uvedeno ve smlouvě. Pokud totiž dojde k výpadku internetového připojení, přestane fungovat telefonní ústředna pro příjem běžných hovorů. Firma se zabývala otázkou, zda nezřídit druhou linku, která by umožňovala připojení k internetu od jiného poskytovatele. Tento návrh zamítla s tím, že mobilní telefony jsou dostačující a výpadky internetového připojení nejsou časté.

- Výpadek elektrické energie

  Stejně jako u výpadku internetového připojení mohou zákazníci využít alternativní cestu, jak kontaktovat firmu. Zákazníci často ani nezpozorují výpadek jimi využívaných služeb a systémů způsobený výpadkem el. energie, neboť jsou tyto výpadky méně časté než výpadky internetového připojení.

- Krádež zařízení

  V případě krádeže zařízení (např. serveru s daty), by firma o data nepřišla, protože jsou zálohována na dvou oddělených místech a zároveň v bance na magnetických páskách. Rovněž je velmi nepravděpodo-bné, že by došlo najednou ke krádeži všech serverů z obou budov.

- Přírodní katastrofa

  Pokud dojde k přírodní katastrofě a tedy ke zničení jedné ze dvou budov firmy, je obnova velmi rychlá, protože data se nacházejí na dvou místech, kde jsou umístěny servery se stejnými daty (dochází k replikaci dat mezi dvěma servery). Pokud by došlo ke zničení obou míst (a obou serverů), kde se nacházejí příslušná data, lze data obnovit z magnetických pásek, avšak pravděpodobně by nešlo o nejaktuálnější data, ale o zálohu několik dní starou.

2. Projektová dokumentace - aktivum

- Porucha HW - server

  Zde jsou opatření stejná jako u poruchy HW - Serveru u aktiva Hlášení zákazníků.

- Výpadek proudu

  Při výpadku proudu se opět nemusíme bát o data, ta jsou pravidelně zálohovaná. V průběhu výpadku také o moc neklesne výkonnost jednotlivých pracovníků na projektových dokumentacích z důvodu, že téměř všichni používají

notebooky, které disponují výdrží na baterii v řádu hodin a jsou vždy plně nabité (jsou pořád připojeny k napájení). Pracovat lze díky tomu, že není nutné být pořád připojen k serverům, kde jsou uloženy veškeré dokumentace, ale je možné pracovat bez připojení k serveru lokálně na svém notebooku a hotovou práci nahrát na server až ve chvíli, kdy dojde k obnovení dodávky proudu do firmy.

- Krádež zařízení

  Zde jsou opatření stejná jako u krádeže zařízení u aktiva Hlášení zákazníků.

- Přírodní katastrofa

  Opatření jsou stejná jako u přírodní katastrofy u aktiva Hlášení zákazníků.

- Krádež dat

  I zde je použito hlavně zálohování projektové dokumentace jak na obě místa se servery, tak i do banky na magnetické pásky.

3. Databázový server (HW) - aktivum

   - Výpadek komunikační linky

     Vypadne-li komunikační linka k internetu, databázový server není tímto výpadkem vůbec ohrožen, protože je umístěn ve vnitřní síti.

4. Databázový server (SW) - aktivum

   - Přírodní katastrofa

     Jsou zde použita stejná opatření jako u aktiva Projektová dokumentace uvedeném výše.

4.4 Plán zvládání rizik k 26. 2. 2016

Podle vyhlášky 316/2014 Sb. by měly být v této části uvedeny cíle a přínosy bezpečnostních opatření pro firmou nalezené hrozby. Dále je zde dobré určit osoby zodpovědné za zajištění prosazování bezpečnostních opatření pro zvládnutí identifikovaných rizik. Uvádí se zde také potřebné finanční, technické, lidské a informační zdroje, kterými firma disponuje pro zvládnutí rizik. Jsou zde určeny termíny zavedení jednotlivých opatření a popis vazeb mezi nalezenými riziky a příslušnými bezpečnostními opatřeními.

Cílem zavedení bezpečnostních opatření je minimalizovat dopad rizik na aktiva firmy CCA.

Pro správnou funkčnost zavedených opatření je nutné pravidelně kontrolovat používaná zařízení používaná v těchto opatřeních (např. kontrola funkčnosti zálohování). Firma

má stanoven plán činností, ve kterém jsou uvedeny činnosti podléhající pravidelné kontrole. Plán má tyto části:

1. **Zálohování**

   Zde je nutné zajistit:

   - pravidelné zálohování zdrojů (firemních dat)
   - zavést pravidelné kontroly úspěšnosti zálohování
   - zavést Disaster Recovery (dále jen DR) testy, při kterých dojde k fingovanému zničení některého nebo veškerého vybavení firmy a následně se snaží firma obnovit zničené vybavení (např. servery, vnitřní infrastrukturu)

   Firma CCA má již vyřešený samotný proces zálohování, avšak je potřeba stanovit kontrolní mechanismy a také zavést DR testování. Firma plánuje v letošním roce 2016 uskutečnit DR testy všech komponent její infrastruktury.

2. **Záložní komunikační infrastruktura**

   Pracovníci Hotline a technická pohotovost musejí mít k dispozici vyhrazená mobilní čísla, na kterých budou k zastižení, a která budou dostatečně známá všem pracovníkům CCA a vybraným zákazníkům.

3. **Záložní zdroje**

   Pro správnou funkčnost záložních zdrojů (UPS - zdroj nepřerušovaného napájení) je potřeba provádět pravidelné kontroly těchto zdrojů. Kontroly ve firmě probíhají a jejich správné chování hlídá interní systém Nagios. Dále je potřeba stanovit pravidla informování zaměstnanců firmy v případě výpadku elektrického proudu v části areálu.

Pro kontrolu zálohování a sledování zdrojů jsou určeni vybraní pracovníci technické podpory. Vnitřní směrnicí jsou stanovena pravidla pro udržování technické pohotovosti. Zajištění potřebných kapacit pro tyto činnosti má na starosti ředitel úseku Vývoj a programování. Pro zajištění funkčnosti služby Hotline jsou vyhrazeni pracovníci pro dobu určenou smlouvou se zákazníkem. Kapacity pro službu Hotline zajišťuje ředitel úseku Zákaznická podpora.

Do 1. poloviny roku 2016 zavede firma CCA polovinu DR testů a do konce roku 2016 jejich zbytek. Vybrané testy budou opakovány měsíčně a jiné v intervalu 3 let.

4.5 Plán rozvoje bezpečnostního povědomí

Do plánu na rozvoj povědomí je vhodné uvést informace, popřípadě plán na rozvoj bezpečnostního povědomí zaměstnanců firmy, který bude obsahovat následující části

dané vyhláškou 316/2014 Sb., především formu, obsah jednotlivých školení a také rozsah těchto potřebných školení. Dále je nutné vybrat a stanovit zaměstnance, kteří budou zodpovědní za vykonávání jednotlivých činností stanovených v tomto plánu.

Informace o školeních, o činnostech, které se provádí při nástupu nebo odchodu zaměstnance jsou uvedeny v sekci Bezpečnostní politika v části 4.1.4.

4.6 Zvládání kybernetických bezpečnostních incidentů

Vyhláška 316/2014 Sb. vyžaduje pro tuto sekci bezpečnostní politiky zavést systém dokumentování toho, jak firma zvládá kybernetické bezpečnostní incidenty. Pro to, aby mohla firma vést tyto záznamy, je potřeba nejprve provést několik kroků pro zavedení a provozování těchto nástrojů na detekci incidentů, než bude možné vůbec dokumentovat proběhlé incidenty. Kroky je možné provést ve stejném pořadí, které uvádí samotná vyhláška.

- Nejprve firma přijme opatření zajišťující oznamování bezpečnostních událostí v jí provozovaném systému, pro který je ze zákona povinna vést bezpečnostní dokumentaci a hlásit bezpečnostní události národnímu bezpečnostnímu CERT týmu. Toto oznamování musejí provádět jak samotní uživatelé, tak i administrátoři a osoby plnící bezpečnostní role.

- Další činností je příprava vhodného prostředí ve kterém bude docházet k vyhodnocování oznámených bezpečnostních událostí a také událostí, které detekovaly technické nástroje pro detekci kybernetických bezpečnostních událostí a pro sběr a vyhodnocení bezpečnostních událostí.

- Následně je nutné tyto události vyhodnotit (zejména jejich závažnost) a určit z těchto událostí bezpečnostní incidenty. Poté, co firma identifikuje incidenty, je potřeba tyto incidenty klasifikovat a přijmout taková opatření, která pomohou firmě buďto odvrátit nebo alespoň zmírnit dopady těchto incidentů.

- Firma je nadále povinna hlásit tyto incidenty Národnímu bezpečnostnímu úřadu podle paragrafu 32 vyhlášky 316/2014 Sb., ve které jsou uvedeny podrobnosti o formě a o náležitostech těchto hlášení bezpečnostních incidentů. Po odeslání hlášení je potřeba shromáždit věrohodné podklady pro následnou analýzu kybernetického bezpečnostního incidentu.

- Posledním krokem je prošetření incidentu za účelem nalezení možných příčin, které umožnily provedení útoku na firemní systém. Pokud se firmě podařilo nalézt

příčinu, měla by zavést taková bezpečnostní opatření, která zamezí možnosti, aby se aktuálně řešený incident v budoucnosti opakoval a znovu poškodil systém nebo samotnou firmu.

Firma nedisponuje směrnicí nebo dokumentem, ve kterém by bylo explicitně definováno, co se musí přesně provádět při zvládání incidentů. Firma používá systém interních hlášení, která vyplňují zaměstnanci v případě výskytu nějakého incidentu. V případě, že někdo ohlásí problém (incident), stanou se tři po sobě jdoucí kroky:

- zjistí se závažnost nalezeného incidentu
- začne se pracovat na jeho rychlém vyřešení i za cenu nedodržení přesných pracovních postupů
- poté, co je již incident úspěšně vyřešen, se provádí analýza příčin incidentu.

Pokud firma najde příčinu, stanoví konkrétní osoby, které dostanou za úkol vyřešit tuto vadu, která způsobila tento incident.

4.7 Strategie řízení kontinuity činností

V této sekci je potřeba stanovit minimální úroveň služeb (pro náš příklad Webového HelpDesku), která bude ještě přijatelná pro uživatele pracující se službou a také pro provoz a správu systému.

Dále je potřeba stanovit dobu, za kterou je firma schopna obnovit minimální funkčnost systému (HelpDesku) po výskytu kybernetického bezpečnostního incidentu. Tedy za jakou dobu budou moci uživatelé se systémem opět pracovat (s různými omezeními). Je možné, že nepoběží veškeré funkce, ale bude alespoň možné částečně se systémem pracovat. Také je potřeba stanovit dobu (termín), do které budou obnovena všechna data systému po proběhlém bezpečnostním incidentu.

Firma má veškeré informace o minimální úrovni jí poskytovaných služeb (tj. nejen HelpDesku) uvedeny v recovery plánu, kde je řečeno, jaké funkce či systémy musí fungovat, aby byla splněna minimální úroveň funkčnosti HelpDesku stanovená v tomto plánu. Obvykle stačí půl dne na obnovení základu, což je vnitřní infrastruktura.

4.8 Přehled právních předpisů

Tato část se zabývá posouzením souladu bezpečnostních opatření s právními předpisy, s vnitřními předpisy a směrnicemi a také smluvními závazky, které se vztahují ke spravovanému významnému informačnímu systému.

Firma používá směrnice a metodiky, ve kterých jsou popsány veškeré činnosti probíhající ve firmě. V těchto dokumentech je uveden způsob, jakým jsou zveřejňovány změny ve směrnicích a metodikách. Také probíhá pravidelná kontrola zaměstnanců jejich příslušnými vedoucími. Pokud dojde k tomu, že nějaký zaměstnanec opakovaně (většinou třikrát) nedodrží a neakceptuje novou změnu ve směrnici (metodice), týkající se zejména bezpečnosti, je jeho chování považováno za hrubé porušení pracovní kázně a vede k jeho okamžitému propuštění.

Kapitola 5

Závěr

Cílem této práce nebylo vytvořit přesnou a úplnou bezpečnostní dokumentaci, ale spíše připravit návod či šablonu pro budoucí vytváření bezpečnostní dokumentace firmou CCA. Z tohoto důvodu se vždy nachází v částech požadovaných zákonem nejprve popis toho, co má být v těchto částech uvedeno a jak se k těmto požadovaným informacím dostat.

Při analýze rizik systému HelpDesk byla pro výpočet hodnot jak aktiv, tak rizik použita metoda váženého průměru ze tří hodnot u aktiv a ze čtyř hodnot u hrozeb. K této metodě jsem se dopracoval postupně, když jsem nejprve použil metodu násobení hodnot aktiv a hrozeb, které ale podle mého uvážení nevedlo k jasným výsledkům. U této metody se totiž ukázalo, že zvýšení hodnoty o jedničku u jednoho ze tří parametrů aktiva vede ke zvýšení výsledné hodnoty o součin zbývajících parametrů. Po tomto zjištění jsem se rozhodl použít aritmetický průměr opět pro výpočet celkové hodnoty aktiva a hrozby, ten se ukázal jako vhodnější z důvodu, že se výsledná hodnota měnila jen o jednu n-tinu, pokud došlo ke zvýšení jednoho parametru o jedničku. Ale ve výsledné tabulce rizik jsem zjistil, že ani aritmetický průměr nedokázal dostatečně odlišit hodnoty rizik, které se pohybovaly kolem podobných hodnot, což znemožnilo jejich rozdělení do příslušných kategorií (nízké, střední, vysoké a kritické riziko), a proto jsem jako nejvhodnější variantu zvolil vážený aritmetický průměr, který již korespondoval s hodnotami parametrů a s jejich změnami.

Zbývající kapitoly se zabývají postupně tématy stanovenými vyhláškou 316/2014 Sb. a to nejprve prohlášení o aplikovatelnosti, které obsahuje nalezená rizika a k nim firmou přijatá opatření sloužící pro jejich odstranění nebo alespoň omezení. Následující kapitola se věnuje plánům a obsahům povinných bezpečnostních školeních, které jsou určeny pro všechny zaměstnance, a mají za úkol seznamovat zaměstnance s aktuálním děním nejen v bezpečnosti, ale i s novými směrnicemi a metodami. Další kapitola se věnuje postupům, jak zvládat narušení bezpečnosti ve firmě, a také jak tyto případné narušení (incidenty) hlásit nejen vedení firmy, ale také vládnímu CERT týmu. Kapi-

tola zabývající se kontinuitou činností obsahuje postupy (recovery plán), ve kterých je uvedeno jaké části systémů musí být po incidentu zprovozněny a také za jakou dobu. Je zde také stanovena minimální úroveň služeb, které musí fungovat co nejdříve po narušení, aby zákazník nebyl nijak výrazně omezen při používání služeb poskytovaných firmou. Poslední kapitola obsahuje popis firemních směrnic a metodik, které jsou ve firmě používány.

Kapitola 6

Zdroje a přílohy

1. Zákon číslo 181/2014 Sb., o kybernetické bezpečnosti.

   Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/zakon-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu-zakon-o-kyberneticke-bezpecnosti/

2. Národní centrum kybernetické bezpečnosti, Vládní CERT (GovCERT.CZ).

   Dostupné z: https://www.govcert.cz/cs/vladni-cert/

3. Národní CSIRT tým České republiky. Dostupné z: https://www.csirt.cz/

4. Milan Goll, IT Systems 7-82013, IT Security.

   Dostupné z: http://www.systemonline.cz/it-security/preventivni-vs.-reaktivni-pristup-k-bezpecnostnim-hrozbam.htm

5. Aktiva v ISMS, VUT Brno.

   Dostupné z: http://www.vutbr.cz/www_base/priloha.php?dpid=74651

6. Řízení rizik. Dostupné z: https://managementmania.com/cs/rizeni-rizik

7. Ing. Danuše Prokůpková, Analýza a řízení rizik, publikováno 1.3.2007.

   Dostupné z: http://www.ucetnikavarna.cz/archiv/dokument/doc-d8966v11782-analyza-a-rizeni-rizik/

8. ZAHÁLKA, J. Analýza rizik v průmyslovém podniku. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2012. 77 s. Vedoucí diplomové práce Ing. Luboš Kotek, Ph.D..

9. František Steiner, auditor CQS (Sdružení pro certifikaci systémů jakosti), ZČU Plzeň.

   Dostupné z: http://bpm-tema.blogspot.cz/2007/11/ppadov-studie-analzy-rizik-informan.html

10. Business Continuity Planning & Risk Assessment, The Power of Business Continuity Planning - RiskPAC.

    Dostupné z: http://www.opensystems-bs.com/BusinessContinuityPlanning/RiskPacRecoveryPac/tabid/108/Default.aspx

11. Mapy povodňového rizika.

    Dostupné z: http://www.dibavod.cz/data/poster_mapy_rizik.pdf?PHPSESSID=-b32f83c256d387bb29c

12. DEJMEK, M. Zavedení ISMS v obchodní společnosti. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2013. 89 s. Vedoucí diplomové práce Ing. Petr Sedlák.

13. Karl E. Wiegers, Požadavky na software - Od zadání k architektuře aplikace. 1. vydání. Brno: Computer Press, a.s., 2008. 448 s. ISBN 978-80-251-1877-1

14. Metody analýzy rizik.

    Dostupné z: www.jh.cz/filemanager/files/file.php?file=132160

15. VYSTRČIL, D. Bezpečnostní audit a politika IT organizace. Brno: Masarykova univerzita, Fakulta informatiky, 2008. 64 s. Vedoucí diplomové práce doc. RNDr. Václav Matyáš, M.Sc., PH.D..

16. Vladímír Smejkal, Karel Rais, Řízení rizik ve firmách a jiných organizacích. 4. aktualizované a rozšířené vydání. Praha: Grada Publishing, a.s., 2013. 488 s. ISBN 978-80-247.4644-9

17. doc. RNDr. Dana Procházková, DrSc., Metody, nástroje a techniky pro rizikové inženýrství, 1. vydání, Praha: České vysoké učení technické v Praze, 2011. 370 s. ISBN 978-80-01-04842-9

18. MAURIC, J. IDS systém SNORT. České Budějovice: Jihočeská univerzita, Katedra informatiky. 2009. 59 s. Vedoucí bakalářské práce Ing. Ladislav Beránek, CSc,. MBA

19. Karen Scarfone, Peter Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology, February 2007, National Institute of Standards and Technology Special Publication 800-94. 127 s.

20. Ming-Chang Lee, Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method, Taiwan: National Kaohsiung

University of Applied Science, International Journal of Computer Science & Information Technology (IJCSIT) Vol 6, No1, February 2014.

21. Lilja, K.K.; Laakso, K.; Palomki, J.; „Using the Delphi method“; Technology Management in the Energy Smart World (PICMET), 2011 Proceedings of PICMET '11:, July 31 2011-Aug. 4 2011, ISBN: 978-1-4577-1552-5

22. Bc. Antonín Krbušek, Využití metod řízení rizik v praxi, Brno: Mendelelova univerzita v Brně, Institut celoživotního vzdělávání, Oddělení Expertního Inženýrství, 2013. 95 s. Vedoucí diplomové práce doc. Ing. Pavel máchal, CSc.

23. Analýza rizik, Brno, 2013.

    Dostupné online z: http://www.vutbr.cz/www_base/priloha.php?dpid=74652

24. Příloha č. 1 k vyhlášce č. 316/2014 Sb.

    Dostupné online z: https://www.nbu.cz/download/nodeid-1067/

Seznam tabulek

Seznam obrázků

Stupnice pro hodnocení aktiv a hrozeb

Tabulka 6.1: Stupnice pro hodnocení důvěrnosti[24]

Úroveň	Popis	Ochrana
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění (např. na základě zákona č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů). Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy orgánu a osoby uvedené v § 3 písm. c) až e) zákona.	Není vyžadována žádná ochrana.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how orgánu a osoby uvedené v § 3 písm. c) až e) zákona, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství podle zákona č. 89/2012 Sb., občanský zákoník, osobní údaje podle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací vnější komunikační sítí jsou chráněny pomocí kryptografických prostředků.
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (např. strategické obchodní tajemství, citlivé osobní údaje).	Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily, a metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.

Tabulka 6.2: Stupnice pro hodnocení integrity[24]

Úroveň	Popis	Ochrana
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy orgánu a osoby uvedené v § 3 písm. c) až e) zákona.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (např. omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených vnějšími komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (např. pomocí technologie digitálního podpisu).

Tabulka 6.3: Stupnice pro hodnocení dostupnosti[24]

Úroveň	Popis	Ochrana
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů orgánu a osob uvedených v § 3 písm. c) až e) zákona. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Tabulka 6.4: Stupnice pro hodnocení dopadů[24]

Úroveň	Popis
Nízký	Dopad je v omezeném časovém období a malého rozsahu a nesmí být katastrofický. Rozsah případných škod nepřesahuje a) 10 zraněných osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty do 5000000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího nejvýše 250 osob.
Střední	Dopad je omezeného rozsahu a v omezeném časovém období. Rozsah případných škod se pohybuje v rozmezí a) do 10 mrtvých nebo od 11 do 100 osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty od 5.000.000 Kč do 50.000.000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 251 do 2500 osob.
Vysoký	Dopad je omezeného rozsahu, ale trvalý nebo katastrofický. Rozsah případných škod se pohybuje v rozmezí a) od 11 do 100 mrtvých nebo od 101 do 1000 osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty od 50.000.000 Kč do 500.000.000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 2501 do 25000 osob.
Kritický	Dopad je plošný rozsahem, trvalý a katastrofický. Rozsah případných škod se pohybuje v rozmezí a) 101 a více mrtvých a 1001 a více osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty převyšující 500.000.000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 25000 osob.

Tabulka 6.5: Stupnice pro hodnocení pravděpodobnosti realizace hrozby[24]

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

Tabulka 6.6: Stupnice pro hodnocení zranitelností[24]

Úroveň	Popis
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření, která jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření.
Střední	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Tabulka 6.7: Námi vytvořená stupnice pro rychlost odhalení rizika

Úroveň	Popis
Nízká	Na narušení aktiva přijdeme hned, maximálně v řádu minut (max 30 min).
Střední	Na narušení přijdeme v průběhu dne, maximálně však do 24 hodin.
Vysoká	Na narušení našich aktiv nepřijdeme vůbec nikdy.

Tabulka 6.8: Námi stanovená stupnice pro hodnocení rizik

Úroveň	Popis
Nízké (1,00 - 3,50)	Riziko je považováno za přijatelné.
Střední (3,51 - 5,00)	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko přijatelné.
Vysoké (5,01 - 9,00)	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritické (9,01 - 16,00)	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

CCA Group a.s.
Krátká 3, Plzeň

Bezpečnostní dokumentace podle zákona 181/2014 Sb.

Návrh bezpečnostní dokumentace pro systém HelpDesk

Plzeň 2016

Bc. Milan Široký

Obsah

1 Bezpečnostní politika

1.1 Systém řízení bezpečnosti informací

Bezpečnost informací je řešena např. následujícími firemními směrnicemi:

- S001_Řízení interních dokumentů
- S002_Řízení externích dokumentů
- S014_Ochrana obchodního tajemství firmy

1.2 Bezpečnostní role

Bezpečnostní role jsou následující:

- manažer kybernetické bezpečnosti - vedoucí oddělení jakosti
- architekt kybernetické bezpečnosti - ředitel úseku výroby a vývoje
- auditor kybernetické bezpečnosti - ředitel úseku zákaznické podpory
- garant aktiv - ředitelé úseků podle typů aktiv

1.3 Bezpečnost lidských zdrojů

Ve firmě je stanoven systém směrnic a metodik, které důkladně popisují pravidla chování uživatelů. Dále je stanoven systém školení, ve kterém jsou uvedeny další informace o tom, kteří zaměstnanci a jak často se musejí účastnit školení. Školení jsou prováděna formou průběžných školení jednou za rok a to prostřednictvím elektronických kurzů a testů. Proběhlá školení se zapisují do Evidence školení a také do systému pro řízení výuky, školení (LMS - Learning Management System). Veškeré informace o proběhlých školeních se společně se záznamy v LMS systémech zapisují do papírové evidence.

Zaměstnanci jsou povinni se řídit např. následujícími směrnicemi:

- S021_Pravidla chování uživatelů v IT prostředí firmy
- S006_Vzdělávání v CCA
- S032_Normy pro znalost anglického jazyka

Ve firmě je zabráněno uživatelům pomocí přístupových oprávnění v přístupu ke všem zdrojům (zejména datům) firmy. Je tedy zřejmé, že každý uživatel má přístup jen k omezené části zdrojů, které potřebuje pro vykonávání svojí práce.

Dále jsou zaměstnanci povinni se řídit např. těmito směrnicemi:

- S004_Interní audit
- S015_Strategie péče o stávající zákazníky
- S018_Projektový zákon

Nástup a odchod zaměstnance se řídí např. těmito směrnicemi:

- S027_Pravidla při nástupu a odchodu pracovníků firmy CCA
- S035_Odměňování za získávání nových pracovníků a patronát

1.4 Fyzická bezpečnost

Zabezpečení objektů a pohyb osob po firmě se řídí např. následujícími směrnicemi:

- S020_Zabezpečovací zařízení
- S026_Režim návštěv a telefonická komunikace

1.5 Řízení provozu a komunikací

Jsou stanovena následující pravidla pro zajištění bezpečného provozu informačního systému:

- Práva a povinnosti osob, které jsou v bezpečnostních rolích, administrátorů a také uživatelů jsou uvedeny ve směrnici "S100_Organizační řád".
- Postupy pro spuštění a ukončení chodu systému, dále postupy pro restart a obnovení po pádu, jsou uvedeny ve směrnici "S037_Zajištění funkčnosti vnitřní infrastruktury a serverů".
- Pro sledování bezpečnostních incidentů nebo jen problémů v síti, či v systému se používá ve firmě standardní systém logování. Pokud nastane nějaký problém, zaměstnanec má povinnost napsat záznam o tomto problému do bezpečnostního deníku. Firma následně provádí pravidelné (jednou za měsíc) vyhodnocování zpráv zapsaných v deníku a přijímá opatření, podle závažnosti zjištěných incidentů.
- Firma má zavedenou technickou pohotovost, která obsahuje pravidla pro postup, pokud uživatel zjistí nějaký technický problém. Zejména jsou zde uvedeny telefonní čísla na osoby, kterým má zaměstnanec v případě problému (typicky neběží server) volat. Tito lidé drží službu většinou od šesti hodin ráno až do jedenácti hodin večer a mají za tuto pohotovost příplatky.

- Ve firmě existuje oddělení lidských zdrojů, které se spolu s vedoucími středisek zabývá sledováním kapacit lidí. Funguje zde také systém vykazování (řízený směrnicí "S028_Výkazy práce"), do kterého zaměstnanci vykazují svoji práci. Díky tomuto přístupu může vedoucí oddělení dobře vidět, jací lidé jsou přetížení nebo mají naopak práce málo. Následně se může rozhodovat, zda bude nutné přijmout další zaměstnance nebo těm, kteří mají málo práce, přidělit nějakou další práci.

1.6 Řízení přístupu k datům a bezpečné chování uživatelů

Zaměstnanci se řídí směrnicí "S021_Pravidla chování uživatelů v IT prostředí firmy", která upravuje problematiku přihlašování a ukládání přihlašovacích údajů. Dále je zde systém zabezpečení, který se stará o přihlašování a také o přidělení práv jen k té části systému, ke které má mít uživatel přístup. Ověření identity uživatele probíhá běžným způsobem autentizací (je ověřena jeho identita - většinou jménem a heslem) a autorizací (dostane přidělen přístup jen k vybraným datům a k části systému).

1.7 Zálohování a obnova dat

Zálohování probíhá v reálném čase replikou dvou úložišť mezi dvěma domy. Ve firmě existuje několik úrovní zálohy a to:

- v reálném čase se replikují nejvíce kritická data okamžitě
- jednou denně se zálohují veškerá data na magnetické pásky
- jenou týdně se tyto pásky odvážejí do banky

Dle povahy dat je určena doba jejich setrvání v bance. Zde se tyto pásky uchovávají v průměru půl roku, ale nejdůležitější data zde zůstávají uložené nejméně po dobu deseti let.

Zálohování je řízeno směrnicí "S021_Pravidla chování uživatelů v IT prostředí firmy".

1.8 Poskytování a nabývání programových licencí

Nákup licencí a instalování programů na počítače uživatelů a kontrolu na výskyt nelegálního programového vybavení řídí směrnice:

- S021_Pravidla chování uživatelů v IT prostředí firmy

Je v ní zejména uvedeno, za jakých podmínek si může uživatel nainstalovat různé programy na svůj pracovní počítač a také jaké postupy musí zaměstnanec dodržet, pokud by si chtěl koupit nějaký program (software).

1.9 Ochrana osobních údajů

Ochrana údajů i dat jak jednotlivých uživatelů, tak i dat celé firmy je realizována pomocí přístupových oprávnění.

1.10 Používání kryptografické ochrany

- Veškerá firemní komunikace je standardně šifrovaná.
- Firma má svoji vlastní certifikační autoritu pro vnitřní záležitosti.
- Telefony zaměstnanců ani paměťové karty (ani flash disky uživatelů) v těchto telefonech nejsou šifrované zejména z důvodu, že v nich zaměstnanci nenosí nic důležitého.
- Heslo potřebné pro připojení přes VPN není nikdy uloženo přímo v telefonu.

1.11 Ochrana před škodlivým kódem

Informace o používaných bezpečnostních opatřeních pro zajištění ochrany před škodlivým kódem jsou uvedeny v sekci 1.5 Řízení provozu a komunikací.

Firma provádí pravidelnou a účinnou aktualizaci antivirů (definic, signatur) a firewallu.

1.12 Nástroj pro detekci kybernetických bezpečnostních událostí

Firma používá pro detekci bezpečnostních incidentů údaje získané z antivirových programů, programů pro filtrování síťového provozu a z logů systému Windows.

2 Metodika pro identifikaci a hodnocení aktiv a rizik

Aktiva a hrozby byly získány formou rozhovoru s klíčovými zaměstnanci firmy. Stejným způsobem byly určeny i příslušné hodnoty aktiv a hrozeb.

3 Zpráva o hodnocení aktiv a rizik

3.1 Identifikovaná a ohodnocená aktiva

Nejprve jsme se pokusili nalézt všechna možná aktiva, která náš systém může obsahovat. Pro hodnocení aktiv použijeme tato tři kritéria, díky kterým je možné zjistit a ohodnotit aktiva zejména podle toho, jak jsou pro nás důležitá a potřebná:

- důvěrnost (pouze oprávněné osoby mají umožněn přístup k těmto datům či službám)
- dostupnost (zajišťuje, že oprávněné osoby budou moci přistoupit k těmto datům či službám v okamžiku jejich potřeby)
- integrita (zajišťuje, že nedošlo k poškození dat v systému nebo při jejich přenosu a také se stará o to, aby data byla správná a úplná)

Tabulka 1: Přehled aktiv identifikovaných v systému HelpDesk firmy CCA - konec kontroly 26. 2. 2016

Informace		**Hardware**
Seznam zákazníků		Databázový server
Hlášení zákazníků		Webový server
Ostatní data		File systém ISZA
Testy		Komunikační kanály
Projektová dokumentace		Vnitřní infrastruktura
		Klientské stanice
Software		**Lidské zdroje**
Databázový server		Znalosti patřičných systémů
ISZA		Pracovníci hotline
HelpDesk		Ostatní pracovníci
Oracle Designer		
Share point		
Telefonní ústředna		
Zdrojové kódy		

Stupnice pro určení hodnoty u jednotlivých kritérií jsou následující (číselné vyjádření je dále použito ve vzorcích pro výpočet celkové hodnoty aktiv):

- nízká - 1
- střední - 2
- vysoká - 3
- a kritická - 4

Pro následný výpočet celkové hodnoty aktiva byly nadefinovány váhy:

- pro důvěrnost váha 0,2,
- pro dostupnost váha 0,4
- a pro integritu váha 0,4.

Celkový dopad každého aktiva je dán vzorcem:
(váha důvěrnosti)*(hodnota důvěrnosti) + (váha dostupnosti)*(hodnota dostupnosti) + (váha integrity)*(hodnota integrity) = celkový dopad (hodnota) aktiva.

Ohodnocená aktiva a jejich míra dopadu se nachází v přiloženém souboru: "DP_Siroky_Vyhodnocena_Rizika.xlsx"na listu "Aktiva".

3.2 Identifikované a ohodnocené hrozby (rizika)

Seznam identifikovaných hrozeb:

- Porucha Hardwaru - Server
- Porucha klientské stanice
- Chyba uživatele
- Výpadek komunikační linky
- Virová nákaza
- DDoS útok
- Výpadek proudu
- Chyba programů
- Chyba administrátora
- Krádež zařízení
- Nepovolený přístup k datům zvenku
- Přírodní katastrofa
- Odchod klíčového zaměstnance
- Krádež dat
- Pošpinění dobrého jména firmy
- Riziko prodlení (nedodržení lhůt)

Hodnocení hrozeb se nachází v přiloženém souboru: "DP_Siroky_Vyhodnocena_Rizika.xlsx"na listu "Hrozby". Zde budou uvedeny jak hrozby, tak i hodnoty u všech čtyř kritérií pro každou hrozbu a výsledná hodnota hrozby, kterou určíme aritmetickým průměrem ze všech čtyř hodnot u každé hrozby.

Celkový dopad je určen váženým průměrem všech čtyř kritérií.
Váhy byly nastaveny takto:

- pro pravděpodobnost hrozby byla určena váha 0,2
- pro dopad hrozby váha 0,4
- pro zranitelnost byla zvolena váha 0,3
- a pro odhalení rizika váha 0,1

Výsledný vzorec vypadá následovně:
(váha pravděpodobnosti hrozby)*(pravděpodobnost hrozby) + (váha dopadu)*(dopad) + (váha zranitelnosti)*(slabina) + (váha odhalení rizika)*(odhalení)

3.3 Výpočet významnosti rizika

Hodnoty rizik se nachází v přiloženém souboru: "DP_Siroky_Vyhodnocena_Rizika.xlsx"na listu "Rizika". Každé riziko jsme zařadili podle jeho závažnosti do jedné ze čtyř skupin:

- nízké,
- střední,
- vysoké
- kritické

Vzorec vypadá v každé buňce následovně:
Riziko = Hodnota aktiva x Hodnota příslušné hrozby, která toto aktivum ovlivňuje

Celá matice s vypočtenými míry rizik se nachází v souboru "DP_Siroky_Vyhodnocena_Rizika.xlsx"na listu "Rizika".

Pro výpočet hodnot aktiv a hrozeb jsme použili vážený aritmetický průměr s vahami uvedenými v kapitolách 3.1 a v 3.2.

Vy výsledné matici, nacházející se v přiloženém souboru "DP_Siroky_Vyhodnocena_Rizika.xlsx", jsou stanovené míry rizika na listu "Rizika". Tyto míry rozdělí rizika do čtyř úrovní:

- nízké - obsahuje rizika s hodnotou 1,00 - 3,50,
- střední - rizika s hodnotou 3,51 až 5,00,

- vysoké - rizika s hodnotami v rozmezí 5,01 až 9,00,
- kritické - rizika s hodnotami 9,01 a 16,00

Výsledný vzorec tedy vypadá následovně:
Hodnota aktiva ((váha důvěrnosti)*(důvěrnost) + (váha dostupnosti)*(dostupnost) + (váha integrity)*(integrita)) **x Hodnota hrozby** ((váha pravděpodobnosti)*(pravděpodobnost hrozby) + (váha dopadu)*(dopad) + (váha zranitelnosti)*(zranitelnost + (váha odhalení)*(odhalení)) **= Výsledná míra rizika**

4 Prohlášení o aplikovatelnosti

Na rizika s nižší závažností (nízkou a střední) nejsou stanovována žádná bezpečnostní opatření.

Nalezená aktiva a k nim příslušné hrozby představující pro firmu závažné narušení bezpečnosti:

1. Hlášení zákazníků - aktivum
    - Porucha HW - server
        - před ztrátou dat uložených na serverech, se firma brání kompletním zálohováním
        - zálohy jsou umístěné na dvou fyzicky oddělených místech ve dvou budovách v jedné ulici
        - rychlá obnova dat díky replikaci dat mezi servery a přechod na druhý server, který bude použit jako primární pro běžící aplikace
    - Výpadek komunikační linky
        - v případě výpadku dojde k výpadku telefonní ústředny
        - zákazník může použít telefonní kontakt uvedený v jeho smlouvě s firmou
        - díky malé četnosti výpadků není potřeba zavádět záložní linku do internetu
    - Výpadek elektrické energie
        - zákazník může zavolat kontaktním osobám firmy na mobilní telefon
        - četnost výpadků elektrické energie je velmi malá
    - Krádež zařízení
        - krádež dat, potažmo serverů, nezpůsobí firmě problémy, díky zálohování těchto dat

  - zálohy dat jsou i na magnetických páskách v bance
  - velmi nepravděpodobná krádež veškerých dat najednou
- Přírodní katastrofa
  - obnova je opět velmi rychlá díky replikaci dat mezi dvěma servery
  - v případě zničení obou serverů se provede obnova z dat uložených v bance
  - data na páskách nezahrnují nejaktuálnější data

2. Projektová dokumentace - aktivum

- Porucha HW - server

  Zde jsou opatření stejná jako u poruchy HW - Serveru u aktiva Hlášení zákazníků.
- Výpadek proudu
  - ochrana dat zajištěna zálohováním
  - výpadek nezpůsobí prodlevy při práci díky používání výhradně notebooků disponujících dlouhou výdrží na baterii
  - práce při výpadku umožněna lokálními kopiemi částí projektových dokumentacích, na kterých zaměstnanci zrovna pracují
  - hotovou práci nahrají zaměstnanci na server ve chvíli, kdy dojde k obnovení dodávky elektrického proudu
- Krádež zařízení

  Zde jsou opatření stejná jako u krádeže zařízení u aktiva Hlášení zákazníků.
- Přírodní katastrofa

  Opatření jsou stejná jako u přírodní katastrofy u aktiva Hlášení zákazníků.
- Krádež dat

  Použito zálohování projektové dokumentace na obě místa se servery, i do banky na magnetické pásky.

3. Databázový server (HW) - aktivum

- Výpadek komunikační linky

  Vypadne-li komunikační linka k internetu, databázový server není tímto výpadkem vůbec ohrožen, protože je umístěn ve vnitřní síti.

4. Databázový server (SW) - aktivum

- Přírodní katastrofa

  Jsou zde použita stejná opatření jako u aktiva Projektová dokumentace uvedeném výše.

5 Plán zvládání rizik

Firma má stanoven plán činností, ve kterém jsou uvedeny činnosti podléhající pravidelné kontrole.

Plán má tyto části:

1. **Zálohování**

   Zde je nutné zajistit:

   - pravidelné zálohování zdrojů (firemních dat)
   - zavést pravidelné kontroly úspěšnosti zálohování
   - zavést Disaster Recovery (dále jen DR) testy, při kterých dojde k fingovanému zničení některého nebo veškerého vybavení firmy a následně se snaží firma obnovit zničené vybavení (např. servery, vnitřní infrastrukturu)

   Firma CCA má již vyřešený samotný proces zálohování, avšak je potřeba stanovit kontrolní mechanismy a také zavést DR testování. Firma plánuje v letošním roce 2016 uskutečnit DR testy všech komponent její infrastruktury.

2. **Záložní komunikační infrastruktura**

   Pracovníci Hotline a technická pohotovost musejí mít k dispozici vyhrazená mobilní čísla, na kterých budou k zastižení, a která budou dostatečně známá všem pracovníkům CCA a vybraným zákazníkům.

3. **Záložní zdroje**

   Pro správnou funkčnost záložních zdrojů (UPS - zdroj nepřerušovaného napájení) je potřeba provádět pravidelné kontroly těchto zdrojů. Kontroly ve firmě probíhají a jejich správné chování hlídá interní systém Nagios. Dále je potřeba stanovit pravidla informování zaměstnanců firmy v případě výpadku elektrického proudu v části areálu.

Pro kontrolu zálohování a sledování zdrojů jsou určeni vybraní pracovníci technické podpory. Vnitřní směrnicí jsou stanovena pravidla pro udržování technické pohotovosti. Zajištění potřebných kapacit pro tyto činnosti má na starosti ředitel úseku Vývoj a programování. Pro zajištění funkčnosti služby Hotline jsou vyhrazeni pracovníci pro dobu určenou smlouvou se zákazníkem. Kapacity pro službu Hotline zajišťuje ředitel úseku Zákaznická podpora.

Do 1. poloviny roku 2016 zavede firma CCA polovinu DR testů a do konce roku 2016 jejich zbytek. Vybrané testy budou opakovány měsíčně a jiné v intervalu 3 let.

6 Plán rozvoje bezpečnostního povědomí

Informace o školeních, o činnostech, které se provádí při nástupu nebo odchodu zaměstnance jsou uvedeny v sekci Bezpečnostní politika v části 1.3.

7 Zvládání kybernetických bezpečnostních incidentů

V případě, že někdo ohlásí problém (incident), stanou se tři po sobě jdoucí kroky:

- zjistí se závažnost nalezeného incidentu
- začne se pracovat na jeho rychlém vyřešení i za cenu nedodržení přesných pracovních postupů
- poté, co je již incident úspěšně vyřešen, se provádí analýza příčin incidentu.

Pokud firma najde příčinu, stanoví konkrétní osoby, které dostanou za úkol vyřešit tuto vadu, která způsobila tento incident.

8 Strategie řízení kontinuity činností

Firma má veškeré informace o minimální úrovni jí poskytovaných služeb (tj. nejen HelpDesku) uvedeny v recovery plánu, kde je řečeno, jaké funkce či systémy musí fungovat, aby byla splněna minimální úroveň funkčnosti HelpDesku stanovená v tomto plánu. Obvykle stačí půl dne na obnovení základu, což je vnitřní infrastruktura.

9 Informace o používání firemních směrnic

Firma používá směrnice a metodiky, ve kterých jsou popsány veškeré činnosti probíhající ve firmě. V těchto dokumentech je uveden způsob, jakým jsou zveřejňovány změny ve směrnicích a metodikách. Také probíhá pravidelná kontrola zaměstnanců jejich příslušnými vedoucími. Pokud dojde k tomu, že nějaký zaměstnanec opakovaně (většinou třikrát) nedodrží a neakceptuje novou změnu ve směrnici (metodice), týkající se zejména bezpečnosti, je jeho chování považováno za hrubé porušení pracovní kázně a vede k jeho okamžitému propuštění.