Vysoká škola ekonomická v Praze
Fakulta managementu v Jindřichově Hradci

Diplomová práce

Bc. Radek Švadlenka
2018

Vysoká škola ekonomická v Praze
Fakulta managementu v Jindřichově Hradci

Katedra exaktních metod

Bezpečnost a ochrana dat v ICT prostředí podniku

Autor diplomové práce: Bc. Radek Švadlenka
Vedoucí diplomové práce: Ing. Vladimír Přibyl, Ph.D.
Rok obhajoby: 2018

Čestné prohlášení

Prohlašuji, že diplomovou práci na téma

„Bezpečnost a ochrana dat v ICT prostředí podniku“

jsem vypracoval samostatně a veškerou použitou literaturu a další prameny jsem řádně označil a uvedl v přiloženém seznamu.

V Jindřichově Hradci dne 5. dubna 2018

.....

podpis

Vysoká škola ekonomická v Praze
Katedra exaktních metod

Fakulta managementu
Akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE

Zpracovatel: **Bc. Radek Švadlenka**

Studijní program: Ekonomika a management

Obor: Management

Název tématu: **Bezpečnost a ochrana dat v ICT prostředí podniku**

Zásady pro vypracování:

1. Cílem práce bude definovat možné bezpečností hrozby podniku v ICT prostředí a analyzovat možnosti ochrany před nimi. Výsledky budou interpretovány v kontextu se zákonem o kybernetické bezpečnosti. Kromě teoretické části bude práce obsahovat i praktický příklad řešení této problematiky na vhodném subjektu (např. z oblasti veřejné správy)

Rozsah práce: 60

Seznam odborné literatury:

1. GRADY, M F. -- PARISI, F. (ed.). The law and economics of cybersecurity. New York: Cambridge University Press, 2006. ISBN 0-521-85527-6.
2. JIROVSKÝ, V. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.
3. Doseděl, Tomáš. 2004. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN:80-251-0106-1.
4. NBÚ. 2014. Zákon o kybernetické bezpečnosti. Národní bezpečnostní úřad. [Online] 19.12.2014. http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/provadeci-pravni-predpisy-k-zakonu-c-1812014-sb-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu/.

Datum zadání diplomové práce: říjen 2015

Termín odevzdání diplomové práce: prosinec 2015

Bc. Radek Švadlenka
Řešitel

Ing. Vladimír Přibyl, Ph.D.
Vedoucí práce

doc. Ing. Vladislav Bína, Ph.D.
Vedoucí ústavu

prof. Radim Jiroušek, DrSc.
Děkan FMJH VŠE

Název diplomové práce:

Bezpečnost a ochrana dat v ICT prostředí podniku

Abstrakt:

Cílem této diplomové práce je definovat možné bezpečností hrozby podniku v ICT prostředí a navrhnout opatření na ochranu citlivých informací. Teoretická část práce shrnuje poznatky a informace o normách a metodikách, vztahujících se k tématu. Analytická část popisuje prostředí konkrétní organizace veřejného sektoru z hlediska nasazení a využívání standardů a norem v oblasti informační bezpečnosti. V praktické části jsou pak na základě teoretických poznatků a praktických zkušeností navržena doporučení k efektivnímu modelu řízení ochrany informací.

Klíčová slova:

Informační bezpečnost, hrozba, zranitelnost, útok, aktivum, riziko

Poděkování:

Na tomto místě bych rád poděkoval **Ing. Vladimíru Přibylovi, Ph.D.**, za ochotu, cenné rady, připomínky a čas, který věnoval mé diplomové práci. Zároveň bych chtěl poděkovat zaměstnancům vybrané organizace za čas a informace, které mi poskytli za účelem analýzy jejich informačního prostředí.

Obsah

Úvod **15**
1 Informační bezpečnost **17**
1.1 Historie informační bezpečnosti 18
1.2 Aktuální trendy informační bezpečnosti 21
1.3 Vybrané pojmy informační bezpečnosti 22
2 Bezpečnostní hrozby a rizika **24**
2.1 Hrozby dle původu 24
2.1.1 Hrozby dle motivace útočníka 24
2.1.2 Metody útoků 25
2.2 Hrozby dle druhu aktiva 28
2.2.1 Metody útoků dle charakteru cíle 28
2.3 Další hrozby 29
2.4 Útočníci 29
2.5 Techniky hackerů (crackerů) 31
2.6 Malware 32
3 Ochrana informací **35**
3.1 Správa informační bezpečnosti 35
3.2 Řešení informační bezpečnosti 36
3.2.1 Systém řízení informační bezpečnosti 38
3.3 Zabezpečení informačního systému 40
3.3.1 Softwarová/hardwarová bezpečnostní opatření 41
4 Kryptografie **47**
4.1 Základní pojmy kryptologie 48
4.2 Symetrické šifry 48
4.3 Asymetrické šifry 50
4.4 Útoky na kryptografické algoritmy 51
5 Legislativa a normy **53**
5.1 NBÚ 53
5.2 Kybernetický zákon 54
5.3 GDPR 56
6 Analýza vybraného subjektu veřejného sektoru **58**
6.1 Základní informace o podniku 58
6.2 Správa a řízení informační bezpečnosti v organizaci 59
6.2.1 RAMSES 60
6.2.2 ISMS 63
6.3 Legislativa 64
6.3.1 Kybernetický zákon 64

6.3.2 GDPR ... 65
6.4 Fyzická a HW bezpečnost ... 65
6.5 Sítě a komunikace ... 66
6.5.1 Segmentace sítě a internet ... 66
6.5.2 LAN (Local Area Network) ... 68
6.5.3 WAN (Wide Area Network) ... 69
6.5.4 Hlasová komunikace a WIFI ... 70
6.6 SW nástroje informační bezpečnosti ... 71
6.6.1 Antivir a antispam ... 71
6.6.2 Mobile device management ... 72
6.6.3 Důvěryhodný archiv ... 72
6.6.4 Identity services engine ... 74
6.6.5 Security information and event management ... 74
6.6.6 Další využívané služby informační bezpečnosti ... 74
7 Shrnutí a doporučení ... 76
Závěr ... 81

Seznam obrázků

Obrázek 1 – Mapa sítě ARPANET USA 1971 19
Obrázek 2 - Historie a vývoj malware 20
Obrázek 3 – Model analýzy rizik organizace 23
Obrázek 4 – Vývoj celkového množství malware v síti internet 32
Obrázek 5- Model pro řízení bezpečnosti informací 39
Obrázek 6- Firewall v modelu OSI 42
Obrázek 7 - NetFlow architektura 45
Obrázek 8 - Princip fungování symetrické šifry 49
Obrázek 9 - Princip asymetrické šifry 50
Obrázek 10 - Model propojení kybernetického zákona s ISMS 55
Obrázek 11 - Časová osa plnění povinností 56
Obrázek 12 - Report souladu s normou ISO v prostředí RAMSES 61
Obrázek 13 – Report stavu protiopatření systému RAMSES 62
Obrázek 14 - Model DMZ s jedním firewallem 67
Obrázek 15 - Topologie LAN 68
Obrázek 16 - Mezinárodní datová síť X-BONE 70
Obrázek 17 - Princip bezpečné archivace 73
Obrázek 18 - Magický čtyřúhelník společnosti Gartner 78

Úvod

Ve své diplomové práci jsem se rozhodl zpracovat téma „Bezpečnost a ochrana dat v ICT prostředí podniku“. Tato oblast je pro mne zajímavá z důvodu mé pracovní specializace v oboru ICT služeb, kde bych rád rozšířil svoje znalosti.

Současná společnost spoléhá na informační a komunikační systémy a stává se na nich závislá. Ohrožení jejich funkčnosti může způsobit nemalé finanční komplikace, ale v některých případech třeba i ztráty na lidských životech. Vlivem dynamiky vývoje ICT prostředí vznikají nové a nové hrozby, před kterými je třeba mít se neustále na pozoru. Jako reakce na nová rizika pro chod státu a jeho institucí byl přijat zákon o kybernetické bezpečnosti, který představuje nový právní rámec pro řešení velkých bezpečnostních incidentů.

Cílem mé práce je definovat možné bezpečností hrozby podniku v ICT prostředí a navrhnout opatření na ochranu informací. Výsledky budou interpretovány v kontextu se zákonem o kybernetické bezpečnosti a porovnány na praktickém příkladu konkrétního subjektu veřejného sektoru. Jedinečnost práce bude zajištěna aktuálními informacemi z prostředí organizace na základě osobních setkání a rozhovorů přímo od odpovědných zaměstnanců daného subjektu. Práce může posloužit jako vodítko pro management IT/ICT oddělení většího podniku, jak správně definovat oblast bezpečnosti a ochrany dat ve své společnosti.

Úvodní kapitola teoretické části obecně definuje pojem informační bezpečnost ve smyslu důležitosti ochrany informací podniku před jejich zneužitím. Zároveň uvádí čtenáře do problematiky současného světa informačních a komunikačních technologií a jeho enormně rychlého vývoje. Druhá kapitola rozkrývá současné bezpečnostní hrozby a rizika v podobě popisu možného ohrožení dat z vnějšího tak i vnitřního prostředí. Kapitola s názvem „Ochrana informací“ se zabývá aktuálními metodami a možnostmi prevence informačních hrozeb. Součástí je i definice a popis možných nástrojů ochrany. Speciální pozornost je věnována šifrování dat jako osvědčené metody pro ochranu přenosu, sdílení a uchovávání informací. Závěr teoretické části patří problematice kybernetického zákona a z něj plynoucích povinností pro vyjmenované subjekty. Součástí je i rozbor souvisejících norem a jejich funkce a důsledků. V praktické části se pokusím navrhnout efektivní řešení ochrany dat formou doporučení pro reálný podnik veřejné sféry korporátní velikosti.

Praktická část práce se věnuje ochraně informací v praxi na příkladu reálného subjektu veřejného sektoru. Pro tuto část práce jsem stanovil dvě hypotézy. První hypotézou je tvrzení, že subjekty kritické infrastruktury veřejné správy jsou efek-

tivně chráněny proti kyberútokům. Druhou stanovenou hypotézou je tvrzení, že současná legislativa ČR, týkající se informační bezpečnosti, dostatečně podchycuje možné informační hrozby pro subjekty kritické infrastruktury veřejné správy. Pomocí techniky expertního rozhovoru se zástupci středního a vyššího managementu odpovědných oddělení vybraného státního podniku zjišťuji, jak je řešena problematika bezpečnosti informací v této organizaci. Výzkumné otázky jsou pokládány od obecných ke specifickým tak, aby výsledek výzkumu byl co nejvěrnější. Výsledky výzkumu pak podrobuji rozboru na základě teoretických znalostí a praktických zkušeností a pokouším se zhodnotit efektivitu ochrany informací a formou doporučení navrhuji vylepšení některých opatření. Z důvodu etiky a také citlivosti informací vztahujících se k interním procesům vybraného podniku není možné zveřejnit analytickou část práce.

1 Informační bezpečnost

Informační bezpečnost je souhrnné označení pro aktivity směřující k ochraně informací. Jejím cílem je zejména ochrana informací a dat před negativními událostmi, jako je jejich ztráta, odcizení, únik, zneužití, zničení, narušení či změna. Informační bezpečnost je součástí organizačního řízení bezpečnosti. Zahrnuje práci s informacemi jako celek. Její součástí je tzv. počítačová bezpečnost, která se zabývá bezpečností na úrovni ICT technologií. „*Počítačová bezpečnost je stav, kdy je dosaženo dostupnosti, integrity a důvěrnosti* (Čech, a další, 2002)."

Dostupnost je definována jako situace, kdy je informace přístupná pro oprávněné uživatele v okamžiku její potřeby. Narušení dostupnosti se označuje jako nedostupnost nebo nežádoucí zničení. Dostupnost je obvykle vyjádřena jako procento času v daném období (Požár, 2005).

Integrita je dle Požára (Požár, 2005) popisována stavem, kdy je zajištěna správnost a úplnosti informací. O nežádoucí modifikaci se proto v informační bezpečnosti hovoří jako o narušení integrity. V případě integrity je třeba si uvědomit, že pokud dojde k nežádoucí změně dat, a to ať už úmyslně, náhodou, nebo technickým selháním v důsledku působení vyšší moci, nemusí být tato nežádoucí změna vůbec odhalena a může uplynout dlouhá doba, než si někdo něčeho všimne. Čím později se na tento bezpečnostní incident přijde, tím závažnější bude jeho dopad.

Důvěrnost je definována jako zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni. O nežádoucím zpřístupnění určitých informací se v informační bezpečnosti proto hovoří jako o narušení jejich důvěrnosti. Většina společností pracuje se spoustou informací, které je třeba klasifikovat a volba vhodného klasifikační schématu je proto pro úspěšné zavedení klasifikace informací ve společnosti naprosto zásadní. V organizacích veřejného sektoru, např. dle Doseděla (Doseděl, 2004), se nejčastěji využívá následujícího schématu:

- **Přísně tajné** – nejvyšší stupeň, nežádoucí zpřístupnění těchto informací může mít zcela zničující dopad na národní bezpečnost.
- **Tajné** – nežádoucí zpřístupnění těchto informací může mít značný dopad na národní bezpečnost.
- **Důvěrné** – nežádoucí zpřístupnění těchto informací může mít významný dopad na národní bezpečnost.
- **Citlivé** ale neklasifikované – nežádoucí zpřístupnění těchto informací by nemělo mít významný dopad na národní bezpečnost.

- **Neklasifikované** – nejnižší stupeň, nežádoucí zpřístupnění těchto informací by nemělo mít žádný dopad na národní bezpečnost.

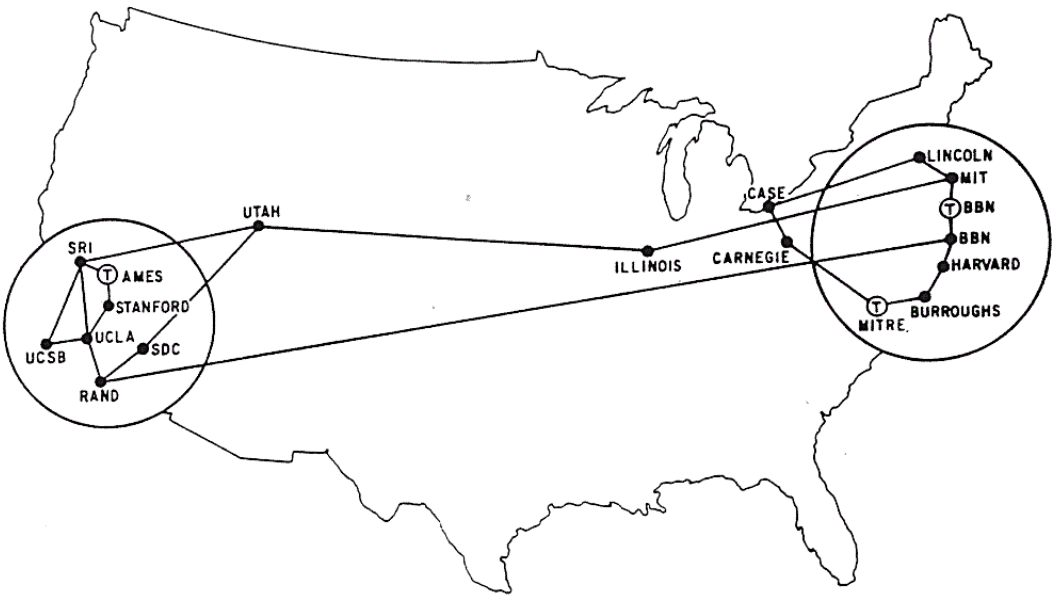
Některé zdroje (Čech, a další, 2002) připouští navíc do oblasti počítačové bezpečnosti i pojem odpovědnost, která přisuzuje uživatelům následky za své aktivity při práci s informacemi.

1.1 Historie informační bezpečnosti

Informační bezpečnost vzniká spolu s informacemi, které bylo potřeba chránit. Prvopočátky ochrany informací je možné nalézt již v historii starší než 2000 let. Mezi nejčastější uživatele patřily různé formy vlád a armádní složky, kde případné zneužití informací představovalo riziko ekonomických ztrát, mocenských bojů či prohrané bitvy. Při zmínkách o této historii je možné hovořit o počátcích kryptografie, která se později vyvinula ve významný vědní obor. Právě luštění kódů se stalo stěžejním momentem druhé světové války, kdy Alan Turing se svým týmem prolomil německou šifru Enigma a napomohl tak k urychlení vítězství spojeneckých sil (Piper, a další, 2006).

Až v šedesátých letech dvacátého století je možné sledovat první pokusy o systematické řešení ochrany dat. A byl to právě extrémně rychlý rozvoj informačních technologií, který napomohl rozvoji této disciplíny. V roce 1969 byla spuštěna první počítačová síť ARPANET (Advanced Research Projects Agency Network), která měla zpočátku za cíl přenos datové komunikace mezi čtyřmi univerzitami ve Spojených státech amerických. Projekt byl financován grantovou agenturou (DARPA) ministerstva obrany USA. ARPANET se postupně šířil do dalších uzlů komunikace a v roce 1973 pronikl do Evropy, kdy se k němu připojilo Norsko a později Velká Británie. ARPANET je možné považovat za předchůdce dnešní sítě internet. V roce 1971 napadl síť ARPANET první počítačový virus s názvem Creeper, který ji vyřadil z provozu. K jeho odstranění byl pak vytvořen program Reaper, který je považován za první antivirový program na světě. Vznik samostatného oboru počítačové bezpečnosti je datován k únoru 1970, kdy byl v USA publikován první odborný článek na téma bezpečnosti počítačových systémů. V sedmdesátých letech byl také navržen koncept digitálního podpisu včetně jeho úspěšného testování v praxi za podpory algoritmu RSA (Jirovský, 2007).

Obrázek 1 – Mapa sítě ARPANET USA 1971



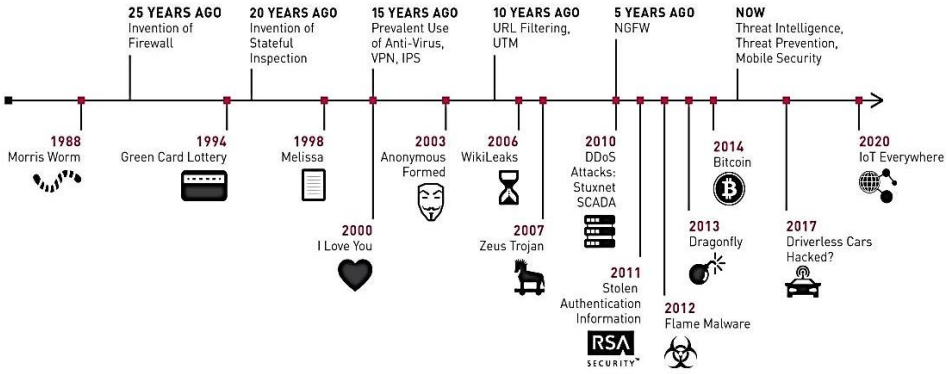
Zdroj: Martin Dodge (An atlas of cyberspaces 2007)

Léta osmdesátá pak začala ve znamení nárůstu aktivit týkajících se počítačové bezpečnosti. Bylo vydáno první číslo odborného časopisu Computers & Security. Organizují se první kryptologické konference. V roce 1983 vzniká Technical Committee on Security and Protection in Information Processing Systems. Roste i aktivita ze strany hackerů. V roce 1981 byl založen Chaos Computer Club jako největší evropská asociace hackerů v německy mluvících zemích. Téhož roku Ian Murphy pod přezdívkou „Captain Zac" pronikl do počítačové sítě AT&T a stal se tak prvním hackerem odsouzeným za počítačovou kriminalitu. V roce 1984 bylo v USA publikováno první vydání časopisu 2600: The Hacker Quarterly. V tomto období se začala vydávat první oficiální kritéria hodnocení bezpečnosti počítačových systémů, dnes známá jako Orange Book. Vznikla první vědecká definice počítačového viru a americký kongres v roce 1986 přijal Computer Fraud and Abuse Act, jako jeden z prvních pokusů legislativního ošetření počítačové bezpečnosti. Masivní rozvoj osobních počítačů podpořil rozvoj počítačových virů. Za zmínku stojí virus „Brain", který byl vytvořen na počátku roku 1986 a jako první napadal osobní počítače kompatibilní s IBM PC a operačním systémem MS-DOS. Mediálně se proslavil i virus Vienna, který na konci osmdesátých let jako první způsobil celosvětovou epidemii. Po aféře s prvním internetovým červem (Morrisův červ), vznikla v roce 1988 skupina Computer Emergency Response Team (CERT), která měla zajistit přiměřenou reakci na bezpečnostní hrozby a incidenty. V roce 1989 bylo vydáno první číslo ča-

sopisu Virus Bulletin, jehož obsah se soustředí na problematiku počítačových virů (Erben, 2014).

Počátek devadesátých let se nesl v duchu růstu využívání sítě internet pro komerční účely. S rozvojem internetových služeb se stále více kladl důraz na informační bezpečnost. V roce 1991 programátor Phil Zimmerman uveřejnil svůj Pretty Good Privacy (PGP) program, který pomocí algoritmu RSA pro asymetrickou kryptografii umožňuje zabezpečení elektronické pošty. Pozadu nezůstali ani tvůrci počítačových virů. V roce 1992 způsobil, alespoň mediálně, digitální apokalypsu počítačový virus Michelangelo. Na miliony uživatelů PC měl zaútočit 6. března a smazat z nich všechna data. Reálně způsobené škody byly ale nakonec minimální. V devadesátých letech se objevují první makroviry napadající textové a tabulkové procesory. Celosvětově známým se stal makrovirus Melissa, který v roce 1999 způsobil přetížení některých internetových serverů. V červnu 1993 byla v Las Vegas uspořádána první z každoročních hackerských konferencí DEF CON. Nejznámějším hackerem této doby se stal bezesporu Američan Kevin Mitnick, který se díky četné počítačové kriminalitě dostal do seznamu deseti nejhledanějších osob FBI. S jeho nelegální činností je poprvé spojováno tzv. sociální inženýrství (manipulace s lidmi za účelem získání informace). Dle Government Accountability Office (GAO) bylo jen v roce 1995 na počítačovou síť amerického ministerstva obrany provedeno více než 250 tisíc útoků, z nichž více než polovina byla úspěšných (Jirovský, 2007).

Obrázek 2 - Historie a vývoj malware



Zdroj: John Yan (Annual security report 2015)

Začátek nového milénia se vyznačuje rapidním rozvojem informačních a komunikačních technologií a s ním přichází stále větší závislost na ICT systémech. Nové možnosti však s sebou přináší stále větší riziko nových hrozeb, proti kterým je nutné se efektivně chránit. Do centra zájmu útočníků se krom tradičních cílů dostávají mobilní platformy, wifi sítě, ale i sociální sítě a instant messaging aplikace s cílem

zisku důvěrných textových informací a obrazových dat. Počátek jednadvacátého století zároveň přinesl masové rozšiřování spammingu za pomoci trojských koní a botů. Zároveň byl zaznamenán vysoký nárůst počtu e-mailových červů, každoročně přibývá pokusů o phishing a útočníci stále častěji využívají spyware jako nástroj k nelegálnímu obohacení (Grady, a další, 2011).

1.2 Aktuální trendy informační bezpečnosti

Růst zájmu o informační bezpečnost je v posledních letech opravdu enormní. Vzhledem k tomu, jak rychle se informační a komunikační technologie mění, vyvíjejí se velmi rychle i kybernetické hrozby. V horizontu mnoha let zpět se útočníci soustředili zejména na nejvíce rozšířené operační systémy společnosti Microsoft. Díky důsledné bezpečnostní politice Microsoftu však již vytvoření škodlivého software není tak jednoduché. Proto je možné sledovat nárůst útoků na jiných platformách a také návrat k technikám sociálního inženýrství. Dá se očekávat, že se hrozby budou stále častěji dotýkat také mobilních platforem a internetu věcí, kde mnohdy neexistují efektivní prvky ochrany. Speciálně mobilní platební systémy se budou stávat terčem mnohých útočníků. Aktuálním oříškem mnohých IT specialistů se stává ransomware, který bude podrobněji popsán v následující kapitole. Společně s růstem obav o důležitá data je možné sledovat využití šifrovacích mechanismů jako standardní součást systémů a aplikací. Ruku v ruce s tím, jak jsou technologie stále běžnější součástí našeho života a tvoří jeden ze základů globální ekonomiky, uvědomují si vlády i firmy rostoucí důležitost znalostí a dovedností souvisejících s informační bezpečností. Někteří autoři (Grady, a další, 2011) zastávají názor, že znalostní propast mezi skutečným a požadovaným stavem se bude nadále prohlubovat. V souvislosti s mezinárodními konflikty, ekonomickou a politickou nestabilitou se stále častěji hovoří o kyberterorismu jakožto nové metodě dosažení cílů za pomoci politicky motivovaných útoků vedených proti informačním sítím, počítačovým programům a datům. Útoky proti komunikačním technologiím jsou stále sofistikovanější a komplexnější. Ze sféry přímého ekonomického prospěchu individuálních útočníků se útoky přesouvají do oblasti organizované kybernetické průmyslové špionáže a kybernetického terorismu. Útočníci se stále více zaměřují na prvky kritické infrastruktury, jako jsou energetické systémy, zdravotnické systémy a informační systémy veřejné správy.

„Rostoucí užití informačních a komunikačních technologií v činnostech organizací vyžaduje, aby při zpracování, přenosu, ukládání a opětovném využití objemů dat nedocházelo ke ztrátě životně důležitých údajů, ke vzniku chyb, kompromitaci či neoprávněné modifikaci dat (Požár, 2005)*.“* Informační bezpečnost se v posledních letech stává významným faktorem úspešnosti organizace, je tedy v zájmu každé

společnosti kvalitně chránit svá aktiva efektivní ochranou citlivých dat a informací. K tomu je zapotřebí podpora na všech úrovních managementu organizace tak, aby definovaná bezpečnostní opatření přijali všichni zaměstnanci společnosti a důsledně se jimi řídili. Důležitou součástí efektivní ochrany informací je opora v legislativě. Ta bohužel zejména díky extrémně rychlému vývoji v této oblasti dost často nereflektuje aktuální potřeby organizací.

1.3 Vybrané pojmy informační bezpečnosti

Informační systém (IS) je *„celek složený z počítačového hardwaru a souvisejícího softwaru, k němuž patří také lidé, kteří je využívají, a procesy (činnosti), které přitom vykonávají za účelem sběru, zpracování a šíření informací potřebných k plánování, rozhodování a řízení* (Blackstone, a další, 2013).*“* Dle Molnára (Molnár, 2009) se jedná o *„soubor lidí, technických prostředků a metod (programů), zabezpečujících sběr, přenos, zpracování, uchování dat, za účelem prezentace informací pro potřeby uživatelů činných v systémech řízení.“* Pro podnikové informační systémy je charakteristická integrace více programů do jednoho celku, který vykonává komplexní úlohy pro celou organizaci. Jádro informačních systémů bývá provozováno na výkonných serverech a jednotliví uživatelé přistupují k datům, často i vzdáleně, prostřednictvím klientských stanic jako jsou stolní počítače, notebooky, tablety či chytré telefony.

Aktivum (Asset) je v podstatě vše, co má pro organizaci nějakou hodnotu. Za nejcennější aktiva jsou považovány peníze, majetek, ale i data a informace, jejichž zneužití, ztráta či modifikace mohou způsobit škodu organizaci (Požár, 2005).

Bezpečnost (Security) je chápána jako vlastnost informačního systému či technologie, která určuje stupeň jeho ochrany proti možným hrozbám či škodám (Jirovský, 2007).

Hrozba (Threat) je potenciální příčina nežádoucího incidentu, který může mít za následek poškození, zničení či ztrátu hodnoty aktiva. Hrozba může narušit bezpečnost (Čech, a další, 2002).

Riziko (Risk) je dle (Požár, 2005) vnímáno jako potenciální možnost, že daná hrozba způsobí poškození nebo zničení aktiv.

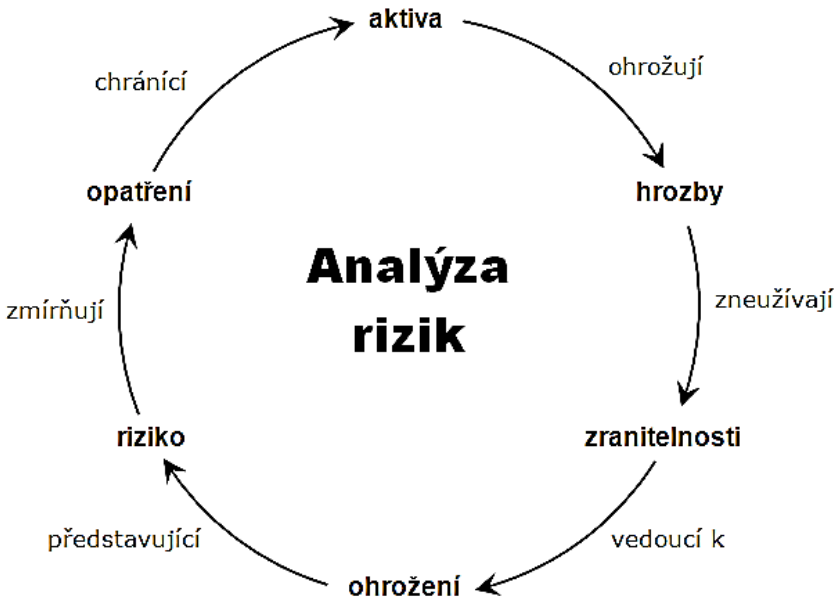
Ocenění rizik (Risk Assessment) je vyhodnocení pravděpodobnosti selhání bezpečnosti, které by se mohlo vyskytnout působením hrozeb na zranitelná místa s dopady na konkrétní aktiva. Výsledkem je zjištění, zda jsou bezpečnostní opatření na takové úrovni, aby se šance na vznik škody snížila na přijatelnou úroveň (Doseděl, 2004).

Zranitelnost (Vulnerability) je slabé místo bezpečnostního systému, které může být zneužito jednou nebo více hrozbami s cílem poškození či zničení hodnoty aktiv (Kurose, a další, 2014).

Útok (Attack) je chápán jako bezpečnostní incident, při kterém, za využití zranitelného místa, dochází ke ztrátám na aktivech organizace (Jirovský, 2007).

Dopad (Impact) je pak výsledkem nežádoucího incidentu.

Obrázek 3 – Model analýzy rizik organizace



Zdroj: www.cleverandsmart.cz

2 Bezpečnostní hrozby a rizika

Součástí všech informačních systémů jsou zranitelná místa, jejichž existence představuje hrozby. Zranitelnost informačních systémů představuje jejich obecnou vlastnost. Situace, kdy hrozba zkouší působit na zranitelné místo s cílem ohrozit informační bezpečnost aktiva, je možné označit za **bezpečnostní událost**. V případě, že se působením hrozby naruší vlastnosti aktiva natolik, že dojde k narušení informační bezpečnosti, vzniká **bezpečnostní incident**. Bezpečnostní incident je možné považovat za stav aktiva a bezpečnostní událost za aktivitu, jež k tomuto stavu vede. Největším problémem rozvoje ICT je rychlý a hlavně nepřetržitý vývoj bezpečnostních hrozeb. Bezpečnostní hrozby je možné dělit dle různých hledisek (GORDIC spol. s r.o., 2017).

2.1 Hrozby dle původu

Z hlediska subjektu iniciace lze hrozby rozdělit na objektivní a subjektivní. Mezi **objektivní** hrozby patří přírodní katastrofy jako povodně, blesky, požáry, zemětřesení. Fyzické a fyzikální příčiny vyvolávají objektivní hrozby v podobě výpadků napětí, elektromagnetického záření atp. a nakonec technické příčiny je možné chápat zejména jako poruchy HW a SW. Naproti tomu **subjektivní** hrozby plynou z působení lidského faktoru. Mohou být **neúmyslné**, např. působení neznalého uživatele či nezkušeného správce systému, anebo **úmyslné**, které jsou spojované s existencí vnějších útočníků, jako jsou hackeři, konkurenti, teroristé, špioni atp., ale i útočníků vnitřních. „***Útočník*** *či narušitel je osoba, která získá, případně se snaží získat větší než přidělená práva nebo neoprávněný přístup k informačnímu systému* (Soriano, 2016)." Dle Požára (Požár, 2005) až 80% útoků na IT je vedeno zevnitř organizace. Aktuální zdroje tento údaj potvrzují (GORDIC spol. s r.o., 2017). Útočníkem bývá často rozzlobený, vydíraný, propuštěný nebo pouze chamtivý zaměstnanec s motivací finančního zisku či pomsty (Požár, 2005).

2.1.1 Hrozby dle motivace útočníka

Autor (GORDIC spol. s r.o., 2017) uvádí, že dle motivace útočníka lze hrozby dělit do následujících skupin:

- Hrozby za účelem získání finančního prospěchu
- Hrozby za účelem získání konkurenční převahy
- Hrozby za účelem dokázání svých schopností
- Hrozby za účelem odplaty
- Hrozby z důvodu neplnění povinností

2.1.2 Metody útoků

Bezpečnostní útoky je možné popsat jako různé druhy systematických činností zacílených na snížení nebo narušení bezpečnosti. Z tohoto hlediska je možno útok definovat jako systematickou hrozbu způsobenou nějakou entitou, a to uměle, úmyslně a inteligentně. Útoky je dle (Soriano, 2016) možné vést:

• **přerušením** (interruption) - aktivní útok na dostupnost (např. ztráta, znepřístupnění, poškození aktiva, porucha periferie, vymazán programu, vymazání dat, porucha v operačním systému),

• **odposlechem** (interception) - pasivní útok na důvěrnost, kdy neautorizovaný subjekt si neoprávněně zpřístupní aktiva (např. okopírování programu nebo o okopírování dat, odposlech prováděný při datových přenosech po síti),

• **změnou** (modification) - aktivní útok na integritu, neautorizovaný subjekt zasáhne do aktiva (např. změna uložených nebo přenášených dat, přidání funkce do programu),

• **přidáním hodnoty** (fabrication) - aktivní útok na integritu nebo útok na autenticitu, tj. případ, kdy neautorizovaná strana něco vytvoří (podvržení transakce, dodání falešných dat).

Bezpečnostní útoky je možné rozdělit do dvou hlavních kategorií:

1. **pasivní útoky**
2. **aktivní útoky**

Cílem pasivních útoků je získat nebo využít informace ze systému. Jedná se o nejstarší formu útoků. Při pasivním útoku útočník pouze monitoruje komunikační kanál a ohrožuje důvěrnost dat. Povaha pasivních útoků tedy spočívá v odposlouchávání či monitorování přenosu s cílem získat přenášené informace (Soriano, 2016).

Definovány jsou dva typy pasivních útoků, které jsou zaměřeny na obsah zpráv nebo na analýzu provozu:

• **Odposlouchávání**

Většina síťové komunikace probíhá v nezabezpečeném formátu, tedy v podobě nešifrovaného textu, což umožňuje útočníkovi, který získal přímý přístup k přenosové cestě v síti, aby „naslouchal“, neboli interpretoval přenášená data. Možnost odposlechu síťového provozu je považována za největší bezpečnostní problém, se kterým se setkávají správci podnikových sítí. Nejsou-li použity silné šifrovací služby

založené na bezpečných kryptografických principech, mohou ostatní uživatelé zcela volně číst data přenášená v síti (Soriano, 2016). Typickým příkladem je síťový odposlech (wiretapping), při kterém dochází k odposlechu síťové komunikace probíhající zpravidla na standardních protokolech TCP/IP.

• **Analýza provozu**

V případě analýzy provozu jde o zachycování a zkoumání přenášených zpráv s cílem odvodit určité informace z typického průběhu komunikace. To je možno provádět i v případě, kdy jsou zprávy šifrovány a nelze je dešifrovat. Obecně platí, že čím větší je počet zpráv, které jsou takto sledovány, nebo dokonce zachyceny a uloženy, tím více poznatků můžeme ze síťového provozu vyvodit (Erben, 2014).

Naproti tomu aktivní útoky usilují o změnu systémových prostředků nebo ovlivnění jejich funkčnosti. Při tomto typu útoku se útočník snaží data přenášená příslušným kanálem odstranit, přidat nebo jinak měnit. Aktivní útočník ohrožuje integritu dat, jakož i autentizaci a důvěrnost. Součástí aktivních útoků je určitá změna datového toku nebo vytvoření toku falešného. Autor (Požár, 2005) uvádí, že tyto útoky je možné rozdělit do následujících kategorií:

• **Podvádění** (Phishing, Spoofing) - Útočník se snaží oklamat uživatele a získat jeho citlivé informace (např. přihlašovací údaje do systému). Typickým příkladem je rozesílání e-mailových zpráv odkazujícího adresáta do falešného systému, který však vypadá zcela důvěryhodně a vyzývá uživatele k zadání osobních nebo přihlašovacích údajů.

• **Maškaráda** (Masquerading) - Jedná se o typ útoku, kdy útočník předstírá, že je oprávněným uživatelem, a jeho cílem je získat přístup k systému, případně větší uživatelská práva, než jaká mu náleží. Jedná se o formu podvodu často s cílem přisvojení nebo vyřazení z činnosti prostředků informačních systémů. Jistou legální formu maškarády je delegace, kdy uživatel deleguje jinému uživateli právo provádět některé úkony nebo operace jeho jménem.

• **Průnik do systému** (System penetration) - Průnik nastává, když se neautorizované osobě podaří získat přístup do systému např. za účelem neoprávněné modifikace dat, získání důvěrných dat, neoprávněného použití zdrojů systému nebo blokování některých služeb. Typickým příkladem je zcizení přihlašovacích údajů uživatele a jejich zneužití neautorizovaným přihlášením do systému.

• **Narušení autorizace** (Autorization violation) - Jedná se o situaci, ve které se útočníkovi podaří provést určitou operaci, na kterou nemá autorizaci (neoprávněná

modifikace dat, získání důvěrných dat, neoprávněné použití zdrojů systému nebo blokování některých služeb). Na rozdíl od průniku do systému se v případě narušení autorizace podaří útočníkovi obejít zabezpečení systému.

• **Škodlivý software** (Malware) - Jedná se o implantaci škodlivého softwaru (počítačové viry, trojské koně, počítačoví červi) na různé řídící nebo uživatelské stanice informačního systému. Zpravidla se jedná o přípravu na další útok (odesílání citlivých nebo přihlašovacích údajů uživatelů, napadání nebo modifikace systému, využívání zdrojů, další šíření na jiné stanice informačního systému apod.).

• **Zpožďování** (Delay) - Při tomto druhu útoku je původní zpráva zlomyslně (podvodně) opakována nebo zpožděna. To provede buď odesílatel, nebo útočník, který data zachytí a znovu odvysílá, například v rámci útoku typu maškaráda.

• **Modifikace přenášených dat** (Modification, Alternation) - V tomto případě útočník odstraní zprávu ze síťového toku, pozmění ji a znovu ji odešle do sítě. Jedná se o falzifikaci dat za účelem oklamat jejich příjemce tak, aby reagoval způsobem škodlivým jeho zájmům. Modifikovaná data mohou sloužit také pro řízení chodu systému způsobem, který útočník zamýšlí.

• **Člověk uprostřed** (Man in the Middle) - Útočník odposlouchává komunikaci mezi dvěma stranami – obvykle mezi koncovým uživatelem a webovým serverem. Útočník může takto získané informace zneužít ke zcizení identity nebo k jiným podvodům.

• **Odepření služby** (DoS – Denial of Service) a **Distribuované odepření služby** (DDoS – Distributed DoS) - Útok typu DoS je incident, při němž uživatel nebo organizace přijde o služby poskytované určitým zdrojem, které by za normálních okolností měly být k dispozici. V případě distribuovaného odepření služby využívá útočník velké množství napadených počítačů (tzv. botnet) k zahlcení cílového systému. Typickým příkladem je blokování služeb zahlcením požadavky (např. zahlcení webového serveru požadavky na příjem www stránek).

• **Trvalá významná hrozba** (APT – Advanced Persistent Threat) - Jedná se o specifický typ útoku, při němž neoprávněná osoba získá přístup k síti a zůstane po dlouhou dobu neodhalena. Cílem útoku APT je obvykle krádež dat, nikoli přímé poškození sítě nebo jejího vlastníka. APT útoky se zaměřují na organizace působící v odvětvích, kde se pracuje s cennými informacemi (např. armáda, průmysl či finančnictví) (Soriano, 2016).

2.2 Hrozby dle druhu aktiva

Dle charakteru cíle je možné hrozby dále dělit do následujících skupin:

- Hrozby pro hardware
- Hrozby pro síť
- Hrozby pro operační systém
- Hrozby pro aplikace
- Hrozby pro informace
- Hrozby pro uživatele (GORDIC spol. s r.o., 2017)

2.2.1 Metody útoků dle charakteru cíle

Útoky na hardware lze vést přerušením, odposlechem nebo přidáním hodnoty. Typickým příkladem útoku přerušením je krádež či destrukce hardwaru. Lze sem však zařadit také neúmyslné útoky jako přírodní katastrofy nebo požáry. K příkladům útoků na hardware odposlechem je možné zařadit např. krádež času procesoru nebo místa v paměti. Útoky na hardware přidáním hodnoty vznikají implementací škodlivého hardwaru či změnou režimu činnosti (Burda, 2005).

Útoky na software lze vést přerušením, odposlechem, změnou, ale i přidáním hodnoty. Mezi neúmyslné útoky přerušením může patřit vymazání softwaru způsobené špatným konfiguračním systémem nebo archivačním systémem, použitím neotestovaných programů nebo chybou operátora. Mezi úmyslné útoky patří např. vymazání programu. Útoky na software odposlechem vznikají typicky prováděním neoprávněných kopií programu. Využití chyb softwaru je typickým příkladem útoku vedeného změnou. Do útoků na software přidáním hodnoty je možné zařadit implantaci virů, červů či trojských koňů (Burda, 2005).

Útoky na data lze opět vést přerušením, odposlechem, změnou nebo přidáním hodnoty. Mezi útoky na data přerušením lze zařadit neúmyslné či úmyslné vymazání dat nebo v extrémním případě sabotáž. Získání neoprávněných kopií dat je možné charakterizovat jako útok vedený odposlechem. Útoky na data odposlechem jsou typicky spojeny s neautorizovanou modifikací dat. A nakonec k útokům na data přidáním hodnoty je možné zařadit např. generování falešných dat či transakcí (Burda, 2005).

2.3 Další hrozby

Dle serveru kybez.cz (GORDIC spol. s r.o., 2017) je hrozby dále možné dělit např. z hlediska směrování na bezpečnostní atributy:

- Hrozby dostupnosti (např. DDoS útok, požár)
- Hrozby integrity (např. chyba v databázové transakci)
- Hrozby důvěrnosti (např. krádež notebooku)

Pravděpodobnost, že se uplatní některá z výše uvedených hrozeb nebo zranitelných míst informačních systémů je vyjádřena hodnotou informačního rizika. Úroveň rizika se zjišťuje v procesu, který se nazývá analýza rizik. Spočívá v odhalení a definici možných hrozeb a v určení pravděpodobnosti, že hrozba bude prostřednictvím nějakých slabin uskutečněna (Požár, 2005).

2.4 Útočníci

Útočníky je možné řadit do kategorií dle různých hledisek. Základní kritéria používaná pro tuto klasifikaci jsou následující:

- **Umístění útočníka vzhledem k napadenému systému**
- **Úroveň útoku**
- **Cíle útoku (důvody útoku)**

Dle umístění je možné definovat útočníky jako vnitřní (**insider**) a vnější (**outsider**). Insider je obecně osoba, která má přístup k vnitřní počítačové síti. Jde tedy o oprávněného uživatele, který se však pokouší získat neoprávněný přístup k datům, systémovým prostředkům a službám, případně zneužívá data, která jsou mu v rámci běžných oprávnění přístupná. Naproti tomu outsider je útočník, který nemá oprávnění k přístupu do vnitřní počítačové sítě, chce do ní však proniknout a k tomu využívá zranitelná místa nebo bezpečnostní díry (Soriano, 2016).

Podle kvalitativní úrovně útoku lze dělit útočníky také do dvou hlavních skupin:

- **Amatéři**
- **Profesionálové**

Amatéři pravidla provádějí méně nebezpečné útoky než profesionálové, protože disponují nižší kvalifikací a horším vybavením. Profesionálové jsou však obvykle

špičkoví počítačoví odborníci, kteří mají přístup ke specializovaným zdrojům, jsou vysoce kvalifikovaní a mají velké zkušenosti. V praxi to znamená, že jsou schopni vést velmi nebezpečné útoky s vážnými následky pro počítačové systémy a sítě (Soriano, 2016).

Asi nejvíce diskutované je dělení útočníků dle motivace při jejich jednání. Zde můžeme klasifikovat dvě kategorie:

- **Hacker**
- **Cracker**

Obecně lze definovat hackery a crackery jako jedince, kteří mají zevrubné znalosti počítačových systémů a zejména síťových mechanismů, jichž však užívají k dosažení odlišných cílů.

Hacker mívá zpravidla vynikající dovednosti v oblasti IT, často se podílí na významných softwarových projektech a jeho znalosti a know-how jsou užitečné při vyhledávání zranitelných míst a bezpečnostních děr ve vyvíjeném systému. Jeho činnost tedy bývá prospěšná a užitečná. Existují dokonce i kodexy (psaná pravidla) pro chování hackerů (Soriano, 2016).

Naproti tomu **crackerem** je označován útočník, který umí překonat protipirátské ochrany počítačových programů a využívá své znalosti neetickým způsobem. Existuje však více definic této skupiny útočníků, které zdůrazňují odlišné oblasti jejich činnosti (Erben, 2014).

Dle Požára (Požár, 2005) označení „cracker“ téměř vymizelo. Hackeři jsou děleni na tzv. **White hats, Balck hats a Grey hats**. White hat hacker nenapadá zabezpečení za účelem způsobit újmu. Jedná se o počítačového odborníka, který bývá zaměstnáván vládními agenturami či soukromými subjekty a jehož pracovní náplní je ochrana počítačových systémů. Termín „white hat“ se v internetovém slangu dá přeložit jako „etický hacker“. Tato klasifikace odpovídá i osobám, jež se zabývají testy průniku do daného softwaru a zranitelnosti v rámci smluvních ujednání.

Black hat je hacker (cracker), který narušuje počítačovou bezpečnost třeba jen ze škodolibosti, nebo k osobnímu prospěchu. Tento typ hackera je také podstatou veřejného mínění, že všichni hackeři jsou kriminálníci. Označení Grey hats patří hackerům, kteří svou činností nikomu nepomáhají, ale ani nejsou vedeni kriminální motivací a systémy nabourávají z recese či pro zábavu (Požár, 2005).

Existují i další skupiny útočníků. Největší z nich jsou tzv. **scriptkiddies** („děti se skripty"). Jedná se o uživatele s nízkou úrovní dovedností v oblasti IT. Ke svým útokům využívají automatizované nástroje, které však napsal někdo jiný, obsahující kódy zaměřené na zneužívání zranitelných míst informačních systémů. Tyto skripty používají, aniž by znali hlubší podstatu jejich fungování (Soriano, 2016).

2.5 Techniky hackerů (crackerů)

Základní metody vedení útoků byly obecně popsány v kapitole 2.1.2. Některé specifické techniky však stojí za hlubší analýzu k lepší orientaci v problematice.

- **Skenování portů (port scanning)**

Jedná se o metodu zjišťování otevřených síťových portů na vzdáleném počítači v síti. Je tak možné získat informaci, jaké služby jsou na vzdáleném počítači spuštěny. Ke zjišťování je používán speciální software. Skenování je považováno za nežádoucí techniku, protože ji často zneužívají crackeři ke zjištění zranitelných míst a následnému útoku. Může mít však i legitimní využití jako nástroj pro zlepšování počítačové bezpečnosti (Požár, 2005).

- **Zachytávání paketů (packet sniffer)**

V tomto případě je do sítě nasazen pasivní přijímač, který zaznamenává kopii každého přenášeného paketu. Využívá se jak v kabelových tak i bezdrátových sítí k zachycování přenášených informací. Tyto pakety mohou obsahovat všechny druhy citlivých informací včetně hesel. Zachycená data pak mohou být analyzována v offline režimu s cílem jejich zneužití (Kurose, a další, 2014).

- **Prolamování hesel**

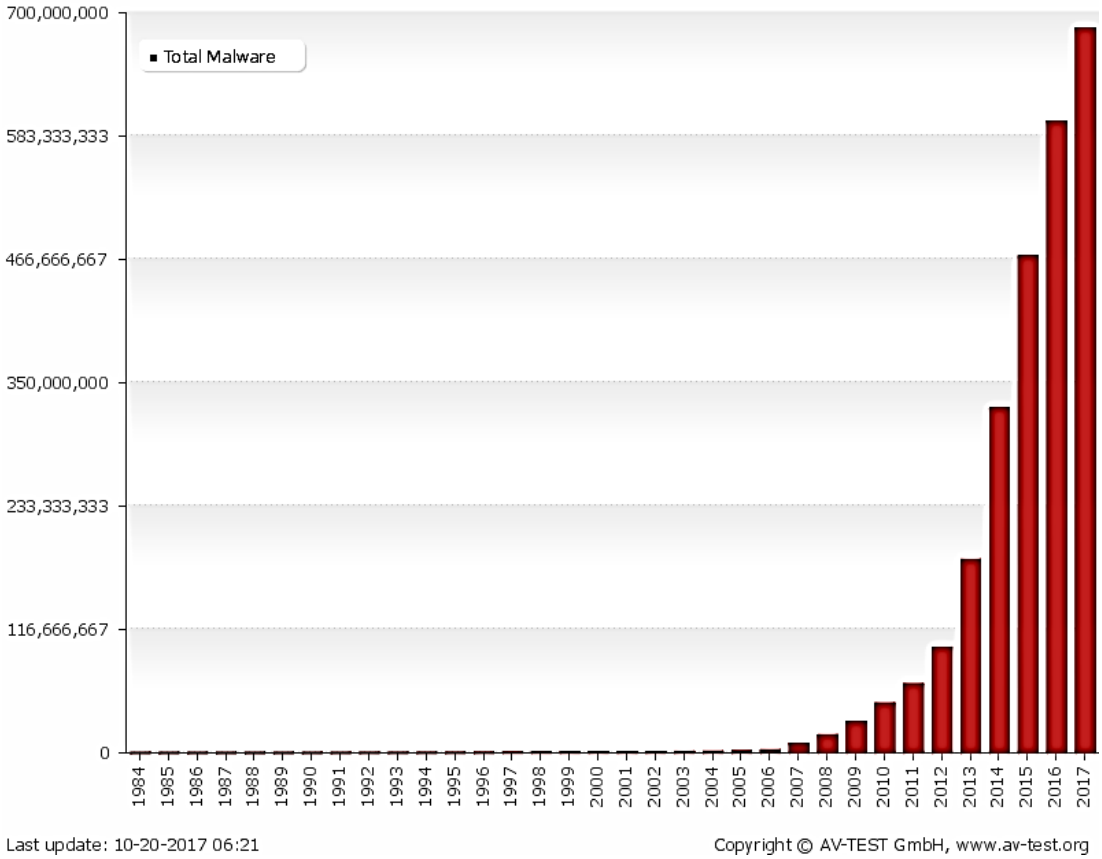
V případě, že chce hacker získat plnou kontrolu nad systémem, musí znát správné heslo. K získání tohoto hesla je možné využít např. útok hrubou silou (brute force attack), kdy speciální program zkouší jako možné heslo všechny existující kombinace znaků až do nalezení správné varianty. Tato metoda může být časově velmi náročná. Alternativní způsob se označuje jako slovníkový útok (dictionary attack), při kterém zkouší speciální program všechna slova ve slovníku jako možné heslo. Tato metoda může být časově úspornější, ale nezaručuje stoprocentní úspěšnost útočníkovi (Požár, 2005).

2.6 Malware

Malware je termín, jímž se označuje jakýkoliv software, který je nainstalovaný na cílovou stanici a vykonává nechtěné úlohy, často ve prospěch třetí strany. Malwarem mohou být označeny programy od jednoduchých obtěžujících oken s reklamou, způsobujících invazi na počítač, až po zničující útoky, kterými jsou například krádeže hesel a dat nebo infikování ostatních zařízení v síti. Kromě již uvedeného, některé typy malware jsou vytvořeny proto, aby odesílaly informace o procházení webu reklamním společnostem nebo jiné třetí straně, bez vědomí uživatele (MIT, 2017).

Do rodiny malware je možné zařadit veškerý škodlivý kód, který je použit k účelu poškození oběti, ať už sběrem citlivých informací, odcizením dat, snížením výkonu či pouhým zobrazením nechtěné reklamy. Pojem malware vychází z anglických slov malicious a software, což v překladu do českého jazyka znamená zlomyslný, podlý nebo také zákeřný software.

Obrázek 4 – Vývoj celkového množství malware v síti internet



Zdroj: www.av-test.org

- **Virus**

Virem se v oblasti počítačové bezpečnosti označuje program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů či dokumentů. Takový program se tedy chová obdobně jako biologický virus, který se šíří vkládáním svého kódu do živých buněk. V souladu s touto analogií se někdy procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel. Pro své šíření potřebují hostitelský soubor, který je virem pozměněn. Viry mohou napadnout další soubory, šířit se dále a poškodit informační systém. Viry je možné děli do různých skupin např. dle cíle infekce na **souborové viry** napadající spustitelné soubory, **bootové viry** ovládající start systému a **klastrové viry** upravující FAT či NTFS tabulku. Mezi speciální druhy virů patří **stealth viry**, které se účinně maskují před antivirovými programy, **makroviry**, jež se šíří v dokumentech kancelářských balíků nebo polymorfní viry, které pomocí mutace mění svůj kód. Počítačové viry jsou na rozdíl od jiných druhů malware v současnosti na ústupu (Soriano, 2016).

- **Červ (Worm)**

„Červi jsou malware, který může napadnout zařízení bez spolupráce uživatele (Kurose, a další, 2014)*.“* Červ se šíří z jednoho počítačového systému do druhého, pokud jsou tyto systémy propojeny sítí. Šíří se převážně s využitím e-mailových klientů nebo prostřednictvím služeb těmito klienty nabízených.

- **Zombie**

Zombie je škodlivý software, který se šíří prostřednictvím sítě. Po jeho úspěšném průniku do informačního systému je možné infikovaný počítač dálkově ovládat a spravovat. Případ, kdy je několik zařízení infikovaných stejným druhem škodlivého softwaru se schopností dálkového ovládání se nazývá botnet.

- **Spyware**

Spyware je program, který shromažďuje statistická data o napadeném zařízení a odesílá je přes internet. Tyto informace se obvykle získávají ze souboru cookies nebo z historie prohlížeče. Existují ale i spyware odesílající hesla a čísla kreditních karet nebo spyware fungující jako zadní vrátka. Spyware se často šíří jako součást shareware, a to jako adware nebo bez vědomí uživatelů. Typickým a velmi nebezpečným příkladem spyware je tzv. keylogger, který zaznamenává uživatelovy stisknuté klávesy a sbírá tak citlivé informace jako jsou uživatelská jména a hesla (Erben, 2014).

- **Trojský kůň**

Trojským koněm se označuje destruktivní program zamaskovaný jako hra, obslužný nebo aplikační program. Trojský kůň naruší počítačový systém a přitom předstírá, že provádí něco užitečného (Požár, 2005).

- **Zadní vrátka (Backdoor)**

Backdoor je metoda, kterou lze obejít standardní autentizační procedury. Backdoor se typicky instaluje pomocí trojského koně nebo červa. Útočník takto napadený počítač vzdáleně ovládá a používá pro rozesílání emailů nebo pro tvorbu botnet. Botnet je sít zombie, počítačů napadených backdoor, řízených centrálně z jednoho místa, využívaných pro Distributed Denial of Service – DDoS útoky (Soriano, 2016).

- **Rootkit**

Rootkit je sada počítačových programů, pomocí kterých lze maskovat přítomnost zákeřného softwaru v počítači, například virů, trojských koní, spywaru a podobně.

- **Ransomware**

Ransomware je druh malware, který zablokuje přístup k datům počítače a žádá za přístup zaplacení výkupného. Některé formy ransomware šifrují soubory na pevném disku (kryptovirální vydírání), jiné jen zamknou systém a výhrůžnou zprávou se snaží donutit uživatele k zaplacení. Prozatím nejnebezpečnější útoky tohoto typu má na svědomí ransomware WannaCry, Petya, Cerber, CryptoLocker a Locky (AVAST, 2017).

3 Ochrana informací

Studie „Budoucnost kybernetické bezpečnosti 2020“ vydaná koncem loňského roku Centrem pro kybernetickou bezpečnost univerzity v Berkeley označuje kybernetický prostor v roce 2020 jako nový Divoký západ. Každý, kdo do něho vstoupí s očekáváním bezpečnosti a práva, konstatuje studie, se o ně bude muset postarat sám. Pocit bezpečí, že mi nemá kdo co ukrást, je mylný. Každá firemní informace je majetek, který má nějakou cenu a jehož zneužití je potenciálním rizikem nejen pro vlastníka, ale i pro jeho zákazníky či obchodní partnery. Pro zajištění bezpečnosti se nejčastěji volí některé z vyzkoušených bezpečnostních řešení. Po jeho nasazení vrcholoví manažeři často nabydou pocitu, že pro kybernetickou bezpečnost své firmy udělali maximum a za peníze, které do ní investovali, musí být přece být jejich firma navždy dokonale chráněna a oni se konečně mohou věnovat tomu, co je reálně živí. Zajištění a rozvoji informační bezpečnosti se tak zejména v menších firmách přestane věnovat dostatečná pozornost. Chybí dlouhodobé plánování, což v sobě zahrnuje i přípravu rozpočtu pro tuto oblast. Bezpečnostní politiky bez úprav stárnou. Vyhodnocování systémových záznamů, které dokáže mnohé odhalit dříve, než dojde k incidentu, se provádí nesystematicky nebo se nedělá vůbec. Bezpečnostní systémy včetně antivirů na pracovních stanicích někdy roky běží bez nezbytných aktualizací a modernizací. Úpravy podnikového IT se nepromítají do jeho zabezpečení a počet zranitelných míst v systémech roste geometrickou řadou. A zatímco management společnosti žije v přesvědčení, že je vše pod kontrolou, katastrofa se může blížit mílovými kroky (Securita, 2017).

Jsou firmy, které investují do bezpečnostních opatření astronomické částky, přestože často nejsou ani přesvědčeni o jejich spolehlivosti. Jiní, aby dosáhli alespoň nějaké ochrany a dodrželi minimální legislativní požadavky, vytvářejí z nedostatku znalostí, prostředků i odborníků ochranné systémy, které jsou z pohledu kybernetických útočníků spíše úsměvné. Statistiky říkají, že dnešní náklady na IT bezpečnost činí zhruba dvacet procent celkových nákladů na podnikové IT a dál výrazně porostou. Nikdy nekončící boj s kybernetickou kriminalitou tak vyžaduje neustále nové a nové investice (Securita, 2017).

3.1 Správa informační bezpečnosti

Bez moderního systému řízení problematiky ochrany informací nelze dosáhnout potřebného bezpečnostního efektu. Jedná se o specifický obor, který vyžaduje znalost řízení, speciální přístup, ale i zkušenosti. Správa informační bezpečnosti je nezbytná pro řízení bezchybného provozu a rozvoje každé organizace. Její nedílnou

součástí je i řešení bezpečnostních incidentů a plánování. Musí být prováděna výhradně pracovníky organizace, případně s pomocí odborné konzultační a poradenské společnosti. Skutečné podmínky provozovatelů informačních systémů se od ideálních obvykle často liší. Bohužel ani při upřímné snaze mnohdy není možné ideálního systémového řešení komplexní informační bezpečnosti dosáhnout. Je však nanejvýš účelné problém informační bezpečnosti organizace začít vůbec řešit. „*Informační bezpečnost vyžaduje trvalý zájem a nasazení, přesnost, důslednost, pečlivost, formalizaci a administrativní pořádek veškeré činnosti* (Požár, 2005)." Bez zájmu a přesvědčení o oprávněnosti ochrany ze strany top managementu organizace informační bezpečnost nelze řešit. V souvislosti s rostoucími hrozbami vzniká nutnost vytvářet v důležitých organizacích zvláštní pracoviště, které se speciálně zabývá komplexní ochranou informací. Praxe ukazuje, že je vhodné tento samostatný a nezávislý útvar zařadit v hierarchii přímo pod vrcholového manažera. Postavení bezpečnostního manažera pak musí být jednoznačné definováno v organizačním řádu, aby se předešlo zbytečným sporům a nedorozuměním. Hlavní činností bezpečnostního manažera je pak vytváření strategie informační bezpečnosti organizace (Požár, 2005).

3.2 Řešení informační bezpečnosti

Proces řešení informační bezpečnosti se dle (Požár, 2005) obvykle skládá ze šesti základních kroků:

- **Cíle a strategie řízení informační bezpečnosti**
- **Analýza rizik informačního systému**
- **Bezpečnostní politika organizace**
- **Bezpečnostní standardy**
- **Implementace informační bezpečnosti**
- **Monitoring a audit**

Základním cílem většiny organizací bývá eliminace přímé a nepřímé ztráty způsobené zneužitím, poškozením, zničením či nedostupností informací, vybudováním nákladově optimalizovaného a efektivně fungujícího řízení bezpečnosti informací. Dalšími cíli pak bývá zhodnocení aktuální úrovně informační bezpečnosti, definice principů řízení, navržení postupu k dosažení požadované úrovně bezpečnosti a příprava prostředí pro udržování a zvyšování úrovně bezpečnosti. Základní dokument, který obsahuje popis současného stavu informační bezpečnosti a vytyčuje hlavní směry dalšího postupu, se nazývá **studie bezpečnosti**. Ve velkých firmách a stát-

ních organizacích, kde se vytváří strategické dokumenty, by studie bezpečnosti měla být jejich součástí a definovat hlavní cíle organizace v oblasti aktiv. Pak obvykle zahrnuje informační bezpečnost, fyzickou a personální bezpečnost.

Každá aktivita organizace je zákonitě spojena s určitým rizikem. Aby bylo možné zjistit, jaká rizika a hrozby organizaci hrozí, je třeba provést **analýzu rizik**. Analýza rizik je základním prvkem pro tvorbu systému řízení informačního systému, na jejím základě je možné určit, které kontrolní mechanismy jsou nezbytné a které naopak zbytečné. Důležité je si uvědomit, že každá taková analýza poskytuje informace o stavu řízení informačních rizik v určitém časovém okamžiku. Vzhledem k neustálému vývoji ve světě informačních technologií je tedy třeba analýzy rizik neustále opakovat a to zejména s ohledem na velikost organizace a její závislost na informačních technologiích. Analýza rizik je tedy klíčovou etapou v procesu řešení bezpečnosti, a pokud je správně uchopena, měla by poskytnout odpověď na následující tři otázky:

- Co se tane, nebudou-li informace chráněny?
- Jak může být porušena bezpečnost informací?
- S jakou pravděpodobností to nastane?

Bezpečnostní politika organizace vychází ze studie bezpečnosti nebo ze zadání organizace ve formě definovaných cílů, požadavků a analýzy rizik. Jedná se o klíčový bezpečnostní dokument schválený vrcholovým managementem organizace, který je závazný pro celou organizaci, jež deklaruje své základní cíle v oblasti informační bezpečnosti. Tím se předchází případným konfliktům mezi bezpečnostními cíli a zájmy organizace. Bezpečnostní politika by měla odpovědět na následující otázky:

- Jaké jsou cíle organizace v oblasti bezpečnostní politiky?
- Jaká aktiva musí být chráněna a jaká je jejich cena?
- Kdo za ně nese odpovědnost?
- Jaká opatření budou efektivnější?
- Jak bude jejich dodržování vynucováno?
- Kdy jak bude bezpečnostní politika uvedena do praxe?
- Jak které osoby budou proškoleny?
- Jak bude zajištěna osobní odpovědnost pracovníků?

Rozsah bezpečnostní politiky pak závisí zejména na kultuře řízení organizace a struktuře interní předpisové základny.

Hlavní oblasti a principy informační bezpečnosti definované v bezpečnostní politice jsou dále rozpracovány do detailní podoby. To se děje pomocí **bezpečnostních standardů** – závazných interních dokumentů společnosti**.** Zatímco bezpečnostní politika je relativně neměnným dokumentem, u bezpečnostních standardů se předpokládá častější frekvence úprav.

Nejdůležitějším krokem v rámci řešení informační bezpečnosti je její **implementace**. Přestože se tento krok zdá být samozřejmým, ve většině organizací je nezbytné tuto fázi řešení bezpečnosti řídit.

Sledování a hodnocení je nedílnou součástí procesu řízení informační bezpečnosti. Jedná se o kontinuální proces. Absence nebo nedostatečná úroveň sledování bývá často příčinou, že bezpečnostní incidenty zůstávají dlouho neodhaleny a vzniklé škody jsou mnohem vyšší než u zavčas odhalených incidentů. **Monitoring** by měl být primárně zaměřen na oblasti s nejvyšším rizikem a další klíčové oblasti činnosti organizace. Možností jednorázového hodnocení je **audit**, který obvykle provádí nezávislá specializovaná firma (Požár, 2005).

3.2.1 Systém řízení informační bezpečnosti

Informační bezpečnost je dnes již nezbytnou součástí každého informačního systému v každé organizaci. Jedná se o důležitou součást fungování podniku i státní sféry a její organizace se stává integrální součástí strategie každé složky. Organizace informační bezpečnosti se řídí systémem pro řízení informační bezpečnosti (Information Security Management System). „*ISMS je soubor pravidel a opatření, po jejichž zavedení má správné a úplné informace (princip integrity) včas k dispozici ten, kdo je skutečně potřebuje (princip dostupnosti) a pouze ten, kdo je k přístupu k nim oprávněn (princip důvěrnosti)* (Požár, 2010).“

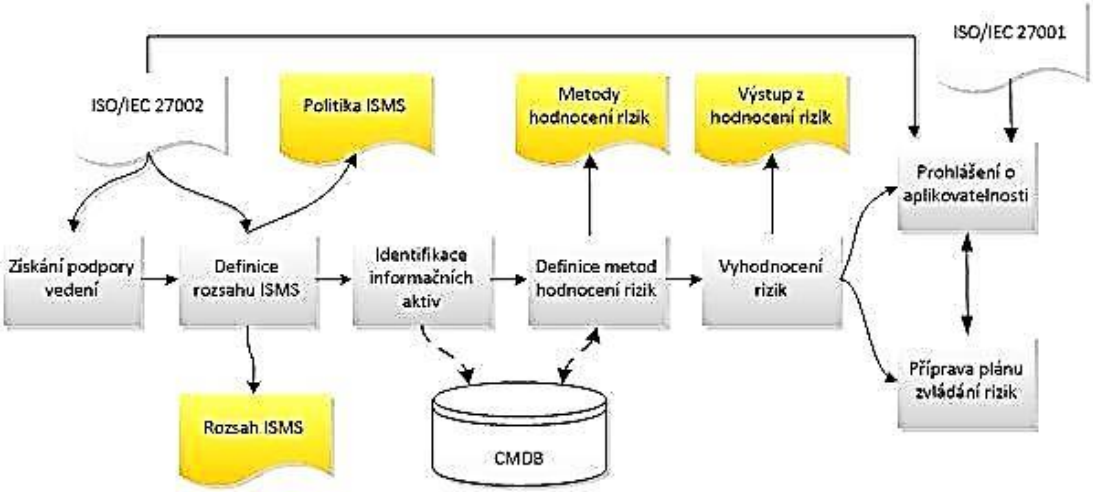
ISMS je systém ve své struktuře určený normou ISO 27001. Ta poskytuje model ustavení, implementování, zpracovávání, monitorování, přezkoumávání, udržování a zlepšování ochrany informačních aktiv, aby byly dosaženy cíle organizace na základě posouzení rizik a úrovní akceptace rizik organizace navržených k efektivnímu ošetření a řízení rizik ztráty či poškození informace (ISO 27000, 2017).

Autor (Požár, 2010) uvádí, že hlavním úkolem ISMS je provádět vhodná opatření za účelem potlačení či minimalizace hrozeb informační bezpečnosti. Opatření jsou závislá na velikosti organizace a počtem aktivit, jež vykonává, přičemž se bere ohled na reálnou rizikovost aktivit organizace. Tato rizikovost je odvislá od toho, v jaké míře organizace zpracovává osobní či důvěrné údaje. Komplexní řešení informační bezpečnosti se týká především velkých organizací, jako jsou finanční instituce, nemocnice, telekomunikační operátoři nebo státní orgány.

V těchto případech je vývoj a implementace samostatného a nezávislého procesu ISMS velmi důležitou a v podstatě jedinou alternativou. Vývoj rámce ISMS zahrnuje následující body:

- vymezení působnosti ISMS
- definice bezpečnostní politiky
- hodnocení rizika
- management řízení rizik
- výběr vhodných opatření
- prohlášení o aplikovatelnosti

Obrázek 5- Model pro řízení bezpečnosti informací



Zdroj: brichacek.net

Systém řízení bezpečnosti informací je podobně jako ostatní systémy řízení založen na modelu PDCA (Plánuj – Dělej – Kontroluj – Jednej). Model je definován následujícími čtyřmi etapami životního cyklu systému řízení:

- **Ustanovení ISMS** – cílem této etapy je upřesnit rozsah a hranice, kterých se řízení bezpečnosti týká, stanovit jasné manažerské zadání a na základě ohodnocení rizik vybrat nezbytná bezpečnostní opatření
- **Zavádění a provoz ISMS** – cílem této etapy je účelně a systematicky prosadit vybraná bezpečnostní opatření do chodu organizace
- **Monitorování a přezkoumání ISMS** – hlavním cílem této etapy je zajištění zpětné vazby a pravidelného sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací

- **Údržba a zlepšování ISMS** – cílem poslední etapy je realizace možností zlepšování systému řízení bezpečnosti informací ať už soustavným zlepšování systému nebo odstraňování zjištěných slabin a nedostatků

ISMS se tak stává cyklickým stále opakujícím procesem. Zavedení bezpečnostní politiky a vymezení působnosti ISMS je častěji se opakující proces řízení strategických cílů. Naopak proces řízení rizik je každodenní provozní činnost.

3.3 Zabezpečení informačního systému

Bezpečnostní cíle jsou dle (Požár, 2010) dílčí přínosy k bezpečnosti, kterou dosahuje informační systém z hlediska udržení důvěrnosti, integrity a dostupnosti. Prostředkem použitým pro dosažení stanovených bezpečnostních cílů informačního systému jsou bezpečnostní funkce. Bezpečnostní funkce je možné kategorizovat např. podle okamžiku uplatnění:

- **Preventivní** - eliminují zranitelná místa nebo zavádí aktivity zvyšující bezpečnostní uvědomění
- **Heuristické** - snižují riziko dané nějakou hrozbou
- **Detekční a opravné** - minimalizují účinek útoku podle schématu „detekce-izolace-zotavení“

Bezpečnostní funkce je možné dále dělit z hlediska způsobu implementace. Implementující bezpečnostní mechanismus může mít charakter fyzického opatření, administrativní akce, může jím být technické zařízení nebo logický nástroj jako procedura či algoritmus (Požár, 2010).

Podle způsobu implementace lze dělit bezpečnostní funkce:

• **Softwarového charakteru** – jde zejména o softwarové řízení přístupu, funkce založené na použití kryptografie, digitálního podepisování, antivirové prostředky, zřizování účtů, standardy pro návrh, kódování, testování a údržbu programů, ochranné nástroje v operačních a aplikačních systémech pro autentizace přístupu a zpráv

• **Administrativního a správního charakteru** – tyto funkce zahrnují výběr a školení důvěryhodných osob, hesla, právní normy, zákony, vyhlášky, předpisy, etické normy, licenční politika, nástroje provozního řízení, zpravodajství o událostech a stavech významných z hlediska bezpečnosti, sběru a analýzy statistik, konfigurace systému

• **Hardwarového charakteru** – funkce zahrnující autentizace na bázi identifikačních karet, autentizační kalkulátory, firewally, archivní prostředky - záložní kopie dat a programů

• **Fyzického charakteru** – např. trezory, zámky, ostraha, identifikační karty, protipožární ochrana, záložní generátory energie, bezpečná místa pro záložní kopie dat

3.3.1 Softwarová/hardwarová bezpečnostní opatření

Základní funkcí informační bezpečnosti je zaručení důvěryhodnosti, dostupnosti a integrity dat v informačních systémech. Hlavním cílem informační bezpečnosti je tedy zajištění maximální dostupnosti nepozměněných informací oprávněným osobám. K zajištění těchto podmínek se využívají následující softwarové prostředky.

- **Firewall**

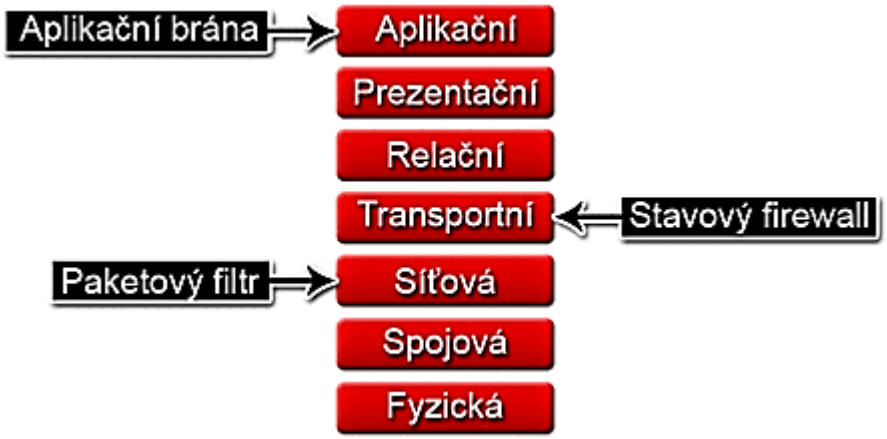
Firewall je specializované zařízení umístěné mezi důvěryhodnými (interní síť organizace) a nedůvěryhodnými (Internet) sítěmi. Jeho hlavní funkcí je kontrolovat veškerá data, která se mezi těmito sítěmi přenášejí a v případě, že určitý datový tok neodpovídá nastaveným pravidlům, musí jej přerušit/zakázat. Firewally je možné rozdělit do tří kategorií na tradiční **paketové filtry, stavové filtry a aplikační brány**.

Veškerá komunikace, která přichází do vnitřní sítě a opouští vnitřní síť, prochází přes tento router, jenž je místem, kde nastává filtrování paketů. **Paketový filtr** prohledává každý datagram samostatně, určuje, zda se má datagramu umožnit průchod nebo by měl být vyřazen na základě zvláštních pravidel určených správcem. Filtrovací pravidla se obvykle provádí na základě zdrojové či cílové IP adresy, typu protokolu v poli IP datagramu (TCP, UDP, ICMP, OSPF), zdrojového a cílového portu TCP/UDP. Správce sítě konfiguruje firewall na základě firemní politiky, která může brát v úvahu produktivitu uživatelů, využití šířky pásma, ale hlavně bezpečnostní zájmy organizace (Kurose, a další, 2014).

U tradičního paketového filtru se filtrovací rozhodování provádí na každém paketu samostatně. **Stavové filtry** naproti tomu sledují TCP spojení a pomocí těchto znalostí provádějí filtrovací rozhodnutí. Stavové filtry tedy vylepšují funkcionalitu paketových filtrů. Stavový firewall poskytuje vyšší efektivitu kontroly jednotlivých paketů, protože pro existující spojení kontroluje jen stavovou tabulku, místo toho, aby kontroloval u každého paketu sadu nadefinovaných složitých pravidel. Stavový firewall nijak nesouvisí s hloubkovou kontrolou paketů. Je schopný udržovat důležité parametry všech spojení v paměti od začátku až do konce.

Nicméně, filtrování samotných paketů není považováno za dostatečnou ochranu. Aby bylo možné účinně blokovat peer-to-peer sítě, je potřeba mít firewall, který umí filtrovat na aplikační úrovni. Prozkoumávání na aplikační úrovni je samozřejmě nesmírně náročné na inteligenci firewallu i na jeho výpočetní výkon. **Aplikační brány** oproti paketovým filtrům úplně oddělí důvěryhodné sítě od nedůvěryhodných. Pro komunikaci mezi těmito sítěmi je pak třeba dvou spojení. Iniciátor spojení kontaktuje aplikační bránu se svým požadavkem, ta jej vyhodnotí. V případě schválení sama aplikační brána kontaktuje cílový server a v ustanoveném spojení pak nadále funguje jako prostředník předávající nezměněná data. Kontrola dat se provádí na sedmé vrstvě síťového OSI modelu, proto aplikační brána. Mezi výhody zde patří značná úroveň zabezpečení, která je ovšem vykoupena vysokou náročností na použití hardware (Kurose, a další, 2014).

Obrázek 6- Firewall v modelu OSI



Zdroj: Wikipedia.org

- **Systémy detekce a prevence průniku**

Jak bylo popsáno v předchozí kapitole, paketový a stavový filtr kontroluje pole záhlaví paketů IP. TCP. UDP a ICPM a potom rozhoduje, které pakety nechá projít. Aby však bylo možné detekovat mnoho typů útoků, je třeba provést **hloubkovou inspekci paketů**, tedy nesoustředit se pouze na záhlaví, ale nahlédnout do skutečných aplikačních dat, která tyto pakety přenášejí. Tento úkol provádí aplikační brána, ale jen pro konkrétní aplikaci. Proto zde vzniká potřeba využití dalšího zařízení, které by nejen zkoumalo záhlaví všech procházejících paketů, ale také provádělo hloubkovou inspekci paketů. Pokud takové zařízení zaregistruje podezřelý paket nebo podezřelou sérii paketů, může takovou aktivitu označit jako

nebezpečnou nebo zabránit ve vstupu do podnikové sítě. Správce systému pak může po detailnější analýze komunikace přijmout vhodná bezpečnostní opatření. Zařízení, které generuje upozornění, když zjistí potenciálně nebezpečnou komunikaci, se nazývá **systém detekce průniku** (Intrusion Detection System – IDS). Zařízení, které filtruje podezřelou komunikaci, je možné označovat jako **systém prevence průniku** (Intrusion Prevention System – IPS). Oba výše zmíněné mechanismy bývají velmi často již implementovány jako součást funkcí firewallu. V současnosti, kdy útoky typu DoS a DDoS neustále zvyšují svou frekvenci a účinnost, je vhodné kritické systémy vybavit **anti-DoS/DDoS** řešením, které blokuje či přesměruje škodlivý provoz a zamezí tak nedostupnosti služeb. Nevýhodou těchto řešení bývá jejich nákladnost (Kurose, a další, 2014).

- **Antivirový program**

Antivirový program je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného malware. Úspěšnost závisí na schopnostech antivirového programu a kvalitě databáze počítačových virů. Vůči ní antivir porovnává data při odhalování nákazy. V současnosti vznikají virové mutace tak rychle, že důvěryhodný výrobce antiviru vydává aktualizaci virové databáze několikrát týdně. Proto pro efektivní správu antiviru je třeba mít i správně nastavené aktualizace tohoto softwaru. S rychlostí vývoje malware přicházejí i softwarové společnosti s novými metodami detekce. Kromě heuristických analýz je využívána např. funkce „Sandbox“, která provádí simulace spustitelných souborů nebo „Whitelisting“, kdy správce systému označí pouze důvěryhodné kódy, čímž se eliminuje veškeré vyhledání zákeřného software.

Spolehlivost antivirového systému bývá testována nezávislými agenturami a to zejména na základě počtu neodhalených hrozeb nebo počtu falešných poplachů Jinou možností jak nahlížet na kvalitu antivirového programu bývá zátěž hardware, na kterém antivir provádí operace, uživatelská přívětivost, či četnost aktualizací virové databáze.

Antispam je inteligentní software, který se snaží rozeznávat spam a přesouvat jej do určené složky v elektronických poštovních schránkách. Za spam je možné označit nevyžádanou poštu, která je obyčejně rozesílána pomocí botů. Často bývá ke spamu přidán i skrytý škodlivý kód. Antispam stejně jako antivir pro svoji funkci využívá rozsáhlou databázi s informacemi o spamu. Proto i zde jsou nutné pravidelné aktualizace (Soriano, 2016).

- **Ochrana koncových bodů sítě**

Data loss prevention (DLP) technologie slouží k identifikaci a ochraně citlivých dat a informací před jejich ztrátou či odcizením. Je vhodná pro organizace, které potřebují mít svá citlivá data chráněna a monitorována. Tato technologie dokáže monitorovat data na koncových stanicích a také na serverech, a to i při jejich přenosu po síti. Díky jejímu nasazení lze efektivně zabránit úniku či ztrátě dat, ať již například přes externí média, jakými jsou flash-disky, USB, externí disky atp., tak i při odeslání dat elektronickou poštou, jejich sdílením do webové sítě či vytisknutím (AEC, 2017).

Podobné politiky bývá často třeba řešit i v oblasti mobilní komunikace, kde se jako nástroj využívá systém **Mobile Device Management** (MDM). MDM řešení automaticky detekuje neautorizované uživatele, ztracená nebo zcizená zařízení a další bezpečnostní rizika. V případě detekce hrozby jsou administrátoři automaticky upozorněni a ohrožená zařízení a přístup k e-mailu, aplikacím a firemním datům může být automaticky zablokován (EMAN, 2017).

- **Autentizace a autorizace**

Autentizace slouží k jednoznačnému určení uživatele, který přistupuje k systému. Cílem autentizace je zajistit, že systém přesně ví, s jakým uživatelem komunikuje, ať už je to člověk nebo jiný systém. Metody autentizace jsou založeny na prokázání identity subjektu. Dle (Rubeš, 2016) existují tři základní způsoby autentizace:

- **Jednofaktorová autentizace** předpokládá, že k ověření dojde pouze pomocí něčeho, co uživatel zná (např. uživatelské jméno a heslo)
- **Dvoufaktorová autentizace** je založena na faktoru, že k ověření dojde ještě navíc pomocí něčeho, co uživatel má (typicky osobní zařízení, jako je mobilní telefon a SMS nebo token a PIN)
- **Třífaktorová autentizace** navíc ověřuje ještě aspekt, který je spojen s člověkem (typicky biometrické prvky)

Autorizací se rozumí proces ověření přístupových oprávnění uživatele vstupující do informačního systému**.** Tento proces ve většině případů navazuje na proces autentizace. Podstatou autorizace je ověřit, zda daný uživatel má oprávnění provést příslušnou akci, například přístup do systému, provádění modifikací, vytváření nových uživatelů atd.

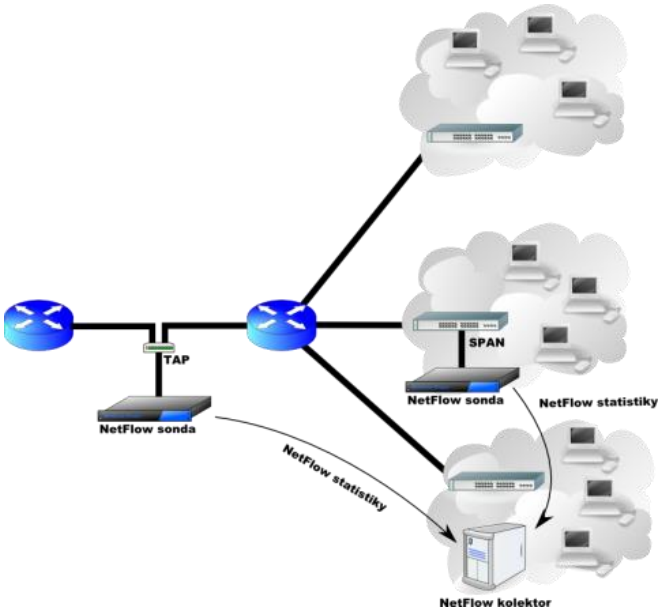
Jednou z možností využití autentizace a autorizace v praxi jsou systémy řízení přístupu k síti (Network access control – NAC). Základní myšlenka systému je postavena na principu, že než je libovolnému zařízení koncového uživatele dovoleno připojení do korporátní sítě, NAC ověří, zda zařízení vyhovuje zásadám zabezpečení

společnosti. NAC využívá protokolu **802.1x** k ověření uživatelů v síti včetně uživatelů bezdrátových sítí WIFI (NOVICOM, 2017).

- **Monitoring datových toků**

NetFlow je standard vyvinutý společností Cisco, který poskytuje informace z třetí a čtvrté vrstvy referenčního modelu ISO/OSI, tedy informace o IP adresách, portech, protokolech, objemu přenesených dat, paketech a další technické detaily. Pomocí sběru, ukládání a analýzy takovýchto informací v agregované podobě mohou síťoví a bezpečnostní administrátoři řešit řadu provozních a bezpečnostních úkolů. Pomocí systémů využívajících tento standard je možné sledovat chování zařízení v síti, díky čemuž lze odhalovat a reagovat na doposud neznámé nebo specifické hrozby. A to včetně těch, pro které neexistuje signatura. Díky NetFlow řešení získávají administrátoři klíčovou výhodu v boji s moderními bezpečnostními hrozbami, které obchází tradiční ochranné prvky, jako jsou firewally, IDS/IPS systémy nebo antivirové programy (Flowmon, 2017).

Obrázek 7 - NetFlow architektura



Zdroj: wikipedie.org

- **Správa bezpečnostních informací a událostí**

Termín **Security Information and Event Management (SIEM)** roku 2005 vytvořili Mark Nicolett a Amrit Williams ze společnosti Gartner v souvislosti s popisem produktu schopného shromažďovat, analyzovat a prezentovat informace ze sítě a bezpečnostních zařízení, pomáhat spravovat identity a přístupy, ohrožená místa,

shody s bezpečnostními politikami atd. Systémy SIEM zahrnují funkcionality sběru logů, korelace událostí, generování výstrah, analýzy a vyšetřování incidentů tak, že automatizují identifikaci a řešení incidentů na základě předdefinovaných pravidel, což umožňuje včasné upozornění na kritické události, zajišťuje soulad se zákonnými normami, ale především přispívá k reálnému řízení bezpečnosti napříč společností. V současné době se jedná o jediný nástroj, který efektivně zvládne monitoring bezpečnostních událostí, které nepřetržitě chrlí podnikové síťové prvky, firewally, IDS, IPS, servery, operační systémy, databáze a aplikace (Sands.cz, 2017).

„Zajištění bezpečnosti informací není hledáním dokonalého způsobu ochrany, ale aplikací takových opatření, která jsou přiměřená hodnotě předmětu ochrany (aktiv) *(Požár, 2010)*.“

4 Kryptografie

Bezpečnost informací je možné zvyšovat různými způsoby, nikdy však není možné úplně zamezit jejich úniku a zneužití. Pro velmi citlivá dat lze použít šifrovacích technik, které významným způsobem sníží nebo eliminují riziko prozrazení důvěrných informací i při získání těchto dat během jejich přenosu nebo při uložení.

„Kryptologie je vědní obor zabývající se tvorbou, používáním a luštěním čili prolamováním šifer (Požár, 2005)*.“* **Kryptografie** je matematická věda zabývající se metodami utajování smyslu zpráv do podoby, jež neoprávněným osobám znemožňuje zjistit jejich obsah. Kryptografie studuje šifrovací algoritmy, kryptografické nástroje, hardwarové implementace šifrovacích algoritmů, kryptografické protokoly atp. Mnoho bezpečnostních aplikací je ve skutečnosti založeno na využití kryptografických algoritmů k šifrování a dešifrování dat (Burda, 2013).

Šifrovací algoritmus je takový mechanismus, jehož cílem je utajit data jejich zašifrováním tak, že je pak nelze přečíst a jsou nesrozumitelná. Kryptografický algoritmus pracuje ve spojení s jedním nebo více klíči s cílem zašifrovat prostý text. Je-li využito pro zašifrování stejného otevřeného textu různých klíčů, vniknou různé šifrové texty. Bezpečnost šifrovaných dat v podstatě závisí na dvou faktorech – na síle kryptografického algoritmu a na utajení klíče. Silný kryptografický algoritmus by měl splňovat následující kritéria:

- Nesmí existovat žádný způsob, jak najít otevřený text, pokud klíč není znám, kromě použití hrubé síly, tzn. testování všech možných klíčů až do nalezení klíče správného.
- Počet možných klíčů musí být tak velký, že je z hlediska dostupného výpočetního výkonu nemožné uskutečnit úspěšný útok hrubou silou v rozumném čase.
- Všechny kryptografické algoritmy, používající symetrický nebo soukromý klíč, musí zajišťovat utajení tohoto klíče. Útočník nesmí být schopen využít kryptografického algoritmu pro zjištění tajného nebo soukromého klíče (Soriano, 2016).

Kryptografický šifrový systém (tvořený šifrováním, dešifrováním a klíčem) umožňuje ukládání citlivých dat nebo jejich přenos nezabezpečenými prostředími (jako je kupříkladu celosvětová síť Internet) tak, aby je nemohl přečíst nikdo kromě oprávněného příjemce. Kryptografické šifrové systémy jsou dnes standardem pro zajištění informační bezpečnosti, důvěryhodnosti, řízení přístupu ke zdrojům, ale i elektronických transakcí.

4.1 Základní pojmy kryptologie

Otevřený text (plain-text) je zpráva, která má být předána příjemci.

Šifrovaný text (cipher-text) je výstup, který vznikne šifrováním otevřeného textu.

Šifrování je proces, při němž konkrétní kryptografický postup přemění, transformuje otevřený text pomocí kryptografického algoritmu a šifrovacího klíče do šifrovaného textu, který brání a znemožňuje každému, kdo nemá k dispozici tajný údaj, tyto informace získat.

Dešifrování je opak šifrování. Jedná se o proces zpětného získání zprávy tvořené otevřeným textem z jeho šifrované podoby, neboli převod šifrovaného textu na otevřený text.

Klíč je slovo, číslo, nebo řetězec, který se používá k zašifrování otevřeného textu nebo k dešifrování šifrovaného textu.

Kryptoanalýza je věda zabývající se prolamováním kódů a šifer.

Hashovací algoritmus je mechanismus, který převede textový řetězec libovolné délky na řetězec pevné délky.

Šifra je kryptografický algoritmus, nebo také matematická funkce používaná pro šifrování a dešifrování.

Správa klíčů je proces, v rámci kterého je klíč vygenerován, uložen, chráněn, přenášen, načítán, používán a zničen (Piper, a další, 2006).

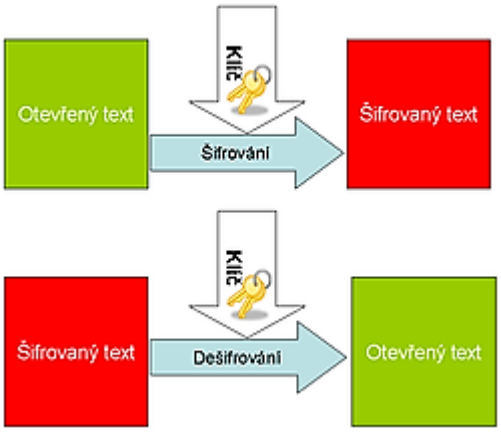
4.2 Symetrické šifry

Proces šifrování a dešifrování pomocí stejného klíče je znám jako kryptosystém s tajným či symetrickým klíčem. Klíče v takovém systému používané k šifrování otevřeného textu a k dešifrování šifrového textu mohou být identické nebo může existovat jednoduchá transformace pro přechod mezi dvěma klíči. Pro zašifrování i dešifrování zprávy je tedy nutné, aby odesílatel i adresát zprávy vlastnili a používali stejný tajný klíč. Vstupem tedy bývá tajný text ze stanovené abecedy a klíč. Šifrovací funkcí se za pomoci klíče tajný text převede na kód, který může být odeslán příjemci zprávy. Příjemce zprávy pak použije dešifrovací funkci se stejným klíčem a tím získá původní utajovaný text. Důležité je, že pro dešifrování musí mít příjemce k dispozici stejný klíč, jakým byl text zakódován. Je tedy vždy třeba zajistit bezpečný způsob doručení klíče zabezpečeným přenosovým kanálem, aby se tento klíč nedostal do nesprávných rukou (Požár, 2005).

Pro šifrování se používají funkce, u kterých platí, že při znalosti vstupního a zakódovaného textu je velice obtížené vygenerovat klíč, přestože samotné šifrování a dešifrování pomocí tohoto klíče probíhá velmi rychle. Obtížnost případného zjištění

klíče záleží zejména na vlastní délce klíče. Šifrovaná zpráva musí odolat útoku hrubou silou, který předpokládá otestování všech možných kombinací klíčů. Mezi symetrické metody kryptografie patří např. algoritmus DES nebo AES (Soriano, 2016).

Obrázek 8 - Princip fungování symetrické šifry



Zdroj: wikipedie.org

Hlavní výhodou symetrického šifrování je snadná a rychlá hardwarová i softwarová implementace. Oproti asymetrickému šifrování je možné pomocí symetrických šifer zpracovat a zašifrovat velké množství informací ve velice krátkém čase a s minimálními nároky na výkon systému. Klíče pro symetrické šifry stačí krátké. Symetrické šifry lze využít jako základ pro vytváření nejrůznějších kryptografických mechanismů, zahrnujících generátor pseudonáhodných čísel, hashovací funkce, schémata pro digitální podpisy atp. Jednoduché symetrické šifry je možné kombinovat a vytvořit tak šifry mnohem silnější. Naopak největší nevýhodou symetrických šifrovacích systémů je skutečnost, že si obě strany mezi sebou musí vyměnit šifrový klíč. To skýtá prostor pro vyzrazení klíče, a může tak útočníkovi poskytnout příležitost, jak snadno prolomit jinak silný algoritmus. Ve velkých sítích je nutné udržovat velké množství různých klíčů. Pro bezpečnou komunikaci je nutné, aby byly klíče dostatečně často obměňovány, což opět naráží na problém s bezpečnou výměnou klíče (Burda, 2013).

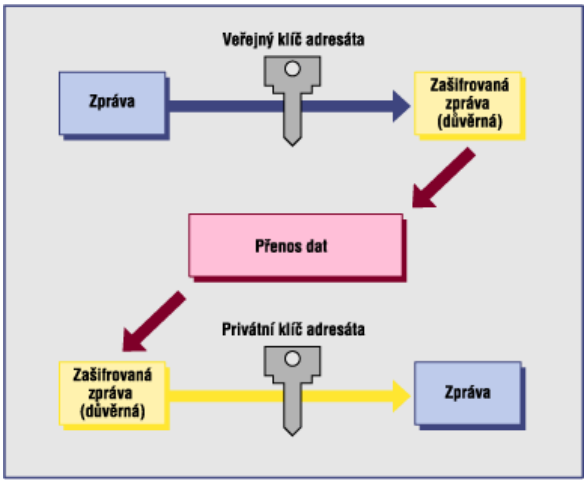
Bezpečnostní rizika spojená s kryptosystémem s tajným klíčem, byla do značné míry překonána kryptografickým systémem s klíčem veřejným. Symetrické systémy se často používají k šifrování dat na pevných discích. Osoba, která šifrování provádí, klíč zná, a v tomto případě odpadá problematika týkající se distribuce klíčů.

4.3 Asymetrické šifry

Kryptosystém s veřejným klíčem vznikl jako reakce na bezpečnostní problémy kryptografie symetrické. Tento postup řeší výše uvedené problémy použitím dvou klíčů namísto jednoho. Metoda s veřejným klíčem tedy využívá dvojici klíčů – jeden pro šifrování a druhý pro dešifrování. Kryptosystém s veřejným klíčem se rovněž označuje jako asymetrický kryptografický systém, protože k dokončení procesu je zapotřebí obou klíčů. V asymetrické kryptografii je jeden z klíčů volně šiřitelný tzv. veřejný klíč a používá se pro šifrování. Proto se tato metoda také označuje jako šifrování s veřejným klíčem. Druhým klíčem je tajný nebo také soukromý klíč a používá se pro dešifrování. Dohromady se klíče nazývají párem klíčů. Soukromý klíč nesmí být šířen. Jak název napovídá, je soukromý pro každý komunikující subjekt. Je třeba vyzdvihnout, že veřejný a soukromý klíč jsou spolu svázány, ale je prakticky nemožné odvodit soukromý klíč na základě znalosti klíče veřejného.

Pokud uživatel chce, aby mu někdo mohl poslat zašifrovanou zprávu, musí nejprve dát k dispozici svůj veřejný klíč. Ten použije odesilatel zprávy pro zašifrování tajné zprávy a kód odešle. Pro dekódování pak potřebuje příjemce mít druhý klíč páru, svůj vlastní soukromý klíč, který jediný dešifruje zprávu do čitelné a srozumitelné podoby. Klíčový pár se většinou tvoří společně. Algoritmus uživateli vygeneruje oba klíče, veřejný klíč uživatel dá k dispozici všem odesílatelům zpráv a soukromý klíč si bezpečně uschová (Soriano, 2016).

Obrázek 9 - Princip asymetrické šifry



Zdroj: wikipedie.org

Nejběžnější algoritmus využívající veřejného klíče je RSA. Jeho název je odvozen z prvních písmem příjmení jeho autorů (Rivest, Shamir, Adleman). Tento algoritmus je považován za první, který je vhodný pro elektronický podpis a i šifrování zpráv. Bezpečnost RSA je postavena na předpokladu, že rozložit velké číslo na součin prvočísel (tzv. faktorizace) je velmi obtížná úloha. Z rovnice **n = p . q** je v rozumném čase prakticky nemožné zjistit činitele p a q. Naproti tomu násobení dvou velkých čísel je elementární úloha. S délkou klíče stoupá obtížnost prolomení šifry. Používá se i dnes, přičemž při dostatečné délce klíče je považován za bezpečný.

Hlavní výhodou asymetrických šifer je fakt, že není třeba nikam posílat soukromý klíč, a tak nemůže dojít k jejímu vyzrazení. Naproti tomu veřejný klíč je možné dát k dispozici všem. Další výhodou je pro kryptosystém s veřejným klíčem možnost použití méně klíčů než u symetrických metod. Pro komunikaci několika osob postačí pro každou osobu jen jeden pár klíčů. Nevýhodou asymetrických metod je rychlost. Tyto metody jsou až tisícinásobně pomalejší než metody symetrické. Další nevýhodou je nutnost ověření pravosti klíče, tedy jednoznačná identifikace majitele veřejného klíče. Pro tyto účely existují např. certifikační autority, které udržují databázi osob s ověřenou totožností a jejich veřejných klíčů. **Certifikační autorita** je v asymetrické kryptografii subjekt, který vydává digitální certifikáty (elektronicky podepsané veřejné šifrovací klíče), čímž usnadňuje využívání veřejných klíčů tak, že svojí autoritou potvrzuje pravdivost údajů, které jsou ve volně dostupném veřejném klíči uvedeny. Na základě principu přenosu důvěry je tak možné důvěřovat údajům uvedeným v digitálním certifikátu za předpokladu, že existuje důvěra k samotné certifikační autoritě (Požár, 2005).

4.4 Útoky na kryptografické algoritmy

Jak již bylo uvedeno, kryptoanalýza se zabývá rozbíjením šifer. Pokud se přibližně ví, co se hledá, kryptoanalytik dokáže na základě četnosti výskytu jednotlivých písmen či slov a statistických údajů pro daný jazyk šifru rozluštit. Existuje velké množství kryptoanalytických metod. Tzv. Kerckhoffův princip uvádí, že spolehlivost šifrovacího systému nesmí záviset na utajení algoritmu. Spolehlivost je ložena pouze na utajení klíče. Mezi základní metody útoku na kryptografické algoritmy patří:

- **Útok hrubou silou** (brute force attack) – Tento typ útoku předpokládá dostatečně výkonný výpočetní systém, kterým se útočník snaží dešifrovat utajovaný text. Je to nejuniverzálnější metoda, kdy jsou zkušeny všechny možné klíče. Postup je tím méně efektivní, čím delší je šifrovací klíč. Má-li tedy zůstat informace utajena,

musí být použit klíč takové délky, aby její dešifrování bylo řádově delší než požadovaná doba utajení.

- **Útok se znalostí šifrového textu** (cipher only attack) – Má-li útočník k dispozici několik šifrovaných textů kódovaných stejným algoritmem a stejným klíčem, pak se mu může podařit takový text rozluštit. Podobný typ útoku je velmi častý, protože se obvykle podaří odposlechnout velké množství šifrovaných informací. Jestliže jsou všechny zprávy šifrovány jedním klíčem, může se důkladnou analýzou odhalit i tento klíč a pak je luštění těchto zpráv velice jednoduché. Při tomto typu útoku se využívá metod lineární kryptoanalýzy, kdy se šifrovací text aproximuje vhodnou lineární funkcí otevřeného textu.
- **Útok se znalostí otevřeného textu** (known plaintext attack) – Tato situace je podobná předchozímu modelu s tím rozdílem, že útočník krom šifrované zprávy disponuje také jejich otevřeným ekvivalentem. Pak útočník hledá pouze šifrovací klíč, což je většinou jednoduché. V tomto případě se používá metoda diferenciální kryptoanalýzy, která je založená na tom, že jsou cíleně zkoumány určité páry šifrovacích textů a to těch, jejichž otevřené protějšky vykazují určité rozdíly.
- **Útok pomocí kompromitace uživatelů** – Kryptoanalytik získá pomocí korupce či nátlaku šifrovací klíč, s jehož pomocí je možné dešifrovat utajovaný text.
- **Timing attack** – Tato metoda je založena na přesném změření času potřebném pro operace se soukromým klíčem., protože šifrovací systém často potřebuje významně jiné množství výpočetní doby pro různé vstupy. V případě zranitelných šifrovacích systémů je tento způsob útoku výpočetně nenáročný a často vyžaduje pouze známý šifrovací text (Požár, 2010).

5 Legislativa a normy

Svět informační bezpečnosti se neustále mění. Pryč jsou doby, kdy hlavním cílem hackerů bylo dokázat svoji výjimečnost a dostat se na titulní stránky novin. Současná kybernetická kriminalita je perfektně organizovaný byznys a dobře zavedené odvětví ekonomiky. Objevují se noví útočníci s novými metodami a s novými motivacemi. Aby s nimi bylo možné bojovat, je třeba mít oporu ve státním aparátu a legislativě.

5.1 NBÚ

Národní bezpečnostní úřad (NBÚ) je orgánem moci výkonné, byl zřízen zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, a to k 1. srpnu 1998. NBÚ je ústředním správním úřadem pro oblasti bezpečnostní způsobilosti a ochrany utajovaných informací včetně výzkumu a vývoje kryptografických prostředků. Ve své činnosti se NBÚ řídí zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Součástí NBÚ bylo i **Národní centrum kybernetické bezpečnosti** (NCKB), jež vzniklo na základě usnesení Vlády ČR ze dne 19. října 2011 č. 781, o ustavení Národního bezpečnostního úřadu. Centrum dle zadání koordinovalo spolupráci na národní a mezinárodní úrovni při předcházení kybernetickým útokům, při navrhování a přijímání opatření k řešení incidentů i proti probíhajícím útokům. Od svého zřízení mimo jiné pracovalo na vytvoření zákona o kybernetické bezpečnosti, který byl dne 2. ledna 2014 schválen vládou k předložení Parlamentu ČR. V roce 2017 byla agenda NCKB vyčleněna z NBÚ a převzata nově vzniklým samostatným Národním úřadem pro kybernetickou a informační bezpečnost. **Národní úřad pro kybernetickou a informační bezpečnost** (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Mezi hlavní činnosti organizace patří:

- provozovat Vládní CERT České republiky (GovCERT.CZ)
- spolupráce s ostatními národními CERT týmy a CSIRT týmy
- spolupráce s mezinárodními CERT týmy a CSIRT týmy
- příprava bezpečnostních standardů pro informační systémy KII a VIS
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti

- výzkum a vývoj v oblasti kybernetické bezpečnosti
- ochrana utajovaných informací v oblasti informačních komunikačních systémů
- kryptografická ochrana

Vládní **CERT** (Computer Emergency Response Team) a týmy typu **CSIRT** (Computer Security Incident Response Team) hrají klíčovou roli při ochraně kritické informační infrastruktury a významných informačních systémů podle zákona o kybernetické bezpečnosti (181/2014 Sb.) a jeho prováděcích předpisů. Každá země, která má své kritické systémy připojeny do internetu, musí být schopna efektivně a účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat činnosti při jejich řešení a účelně působit při předcházení incidentům (NÚKIB, 2017).

5.2 Kybernetický zákon

Zákon 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů, tzv. kybernetický zákon, upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti s cílem zajistit bezpečnost informací, služeb a sítí v kybernetickém prostoru. Zákon je účinný od 1. ledna 2015. Dne 1. srpna 2017 vstoupil v účinnost zákon č. 205/2017 Sb., kterým se mění zákon o kybernetické bezpečnosti a některé další zákony. Novela kybernetického zákona přináší, zejména v souvislosti s implementací směrnice Evropského parlamentu a Rady EU 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a infomačních systémů v Evropské unii (směrnice NIS), do zákona značné množství změn (NÚKIB, 2017).

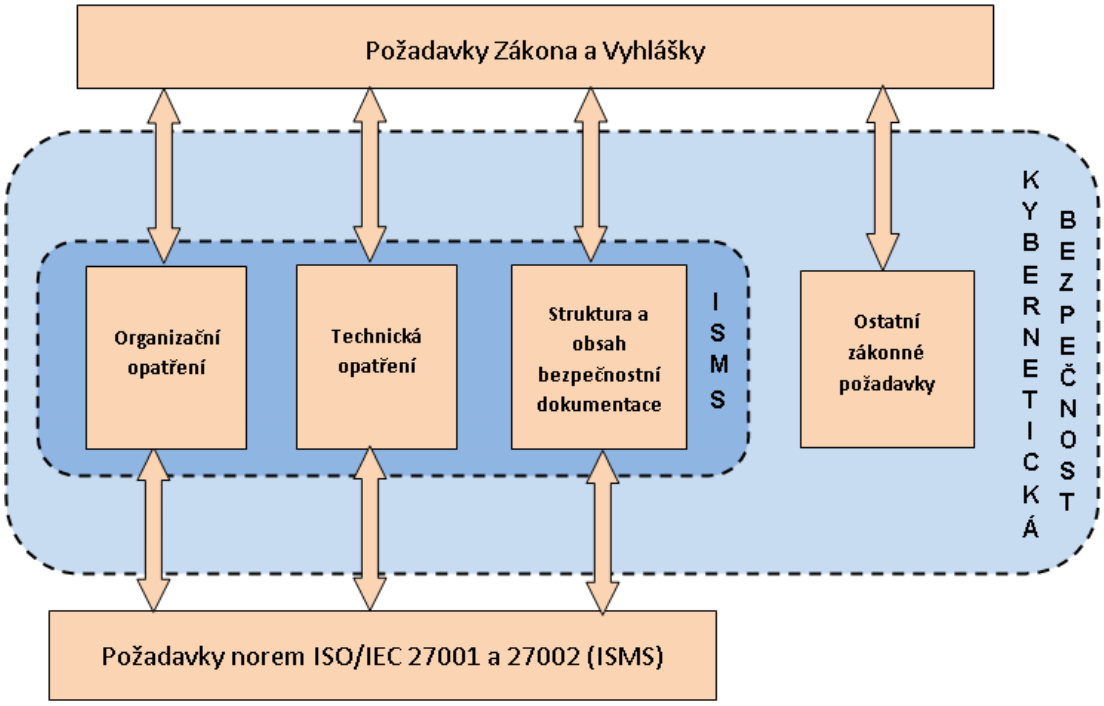
Základním cílem kybernetického zákona je zvýšení bezpečnosti kybernetického prostoru a zejména se snažit ochránit tu část infrastruktury, která je pro fungování státu důležitá a jejíž narušení by vedlo k poškození nebo ohrožení zájmu České republiky (NBÚ, 2014).

Se zmíněným zákonem úzce souvisejí následující prováděcí předpisy:

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

Zákon stanovuje, jakým způsobem má být kybernetická bezpečnost zajištěna a určuje způsob reakce na kybernetické hrozby nebo řešení nastalého incidentu. Podrobnosti ke způsobu realizace bezpečnostních opatření, ke komunikaci s kontaktními místy, vedení bezpečností dokumentace a kategorizaci kybernetických bezpečnostních incidentů určuje Vyhláška (NBÚ, 2014).

Obrázek 10 - Model propojení kybernetického zákona s ISMS



Zdroj: www.tsoft.cz

Zákon dále zavádí nové pojmy:

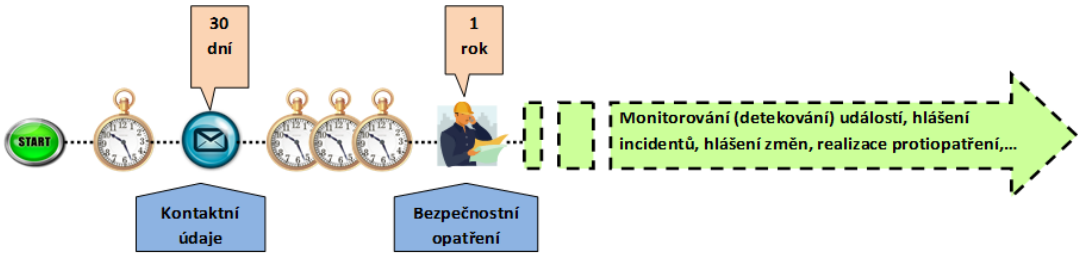
- **Kybernetický prostor** – digitální prostředí umožňující zpracování informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací
- **Kritická informační infrastruktura** – prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti
- **Kybernetická bezpečnostní událost** – událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací
- **Kybernetický bezpečnostní incident** – narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události

- **Stav kybernetického nebezpečí** – stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací (NBÚ, 2014)

Pro orgány a osoby, které určuje zákon, vznikla řada nových povinností v oblasti zajištění bezpečnosti informačních a komunikačních systémů a komunikace s určenými kontaktními místy. Mezi hlavní povinnosti správce informačního systému kritické informační infrastruktury a Správce komunikačního systému kritické informační infrastruktury patří:

- Oznámit NÚKIB kontaktní údaje do 30 dnů ode dne určení prvkem kritické informační infrastruktury
- Detekovat kybernetické bezpečnostní události
- Hlásit NÚKIB kybernetické bezpečnostní incidenty do 1 roku ode dne určení prvkem kritické informační infrastruktury
- Zavést bezpečnostní opatření do 1 roku ode dne určení prvkem kritické informační infrastruktury
- Provádět reaktivní opatření
- Provádět ochranné opatření (NBÚ, 2014)

Obrázek 11 - Časová osa plnění povinností



Zdroj: www.tsoft.cz

5.3 GDPR

Obecné nařízení o ochraně osobních údajů (**General Data Protection Regulation** neboli **GDPR**) je nová legislativa EU, která má výrazně zvýšit ochranu osobních dat občanů. Nařízení bylo přijato v roce 2016 a účinnosti nabude 25. května 2018. Přináší největší revoluci v ochraně osobních údajů s cílem hájit práva občanů EU proti neoprávněnému zacházení s jejich osobními údaji a daty. GDPR se týká všech subjektů zpracovávajících osobní údaje. V Česku nařízení nahradí současnou právní

úpravu ochrany osobních údajů v podobě směrnice 95/46/ES a související zákon č. 101/2000 Sb., o ochraně osobních údajů. To, že GPDR bylo přijato formou evropského nařízení, zamezuje vládě a státním zákonodárcům jakkoliv ohýbat či přizpůsobovat toto nařízení v rámci jednoho státu. Období od dubna 2016 do května 2018 je určeno k přípravě na toto nařízení. Během této doby musí všechny organizace, kterých se nařízení GDPR týká, zrevidovat své informační systémy a postupy zpracování osobních dat. Regulátorem pro Českou republiku bude nadále Úřad pro ochranu osobních údajů (ÚOOÚ). Bude však částečně podřízen Evropskému sboru pro ochranu osobních údajů (EDPB).

Nařízení nově zavádí princip tzv. zodpovědnosti, který spočívá v povinnosti správců a zpracovatelů údajů bez ohledu na jejich velikost nebo počet zaměstnanců zavést technická, organizační a procesní opatření za účelem prokázání souladu s principy GDPR. Tento princip s sebou nese další nemalé časové a finanční investice. Ty se budou týkat zejména následujících oblastí:

- implementace záměrné a nezbytné ochrany dat
- vypracování posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment - DPIA)
- jmenování pověřence pro ochranu osobních údajů neboli DPO (Data Protection Officer)
- zavedení tzv. pseudonymizace osobních údajů
- vedení záznamů o činnostech zpracování
- konzultace s dozorovým orgánem před samotným zpracováním osobních údajů

S GDPR dochází také k rozšíření definice osobních údajů. Nově sem spadají i technické parametry jako e-mail, IP adresa nebo tzv. cookies v zařízení uživatele. Nová je také kategorie tzv. genetických a biometrických údajů, jejichž zpracování bude podléhat přísnějšímu režimu. Největším úskalím se stává oznamovací povinnost v případě úniku či narušení bezpečnosti osobních údajů. V této situaci je subjekt povinen do 72 hodin ohlásit tuto událost ÚOOÚ. V některých případech bude nutné oznámit tento incident také osobám, kterých se únik týkal. V případě, že organizace nebude reagovat a nebude se připravovat na příchod nového evropského nařízení, hrozí poměrně vysoké někdy až likvidační sankce (Škorničková, 2017).

6 Analýza vybraného subjektu veřejného sektoru

Ve své praktické části práce jsem se rozhodl zhodnotit způsoby zabezpečení informací konkrétního podniku veřejného sektoru. Pro získání informací jsem využil metody expertního rozhovoru se třemi odpovědnými zástupci středního a vyššího managementu dané organizace. Každé setkání trvalo v průměru 90 minut a ve vyhrazeném čase jsem se snažil otevřenými otázkami získat maximální množství informací vztahujících se k dané problematice. Otázky byly kladeny vždy postupně od obecných, týkajících se širší oblasti problematiky, až po specifické, kde jsem cílil na detailní informace organizace a jejího řízení. Veškerá takto získaná data jsem zpracoval do ucelených kapitol dle jednotlivých oblastí informační bezpečnosti, které jsem na základě teoretických znalostí a praktických zkušeností podrobil analýze. V případech, kde se mi aktuální situace nezdála efektivní, jsem se pokusil navrhnout alternativní či doplňující řešení. V závěru praktické části jsou veškeré výsledky shrnuty a interpretovány. Na základě tohoto shrnutí jsem se pak pokusil potvrdit nebo vyvrátit hypotézy definované v úvodu práce. Vzhledem k citlivosti informací týkajících se dané organizace není možné praktickou část mé práce uveřejnit.

6.1 Základní informace o podniku

Řízení letového provozu, s.p. je organizací veřejného sektoru jejímž zřizovatelem je stát a výkonem svých funkcí spadá do rezortu ministerstva dopravy. Hlavním úkolem podniku je zajistit bezpečné služby ve vzdušném prostoru České republiky. Podnik již déle než deset let sídlí ve specializovaném objektu v Jenči, kde se nachází hlavní část technologického zázemí, většina dispečerů letového provozu včetně podpůrných a administrativních složek. Společnost krom bezpečnosti celého vzdušného prostoru zajišťuje přibližovací služby na letišti Václava Havla, v Brně, Ostravě a Karlových Varech. K technologickému vybavení společnosti náleží dva aktivní radary, strategicky umístěné v lokalitách Buchtův Kopec a Kopec Písek, a také síť pasivních radarů rozmístěných v okolí Prahy, Brna a Ostravy. Radary slouží jako primární zdroj informací dispečerům letového provozu ohledně polohy letadel. Pro případ výpadku primárních radarů jsou v pohotovosti udržovány záložní aktivní radary v lokalitách Kopec Praha a Kopec Skalky, které jsou v případě nouze okamžitě připraveny převzít činnost. Kromě této strategické infrastruktury podnik disponuje sítí sběrných stanic po celé České republice, odkud získává zejména meteorologická data. Ve výkonu svých činností podnik spolupracuje s dalšími subjekty veřejné správy jako je Český Aeroholding, Český hydrometeorologický ústav nebo

Armáda ČR. Bezpečnost není v tomto oboru pouze ekvivalentem finanční hodnoty, ale v extrémních případech může jít o lidské životy. Do konceptu bezpečnosti společnosti bezesporu spadá i ochrana informací, bez kterých podnik není schopen odpovědně poskytovat své služby.

Přestože není organizace financována z veřejného rozpočtu, vztahuje se na ni zákon o veřejných zakázkách, což v některých případech do určité míry ztěžuje výběr strategických dodavatelů služeb a technologií. Podnik je dle české legislativy také zařazen do kategorie správce kritické infrastruktury, z čehož mu vyplývají specifické povinnosti.

6.2 Správa a řízení informační bezpečnosti v organizaci

Řízení letového provozu zaměstnává bezmála tisíc pracovníku, z nichž valná většina sídlí v centrální budově v Jenči. Vzhledem k nadprůměrným podmínkám, které organizace nabízí svým zaměstnancům, je fluktuace pracovních sil téměř nulová. To je však vykoupeno vysokými požadavky na nové zaměstnance včetně časové náročnosti potřebné pro adaptaci jedince na pracovní prostředí a kolektiv. Zejména strategické a z hlediska bezpečnosti kritické pozice jsou obsazovány až po několikaleté zkušenosti v rámci organizace. Organizační změny ve struktuře jsou prováděny velmi zřídka a spíše postupnými a předem dlouho oznámenými kroky, nikoli skokově. Z hlediska informační bezpečnosti, kde většina hrozeb pochází zevnitř organizace, je výše popsaný stav personální politiky velmi výjimečný a hlavně žádoucí.

Podnik je z hlediska řízení rozdělen do několika divizí, kde útvar bezpečnosti zaujímá stále významnější postavení v rámci hierarchie společnosti. Je nezávislý na ostatních organizačních celcích, ředitel bezpečnosti je přímo podřízen generálnímu řediteli, je tedy přítomen každému strategickému rozhodnutí organizace a má přímý vliv na fungování podniku. Útvar bezpečnosti je také odpovědný za bezpečnostní politiku organizace včetně informační. Politika informační bezpečnosti je zařazena mezi strategické dokumenty organizace a má plnou podporu nejvyššího vedení společnosti při její realizaci. Obsahuje základní pravidla práce s informacemi jako je:

- zajištění personální bezpečnosti, s cílem snížit rizika spojená s lidským faktorem (chyby, krádeže, podvody, nesprávné použití či zneužití informací a informačního systému
- zajištění fyzické bezpečnosti, s cílem snížit rizika lidského neoprávněného vniknutí, poškození nebo zničení technických zařízení informačního systému

- zacházení s citlivými informacemi v podniku včetně klasifikace informačních aktiv
- řízení přístupu uživatelů, dále definici a správu přístupových práv četně vzdáleného přístupu, práci s mobilními zařízeními a modelu „home office“
- přehled základních bezpečnostních opatření při zpracování a výměně informací
- proces vývoje a údržby informačních systémů
- řízení kontinuity všech činností a havarijního plánování informačního systému
- ochrana informací a informačních aktiv organizace, ke kterým mají přístup třetí strany na základě smluvního vztahu
- správa a rozvoj informační politiky, hlavně kontrola plnění, aktualizace, zajištění shody s legislativou a smluvními závazky a provádění auditu informační bezpečnosti

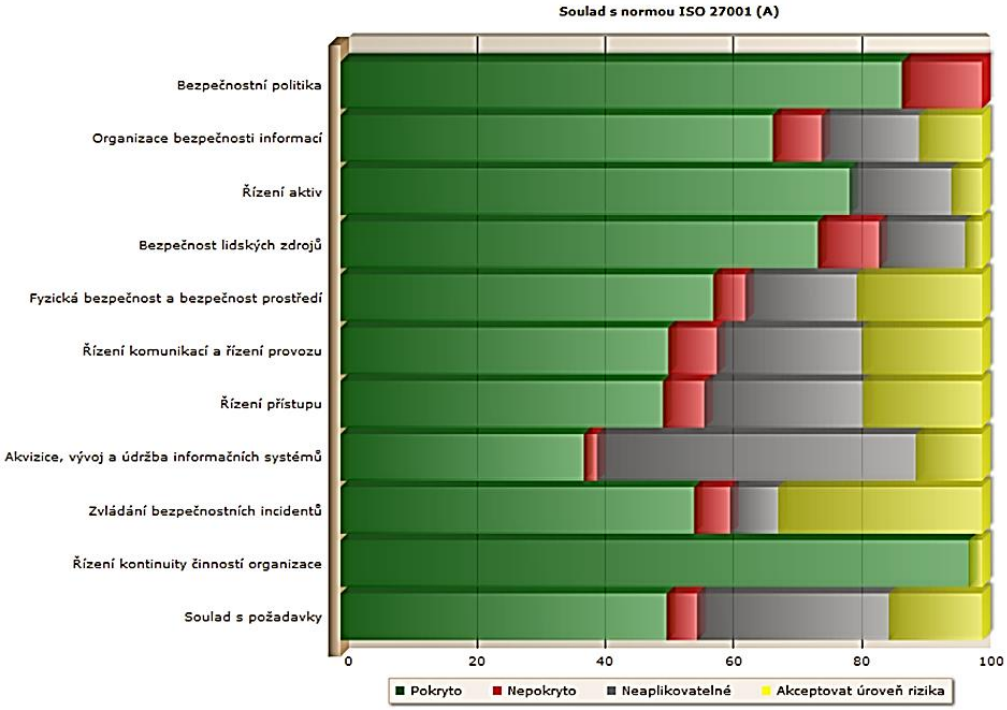
Přestože organizace nedisponuje certifikací ISO/IEC C27001, její bezpečnostní politika se striktně drží této normy.

6.2.1 RAMSES

Pro účely řízení systému bezpečnosti informací organizace využívá softwarový nástroj RAMSES dodaný společností RAC, která se specializuje na metodiku a podporu ISMS. RAMSES (Risk Analysis and Management System for Enhanced Security) je nástroj pro podporu řízení informační bezpečnosti. Použitý model SaaS (Software as a Service) nabízí efektivní a rychlý přístup k RAMSES s nízkými náklady a bez investic do infrastruktury.

RAMSES je efektivní nástroj pro podnikový útvar bezpečnosti, který provozuje systémy řízení bezpečnosti a kontinuity (ISMS, BCM). Nástroj RAMSES je založen na osvědčené metodice RAMSES, která vychází z metodiky CRAMM. Webové rozhraní RAMSES dovoluje jednoduchý přístup definovanému počtu uživatelů, kteří vyplňují dotazníky hrozeb a zranitelností, pracují s knihovnou protiopatření nebo zadávají parametry BCM (Business continuity management). Nástroj obsahuje přednastavené reporty ukazující úroveň souladu s ISO 27001, ISO 27002 a ISO 22301.

Obrázek 12 - Report souladu s normou ISO v prostředí RAMSES



Zdroj: interní dokument RAC

Uživatelé ŘLP pracují v RAMSES na základě rolí, které jim jsou přiděleny. Role odpovídají jejich pracovnímu zařazení a odpovědnosti za jednotlivá aktiva nebo určité oblasti.

RAMSES je plně v souladu se základními bezpečnostními standardy a zákony:

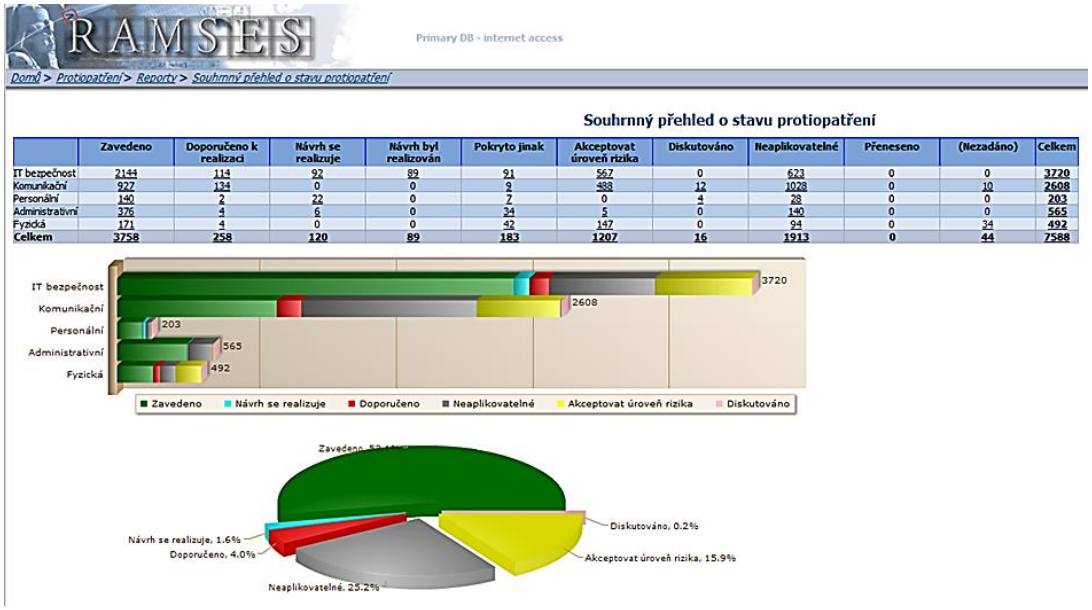
- **ČSN ISO/IEC 27001**
- **ČSN ISO/IEC 27002**
- **ČSN EN 16495**
- **ČSN ISO/IEC 27005**
- **ČSN ISO/IEC 22301**
- **zákon o kybernetické bezpečnosti**

Všechny kroky procesu řízení informačních rizik a řízení kontinuity plně korespondují z požadavky uvedených standardů a legislativy.

Řízení letového provozu pomocí nástroje RAMSES cílí zejména na následující plány a povinnosti:

- provést hodnocení rizik informačního systému v souladu s normou ISO/IEC 27005
- provést hodnocení rizik v souladu s požadavky zákona o kybernetické bezpečnosti.
- detailně určit hodnotu dat zpracovávaných v informačním systému
- stanovit nejrizikovější části informačního systému
- navrhnout protiopatření snižující zjištěná rizika
- plně podporovat proces zavádění ISMS v souladu s normou ISO/IEC 27001
- vytvořit a neustále aktualizovat kompletní bezpečnostní dokumentaci
- připravit celý systém na certifikaci podle ISO/IEC 27001
- analyzovat všechny druhy informačních systémů, ve všech fázích jejich životního cyklu

Obrázek 13 – Report stavu protiopatření systému RAMSES



	Zavedeno	Doporučeno k realizaci	Návrh se realizuje	Návrh byl realizován	Pokryto jinak	Akceptovat úroveň rizika	Diskutováno	Neaplikovatelné	Přeneseno	(Nezadáno)	Celkem
IT bezpečnost	2144	114	92	89	91	567	0	623	0	0	3720
Komunikační	927	134	0	0	9	488	12	1028	0	10	2608
Personální	140	2	22	0	7	0	4	28	0	0	203
Administrativní	376	4	6	0	34	5	0	140	0	0	565
Fyzická	171	4	0	0	42	147	0	94	0	34	492
Celkem	**3758**	**258**	**120**	**89**	**183**	**1207**	**16**	**1913**	**0**	**44**	**7588**

Zdroj: interní dokument RAC

6.2.2 ISMS

Výše popsaný nástroj dokáže efektivně řešit problematiku řízení informační bezpečnosti, nicméně samotná analýza a následné výstupy se neobejdou bez praktických zkušeností, jimiž organizace nedisponuje. Proto se podnik v roce 2015 obrátil na profesionály ze společnosti ICA (První certifikační autorita) s cílem zajistit kompletní analýzu rizik ve spolupráci s odpovědnými zaměstnanci podniku. Hlavním úkolem této spolupráce byla revize a aktualizace analýzy rizik ISMS a kvantifikace míry rizika s využitím nástroje RAMSES. Hlavní práce byly rozděleny do následujících čtyř etap:

- **Identifikace aktiv a služeb, vytvoření modelu informačních aktiv, poskytnutí podkladů pro vytvoření metodiky hodnocení rizik** - výstupem z této etapy je zpráva o vytvoření modelu informačních aktiv v nástroji RAMSES, dalším výstupem z této etapy jsou podklady umožňující organizaci následné vytvoření metodiky hodnocení rizik (stupnice pro hodnocení hrozeb a zranitelnosti, rozsah kritérií pro hodnocení rizik);
- **Hodnocení informačních aktiv z pohledu následku narušení jejich bezpečnosti, analýza dopadů** - výstupem z této etapy je zpráva o analýze dopadů
- **Stanovení velikosti výsledného rizika** - výstupem z této etapy je zpráva o hodnocení rizik
- **Návrh bezpečnostních opatření na pokrytí identifikovaných rizik, výběr opatření k realizaci, vytvoření plánu pro zvládání identifikovaných rizik** - výstupem z této etapy jsou dokumenty Prohlášení o aplikovatelnosti obsahující přehled vybraných a zavedených bezpečnostních opatření a Plán zvládání rizik zahrnující též popis vazeb mezi riziky a příslušnými navrhovanými bezpečnostními opatřeními

Při realizaci vytyčených cílů probíhaly rozhovory pracovníků ICA s jednotlivými odpovědnými pracovníky ŘLP s cílem co nejlépe popsat jednotlivé segmenty organizace a jejich funkce. Zakázka byla dokončena na konci roku 2017 a její výstupy budou promítnuty do bezpečnostní politiky organizace a souvisejících dokumentů. Zaměstnanci podniku jsou se změnami a aktualizacemi seznamováni na pravidelných školeních.

6.3 Legislativa

ŘLP, s.p. je organizací veřejného sektoru, která podléhá celé řadě mezinárodních norem a standardů týkajících se bezpečnosti letového provozu. Z hlediska české legislativy a oblasti informační bezpečnosti je subjekt povinen dodržovat nařízení plynoucí z kybernetického zákona a zákona o ochraně osobních údajů, který bude v květnu 2018 nahrazen evropskou směrnicí GDPR.

6.3.1 Kybernetický zákon

Zákon o kybernetické bezpečnosti definuje tzv. Správce informačního systému kritické informační infrastruktury a Správce komunikačního systému kritické informační infrastruktury. Do této kategorie spadá i ŘLP, z čehož mu plynou specifické povinnosti. Všechny organizace provozující kritickou infrastrukturu měly již dávno oznámit kontaktní údaje a zavést bezpečnostní opatření podle zákona. Tento krok je třeba učinit nejpozději do jednoho roku od okamžiku, kdy se prokáže, že daný informační nebo komunikační systém je kritická infrastruktura. Vznikl zde tedy určitý prostor na vylepšení či dopracování systému jako systému bezpečného a zajištění veškeré bezpečnostní dokumentace. Dalšími povinnostmi jsou detekce bezpečnostních událostí a oznamování bezpečnostních incidentů. V případě sledovaného subjektu nebyl prozatím oznámen žádný bezpečnostní incident.

Ustanovení § 5 kybernetického zákona uvádí, že bezpečností opatření sestávají z organizačních opatření a technických opatření. Lze mezi ně podřadit výše zmíněný systém řízení bezpečnosti, provádění řízení rizik, definování bezpečnostní politiky, nastavení organizační bezpečnosti, stanovení bezpečnostních požadavků pro dodavatele, řízení aktiv, zajišťování bezpečnosti lidských zdrojů atd. Kromě organizačních opatření existují i technická opatření, z nichž některá jsou nástroji, další jsou aplikační, bezpečnostní, nalezneme zde ale třeba i kryptografické prostředky.

NÚKIB je oprávněn kontrolovat dodržování stanovených zákonných povinností a ukládat nápravná opatření k odstranění nedostatků. Neplnění některých povinností je považováno za správní delikt s výší pokuty až 100 000 Kč. Podobná kontrolní akce zatím nebyla v rámci ŘLP provedena.

K naplnění zákonných povinností ŘLP zřídilo tzv. kybernetický výbor, který sdružuje manažery útvaru bezpečnosti s odpovědnými zástupci jednotlivých divizí společnosti, kterých se nařízení prakticky dotýká. Kybernetický výbor se setkává na pravidelné bázi s cílem sjednotit strategii podniku v oblasti kybernetické bezpečnosti, sledovat odchylky reálného fungování od zákonných povinností navrhovat zlepšení.

6.3.2 GDPR

Směrnice GDPR se týká všech subjektů v České republice, které zpracovávají osobní údaje, ŘLP nevyjímaje. Na rozdíl od kybernetického zákona však organizaci neukládají žádné specifické povinnosti z titulu subjektu veřejné sféry. V ŘLP byl v rámci útvaru bezpečnosti a lidských zdrojů zřízen tzv. „GDPR tým“, který má za úkol analyzovat veškeré činnosti podniku týkající se správy osobních údajů, zajistit efektivní pravidla na práci a ukládání těchto údajů a navrhnout technická a organizační opatření, která by eliminovala kolize se směrnicí. V řízení letového provozu se s osobními údaji pracuje zejména na personálním oddělení, jehož zástupci tvoří nedílnou součástí GDPR týmu.

Nařízení nově zavádí princip tzv. zodpovědnosti, který spočívá v povinnosti správců a zpracovatelů údajů bez ohledu na jejich velikost nebo počet zaměstnanců zavést technická, organizační a procesní opatření za účelem prokázání souladu s principy GDPR. Uplatnění principu zodpovědnosti bude představovat pro ŘLP nemalé časové a finanční investice. Ty se budou týkat zejména těchto oblastí:

- implementace záměrné a nezbytné ochrany dat
- vypracování posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment – DPIA)
- jmenování pověřence pro ochranu osobních údajů neboli DPO (Data Protection Officer)
- zavedení tzv. pseudonymizace osobních údajů
- vedení záznamů o činnostech zpracování
- konzultace s dozorovým orgánem před samotným zpracováním osobních údajů

6.4 Fyzická a HW bezpečnost

Budova ŘLP v Jenči, kde sídlí většina personálu organizace, byla navržena tak, aby splňovala veškeré standardy fyzické bezpečnosti. Budova je fyzicky i administrativně rozdělena do dvou částí dle úrovně bezpečnosti. V přední části budovy mají zázemí zejména administrativní pracovníci, zadní část budovy je vybavena dalšími bezpečnostními prvky a sídlí zde dispečeři letového provozu včetně jejich přímé technické podpory a management organizace. Tato část budovy včetně interního datového centra je designována jako protiatomový kryt a je odstíněna od externího elektromagnetického záření včetně radiových vln. Vstup do budovy je zabezpečen předsunutou recepcí s nepřetržitou ostrahou vzdálenou přibližně 100 metrů od hlavní budovy, kde dochází k první identifikaci vstupujících do budovy organizace.

Hned u hlavního vchodu je umístěna druhá recepce s ostrahou vybavená rentgenem, kterým musí projít každá osoba mířící do administrativní části budovy, vyjma zaměstnanců. Každý vstupující je také vybaven čipovou identifikační kartou, kterou musí mít po celou dobu umístěnu na viditelném místě. Karta opravňuje ke vstupu do administrativní nebo provozní části budovy, která je vybavena další recepcí s ostrahou a rentgenem, kterým již vždy musí projít každá osoba vstupující do této zóny budovy. Celá budova je dále zajištěna důmyslným kamerovým systémem, který zachycuje a ukládá veškerý pohyb osob po objektu. Velmi podobně, byť s redukovanými bezpečnostními prostředky, jsou vybaveny i regionální pracoviště v Brně, Ostravě, Karlových Varech a radarových základnách. Speciálním a zároveň klíčovým objektem ŘLP je budova tzv. technického bloku, situovaná v areálu Letiště Praha, která slouží jako disaster recovery objekt, jenž je schopen v omezeném režimu převzít agendu centrální budovy v případě přírodní či jiné katastrofy. Veškerá zařízení kritické infrastruktury organizace včetně datového centra mají vždy dva nezávislé zdroje napájení doplněné o UPS/diesel agregát pro případ výpadku napájení. Veškeré kritické provozní systémy jsou dimenzovány na mnohonásobně vyšší než průměrnou zátěž a každé zobrazovací zařízení využívané k řízení letového provozu využívá několika zdrojových systémů, aby případná ztráta komunikace měla co nejmenší dopad na dispečery a jejich činnost. Veškerá firemní komunikace je pro případ následného šetření šifrována a archivována. Archivace v pravidelných intervalech probíhá i na úrovni kritických systémů a dokumentů pro případ nouzové obnovy při neočekávané ztrátě dat. K přístupu na zabezpečené servery se v organizaci používají hardwarové tokeny využívající standardizovaný symetrický šifrovací algoritmus AES, které musí oprávněný uživatel zapojit do čtečky před zadáním přístupového jména a hesla. Toto řešení je užíváno jak pro interní zaměstnance, tak pro externí firmy, které spravují systémy na základě smluvního vztahu.

6.5 Sítě a komunikace

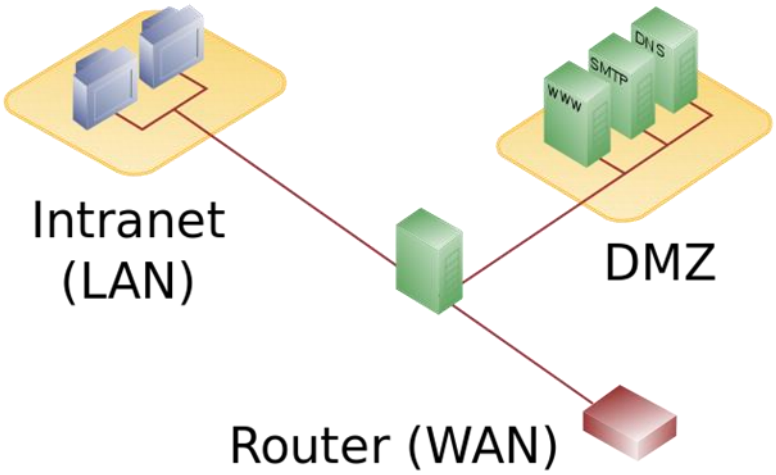
6.5.1 Segmentace sítě a internet

Informační systémy jsou z hlediska provozu a bezpečnosti funkčně, ale i fyzicky rozděleny do dvou oblastí: ATC (Air traffic control) a MIS (Management information system). Do ATC segmentu, jak už význam napovídá, spadají veškeré informační a komunikační prostředky využívané pro primární účel organizace. Jedná se o kritické systémy, jejichž selhání by mohlo mít katastrofické následky. Tato část sítě se udržuje z hlediska inovací v naprosto konzervativním duchu z důvodu potřeby maximální spolehlivosti jednotlivých komponent. Systém je naprosto autonomní a

jakýkoliv zásah podléhá předem definovanému procesu. Naproti tomu MIS oblast infrastruktury zahrnuje administrativní, ekonomické a další podpůrné systémy, jejichž výpadek ovlivní některé činnosti organizace, ale neohrozí bezpečnost letového provozu.

Segmenty sítě jsou fyzicky oddělené pomocí firewallů výrobce Juniper a poskytují nepřetržitou ochranu provozních systémů před externími hrozbami lidského faktoru zejména prostřednictvím sítě internet. ŘLP je připojeno do celosvětové sítě internet prostřednictvím dvou nezávislých konektivit dvou poskytovatelů pro případ výpadku služeb jednoho z providerů. Internetová konektivita je připojena pouze do segmentu sítě MIS a o její bezpečnost se stará dvojice firewallů amerického výrobce Check Point. Firewally fungují jako stavové paketové filtry s kontrolou protokolů a IDS s pokročilou ochranou proti externím útočníkům.

Obrázek 14 - Model DMZ s jedním firewallem



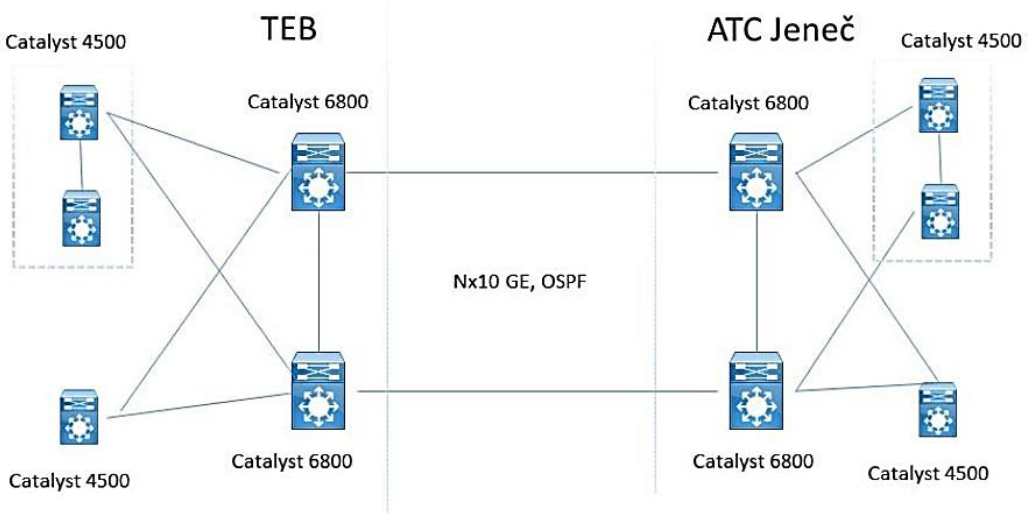
Zdroj: wikipedie.org

V demilitarizované zóně (DMZ) jsou umístěny služby e-mailu, webové služby a DNS. Služby v DMZ mají omezené připojení k vybraným počítačům ve vnitřní síti, naopak komunikace s ostatními službami v DMZ a venkovní sítí je povolena. To umožňuje severům v DMZ poskytovat služby jak pro vnitřní, tak i pro vnější sítě, zatímco firewall kontroluje provoz pouze mezi servery v DMZ a klienty vnitřní sítě.

6.5.2 LAN (Local Area Network)

Vnitrofiremní síť je postavena výhradně na produktech společnosti Cisco systems, díky čemuž je řešení homogenní a jednotlivé komponenty jsou vzájemně plně kompatibilní. Vysoká dostupnost je zajištěna použitím redundantních boxů, napájecích zdrojů a supervisorů u modulárních přepínačů. Páteřní síť tvoří přepínače řady Cisco Catalyst 6800, které jsou zároveň páteřními přepínači na obou kritických lokalitách (ATC, Technický blok). Spojení v rámci páteře má aktuálně k dispozici propustnost 2 x 10 GE, do budoucna je plánováno jako Nx10 GE. Byla zvolena topologie páteřních boxů ve tvaru čtverce, neboť křížová topologie na optických okruzích nepřináší žádné výhody. Přístupová síť je tvořena přepínači řady Catalyst 4500, kde každý přepínač je připojen pomocí agregovaných linek na oba páteřní přepínače Catalyst 6800 využitím topologie dvojité hvězdy.

Obrázek 15 - Topologie LAN



Zdroj: interní dokument ŘLP

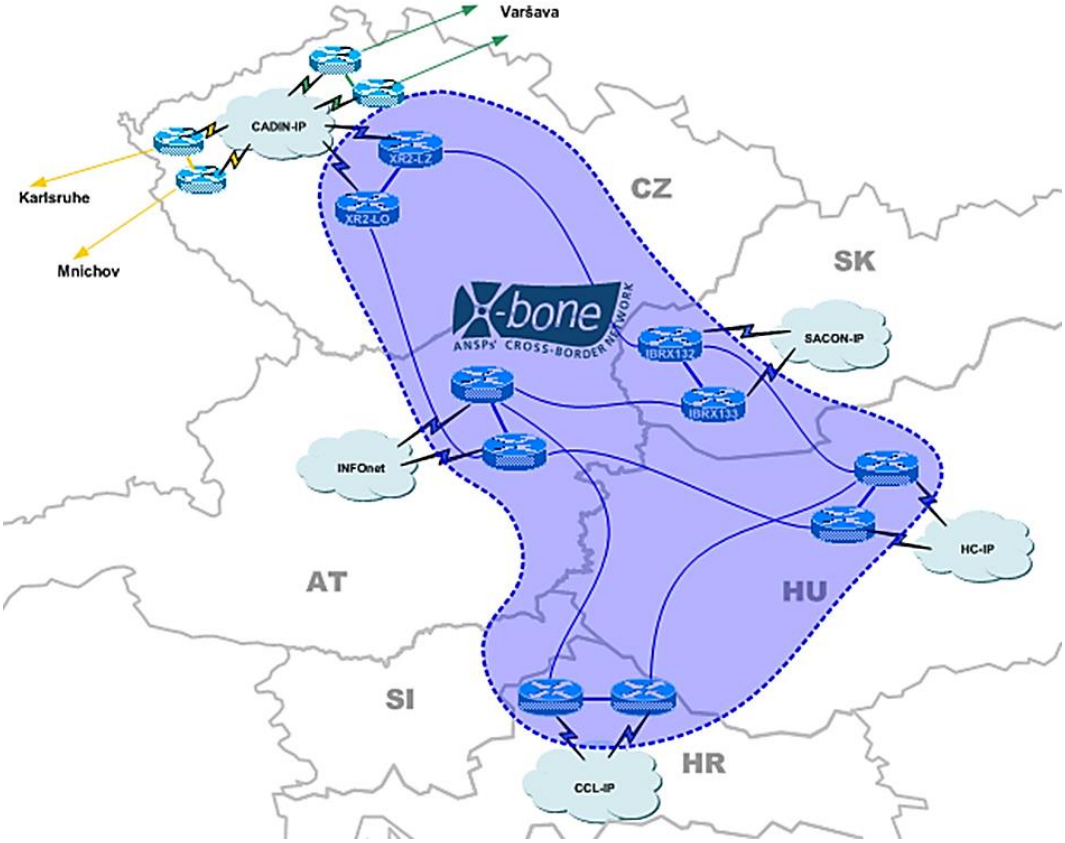
Menší pobočky podniku jsou postavené na jednotném principu, kde jako core/access prvek slouží Catalyst 3650, zapojený ve stohu. K němu jsou připojeni uživatelé a technologická zařízení. Pro filtrování odchozí komunikace do jiných lokalit, případně pro komunikaci do internetu, jsou implementována pravidla na přepínači.

6.5.3 WAN (Wide Area Network)

Datová komunikace mezi centrálou, regionálními letišti a radary je naprosto klíčová pro fungování primárních řídících služeb organizace. Po těchto datových linkách probíhá výměna citlivých informací, které jsou nezbytné pro bezproblémový provoz podniku. Vzhledem k nárokům na vysokou bezpečnost, dostupnost, kvalitu a kapacitu přenosových linek byla síť navržena jako autonomní systém mimo veřejnou síť internet, kde je dosaženo bezpečného datového přenosu. Kvalita a variabilní kapacita spojení je zajištěna pomocí optické infrastruktury, která je individuálně připojena do každé lokality ŘLP vždy ze dvou nezávislých zdrojů. Vysokou dostupnost datových služeb pak zajišťuje topologie sítě, kde každá přípojka má nezávislou plně automatickou zálohu s nezávislým koncovým zařízením z produktové řady Cisco Systems. Datovou komunikaci pro ŘLP zajišťuje společnost O2, která garantuje nezávislost připojení v celém průběhu komunikačních tras. Služba je postavena na protokolu MPLS (Multiprotokol Label Switching), který eliminuje možnost výpadků služby v páteřní síti a zároveň nabízí garantované parametry přenosových linek jako je např. zpoždění, ztráta paketů, atp. Na stejném principu a se stejnými parametry je poskytována dedikovaná síť vyhrazená pro radiovou komunikaci na IP protokolu mezi dispečery a letadly. Zde jsou krom výše zmíněných garancí kladeny extrémní nároky na parametr zpoždění linky.

Komunikace s mezinárodními partnery (Řízení letových provozů sousedících zemí) je provozována vždy na nezávislé dvojici pronajatých metalický okruhů, které poskytují maximální dostupnost služeb v mezinárodním standardu s garantovanou propustností a zabezpečením, neboť jsou také vyhrazené pouze pro účely této komunikace bez závislosti na veřejné síti internet. V rámci uskupení FAB CE, do kterého krom ŘLP ČR patří Austro Control (Rakousko), LPS SR (Slovensko), HungaroControl (Maďarsko) a Croatia Control (Chorvatsko) vznikla v roce 2016 nezávislá komunikační síť zajišťující výměnu koordinačních a radarových dat pod názvem X-BONE (Cross-Border Network). Síť je postavena na výše zmíněných pronajatých okruzích se speciální topologií podporující maximální dostupnost služeb, jak je nastíněno na schématu níže.

Obrázek 16 - Mezinárodní datová síť X-BONE



Zdroj: interní dokument ŘLP

6.5.4 Hlasová komunikace a WIFI

Standardní hlasová komunikace není z hlediska provozování řídících služeb nijak kritická, proto se významně neliší od komunikačních platforem komerčních subjektů. Fixní hlasová komunikace probíhá na IP protokolu platformy Cisco Call Manager a pomocí hlasové brány jsou hovory směrovány do digitální sítě operátora. Veškerá komunikace je nahrávána šifrována a archivována podpůrným systémem dodaným společností Retia za účelem důkazních materiálů. Platforma Call Manager je rozšířena také o videokonference, které jsou využívány zejména k mezinárodním hovorům. Pro tento účel je zřízena dedikovaná linka do internetu a veškerý provoz probíhá šifrovaným kanálem. Veškeré budovy ŘLP jsou vybaveny bezdrátovým přístupem WIFI do firemní sítě. Objekty ŘLP jsou odstíněny od okolní komunikace, tedy ani wifi signál neproniká přes ochrannou vrstvu stěn ven z budovy. Veškerý provoz je šifrován pomocí algoritmu WPA2. Autentizace přístupu je řešena jinými

softwarovými prostředky popsanými v následující kapitole. Bezdrátová komunikace je také umožněna návštěvám v centrální budově v Jenči, kde jim je vystaven časově omezený přístup do internetu po zadání systémem vygenerovaného jména a hesla. Komunikace směrem do internetu probíhá po vyhrazené lince bez možnosti narušení centrální internetové přípojky. Někteří zaměstnanci využívají modelu „home office“, kdy jim je zabezpečeným šifrovaným kanálem umožněn přístup do některých segmentů podnikové sítě pomocí internetu. Mobilní hlasová a datová komunikace je zajišťována společností O2 a z hlediska požadavků na bezpečnost nemá ŘLP žádné speciální služby oproti jiným subjektům.

6.6 SW nástroje informační bezpečnosti

6.6.1 Antivir a antispam

Řízení letového provozu používá kompletní antimalware řešení od finské společnosti **F-secure**. Přestože výrobce na svých stránkách deklaruje plnou ochranu před ransomware, organizace se v roce 2017 potýkala s kybernetickým útokem právě tímto typem škodlivého software. Škodlivý kód zašifroval některé administrativní soubory, ale nijak neohrozil provoz společnosti. Díky pravidelným zálohám byl obnoven poslední uložený bod a organizace tak nemusela provádět platbu výkupného za dešifrování souborů téměř bez ztráty dat. Z pohledu kybernetického zákona se nejednalo o bezpečnostní incident týkající se kritické infrastruktury. F-secure řešení prozatím není rozšířeno na mobilní zařízení organizace.

Jako spamový filtr používá podnik řešení od společnosti Cisco Systems **IronPort**. Zařízení pracuje jako transparentní poštovní filtr, na který se nasměrují MX záznamy filtrovaných poštovních domén a po odfiltrování Ironport čistou poštu doručí cílovým poštovním serverům, a to jak ve směru příchozí tak odchozí pošty. Základem filtrace je online databáze s údaji o IP adresách poštovních serverů, nazvaná Senderbase. Na základě údajů ze Senderbase se buď mail okamžitě zahodí (takto se bez větších nároků na složitou analýzu odstraní až 99% spamu) nebo propustí k další analýze. V dalších krocích se z online databází Ironport porovnají tzv. otisky známých spamů s kontrolovanými maily, provedou se uživatelem zadaná pravidla a pokud je pošta vyhodnocena jako čistá, je doručena. Pomocí LDAP se udržuje seznam platných mailových adres s MS Exchange. Zařízení je odolné proti DoS útokům (zablokuje komunikaci s útočícími IP adresami) i proti přetížení, má samostatné fronty pro jednotlivé IP adresy, takže fronta se tvoří pouze pro intenzivně odesílající servery a ostatní jsou odbavováni průběžně. Zařízení pracuje spolehlivě ke spokojenosti IT administrátorů ŘLP.

Kybernetický výbor ŘLP na konci roku 2017 doporučil implementaci nové bezpečnostní platformy Cisco Umbrella, která analyzuje internetový provoz a na základě zkušeností automaticky blokuje škodlivý obsah a pokusy o útoky na severy a koncové stanice. Doplňuje tak činnosti firewallu a antimalwaru.

6.6.2 Mobile device management

Zaměstnanci ŘLP využívají mobilní zařízení napříč systémy iOS, Windows mobile i Android a v tomto směru neexistují žádné požadavky na sjednocení platformy. Z tohoto důvodu byl vybrán produkt společnosti Mobileiron, který s podporou všech mobilních platforem řeší zabezpečení firemních dat před nesprávnou manipulací nebo jejich ztrátou. Produkt dále umožňuje centrální správu mobilních aplikací, kontrolu a dohled nad užíváním zařízení a firemních dat a také uplatňování firemní politiky používání zařízení, aplikací a dokumentů. Mobileiron nabízí technické prostředky pro uplatňování ochrany osobních údajů v souladu s nařízením GDPR. Platforma je také vhodná pro stále atraktivnější model BYOD (Bring Your Own Device). V ŘLP není tento model podporován. Funkce produktu je také možné rozšířit na standardní PC a notebooky v režimu DLP (Data Leak Protection), ale ani toto rozšíření není v podniku aplikováno.

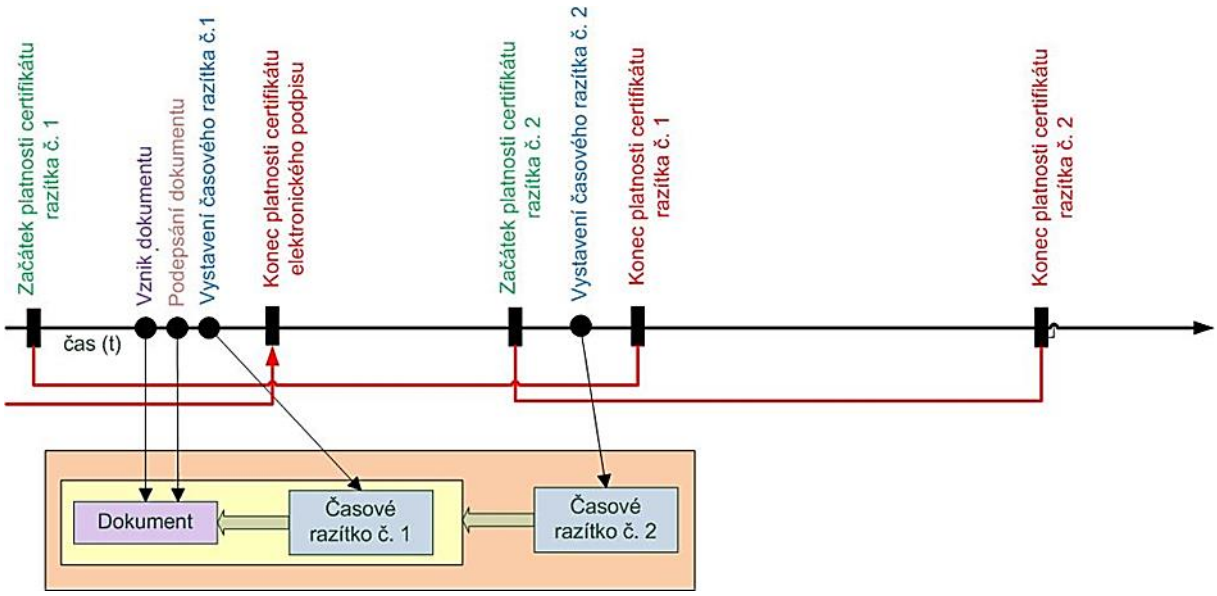
6.6.3 Důvěryhodný archiv

Každý podnik uchovává značné množství dokumentů, jako jsou smlouvy, účetní a daňové dokumenty, které dle platné legislativy musí být archivovány po dobu tří, pěti a v některých případech i deseti let. Tato pravidla platí i pro organizace veřejné správy, ŘLP nevyjímaje. Za účelem dlouhodobé a bezpečné archivace těchto dokumentů se ŘLP rozhodlo implementovat do svých administrativních systémů produkt společnosti O2 – důvěryhodný archiv. Při definování potřeb služby byly vytyčeny níže uvedené požadavky:

- **Integrita dokumentu** - možnost v kterémkoliv okamžiku života dokumentu prokazatelně zjistit, byl-li dokument porušen či nikoliv
- **Neodmítnutelnost odpovědnosti** - možnost nezpochybnitelným způsobem prokázat konkrétnímu subjektu autorství nebo účast v procesu zpracování dokumentu
- **Časové určení dokumentu** - možnost nezpochybnitelným způsobem prokázat přesný časový údaj o vzniku nebo úpravě dokumentu

Integrita dokumentu je zajištěna pomocí zaručeného elektronické podpisu nebo elektronické značky. Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu. Tím je garantována neodmítnutelnost odpovědnosti. Časové určení dokumentu je zajištěno kvalifikovaným časovým razítkem, které vydal kvalifikovaný poskytovatel certifikačních služeb, a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem. Při potřebě jakékoliv manipulace s dokumenty je třeba elektronicky podepsané žádosti, která se archivuje stejným způsobem jako vlastní dokumenty. Na obrázku č. 17 níže je patrný princip dlouhodobé a bezpečné archivace dokumentů v prostředí důvěryhodného archivu.

Obrázek 17 - Princip bezpečné archivace



Zdroj: interní dokument O2

V prostředí ŘLP je za pomoci tohoto produktu archivována většina dokumentů ekonomické, finanční a obchodní povahy, které vyžadují dlouhodobou validitu a v případě sporu i právní oporu.

6.6.4 Identity services engine

V roce 2016, v zájmu sjednocení přístupových oprávnění, bezpečnostní útvar ŘLP doporučil implementaci protokolu 802.1X pro autentizaci, autorizaci přístupu a správu MAC adres zařízení na LAN a WIFI síti. Vzhledem k tomu, že komponenty LAN i WIFI sítě podniku jsou od stejného výrobce, v zájmu homogenity bylo vybráno řešení ISE (Identity Service Engine) od společnosti Cisco, které nabízí jednotnou platformu centrální řízení přístupu do podnikové sítě. Implementace řešení aktuálně probíhá.

6.6.5 Security information and event management

V souladu s požadavky kybernetického zákona od roku 2015 ŘLP využívá produkt SIEM (Security Information and Event Management) Arcsight společnosti HP. Řešení bylo implementováno on premise do technologického prostředí organizace s cílem:

- pružnější a rychlejší reakce na útoky
- úspěšnější detekce útoků
- zefektivnění správy infrastruktury
- získávání automaticky vytvářených statistik o infrastruktuře

Aktuálně jsou do SIEM řešení připojeny aktivní síťové prvky, firewally a antimalware za účelem sběru logů a veškeré vyhodnocovací práce jsou plně pod kontrolou vyškolených administrátorů podniku. Analýza výstupů ze SIEM se v praxi ukázala jako velmi časově náročná a aktuálně chybí v ŘLP kapacity na rozšíření monitorovaných systémů, přestože technické prostředky řešení jsou k dispozici.

6.6.6 Další využívané služby informační bezpečnosti

Každý den se na světě objevují stovky nových zranitelností a jsou odhaleny tisíce bezpečnostních incidentů. Jelikož je oblast informační bezpečnosti velmi rozsáhlá a rychle se rozvíjí, bývá obtížné ji pokrýt z interních zdrojů. Většina organizací proto volí bezpečnostní ověření třetí nezávislou stranou, která se na oblast bezpečnosti úzce specializuje. Řízení letového provozu si v pravidelných ročních intervalech objednává nezávislé penetrační testy, které kromě primárního cíle - odhalit co nejvíce vážných zranitelností a ověřit odolnost vůči cílenému průniku, mohou výsledky penetračního testu pomoci při vzdělávání vývojářů a správců systémů, či jiných zaměstnanců. Tato oblast se zdá být v podniku obecně podceněna, neboť byl v roce 2017 zaznamenán případ, kdy zaměstnanec podniku podlehl hrozbě sociálního in-

ženýrství, když byl proplacen účtárnou doklad, který nebyl nikde evidován a nebyl podložen žádnou obchodní aktivitou.

V dnešní době ŘLP využívá také informační služby o kybernetických hrozbách, které upozorňují na aktuální zranitelnosti na využívaných platformách. Služba zajišťuje varování před kybernetickými hrozbami, které již byly popsány a umožní tak organizaci přijmout preventivní opatření k eliminaci hrozeb formou aktualizací či SW záplat. Obecně jsou v podniku prováděny pravidelné aktualizace software vyjma provozního prostředí, které je na základě „best practice“ udržováno v konstantním módu.

7 Shrnutí a doporučení

Řízení letového provozu je jedinečným a velmi specifickým subjektem veřejného sektoru a od toho se odráží i veškerá organizace a řízení informační bezpečnosti. Veškeré aktivity organizace jsou striktně podřízeny primárnímu cíli podniku v podobě zajištění bezpečnosti a plynulosti letového provozu. Organizace je z hlediska legislativy považována za správce kritické infrastruktury, ale zároveň podléhá povinnostem plynoucím ze zákona o veřejných zakázkách. Tyto zákony přímo nekolidují, ale rozhodně ztěžují rozhodování o výběru vhodných bezpečnostních opatřeních poskytovaných třetími stranami. Veškerá mnou navrhovaná doporučení je tedy třeba brát velmi rezervovaně právě z důvodu složitosti problematiky veřejných zakázek, kde ekonomická výhodnost vždy hraje významnou roli. Zároveň je třeba připomenout, že každé bezpečnostní opatření s sebou nese také určitou zátěž v podobě finančních a lidských zdrojů a také procesů, které většinou snižují komfort a efektivitu práce uživatelům informačních systémů. Bezpečností opatření by tedy měla být implantována s rozumem a zejména s ohledem na potenciální efekt dané hrozby.

Řízení letového provozu je vybaveno robustní infrastrukturou, která odpovídá celosvětovým standardům podobných organizací. Fyzická bezpečnost je garantována již samotnou konstrukcí budovy se zavedenými bezpečnostními prvky jako několikanásobná kontrola vstupu do objektů, kamerový systém a systém indentifikačních karet, které autorizují osoby ke vstupu do určité části objektu. Bezpečnostní opatření by pravděpodobně neodolala cílenému fyzickému útoky za pomocí střelných zbraní a jiných násilných metod, ale pravděpodobnost podobné akce je velmi nízká a podobná rizika jsou přenesena na jiné odpovědné složky státu, jako je policie nebo armáda ČR. Zajímavé by mohlo být doplnění bezpečnostních prvků o biometrické údaje k dosažení vícefaktorové autentizace. Tím by bylo sníženo potenciální riziko zneužití HW či SW prostředků. Fyzická infrastruktura je dimenzována na mnohonásobně vyšší zátěž a proti externím hrozbám je zajištěna několikanásobnou systémovou, HW, ale i SW redundancí. V organizaci jsou zpracovány krizové scénáře, které řeší disaster recovery plány. Z tohoto pohledu se zdají být opatření dostatečná snad s výjimkou datového centra, které nemá v případě kompletního výpadku adekvátní výkonovou náhradu. Za potenciální hrozbu v tomto ohledu je možné považovat např. teroristický útok, přírodní či leteckou katastrofu s následkem fyzické destrukce datového centra organizace. Pro zajištění plné redundance služeb datového centra bych doporučil zvážit možnosti záložního hostingového centra s principem tzv. geoclusteru, který by řešil případy nedostupnosti služeb primárního datového centra. Návrh samozřejmě naráží na

ekonomickou náročnost řešení, ale také na logické propojení systémů s činnostmi jednotlivých uživatelů.

Personální politika organizace plně koresponduje s požadavky na vysoce kvalitní personální obsazení společnosti. Díky štědré personální politice si podnik může dovolit cílit na profesionály ve svém oboru s vysokými nároky na jejich kvalifikaci a praxi. Vedle toho se tento princip také ukazuje jako velmi stabilní z hlediska fluktuace zaměstnanců, což s sebou přináší eliminaci hrozeb přicházejících zevnitř organizace. Drobné nedostatky jsem objevil v problematice vzdělávání administrativních pracovníků v oblasti informační bezpečnosti, kde bych navrhoval zapojit online nástroje vzdělávacích kurzů do prostředí podnikového intranetu, doplněné o interní penetrační testy, které by ověřily dodržování bezpečnostních zásad uživatelů v praxi. Jako potenciální riziko zde vidím zejména metody sociálního inženýrství, které, jak již praxe ukázala, mohou zejména v kombinaci s dalšími nekalými činnostmi zkomplikovat život jakékoliv firmě.

Z hlediska organizace a řízení bezpečnosti není snadné něco podniku vytknout. Útvar bezpečnostní má nezávislou funkci na ostatních divizích společnosti a podílí se na veškerých strategických rozhodnutích podniku s přímým vlivem na generálního ředitele. Bezpečnostní politika se řídí doporučeními vycházejícími z normy ISO/IEC 27001, což zároveň koresponduje s některými povinnostmi zákona o kybernetické bezpečnosti. V oblasti řízení bezpečnosti informací třeba je v rámci podniku striktně odlišovat primární provozní systémy v síti ATC, jejichž výpadek by mohl mít drastické následky, od podpůrných systémů v síti MIS, jejichž nečinnost má pouze dílčí vliv na fungování organizace. Bezpečnostní politika a návazné procesy jsou plně v souladu s kybernetickým zákonem a překvapila mne snad pouze informace, že příslušný úřad doposud neprovedl v podniku audit v souladu se zákonem. Připravovaná směrnice GDPR sice znamená pro podnik určitá opatření, nicméně dopady za porušení pravidel jsou čistě ekonomické, byť významné.

Kritická komunikační infrastruktura je postavena na standardech nejvyšší kvality s maximálním důrazem na dostupnost a bezpečnost přenášených informací. Pro účely této komunikace je vyhrazena dedikovaná síť naprosto nezávislá na síti internet. Administrativní a podpůrná část sítě je fyziky i logicky oddělena a s pomocí firewallu propojena se sítí internet. Aktuálně využívaný firewall Check Point již slouží v síti více než šest a let, a i přes jeho opakovaný upgrade, model výkonově nedostačuje stále zvyšujícím se potřebám komunikace podniku s potenciálním rizikem ohrožení fungování administrativní části podniku. Z hlediska kvality produktu, na základě magického čtyřúhelníku společnosti Gartner, doporučuji stávající řešení nahradit některým z modelů výrobců PaloAlto, Fortinet, Cisco Systems nebo zůstat

o nové modelové řady aktuálního výrobce. Všichni zmínění výrobci nabízejí produkty vysoké kvality s nejnovějšími prvky ochrany před kybernetickými hrozbami.

Obrázek 18 - Magický čtyřúhelník společnosti Gartner

Zdroj: gartner.com

Podnik také nedisponuje účinným řešením proti DDoS útokům, které by mohly dočasně ochromit podpůrné činnosti organizace spojené s internetovými službami. AntiDDoS produkty bývají obecně velmi nákladné a jejich účinnost je teoreticky omezena různými charakteristikami. Protože internetové připojení netvoří kritickou část infrastruktury podniku, vynaložení nemalých prostředků na pořízení této technologie je v tomto případě opravdu neefektivní. Zajímavou kompromisní formou může být nabídka antiDDoS řešení přímo ze strany poskytovatele internetu. Např. O2 nabízí efektivní řešení formou služby od společnosti Arbor. Za jednoznačně nevyhovující softwarový prostředek považuji aktuální antivirový systém od společnosti F-Secure. K tomuto závěru mne vede jednak výše popsaný úspěšný útok ransomwaru a zároveň nezávislé testy uveřejňované na stránkách av-test.org. Dle

těchto testů dosahují aktuálně nejlepších hodnot enterprise produkty společností Kasperky, Trendmicro nebo Bitdefender. Zároveň doporučuji rozšířit oblast detekce malware i pro mobilní zařízení. Rizika spojená s malware neustále rostou a přestože by neměla mít vliv na primární činnost organizace, tuto hrozbu není možné podceňovat.

Mobileiron platforma patří dle společnosti Gartner ke špičce v oblasti řešení správy mobilních zařízení. V prostředí ŘLP je však využívána pouze malá část z komplexního řešení. Za účelem ochrany proti zneužití dat doporučuji zavést restriktivní politiky nad mobilními přístroji včetně zavedení hesel pro přístup do mobilních zařízení. Platformu doporučuji rozšířit i na firemní PC a notebooky k zamezení ztráty či poškození dat. Navrhovaná opatření jsou v souladu s normou GDPR a zároveň může omezení posloužit pro start modelu BYOD v organizaci.

Velmi pozitivně hodnotím rozhodnutí o zavedení jednotné autentizační a autorizační platformy nad protokolem 802.1X, které přinese sjednocení bezpečnostních opatření přístupu pro LAN a WIFI síť a zavede jasná pravidla pro přístup k informacím. Žádné komplikace ani kolize se zákonem jsem neshledal na prostředcích bezpečné archivace a aktualizace softwaru. Spamový filtr Ironport, který dle společnosti Gartner patří mezi špičku v oboru, funguje spolehlivě a implementace platformy Umbrella jen dokazuje, že ŘLP patří mezi organizace, které nešetří na zabezpečení svých podnikových dat.

Jako další prvek ochrany před kybernetickými hrozbami bych doporučil řešení postavené na standardu NetFlow. NetFlow výrazně zefektivňuje řadu úloh, jako je například řešení provozních problémů v síti, plánování kapacity, řízení výkonnosti, a poskytuje informace důležité pro ochranu podniku před jinak skrytými kybernetickými hrozbami. Implementace řešení však znamená umístění dalších prvků (kolektor, sonda) do vnitřní infrastruktury, proto doporučuji zavést platformu pouze do administrativní části sítě mimo provozní systémy. Každé zařízení v síti navíc představuje další bezpečnostní rizika, která by mohla síť ATC spíše ohrozit.

Nakonec této kapitoly bych rád zhodnotil implementaci SIEM do prostředí ŘLP. Co se týče samotného produktu Arcsight, jedná se špičkový produkt, který se pravidelně umísťuje na čelních pozicích v hodnocení společnosti Gartner. Z dostupných informací je však patrné, že zdaleka ne všechna zařízení, která by mohla být do SIEM připojena, jsou tímto způsobem monitorována a analyzována. ŘLP má tedy k dispozici mocný nástroj, ale hlavním úskalím je nedostatek pracovních sil pro analýzu výstupů ze systému. Jedná se bohužel o relativně častý jev u těchto produktů. Řešením může být samozřejmě posílení personálního stavu, nicméně je možné,

třeba jen dočasně, využít profesionály třetích např. v podobě tzv. SOC (Security operation center) k analytickým a vyhodnocovacím činnostem.

Závěrem je možné prohlásit, že ŘLP je v současné době dostatečně chráněno před kybernetickými hrozbami v souvislosti s poskytováním primárních služeb nad kritickou infrastrukturou. Veškerá má doporučení se týkají pouze podpůrných složek a systémů, které nemají vliv na služby řízení letového provozu. Ze získaných informací jsem také došel k závěru, že bezpečnost a ochrana informací v podniku je v souladu s aktuálně platnou legislativou.

Závěr

Hlavním cílem mé práce bylo definovat a popsat bezpečnostní hrozby týkající se informačních aktiv organizace a doporučit vhodná technická a organizační opatření na jejich ochranu. Zaměřil jsem se na oblast ochrany informací v prostředí organizace veřejného sektoru, nicméně převážná většina výstupů práce je aplikovatelná i pro podniky komerční sféry. Teoretická část práce uvedla čtenáře do problematiky informační bezpečnosti a představila stěžejní témata, jako jsou bezpečnostní hrozby, ochranu dat, související legislativu, ale i základy kryptografie, a měla by posloužit jako funkční základna pro analytickou část práce. Ta se pak věnuje zejména analýze ochrany dat v prostředí vybraného podniku veřejného sektoru na základě výstupů z expertních rozhovorů s odpovědnými pracovníky dané organizace. Na základě získaných informací jsem zhodnotil aktuální stav informační bezpečnosti společnosti a navrhl technické a organizační změny, které by měly přispět k efektivnější ochraně podnikových dat.

Jako významný, nikoli však kritický, nedostatek jsem označil nízkou úroveň praktických znalostí z oblasti kybernetických hrozeb mezi administrativními pracovníky organizace. Tento stav není vzhledem k rychlému vývoji informačních a komunikačních technologií žádným překvapením a s podobným problémem se aktuálně potýká převážná většina firem. Podceněním této oblasti mohou dotčeným organizacím vzniknout nemalé finanční ztráty. K řešení této situace doporučuji nasazení e-learnigových výukových nástrojů s podporou interních penetračních testů třetích stran.

Další problémovou oblastí je nedostatek odborných kapacit v oblasti informační bezpečnosti. Rapidní růst kybernetických hrozeb nutí organizace k zajištění technických ochranných opatření, což s sebou přináší potřebu stále větší pracovní kapacity a hlubších expertních znalostí. Tento trend se bude pravděpodobně objevovat stále častěji a jeho řešením může být předání vybraných částí bezpečnostní agendy specializovaným odborníkům dodavatele. Zákon tuto variantu nijak nevylučuje.

Ostatní doporučení se týkala zejména softwarových prvků ochrany informací, kde jsem narazil na problematiku efektivního výběru dodavatelů těchto produktů a služeb. Organizace veřejné sféry jsou povinny dodržovat ustanovení zákona o veřejných zakázkách, které jsou postaveny zejména na ekonomické výhodnosti řešení, což významně ztěžuje výběr bezpečnostních produktů a služeb třetích stran.

Dílčím cílem práce byla analýza povinností vyplývajících z aktuálně platné legislativy, zejména pak kybernetického zákona, a jejich plnění v praxi. Kybernetický

zákon představuje klíčovou normu pro subjekty veřejné správy v oblasti informační bezpečnosti. Novela zákona z roku 2017 uvádí zákon do souladu s mezinárodními směrnicemi EU. Speciální požadavky klade na správce kritické informační a komunikační infrastruktury. Na rozdíl od jiných norem, jsou v zákoně zakotveny některé povinnosti ve formě cílového stavu a je na každém subjektu, aby si zajistil efektivní cestu k jeho dosažení. Velmi podobně je na tom i směrnice GDPR, která navíc přináší obrovská rizika v podobě ekonomických sankcí při nesplnění povinností.

Na základě získaných informací sledovaný subjekt veřejného sektoru naplňuje veškeré povinnosti související s kybernetickým zákonem a připravuje vhodná opatření ke splnění požadavků vyplývajících ze směrnice GDPR. Kontrola souladu opatření organizace s kybernetickým zákonem ze strany regulátora však ještě nebyla provedena.

V úvodu práce jsem stanovil dvě hypotézy: *„Subjekty kritické infrastruktury veřejné správy jsou efektivně chráněny proti kyberútokům." „Současná legislativa ČR, týkající se informační bezpečnosti, dostatečně podchycuje možné informační hrozby pro subjekty kritické infrastruktury veřejné správy."* Analytická část mé práce dokazuje, že sledovaný podnik disponuje efektivními nástroji na ochranu informací s maximálním důrazem na kritickou část infrastruktury. Prostou metodou indukce, tedy zobecnění sledovaného jevu na množinu subjektů, mohu s klidným svědomím potvrdit první hypotézu. Legislativa ČR v posledních letech udělala značné kroky ke sjednocení standardů v problematice informační bezpečnosti. Oporu může hledat i v mezinárodním prostředí Evropské unie. Na druhou stranu analytická část mé práce prokázala, že normy v oblasti informační bezpečnosti zdaleka nepodchycují veškeré informační a hrozby a povinnosti vyplývající ze zákona často poukazují pouze na požadovaný stav a jeho vynucování pod sankcemi. Druhou stanovenou hypotézu tedy nemohu potvrdit. V této oblasti však není možné ani v budoucnu čekat na zázrak. Vývoj kybernetických hrozeb je tak dynamický, že zkostnatělá zákonodárná moc nemůže včas reagovat na aktuální nedostatky.

Informační bezpečnost je stále obecně podceňovaná oblast. Přitom většina organizací je na informacích v podstatě životně závislá. Při analýze vybraného podniku jsem byl velmi mile překvapen, jak daleko je organizace v oblasti ochrany informací a nemám nejmenší důvod se domnívat, že s vývojem nových kybernetických hrozeb se organizace efektivně nevypořádá.

Seznam literatury

AEC. 2017. řešení DLP. *DLP.* [Online] AEC, 2017. https://www.ami.cz/reseni-a-sluzby/bezpecnost-dat/data-loss-prevention-1.

AVAST. 2017. ransomware. *ransomware.* [Online] AVAST, 2017. https://www.avast.com/cs-cz/c-ransomware.

Blackstone, John a Cox, James. 2013. *APICS dictionary.* Chicago : APICS, 2013. ISBN10: 1558221956.

Burda, Karel. 2013. *APLIKOVANÁ KRYPTOGRAFIE.* Brno : VUTIUM, 2013. 978-80-214-4612-0.

Burda, Karel. 2005. *Bezpečnost informačních systémů.* Brno : FEKT VUT Brno, 2005.

Čech, Pavel a Zelenka, Josef. 2002. *Ochrana dat: informační bezpečnost - výkladový slovník.* Hradec Králové : Gaudeamus, 2002. ISBN 80-7041-197-X.

Doseděl, Tomáš. 2004. *Počítačová bezpečnost a ochrana dat.* Brno : Computer Press, 2004. ISBN:80-251-0106-1.

EMAN. 2017. MDM. *Mobile devoce management.* [Online] EMAN, 2017. https://www.eman.cz/sluzby/mobile-device-management/.

Erben, Lukáš. 2014. *Úsvit hackerů: První géniové kyberprostoru.* [E-kniha] Praha : Internet Info, s.r.o., 2014.

Flowmon. 2017. ADS. *flowmon.* [Online] 2017. https://www.flowmon.com/cs/products/flowmon/anomaly-detection-system.

GORDIC spol. s r.o. 2017. KYBEZ. *KYBEZ.* [Online] GORDIC spol. s r.o., 2017. https://www.kybez.cz/bezpecnost/pred-cim-chranit.

Grady, Mark a Parisi, Francesco. 2011. *The Law and Economics of Cybersecurity.* New York : Cambridge University Press, 2011. ISBN: 9781107403109.

ISO 27000. 2017. ISO 27000 online. *ISO 27000.* [Online] listopad 2017. http://www.27001-online.com/.

ISO. 2013. ISO/IEC 27001:2013. *ISO.* [Online] International Organization for Standartization, 2013. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534.

Jirovský, Václav. 2007. *Kybernetická kriminalita.* Praha : Grada, 2007. ISBN: 978-80-247-1562-2.

Kurose, James a Ross, Keith. 2014. *Počítačové sítě.* Brmo : Computer Press, 2014. ISBN 978-80-251-3825-0.

MIT. 2017. Viruses, Spyware, and Malware. *IST.* [Online] MIT, listopad 2017. https://ist.mit.edu/security/malware.

Molnár, Zdeněk. 2009. *Podnikové informační systémy.* Praha : ČVUT, 2009. ISBN:978-80-01-04380-6.

NBÚ. 2014. Zákon o kybernetické bezpečnosti. *Národní bezpečnostní úřad.* [Online] 19. 12 2014. http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/provadeci-pravni-predpisy-k-zakonu-c-1812014-sb-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu/.

NOVICOM. 2017. ADDNET. *ADDNET.* [Online] listopad 2017. https://www.novicom.cz/addnet_nac.

NÚKIB. 2017. govcert.cz. *govcert.cz.* [Online] 2017. https://www.govcert.cz/cs/vladni-cert/govcert-cz/.

Piper, Fred a Murphy, Sean. 2006. *Kryptografie.* Praha : Dokořán, s.r.o., 2006. ISBN: 80-7363-074-5.

Požár, Josef. 2005. *Informační bezpečnost.* Plzeň : Aleš Čeněk s.r.o., 2005. ISBN: 80-86898-38-5.

Požár, Josef. 2010. *Systém řízení informační bezpečnosti.* Brno : Tribun EU, 2010. ISBN: 978-807399-067-1.

Rubeš, Michal. 2016. *Návrh zabezpečení informačního systému podniku střední velikosti ve více lokacích.* [Diplomová práce] Zlín : Univerzita Tomáše Bati ve Zlíně, 2016.

Sands.cz. 2017. SIEM. *SIEM.* [Online] 2017. http://www.sands.cz/sluzby-produkty/bezpecnost-ict/security-information-and-event-management-siem.

Securita. **Jeger, Dag. 2017.** Praha : Economia, a.s., 2017. ISBN: 978-80-85378-46-7.

Soriano, Miguel. 2016. *Zabezpečení informací a sítí.* Praha : České vysoké učení technické v Praze, 2016. ISBN: 978-80-01-05296-9.

Škorničková, Eva. 2017. gdpr.cz. *GDPR.* [Online] 2017. https://www.gdpr.cz/gdpr/.