Metriky pro oblast bezpečnosti informací

Bakalářská práce

Karel Jína

Vedoucí bakalářské práce:
Ing. Ladislav Beránek, CSc., MBA

Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta
Katedra informatiky
Rok 2010

Prohlášení

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

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

V Českých Budějovicích dne 22.4.2010

….....

Karel Jína

Anotace

Cílem této práce je podat přehled o tom, jak se v praxi řeší a hodnotí úroveň informační bezpečnosti. Čtenáři se dozví, co jsou metriky, k čemu se používají a jakou hrají roli v systému řízení bezpečnosti informací ISMS. Samotný systém je v práci rovněž vysvětlen. Praktickou část pak představuje provedení průzkumu stavu bezpečnosti informací v několika organizacích a návrh několika kandidátních metrik, které by bylo možné použít v prostředí Jihočeské univerzity.

Abstract

The aim of this bachelor thesis is to provide an overview about how the level of information security is solved and evaluated in practice. The readers will learn what metrics are, what are they used for and what role do they play in the Information Security Management System (ISMS). The system itself is being explained as well. The practical part presents execution of a research concerning the status of information security in several organizations and a proposal of several candidate metrics that could be used in the environment of Jihočeská univerzita.

Poděkování

Děkuji panu Ing. Ladislavu Beránkovi, CSc., MBA za příkladné vedení mé bakalářské práce. Dále bych chtěl poděkovat všem respondentům, kteří byli ochotni účastnit se průzkumu stavu bezpečnosti v jejich organizacích. Zejména pak paní manažerce informační bezpečnosti JU, která mi poskytla základní informace o systému řízení bezpečnosti informací ISMS na Jihočeské univerzitě a objasnila mi, jak se zavádění takového systému v praxi realizuje.

Obsah

1 ÚVOD 9

2 VYMEZENÍ BEZPEČNOSTI INFORMACÍ 11

2.1 INTEGRITA, DOSTUPNOST, DŮVĚRNOST 12

2.1.1 Integrita 12

2.1.2 Dostupnost 12

2.1.3 Důvěrnost 12

2.2 BEZPEČNOSTNÍ INCIDENT 12

2.3 AKTIVUM 13

2.4 HROZBA 13

2.5 ZRANITELNOST 13

2.6 OPATŘENÍ 14

2.7 RIZIKO 14

3 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ 15

3.1 ISMS 17

3.2 FÁZE USTANOVENÍ ISMS 18

3.2.1 Definice rozsahu ISMS 18

3.2.2 Politika ISMS 19

3.2.3 Analýza rizik 19

3.2.4 Prohlášení o aplikovatelnosti 19

3.3 FÁZE ZAVEDENÍ A PROVOZOVÁNÍ ISMS 19

3.3.1 Plán zvládání rizik 20

3.3.2 Školení 20

3.3.3 Navržení metrik a způsobu měření účinnosti ISMS 20

3.4 FÁZE MONITOROVÁNÍ A PŘEZKOUMÁVÁNÍ ISMS 22

3.4.1 Audit bezpečnosti 22

3.5 FÁZE UDRŽOVÁNÍ A ZLEPŠOVÁNÍ ISMS 23

3.6 NORMY ISO/IEC 27XXX PRO ŘÍZENÍ BEZPEČNOSTI INFORMACÍ 23

3.7 METODIKY PRO ŘÍZENÍ IT SLUŽEB 24

3.7.1 COBIT 24

3.7.2 ITIL 25

4 METRIKY 27

4.1 POJEM METRIKA 27

4.2 VLASTNOSTI SPRÁVNÉ METRIKY 27
4.2.1 Objektivně měřitelná metrika 28
4.2.2 Levná metrika 28
4.2.3 Opakovatelná metrika 29
4.2.4 Výsledek měření vyjádřen konkrétním číslem 29
4.2.5 Výsledek měření vztažen ke konkrétní veličině 29
4.3 ČLENĚNÍ METRIK 29
4.3.1 Tvrdé a měkké metriky 30
4.3.2 Kontinuální a diskrétní metriky 30
4.3.3 Metriky z pohledu úrovní řízení 31
4.3.4 Interní, externí metriky 31
4.3.5 Metriky podle BSI Group 31
4.3.6 Metriky podle NIST 32
4.3.7 Metriky v rámci metodik ITIL a COBIT 36
4.4 METRIKY V OBLASTI OUTSOURCINGU 37
4.5 UKÁZKA KONKRÉTNÍCH METRIK 38
4.6 NÁSTROJE PRO AUTOMATICKÝ SBĚR DAT 38

5 PRŮZKUM STAVU BEZPEČNOSTI INFORMACÍ 39

5.1 CÍL PRŮZKUMU, POČÁTEČNÍ PŘEDPOKLADY 39
5.2 METODIKA TVORBY DOTAZNÍKU 39
5.3 ORGANIZACE BEZPEČNOSTI 42
5.4 OUTSOURCING 44
5.5 STANDARDY VYUŽÍVANÉ PRO ŘÍZENÍ BEZPEČNOSTI 45
5.6 METRIKY 47
5.7 AUDITY BEZPEČNOSTI 50
5.8 PENETRAČNÍ TESTOVÁNÍ 50
5.9 FYZICKÉ ZABEZPEČENÍ 52
5.10 ŠKOLENÍ ZAMĚSTNANCŮ 52
5.11 ANALÝZA RIZIK 54
5.12 MONITORING ČINNOSTI ZAMĚSTNANCŮ, KAMEROVÉ SYSTÉMY 55
5.13 ZÁVĚREČNÉ SHRNUTÍ 57

6 ISMS A METRIKY NA JIHOČESKÉ UNIVERZITĚ 59

6.1 SOUČASNÝ STAV ISMS NA JČU 59
6.2 NÁVRH VLASTNÍCH METRIK 61

6.2.1 Šablona *62*
6.2.2 Celková bezpečnostní politika *63*
6.2.3 Školení o ochraně osobních údajů a nakládání s nimi *64*
6.2.4 Školení v oblasti bezpečnosti informací *65*
6.2.5 Počet bezpečnostních incidentů *67*
6.2.6 Shrnutí *68*

7 ZÁVĚR 69

LITERATURA 71

SEZNAM PŘÍLOH 75

1 Úvod

V současnosti je informační bezpečnost vzhledem k rostoucí hodnotě informací stále frekventovanějším pojmem, a to jak v komerční, tak i státní sféře. Firmy i státní instituce uchovávají čím dál více důležitých dat, jejichž ztráta, změna či odcizení by mohly mít pro jejich chod a existenci nedozírné následky. Je proto nutné se proti potenciálním hrozbám chránit.

Existuje velké množství bezpečnostních technologií od síťových monitorovacích systémů až po antivirové programy. Příkladem hardware mohou být firewally, IDS systémy, architektury založené na DMZ a mnoho dalších. Softwarovými řešeními pak mohou být například různé antivirové či antispamové programy. Nikdy si však nemůžete být jisti tím, že jsou vaše data v absolutním bezpečí. Samotné zabezpečení proto nestačí. Pokud chce být organizace opravdu úspěšná, musí umět rozpoznat, co je pro ni důležité, co přesně chránit, jak to provést a pravidelně monitorovat a měřit úroveň bezpečnostních opatření. Důležité je držet krok s dobou a hlavně s konkurencí.

To, jak efektivně řídit bezpečnost informací, není potřeba nějak složitě vymýšlet. Existují systémy řízení bezpečnosti, založené na mezinárodně uznávaných standardech, které vycházejí z praktických zkušeností odborníků na danou problematiku. V současné době se jako optimální využívá systém řízení bezpečnosti informací (ISMS - Information Security Management System), ustanovený dle normy ČSN ISO/IEC 27001, který kombinuje různé přístupy od řízení lidských zdrojů až po řízení systémů. Součástí tohoto systému je i měření a monitoring stávající úrovně bezpečnosti.

Existují různé metriky pro oblast bezpečnosti informací. Tyto metriky mohou být založeny jak na tvrdých ukazatelích, jako je množství financí vkládaných do oblasti bezpečnosti informací, tak i na měkkých ukazatelích, jako je strategické plánování.

Obsah této práce lze rozdělit na dvě části. V té první se čtenář seznámí se základními pojmy z oblasti bezpečnosti informací. Bude mu představen systém řízení bezpečnosti informací jako celek a poté mu bude vysvětleno, co je metrika a měření a v jakém jsou vztahu k řízení bezpečnosti informací. Praktickou část bakalářské práce pak představuje průzkum provedený v několika organizacích na základě předem vytvořeného dotazníku, jehož cílem je podat přehled o tom, jakým způsobem se řeší a hodnotí informační bezpečnost. Dále pak zjištění stavu systému ISMS na Jihočeské univerzitě a návrh několika kandidátních metrik, které by mohly být v univerzitním prostředí použity.

2 Vymezení bezpečnosti informací

Nelze mluvit o řízení bezpečnosti informací a metrikách pro oblast bezpečnosti informací bez znalostí základních pojmů a porozumění samotnému termínu informační bezpečnost. Z tohoto důvodu je nejprve vysvětleno, co znamená bezpečnost informací a jak by se dala charakterizovat.

Zajistit bezpečnost informací znamená zachovat jejich důvěrnost, integritu a dostupnost, přičemž informace mohou mít různou formu. Nemusí se nutně jednat o informace v elektronické podobě. Mohou být i v podobě písemné či formě myšlenky (znalost, kterou někdo nabyl v daném prostředí). Takovými citlivými informacemi mohou být například utajované výrobní postupy a různé receptury nebo znalost přístupových hesel. Zajistit bezpečnost informací v této podobě se může jevit jako dosti obtížné, neboť lze jen stěží zamezit tomu, aby si někdo „pustil pusu na špacír“. Existují však prostředky, které mohou riziko vyzrazení snížit. Jedním z opatření může být dohoda o mlčenlivosti, jejímž podpisem se daná osoba zavazuje k diskrétnosti.

V souvislosti s termínem bezpečnost informací je nutno zmínit také dva další pojmy, a to bezpečnost organizace a bezpečnost IT/ICT.

Pod pojmem bezpečnost organizace si lze představit především zajištění její fyzické bezpečnosti například pomocí různých kamerových systémů, biometrických systémů či ostrahu objektů a areálů prostřednictvím strážní služby, což napomáhá zajištění bezpečnosti IS/ICT.

Naopak bezpečnost IS/ICT má za úkol chránit výhradně jen ta aktiva, která jsou součástí informačního systému organizace. Tedy aktiva nehmotná. [2]

2.1 Integrita, dostupnost, důvěrnost

2.1.1 Integrita

Zajistit integritu informací znamená učinit taková opatření, aby byly informace správné a úplné. V praxi se často může stát, že na základě nějaké události dojde k nežádoucí změně dat. Pokud je tato změna včas odhalena, je možné opětovnou správnost zajistit například pomocí záloh.

2.1.2 Dostupnost

Zajistit dostupnost znamená podniknout takové kroky, aby informace byla k dispozici všem oprávněným uživatelům v okamžiku, kdy ji potřebují.

2.1.3 Důvěrnost

Zajistit důvěrnost informací znamená provést taková opatření, aby informace byly přístupné pouze oprávněným osobám.

2.2 Bezpečnostní incident

Bezpečnostním incidentem je jakákoli událost, která má za následek narušení integrity, dostupnosti nebo důvěrnosti informací. Mnohdy se za bezpečnostní incident považují i pokusy překonat bezpečnostní opatření či porušení bezpečnostní politiky. Abychom mohli na bezpečnostní incident reagovat, musíme ho nejprve umět detekovat a zanalyzovat. Samotná detekce může být prováděna jak manuálně (oznámením zaměstnance), tak i automaticky pomocí různých monitorovacích systémů. Poté je zapotřebí stanovit závažnost incidentu například podle hodnoty aktiva, jehož integrita, důvěrnost nebo dostupnost byla narušena. [1]

2.3 Aktivum

Jako aktivum lze označit cokoli, co má pro organizaci nějaký význam, nějakou cenu. Základní dělení rozlišuje aktiva na aktiva primární a sekundární, přičemž větší důležitost se obvykle přisuzuje právě primárním aktivům, neboť se jimi myslí zejména aktiva nehmotná, jako jsou data důležitá pro chod organizace. Sekundární aktiva jsou pak zejména ty prostředky, které mají hmotnou podobu.

- Primární aktiva – např. data, služby, programové vybavení, pracovní postupy.
- Sekundární aktiva – např. technické prostředky (PC, tiskárna apod.), ale i zaměstnanci či samotné prostory a budovy. [2]

2.4 Hrozba

Hrozbou je myšlena jakákoli událost, která by mohla ohrozit bezpečnost. Existuje celá řada hrozeb od přírodních katastrof, jako jsou požáry či zemětřesení až po hrozby ze strany člověka. Lidskou hrozbou je myšlen kupříkladu nějaký naschvál či pomsta nespokojeného zaměstnance, nějaký neúmyslný čin způsobený nedostatečnou odborností nebo zanedbání povinností. Pro informační aktiva je největší hrozbou náhodné, neoprávněné nebo úmyslné:

- upravení – porušení integrity dat,
- zničení dat,
- prozrazení důležitých interních informací. [2]

2.5 Zranitelnost

Zranitelnost lze definovat jako jakoukoli slabinu aktiva. Prostřednictvím slabých míst může docházet k neautorizovaným přístupům ke zdrojům

systému. Zranitelnost pak lze rozdělit na fyzickou (budovy, místnosti), programových prostředků, nosičů dat, kabelových rozvodů (např. nebezpečí odposlechu) a personální. [2]

2.6 Opatření

Jako opatření lze označit jakoukoli techniku, aktivitu nebo zařízení, které omezí účinky hrozby či ji dokonce naprosto eliminují. Tato opatření mohou být jak fyzická, tak i technická a administrativní. [2]

- Fyzická opatření – používání trezorů, vchody do důležitých prostor opatřeny snímači čipových karet či biometrickými zařízeními (např. snímač otisků prstů).
- Technická a technologická opatření – např. použití hesla pro přístup do systému.
- Administrativní – různé směrnice a pokyny pro používání IS/ICT.

2.7 Riziko

Riziko lze definovat jako kombinaci hrozby, která působí na aktivum a zranitelnosti tohoto aktiva. Působící hrozba může snížit hodnotu tohoto aktiva – způsobit škodu. Potom říkáme, že má na aktivum dopad. Dopad je tedy škoda, která vznikla účinným působením hrozby na dané aktivum. [2]

3 Systém řízení bezpečnosti informací

Zajištění bezpečnosti informací se na první pohled může zdát jako jednoduchá záležitost. Není tomu ovšem tak. Jedná se o důmyslný proces, který by měl být řízen. Měla by být jasně daná pravidla, postupy a zejména kontroly a měření, na jejichž základě lze vylepšit stávající bezpečnostní opatření a předejít tak možným bezpečnostním incidentům. Velmi důležitou věcí je také množství financí, které je vynaloženo do bezpečnosti informací. Organizace by neměly bezmyšlenkovitě vynakládat finance do bezpečnostních opatření, která by pro jejich účely byla nevýznamná, ba dokonce zcela nepotřebná. Je proto nutné analyzovat aktuální bezpečnostní úroveň a poté aplikovat vhodné prostředky.

Jak již bylo řečeno, zajistit informační bezpečnost není jednoduchou záležitostí. Existuje však značné množství metodik či systémů pro řízení bezpečnosti informací, které ve většině případů vycházejí z praktických zkušeností odborníků znalých dané problematiky. Není proto nutno pracně vyvíjet nějaké nové postupy, ale je možno zavést postupy již řádně zdokumentované a v praxi odzkoušené nebo se jimi alespoň nechat inspirovat.

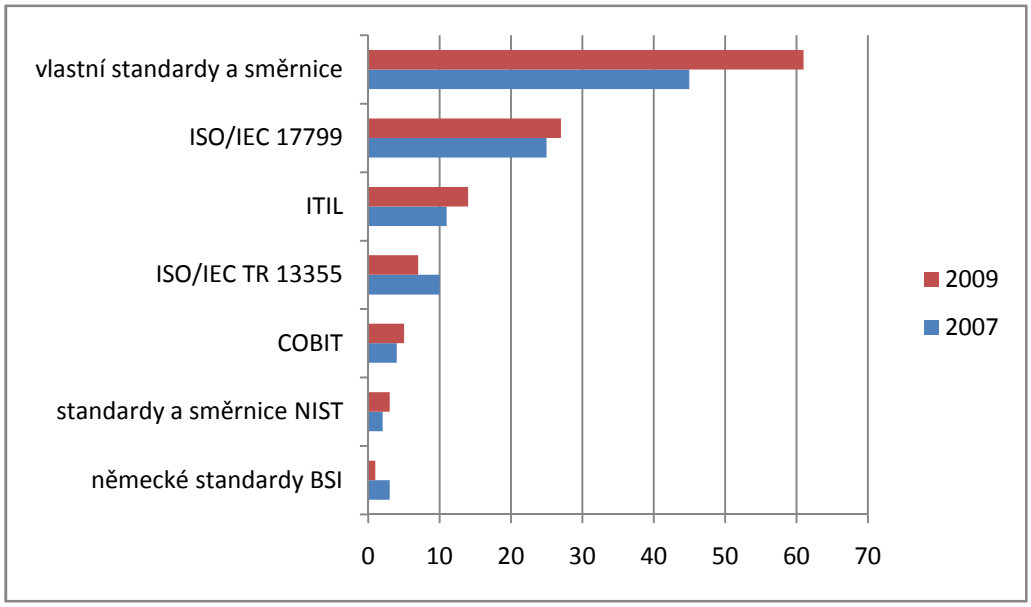
Z průzkumů stavu informační bezpečnosti v ČR, který je každý lichý rok počínaje rokem 1999 prováděn prostřednictvím společnosti Ernst & Young, Národního bezpečnostního úřadu a časopisu DSM vyplývá, že nejvíce společností v posledních letech využívá k řešení bezpečnosti informací vlastní interní směrnice a standardy. Z veřejně známých a všeobecně uznávaných standardů pak je nejvíce rozšířena norma ISO/IEC 17799 (ISO/IEC 27001), na které je založen systém pro řízení bezpečnosti informací ISMS. Dále pak následují další používané standardy a metodiky, jako COBIT, ITIL či NIST. Pro zajímavost je uvedena tabulka a graf znázorňující rozšíření používaných bezpečnostních standardů vyplývajících z průzkumu PSIB z roku 2007 [3] a 2009 [4]. Ještě je nutné dodat, že do průzkumu byly zahrnuty pouze

společnosti s nejméně 100 zaměstnanci, a to z různých oborů působnosti (energetika, státní správa, bankovnictví, strojírenství…).

Rok	Osloveno organizací	Množství vyplněných dotazníků	Obory působnosti
2007	1100	333	14
2009	1100	280	18

Tab. 1: Počty respondentů PSIB 2007, 2009

Rozšíření bezpečnostních standardů pak znázorňuje následující obrázek. Důležitým zjištěním je pak stoupající tendence zavádění standardu ISO/IEC 27001 (ISO/IEC 17799), ze kterého vychází systém řízení bezpečnosti informací ISMS, o kterém bude na následujících stranách pojednáno.

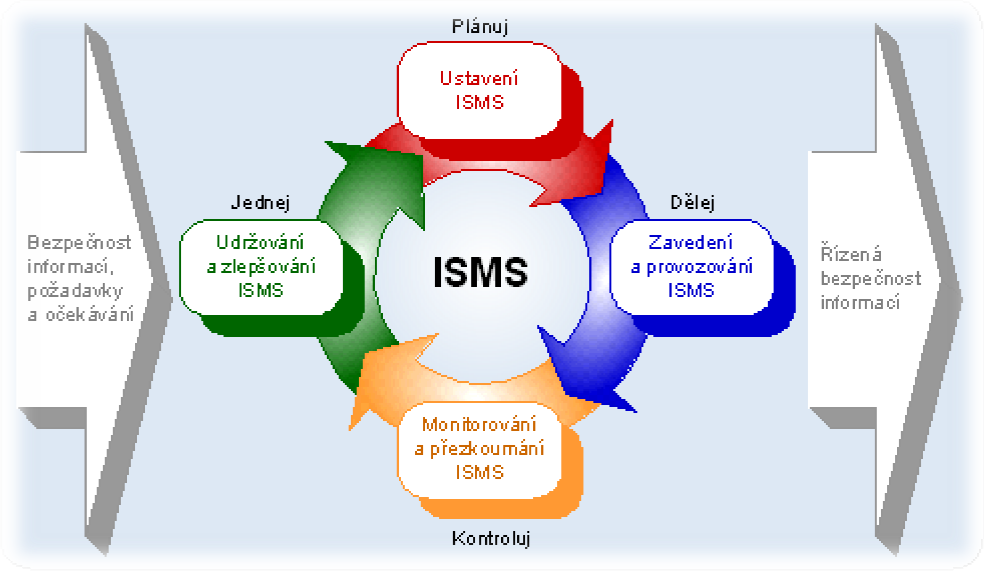


Obr. 1: Používané standardy bezpečnosti informací dle zjištění PSIB 07 a 09

Dalším zajímavým poznatkem vyplývajícím z průzkumu je to, že 31% respondentů využívá více standardů. Nejčastěji jsou spojovány standardy ITIL s ISO/IEC 17799 a interními pravidly a směrnicemi či metodikou COBIT.

3.1 ISMS

ISMS (Information Security Management System) lze přeložit jako systém pro řízení bezpečnosti informací. Jedná se o jednu z částí celkového systému řízení organizace. Podobně jako ostatní systémy řízení QMS, EMS a OHASMS (po řadě systém řízení jakosti, systém řízení vztahu k okolí a řízení bezpečnosti a zdraví při práci) je založen na modelu PDCA. Model PDCA navrhl jeden z předních statistiků 20. století, William Edwards Deming. Zkratka PDCA je složena z anglických slov Plan (plánuj), Do (dělej), Check (kontroluj) a Act (jednej). PDCA cyklus pro systém řízení bezpečnosti ISMS je zobrazen na obrázku Obr. 2.



Obr. 2: Model PDCA pro systém řízení bezpečnosti informací ISMS [5]

Z obrázku je patrno, že zavedení systému ISMS není pouze jednorázovou aktivitou, nýbrž neustálým koloběhem, ve kterém se opakují jednotlivé kroky nezbytné pro správné řízení bezpečnosti informací. Vychází se přitom z normy ISO/IEC 27001, která stanovuje, co musí být v každé fázi provedeno.

Jednou z hlavních výsad ISMS je, že tento systém řízení bezpečnosti může zavést jakákoli organizace, ať už se jedná o státní instituci, neziskovou

organizaci či firmu, a to bez ohledu na její velikost. Může to být jak organizace s deseti zaměstnanci, tak i velká firma. Norma ISO/IEC 27001 toto nerozlišuje. Odlišnosti při zavádění budou pouze v rozsahu potřebných bezpečnostních opatření, kde se dá předpokládat, že velká firma bude mít zavedená opatření rozsáhlejší oproti menším organizacím.

Důvody pro rozhodnutí zavést systém řízení bezpečnosti informací ISMS přitom mohou být různé. Zatímco u některých organizací může být tím hlavním podnětem zvýšení důvěryhodnosti pro případné obchodní partnery či lepší postavení v rámci výběrových řízení (v případě, že je ISMS certifikován), pro jiné, zejména pak pro státní instituce, může být tím hlavním popudem soulad s legislativou, zejména pak se zákonem č. 101/2000 Sb., o ochraně osobních údajů.

3.2 Fáze ustanovení ISMS

Fáze ustanovení je prvním krokem při budování ISMS. V této etapě se vlastně rozhoduje o tom, v jakém rozsahu bude ISMS zaveden. Dále je potřeba provést analýzu rizik, včetně určení hodnoty aktiv a jejich vlastníků. Stěžejním dokumentem, který musí být v této fázi vydán a odsouhlasen vedením, je prohlášení o politice ISMS.

Výhodou je, že na trhu existuje poměrně velké množství firem, které se zaváděním ISMS zabývají. Tyto firmy nabízejí jak poradenství, provádění analýzy rizik, tak i pomoc při zpracovávání dokumentace, audity bezpečnosti informací a další nepřeberné množství služeb.

3.2.1 Definice rozsahu ISMS

Na začátku budování ISMS je potřeba stanovit rozsah a hranice, ve kterých bude ISMS aplikován. V ideálním případě se bude týkat celé společnosti. Existuje však i možnost systém zavést například prozatím pouze ve vybrané pobočce a až po nabytí zkušeností ho rozšířit do ostatních částí. [2]

3.2.2 Politika ISMS

Prohlášení o politice ISMS je jedním ze stěžejních dokumentů spjatých s budováním ISMS. Je potřeba, aby bylo schváleno vedením organizace, které se jeho schválením zavazuje k aktivní podpoře zavádění ISMS současně s tím, že pro budování a chod vyhradí potřebné finance i lidské zdroje. Toto prohlášení nemusí být nikterak obsáhlé. Mělo by být ale věcné. Jedná se zároveň o jeden z dokumentů, který musí být předložen auditorovi při případné certifikaci ISMS.

3.2.3 Analýza rizik

Pro účinné řízení informační bezpečnosti je nutné určit hodnotu našich aktiv a zároveň umět stanovit rizika, která těmto aktivům hrozí. Jenom přesná znalost rizik umožní výběr a nasazení vhodných opatření pro snížení negativních dopadů, které by rizika na aktiva mohla mít. Existuje řada metod a nástrojů pro hodnocení rizik. Samotný postup řízení rizik pak musí být zdokumentován (vyžaduje to přímo norma ISO/IEC 27001).

3.2.4 Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti je dalším důležitým dokumentem souvisejícím s budováním ISMS. Je rovněž nezbytný pro udělení certifikátu dle ISO/IEC 27001. Jedná se o doložení toho, jaká bezpečnostní opatření na potlačení bezpečnostních rizik byla vybrána. Vztahy mezi riziky a bezpečnostními opatřeními jsou často znázorňovány formou matic.

3.3 Fáze zavedení a provozování ISMS

Fáze zavedení a provozování následuje hned po fázi ustanovení ISMS. V této etapě je potřeba navrhnout a implementovat plán zvládání rizik, provést školení zaměstnanců a zejména pak stanovit vhodné ukazatele a způsoby měření a vyhodnocování úrovně zavedených bezpečnostních opatření. Důležité

je také zformulovat Příručku bezpečnosti informací, která by měla popisovat jednotlivá použitá bezpečnostní opatření.

3.3.1 Plán zvládání rizik

Předmětem tohoto dokumentu je popsat všechny činnosti, které jsou potřeba při řízení rizik a rozdělit a určit, kdo bude mít tyto činnosti na starost, kdo za ně bude zodpovídat. Plán rizik je sestaven jednak na základě informací zjištěných v etapě ustanovení (tj. na základě údajů uvedených v prohlášení o aplikovatelnosti a ve zprávě o hodnocení rizik), jednak z poznatků, které vyplývají z neustálého zkoumání a hodnocení úrovně ISMS.

3.3.2 Školení

Velmi důležitou roli v procesu zavádění ISMS hraje školení a prohlubování znalostí vlastních zaměstnanců. Je potřeba poučit je, jakým způsobem se mají chovat, aby neohrozili chod organizace. Všichni by měli být seznámeni s tím, že je zaváděn systém ISMS. Školení mohou být prováděna jak vlastními zaměstnanci, tak i externisty či prostřednictvím e-learningových kurzů.

3.3.3 Navržení metrik a způsobu měření účinnosti ISMS

Měření účinnosti ISMS je z pohledu této práce klíčovou oblastí. Právě v této fázi dochází k navrhování vhodných metrik a indikátorů a stanovení toho, jakým způsobem se bude měřit a vyhodnocovat. Zejména pak také to, kdo bude měření provádět, dokumentovat a reportovat. Samotné měření a vyhodnocování dle navržených ukazatelů a postupů měření pak probíhá v další fázi, tedy ve fázi monitoringu a přezkoumávání ISMS.

A proč vlastně měřit účinnost bezpečnostních opatření? Odpověď je snadná. Jak jinak zjistit, zda jsou opatření účinná či demonstrovat pokračující zlepšení, než právě měřením. Mimoto je měření taktéž nutným požadavkem pro získání certifikátu [8]. Hlavními přínosy měření jsou tedy:

- Získání hmatatelných důkazů o snižování nákladů.
- Omezení bezpečnostních incidentů – na základě měření a porovnávání s předchozími výsledky je možné začlenit efektivnější bezpečnostní opatření na místech, kde je to potřeba.
- Poskytnutí hmatatelných důkazů pro auditory o tom, že ISMS je správně nastaven.

Na tomto místě je vhodné podotknout, že měření nemusí probíhat pouze v rámci zavedeného systému ISMS. Některé organizace sledují určité záznamy, nejčastěji logy ze zařízení, jako jsou firewally či antivirové programy, bez jakéhokoli systematického a cíleného řízení bezpečnosti informací. Tyto informace nám sice mohou poskytnout určitý přehled o pokusech narušit bezpečnost, avšak pokud nejsou sledovány pravidelně a následně dokumentovány a vyhodnocovány, nemají valného významu (bez možnosti porovnání s předchozími výsledky lze jen s obtížemi zjistit, zda se situace zlepšuje či zhoršuje).

Samotný proces měření účinnosti ISMS lze popsat taktéž jako PDCA cyklus.

V etapě Plánuj je potřeba především navrhnout koncept měření. Tím je myšleno, jakým způsobem se bude měřit, kdo bude vyhodnocovat výsledky měření a komu mají být výsledky určeny. Dále je nutné navrhnout vhodné metriky, na jejichž základě bude probíhat měření účinnosti ISMS, periodu sběru dat a způsoby výpočtu a vizualizace. Co je metrika, je vysvětleno podrobně v kapitole 4.

Po fázi Plánuj pak následuje etapa Dělej, ve které je potřeba integrovat systém monitoringu a sběru dat do celkového informačního systému.

Ve fázích Kontroluj a Jednej pak probíhá samotné měření a sběr dat, respektive reportování zjištěných faktů vedení, načež mohou být provedena nápravná opatření a zlepšování. Jedná se tedy o jakousi zpětnou vazbu.

3.4 Fáze monitorování a přezkoumávání ISMS

Další etapou PDCA cyklu je etapa, ve které probíhá monitoring a zkoumání ISMS. V této fázi se provádí audity bezpečnosti, a to jak interní, tak i externí. Taktéž je nutné provést kontroly, a to zejména zjistit přínosy použitých bezpečnostních opatření a provést měření na základě stanovených postupů z etapy zavedení a provozování ISMS. Alespoň jedenkrát v roce by pak mělo proběhnout přezkoumání ISMS ze strany vedení organizace.

3.4.1 Audit bezpečnosti

Audit bezpečnosti je důležitým nástrojem pro ověření správného chodu ISMS. Existuje několik typů auditů s trochu odlišným zaměřením. Aby byly výsledky auditu objektivní, je nutné, aby audit prováděly nezaujaté a nestranné osoby. Z pohledu, kým a pro jaké účely je audit prováděn, lze audity rozdělit na audity první, druhou a třetí stranou.

Audity první stranou jsou prováděny za účelem ověření, zda je systém správně nastaven, zda správně funguje. Může být prováděn specializovanou firmou. Do této kategorie by bylo možné zahrnout i předcertifikační audity, při kterých si organizace toužící po certifikátu nechá s předstihem zjistit, zda je ISMS v takovém stavu, aby mohl být certifikován. Někdy bývají audity doprovázeny ověřováním bezpečnosti a slabin systému prostřednictvím penetračních testů [9].

Audity druhou stranou mohou být prováděny ze strany odběratele. Odběratel na základě smluvních podmínek může požadovat provedení auditu u obchodních partnerů či dodavatelů.

Audit třetí stranou neboli certifikační audit probíhá tehdy, pokud se organizace rozhodne, že chce mít systém ISMS certifikován. Provádějí ho certifikační orgány, které musejí mít k této činnosti akreditaci. Při certifikaci se sleduje hlavně to, jestli je řádně vedena potřebná dokumentace, jsou nastaveny

metriky a provádí se měření. Tedy to, zda je ISMS zaveden v souladu s normou ISO/IEC 27001. Jen pro zajímavost - dle posledních údajů Mezinárodního registru ISMS certifikací (březen 2010) je v České republice 85 organizací s certifikovaným systémem ISMS [10].

3.5 Fáze udržování a zlepšování ISMS

V této etapě by mělo docházet ke zlepšování ISMS. Případné nedostatky a problémy, které byly zjištěny během auditů, by měly být odstraňovány.

3.6 Normy ISO/IEC 27xxx pro řízení bezpečnosti informací

Existuje celá řada norem, které definují pravidla pro systém ISMS. [12]

ISO/IEC 27000:2009 definuje základní termíny související se systémem ISMS a popisuje ISMS systém, včetně modelu PDCA. Mimoto tato norma zobrazuje vztahy mezi jednotlivými standardy souvisejícími s ISMS.

ISO/IEC 27001:2005 vychází z britské normy BS 7799-2. Tento standard definuje požadavky na ISMS. Jedná se vlastně o jakýsi sumář všech požadavků a podmínek, jejichž splnění je potřebné pro správný chod ISMS.

ISO/IEC 27002:2005 obsahuje postupy pro řízení bezpečnosti informací. Tato norma má stejnou strukturu jako norma ISO/IEC 27001:2005, ale na rozdíl od ní se nejedná o nařízení, ale doporučení.

ISO/IEC 27003:2010 vyšla v únoru 2010. Jedná se o směrnici, která má pomoci při zavádění systému ISMS. Zaměřuje se na kritické aspekty potřebné pro úspěšnou implementaci ISMS dle normy ISO/IEC 27001:2005.

ISO/IEC 27004:2009 je taktéž nová norma, která vyšla v platnost teprve v prosinci roku 2009. Tato norma zahrnuje oblast měření a bezpečnostních metrik. Klíčovými body této normy jsou:

- celkový pohled na měření bezpečnosti informací
- zodpovědnost vedení organizace

- metriky a vývoj měření
- operace měření
- analýza dat a reporting výsledků měření
- zlepšování ISMS na základě výsledků měření

Krom toho tato norma obsahuje i šablonu pro zaznamenávání metrik a konkrétní metriky, které mohou být použity v provozu.

ISO/IEC 27005:2008 je nástupcem standardu ISO/IEC TR 13335-3. Jedná se o směrnici pro řízení rizik informační bezpečnosti.

ISO/IEC 27006:2007 stanovuje pravidla, jakým způsobem mají postupovat certifikační orgány při certifikaci systému ISMS.

Existují ještě další normy, které se přímo specializují na určitá odvětví, jako např. norma ISO/IEC 27799:2008, která vychází z normy ISO/IEC 27002. Tato norma specifikuje sadu detailních ovládacích prvků pro zajištění informační bezpečnosti přímo ve zdravotnických zařízeních.

Kromě těchto norem, které již byly vydány, je v současné době ve fázi vývoje a přípravy k vydání více než deset dalších dokumentů. Ještě v roce 2010 by měla vyjít směrnice pro auditory ISMS s označením ISO/IEC 27007.

3.7 Metodiky pro řízení IT služeb

Na začátku kapitoly 3 bylo uvedeno, že některé organizace využívají více bezpečnostních standardů. Nejčastěji pak kombinace vlastních interních směrnic a norem, ze kterých vychází systém řízení ISMS. Lze využít i metodiky COBIT a ITIL.

3.7.1 COBIT

COBIT je univerzální metodika, která byla vytvořena americkou organizací ISACA v roce 1996. Jedná se o soubor návodů, ukazatelů a nejlepších zkušeností z praxe, které mají sloužit zejména manažerům, auditorům

a správcům IT. Nejnovější verze příručky COBIT, která byla vydána v roce 2007, nese označení COBIT 4.1. [13]

Metodika COBIT dělí IT aktivity do čtyř domén. Každá doména pak zahrnuje jednotlivé procesy, kterých je dohromady 34. Těmito doménami jsou:

- PLAN AND ORGANISE – PO (Plánování a organizace)
- ACQUIRE AND IMPLEMENT – AI (Akvizice a implementace)
- DELIVER AND SUPPORT – DS (Dodávka a podpora)
- MONITOR AND EVALUATE – ME (Měření a vyhodnocování)

Procesy domény PO pokrývají, jak již samotný název napovídá, oblast řízení a plánování. Činnosti spadající do této domény jsou např. řízení projektů, lidských zdrojů, správa investic do IT nebo definování strategického plánu IT.

Doména AI pak zahrnuje činnosti spojené s nákupem a vývojem technologií, jako např. pořízení a údržbu SW, pořízení a údržbu technologické infrastruktury.

Doména DS zahrnuje procesy související s provozem IT služeb. Příkladem činností spadajících do domény DS mohou být např. řízení provozu, zajištění bezpečnosti systému či řízení výkonnosti a kapacity.

Poslední doménou je doména ME. Do této domény patří činnosti spojené s měřením a průběžným hodnocením výkonnosti IT. Tyto činnosti by měly poskytnout zpětnou vazbu vedení.

3.7.2 ITIL

ITIL je zkratka Information Technology Infrastructure Library. Jedná se o komplexní dokumentaci, která zahrnuje nejlepší praktiky pro řízení služeb IT. Původně tvořilo příručku ITIL 46 svazků. Později byl tento počet redukován. Nejnovější verze ITIL Version 3, která byla vydaná v roce 2007, zahrnuje tyto dokumenty:

- Service Strategy (Strategie služeb)
- Service Design (Návrh služeb)
- Service Transition (Implementace služeb)
- Service Operation (Provoz služeb)
- Continual Service Improvement (Neustálé zlepšování služeb) [14]

Metodiky COBIT i ITIL představují komplexní řešení pro řízení služeb spojených s IT. Do jisté míry se zabývají též měřením účinnosti a návrhem ukazatelů pro zjišťování aktuální úrovně IT, včetně bezpečnosti. Nicméně bezpečnosti informací se nevěnují tak detailně jako systém řízení bezpečnosti informací ISMS.

4 Metriky

V předchozí kapitole bylo uvedeno, že ke zjištění efektivity bezpečnostních opatření a účinnosti řízení bezpečnosti informací je potřeba navrhnout vhodné metriky, provádět pravidelná měření a vše řádně zaznamenávat a dokumentovat. Nyní bude vysvětleno, co si lze představit pod pojmem metrika, k čemu metriky slouží, jaké vlastnosti by měla mít dobrá metrika a zejména, jak lze metriky kategorizovat.

4.1 Pojem metrika

Pavel Učeň v knize Metriky v informatice [15] definuje metriku jako přesně vymezený finanční či nefinanční ukazatel nebo hodnotící kritérium, které jsou používány k hodnocení úrovně efektivnosti konkrétní oblasti řízení podnikového výkonu a jeho efektivní podpory prostředky IS/IT. Skupinu metrik sdružených za určitým cílem pak nazývá portfoliem metrik.

4.2 Vlastnosti správné metriky

Existuje velké množství již navržených metrik pro hodnocení úrovně bezpečnosti informací. Samozřejmě je možné navrhnout si i metriky vlastní, které budou měřit přesně to, co měřit potřebujeme. Jsou však jisté zásady - pokyny pro navrhování metrik, které na základě praktických zkušeností uvádějí odborníci znalí dané problematiky. Andrew Jaquith v publikaci Security Metrics [16] uvádí pět základních požadavků, kterým by měla metrika vyhovovat. Podle těchto pravidel by dobrá metrika měla být taková, aby:

- měření bylo objektivní
- získání vstupních dat by nemělo být nákladné
- měření mohlo být prováděno opakovaně
- výsledek měření mohl být vyjádřen jako číslo či procento
- výsledek měření byl vztažen ke konkrétní veličině

4.2.1 Objektivně měřitelná metrika

Tuto podmínku metrika splňuje, pokud výsledky měření provedeného rozličnými osobami jsou vždy shodné. Měření tedy nemohou ovlivnit pocity osob, které měření provádějí. Nejvhodnějším řešením, jak tuto podmínku splnit, je měření zautomatizovat. Existuje řada nástrojů pro automatické měření, vyhodnocování a vizualizaci výsledků. Ne vše však lze měřit automaticky.

4.2.2 Levná metrika

Při navrhování ukazatelů je důležité stanovit, jak často má měření probíhat (s jakou frekvencí). Platí přitom, že ukazatele, které je třeba sledovat častěji, by neměly být náročné na výpočty a na čas strávený sběrem dat. Měly by být tedy levné – náklady na získání takovýchto dat by měly být co možná nejnižší.

	Frekvence měření	
	Vysoká	**Nízká**
Vysoký význam	**Krizové řízení** • Metriky hrozeb • Detekce průniků do systému	**Strategické plánování** • Rozpočty • Alokace zdrojů • Soulad s požadavky • Řízení aktiv
Nízký význam	**Operativní řízení** • Ochrana proti škodlivým programům • Řízení sítí • Řízení bezpečnosti • Udržování/správa	**Programové plánování** • Řízení zdrojů • Ukazatelé životního cyklu vývoje aplikací • Analýza auditních a logovacích záznamů
	Málo času, málo parametrů	Mnoho času, hodně parametrů

Tab. 2: Schéma ukazatelů dle významu a frekvence měření [16], překlad

4.2.3 Opakovatelná metrika

Metrika by měla být navržena tak, aby měření mohlo probíhat opakovaně. Je potřeba předem stanovit periodu měření. Měřit můžeme v libovolných rozestupech, ať už denně, týdně, čtvrtletně či v jiných časových intervalech.

4.2.4 Výsledek měření vyjádřen konkrétním číslem

Výsledek správné metriky by mělo vyjadřovat konkrétní číslo. Mělo by to být tedy kardinální číslo, ne jen nějaký popis či vyjádření stavu, jako kupříkladu vysoký, středně vysoký, nízký. Těmito popisy však může být konkrétní hodnota doprovázena. Pro snazší pochopení a lepší představu je proto mnohdy vhodné konkrétní hodnotu takovými popisy doplnit.

4.2.5 Výsledek měření vztažen ke konkrétní veličině

Pokud to okolnosti vyžadují, je potřeba výsledek měření vztáhnout ke konkrétní veličině (např. k jednotce času). Když bychom zaznamenávali počet pokusů o průnik do podnikové sítě, samotné číslo 250 by nám toho moc neřeklo. Když ale bude doplněno tím, že se tomu událo například během jedné hodiny, lze si udělat konkrétnější představu.

4.3 Členění metrik

Existuje mnoho způsobů, jak kategorizovat metriky. Různí autoři používají odlišná dělení.

Z obecného hlediska lze metriky rozdělit na tvrdé a měkké. Dále pak například z pohledu úrovně řízení na metriky operativní, taktické a strategické. Lze také metriky rozčlenit dle opakovatelnosti použití na metriky kontinuální a diskrétní či z pohledu hodnocení efektivnosti inovace IS/IT na metriky interní a externí. Tímto způsobem jsou metriky děleny v publikaci Metriky v informatice [15]. Toto členění je však obecněji zaměřené, neboť ho lze

vztáhnout k širší oblasti informatiky (tedy ne pouze k oblasti bezpečnosti informací).

Máme-li se zabývat přímo oblastí bezpečnosti informací, je vhodné si představit, jak metriky dělí dva přední světové instituty pro tvorbu standardů. Tím prvním myslím americký National Institute of Standards and Technology (Národní institut standardů a technologií) a tím druhým britský BSI Group, který je jedním z členů ISO (International Organization for Standardization).

Metriky a měření jsou pak součástí i metodik COBIT a ITIL, které byly ve stručnosti popsány v bodě 3.7.

4.3.1 Tvrdé a měkké metriky

Tvrdá metrika je objektivně měřitelný ukazatel, který by měl být lehce měřitelný a levný. To znamená k dispozici bez dodatečných nákladů. Výsledkem tvrdé metriky by měla být konkrétní hodnota, ve většině případů převeditelná na finanční vyjádření. Mimo ukazatelů existují také indikátory, což jsou metriky, které mají stanoveny meze, které představují žádoucí stav. Jakákoli odchylka od ideální hodnoty směrem k horšímu znamená problém (nežádoucí stav).

Měkké metriky jsou naopak takové ukazatele, které nejsou objektivně měřitelné. Jedná se o subjektivní vyjádření určitého stavu, kupříkladu úrovně spokojenosti zákazníka či pověsti podniku (zlepšení jeho dobrého jména).

4.3.2 Kontinuální a diskrétní metriky

Pokud měření probíhá opakovaně v předem stanovené periodě, jedná se o metriky kontinuální. Oproti tomu diskrétní metriky jsou aplikovány sice opakovaně, ale pouze v časově omezeném období. Kupříkladu během inovace zařízení, kdy srovnáváme aktuální stav se stavem před inovací.

4.3.3 Metriky z pohledu úrovní řízení

Z pohledu úrovní řízení lze metriky rozdělit na operativní, strategické a taktické. Strategické metriky představují především kontinuální tvrdé metriky (v nejlepším případě indikátory). Výsledky těchto metrik jsou určeny především pro vedení organizace. Operativní metriky pak mohou být jak tvrdé, tak i měkké metriky, které by měly poskytovat informace o provozu. Metriky taktické úrovně pak představují zejména výsledkové metriky. To jest takové ukazatele, které jsou zaměřeny na dosahování cílů (porovnání skutečného stavu oproti našim plánům).

4.3.4 Interní, externí metriky

Z pohledu hodnocení efektivnosti inovace IS/IT lze metriky rozčlenit na metriky interní a externí. Interní metriky jsou určeny především k hodnocení efektivnosti vložených prostředků a úrovně poskytovaných služeb. Tyto metriky navrhuje přímo uživatelský podnik. Externí metriky pak jsou navrhovány nejen uživatelským podnikem, ale i subjektem, který se podílí na inovaci IS/IT. Externí metriky lze tedy jinak označit jako metriky dodavatelské.

4.3.5 Metriky podle BSI Group

BSI Group byla založena v Londýně roku 1901 pod jménem Engineering Standards Committee. Jedná se o nejstarší organizaci zabývající se vydáváním průmyslových standardů a souvisejícími službami, jako certifikacemi systémů řízení. V současné době má společnost BSI, která je mimochodem i členem organizace ISO, na kontě více než 27000 již vydaných standardů a ve stádiu vývoje se jich nachází kolem 6000. Nejpopulárnějšími standardy vydanými touto společností jsou celosvětově rozšířené mezinárodní normy pro řízení jakosti. Konkrétně pak norma ISO 9001 – Požadavky na systémy řízení jakosti, kterou používá více než 670000 organizací z celého světa [18]. BSI je mimo

jiné autorem norem z rodiny 27000, na kterých je postaven systém ISMS. Již bylo napsáno, že součástí systému ISMS je měření a vyhodnocování jeho účinnosti, stejně tak jako návrh metrik, které tedy BSI kategorizuje na metriky:

- manažerské
- obchodní
- operační
- technické

Manažerské metriky jsou, jak již samotný název napovídá, určeny zejména pro potřeby vedení. Příkladem oblastí zkoumaných manažerskými metrikami mohou být kupříkladu bezpečnostní politika či obchodní cíle. Do metrik obchodních pak lze zařadit metriky, které souvisejí zejména s analýzou rizik. Operační metriky souvisejí s procesy operačního charakteru. Používají se tedy kupříkladu k hodnocení zálohování dat. Poslední skupinou jsou metriky technické. Technickými metrikami lze chápat takové ukazatele, které slouží k hodnocení parametrů konkrétních systémů. Technické metriky mohou zkoumat například rozsah ochrany proti spamu nebo počet pokusů o průnik do systému. [17]

4.3.6 Metriky podle NIST

Národní institut pro normy a technologie byl založen v roce 1901 s cílem podporovat průmyslové inovace prostřednictvím norem, technologií a aplikovaného využití vědy. V současné době NIST zaměstnává kolem 2900 vědců, inženýrů, techniků a administrativních pracovníků [19]. Jak již bylo uvedeno, NIST se zabývá převážně vývojem směrnic a norem, a to samozřejmě i pro oblast bezpečnosti informací. Stěžejním dokumentem pro oblast měření úrovně bezpečnostních opatření a metrik pro oblast bezpečnosti informací je směrnice označovaná jako NIST SP 800-55 Revision 1, která byla publikována v roce 2008 [20]. Normy NIST pro oblast řízení bezpečnosti informací jsou často využívány jako alternativa k standardům organizace BSI. Nepopiratelnou

výhodou norem a směrnic NISTu je jejich nulová cena a dostupnost (normy dostupné na internetu volně ke stažení). Tyto dokumenty jsou vydávány s cílem podporovat ekonomický růst a vývoj nových technologií. Vláda USA do tohoto institutu vkládá každoročně nemalé finanční prostředky. Oproti tomu normy vydávané organizací BSI zdarma nejsou. Směrnice SP 800-55 v sobě zahrnuje nejen popis metrik, jejich rozčlenění, návod pro jejich vývoj a implementaci, ale i vzorovou šablonu a příklad již navržených a v praxi odzkoušených ukazatelů.

NIST rozděluje metriky v souvislosti s vyzrálostí bezpečnostního programu společnosti na metriky:

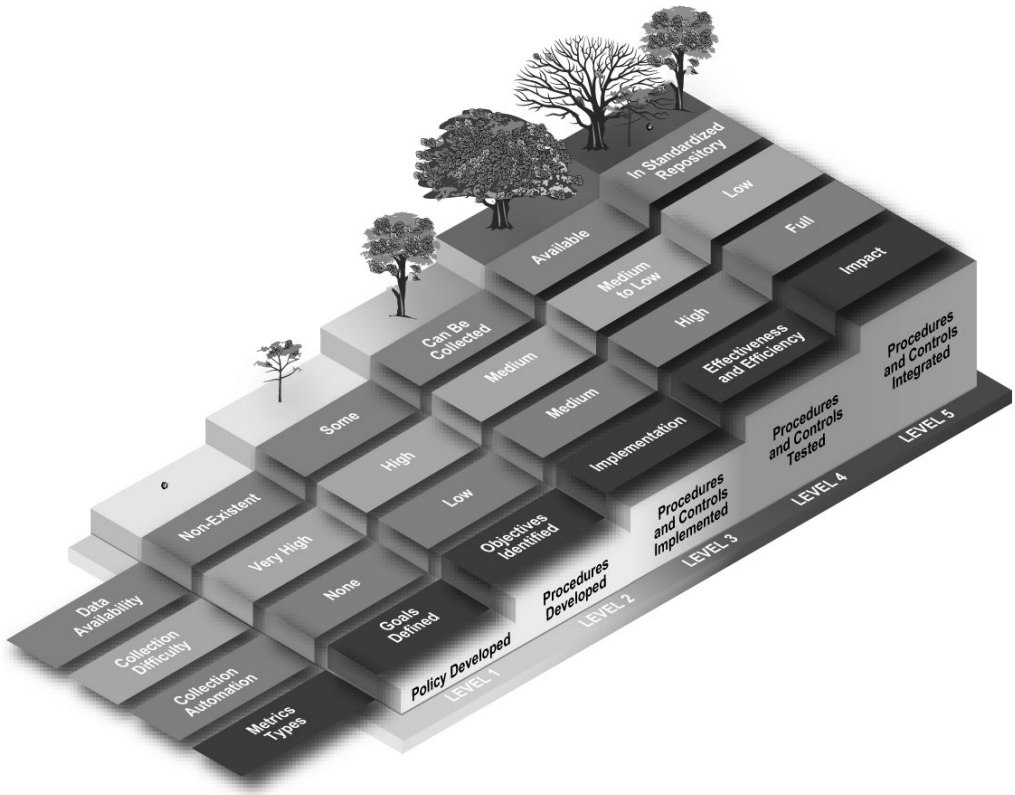
- implementační (implementation measures)
- výkonnostní (effectiveness/efficiency measures)
- dopadové (impact measures)

Stupně zralosti bezpečnostního programu jsou definovány ve směrnici, která nese označení 800-26 [21].

- Stupeň 1: kontrolní cíl je doložený v bezpečnostní politice
- Stupeň 2: bezpečnostní kontroly jsou doloženy jako procesy
- Stupeň 3: procesy jsou zrealizovány
- Stupeň 4: procesy a bezpečnostní kontroly jsou testovány a revidovány
- Stupeň 5: procesy a bezpečnostní ovládací prvky jsou plně integrovány do celkového bezpečnostního programu

Samotný proces vývoje metrik ve vztahu k vyzrálosti celkového bezpečnostního programu organizace zachycuje obrázek Obr. 3. Z obrázku je patrno, že s tím, jak bezpečnostní program dospívá, se jeho politika stává detailnější a snáze dokumentovatelnou, procesy se stávají opakovatelnými a standardizovanými a zároveň s tím můžeme získávat stále více dat, na jejichž základě lze provádět měření. Je patrno, že před budováním systému řízení

bezpečnosti je potřeba nejprve definovat rozsah a cíle, kterých chceme dosáhnout. Na začátku, to jest při samotném zavádění systému řízení bezpečnosti informací, se využívají implementační metriky. S postupným zdokonalováním bezpečnostního programu se přechází na metriky výkonnostní a nakonec na metriky dopadové.



Obr. 3: Metriky v souvislosti se zralostí bezpečnostního programu [22]

Implementační metriky se využívají k vyjádření pokroků během zavádění bezpečnostního programu. Příkladem implementačních metrik může být procento zaměstnanců odpovědných za informační bezpečnost, kteří absolvovali školení nebo procento zaměstnanců s umožněným přístupem do informačního systému až poté, co potvrdili, že jsou srozuměni a souhlasí s bezpečnostními pravidly organizace nebo procento serverů se standardní konfigurací. V prvním a druhém stupni zralosti bezpečnostního programu se očekává, že výsledky těchto metrik nebudou dosahovat 100%. Jakmile dosáhne

organizace třetího stupně, výsledky metrik by měly dosáhnout a zůstat na 100%. Po dosažení této úrovně by se měla organizace oprostit od metrik implementačních a zaměřit se na metriky výkonnostní a později dopadové.

Výkonnostní metriky se využívají k sledování toho, zda jsou bezpečnostní opatření implementována správně a dosahují požadovaných účinků. Výkonnostní metrikou může být například procento vzdálených přístupových bodů použitých k získání neautorizovaného přístupu nebo procento uživatelů s přístupem ke sdíleným účtům.

Dopadové metriky se využívají k vyjádření toho, jaký vliv mají bezpečnostní opatření na plnění obchodních plánů organizace. Příkladem dopadové metriky může být podíl financí vynaložených na bezpečnost informací vůči celkovým financím uvolněným na správu a provoz IS/IT.

Dokument NIST 800-55 obsahuje také návod, jak by měla organizace postupovat při návrhu vhodných metrik, včetně šablony pro metriky, která je zobrazena jako tabulka Tab. 3.

Pole	Data
ID metriky	jednoznačný identifikátor metriky
Cíl	strategický a/nebo bezpečnostně-informační cíl
Metrika	numerické sdělení – procento, číslo, frekvence
Typ metriky	implementační/ výkonnostní/ dopadová
Vzorec pro výpočet	vzorec pro výpočet metriky
Prahová hodnota	vyhovující hodnota, se kterou se porovnává výsledek metriky
Evidence implementace	evidence implementace se používá k výpočtu metriky, potvrzení, že měření bylo provedeno a k identifikaci pravděpodobných příčin neuspokojivých výsledků
Frekvence	• frekvence sběru a analýzy dat (např. čtvrtletně) • frekvence reportingu výsledků

Zodpovědné strany	• vlastník dat – např. vedení • sběratel dat – osoba odpovědná za měření • zákazník – identifikuje část organizace či jednotlivce, pro které budou data určena
Zdroj dat	Zdroj dat, ze kterých je metrika počítána – např. zaměstnanci (počet proškolených zaměstnanců), databáze, sledovací nástroje (antivirové programy, firewall) apod.
Formát hlášení – vizualizace výsledků měření	Oznámení, jakým způsobem bude prezentován výsledek. Může to být sloupcový diagram, kruhový diagram, spojnicový diagram či jiný způsob vyjádření.

Tab. 3: Náležitosti šablony pro metriky dle doporučení NIST 800-55 [20], úprava autora

4.3.7 Metriky v rámci metodik ITIL a COBIT

V rámci metodik ITIL a COBIT mají metriky taktéž specifické označení a umístění.

V dokumentu COBIT 4.1 jsou metriky děleny do dvou skupin. A to na:

- Outcome measures (výsledkové metriky) – dříve označovány jako KGI
- Performance indicators (ukazatele výkonu) – dříve označovány jako KPI

Toto dělení je úzce spjato s cíly organizace, které COBIT dělí na cíle IT, cíle procesní a cíle aktivit. Pro každé cíle existují odpovídající metriky. Výsledkové metriky slouží k hodnocení toho, zda bylo dosaženo plánovaných cílů. Ukazatele výkonu se používají v průběhu procesu uskutečňování cílů k určení pravděpodobnosti, zda těchto cílů bude opravdu dosaženo. [23]

Metodika ITIL se orientuje na poskytování služeb z oblasti IT. Z toho také vychází při návrhu metrik, které mají sloužit především k hodnocení výkonu, spolehlivosti a dostupnosti těchto služeb. Ukazatele pak tato metodika pojmenovává jako KPI (Key Performance Indicators). [24]

4.4 Metriky v oblasti outsourcingu

Zajistit správu a údržbu IT lze dvěma způsoby. Buďto pomocí vlastních zaměstnanců, nebo pomocí jiné firmy prostřednictvím outsourcingu. Outsourcing lze tedy vysvětlit jako vymezení určité činnosti, kterou pak za nás, na základě smlouvy, provádí externí firma. V reálném světě lze outsourcovat téměř vše od dopravy po úklidové služby. I v oblasti IT existuje mnoho firem, které se přímo outsourcingem živí. Nabízejí různé služby od školení zaměstnanců přes správu sítě, zálohování dat a pronájem techniky až po audity bezpečnosti. Je jen na samotné organizaci, aby se rozhodla, které činnosti svěří někomu jinému. A proč vlastně outsourcovat? Jako hlavní důvod se udává finanční úspora. Zejména u velmi malých firem s pár počítači se s velkou pravděpodobností nevyplatí zaměstnávat na plný úvazek nějakého správce sítě. Zároveň se předpokládá, že poskytnuté služby budou na určité úrovni. Úroveň je specifikována ve smlouvě o úrovni poskytovaných služeb SLA (Service Level Agreement).

Samotný přechod do režimu outsourcingu není nikterak jednoduchou záležitostí. Tím hlavním, co je potřeba udělat, je provést audit současného stavu, rozhodnout se, jaké činnosti mají být svěřeny do rukou někoho jiného, zpracovat plán a definovat SLA, včetně vhodných metrik a jejich prahových hodnot. Metriky přitom mohou být jak tvrdé, tak i měkké. [25]

- Tvrdé metriky – např. mezní doba opravy/výměny nefunkčního zařízení (např. oprava PC).
- Měkké metriky – např. hodnocení účastníka školení.

Zajišťování služeb pomocí outsourcingu s sebou však nese i určitá rizika, která většinou vyplývají z nevýhodné smlouvy či nejednoznačných podmínek poskytování služeb. Velkým rizikem je také to, že vlastně umožňujeme přístup k našim datům nějaké cizí osobě, která by je mohla vědomě zneužít.

4.5 Ukázka konkrétních metrik

Existuje celá řada již vytvořených metrik, které lze použít pro hodnocení systému řízení bezpečnosti informací. Nemusí se však nutně jednat o metriky obsažené v normě ISO/IEC 27004. Inspiraci lze hledat i v různých článcích a standardech či směrnicích. V tabulce Tab. 4 je uvedeno několik příkladů konkrétních metrik převzatých z různých zdrojů.

Metrika	Frekvence reportingu
Celkový čas strávený řešením bezpečnostních incidentů	čtvrtletně
Procento porušení SLA IT	čtvrtletně
Celkový počet bezpečnostních incidentů a událostí	měsíčně
Procento úspěšného obnovení dat ze záloh	čtvrtletně
Procento proškolených zaměstnanců	čtvrtletně
Podíl financí vynaložených na bezpečnost informací vůči celkovým financím uvolněným na správu IS/IT	ročně

Tab. 4: Příklad konkrétních metrik [2], [8]

4.6 Nástroje pro automatický sběr dat

Sběr potřebných dat pro metriky je možno provádět buďto ručně anebo prostřednictvím speciálních nástrojů. Zejména v případech, kdy je potřebné provádět sběr dat s velkou frekvencí, je výhodné použít tyto nástroje pro automatizovaný sběr. Ukázkovým příkladem jsou produkty SIEM (Security Incident and Event Manager), které kontrolují chování sítě a poskytují přesné informace o bezpečnostních hrozbách (identitu útočníka, závažnost útoku atd.). [28]

5 Průzkum stavu bezpečnosti informací

5.1 Cíl průzkumu, počáteční předpoklady

Cílem průzkumu je zjistit, jakým způsobem se v praxi řeší informační bezpečnost a ověřit předpoklady, které byly uváděny v prostudované literatuře. Zejména pak v publikaci Řízení bezpečnosti informací [2]. Hlavním předpokladem je, že v dnešní době by měla každá organizace (nebo alespoň ty větší) nějakým způsobem řídit bezpečnost informací. Měl by být zaveden určitý systém řízení, který by mohl vycházet jednak z oficiálních standardů, jednak z interních směrnic organizace. Dalším důležitým aspektem řízení bezpečnosti informací je zavedení a použití metrik. Lze předpokládat, že nějaké základní metriky by, v souvislosti s řízením bezpečnosti informací, měly mít zavedeny všechny organizace.

Hlavním cílem průzkumu je tedy ověřit, zda je ve všech organizacích bezpečnost informací systematicky řízena, jestli je k tomu využíváno nějakých známých či vlastních standardů a směrnic, do jaké míry jsou zaváděny metriky jako nástroj pro hodnocení stávající úrovně a účinnosti zavedených bezpečnostních opatření a kdo vlastně za bezpečnost informací v organizacích zodpovídá.

5.2 Metodika tvorby dotazníku

Dotazník vznikal na základě prostudované literatury. Uvažovány byly i věcné připomínky vedoucího práce – pana inženýra Ladislava Beránka. Bylo vytipováno deset oblastí týkajících se bezpečnosti informací, které by měly poskytnout základní přehled o tom, jak se v praxi řeší informační bezpečnost. Jednotlivé okruhy jsou zaměřeny na:

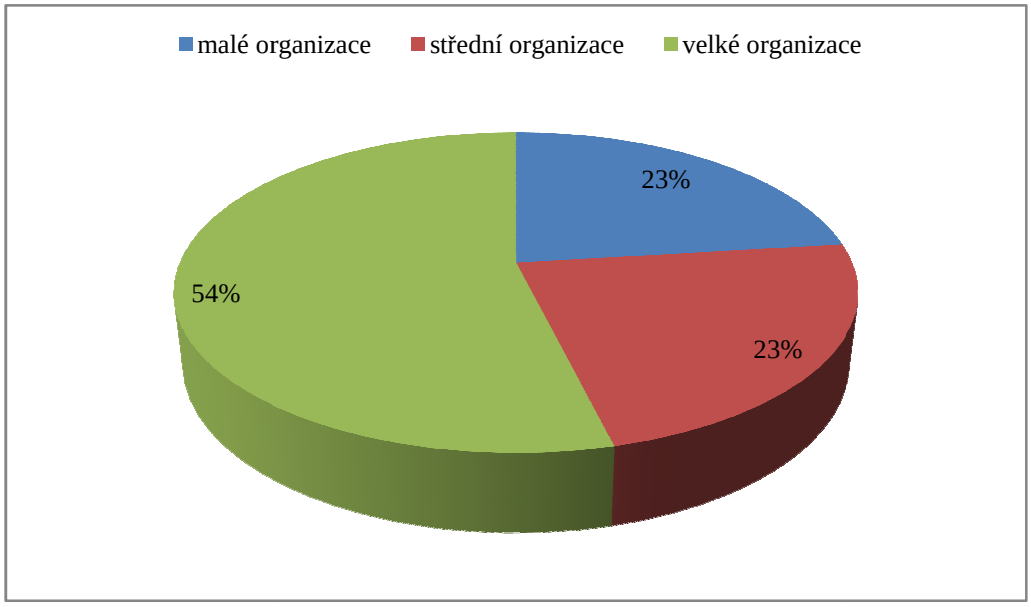
- organizaci bezpečnosti
- outsourcing

- standardy využívané pro řízení bezpečnosti
- metriky a nástroje využívané k řešení bezpečnosti
- bezpečnostní audity
- penetrační testování
- fyzické zabezpečení – omezování přístupu
- školení zaměstnanců
- analýzu rizik
- sledování činnosti zaměstnanců v pracovní době

Osloveno bylo více než dvacet respondentů – zástupců organizací. S vyplněním dotazníku nakonec souhlasilo třináct z nich. Ne každý byl však ochoten osobně se sejít a nad dotazníkem podiskutovat. Bylo proto nutné upravit otázky tak, aby bylo vyplnění dotazníku možné i na dálku (myšleno prostřednictvím emailové komunikace) a z časových důvodů zabralo samotné vyplnění co možná nejkratší dobu. Otázky proto byly formulovány tak, aby byly co možná nejsrozumitelnější. U většiny otázek je tedy možné vybrat jednu či více vyhovujících možností. Některé otázky pak byly řešeny doplněním chybějícího údaje – zejména profesní detaily (funkce dotazovaného respondenta) a velikost organizace. Z celkového počtu třinácti respondentů se k osobní konzultaci uvolilo šest z nich. V těchto případech byl dotazník vyplňován na základě odpovědí samotným autorem dotazníku a případné dodatečné informace nad rámec nabízených odpovědí či věcné připomínky a dodatky byly zaznamenány. Co se týče samotného vyhodnocení jednotlivých otázek, snahou je výsledky zpřehlednit a co možná nejsrozumitelněji znázornit. Nejvhodnějším řešením, které se nabízí, je znázornění výsledků ve formě grafů s následným vysvětlením a vyvozením závěrů.

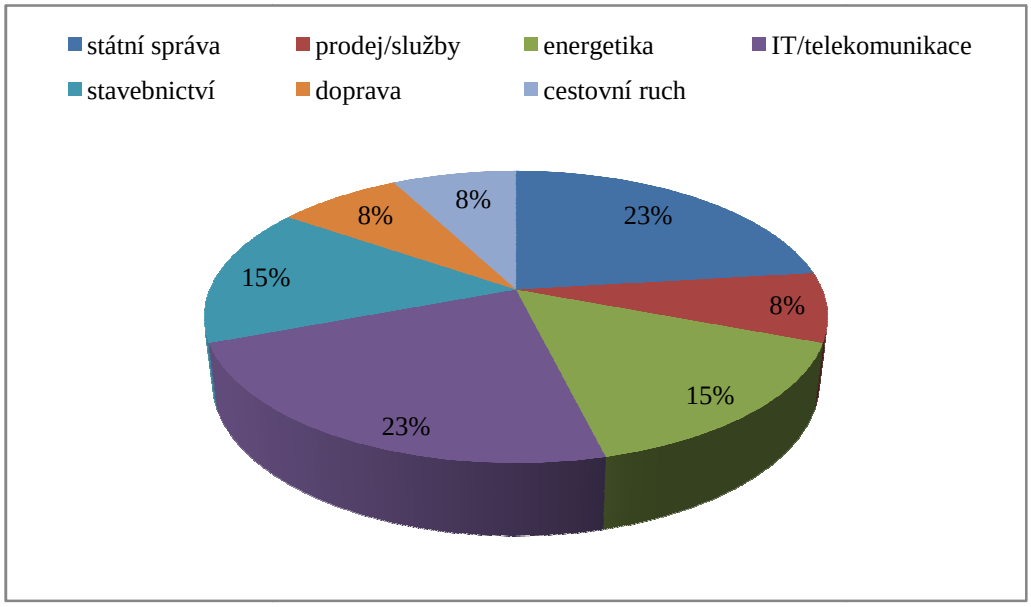
Pro přesnější přehled byly vytipovány organizace dle různých velikostí a oblastí působnosti (odvětví). Dle velikosti lze organizace rozdělit na malé (do 50 zaměstnanců), střední (50 – 250 zaměstnanců) a velké organizace (nad 250

zaměstnanců). Dotazované organizace pak působí v šesti různých odvětvích. Podíl dotazovaných organizací dle velikosti je zobrazen na obrázku Obr. 4.



Obr. 4: Podíl dotazovaných organizací dle jejich velikosti

Podíl zastoupení organizací v jednotlivých odvětvích je znázorněn na obrázku Obr. 5.



Obr. 5: Odvětvové zastoupení dotazovaných organizací

Zastoupení funkcí dotazovaných pak je následující:

- šéf IT (1×)
- správce IT (7×)
- syn majitele organizace – příležitostný správce sítě (1×)
- manažer informační bezpečnosti (2×)
- specialista bezpečnosti, interní auditor (1×)
- obchodní ředitel (1×)

5.3 Organizace bezpečnosti

Rozdělení zodpovědnosti za bezpečnost informací se může v jednotlivých organizacích lišit. Jak je zodpovědnost rozdělena, se většinou odvíjí od velikosti organizace nebo její specializace. Zejména pak záleží na tom, v jakém rozsahu a objemu využívají informační a komunikační technologie.

Zatímco v některých menších organizacích lze očekávat, že bezpečnost informací bude mít na starost buďto jedna osoba – vlastní zaměstnanec organizace nebo někdo z vnějšku (outsourcing), ve větších firmách s větším množstvím výpočetní techniky může mít bezpečnost na starost více pověřených pracovníků, kde každý zodpovídá pouze za svůj úsek.

Cílem této oblasti je zjistit, kdo v organizacích zodpovídá za informační bezpečnost a zda se v organizaci nachází specializované oddělení bezpečnosti informací. Respondenti si mohli zvolit z několika nabízených možností tu, která je vyhovující. V případě, že se mezi nabízenými možnostmi žádná vhodná neobjevila, měli zvolit jinou možnost a doplnit její znění.

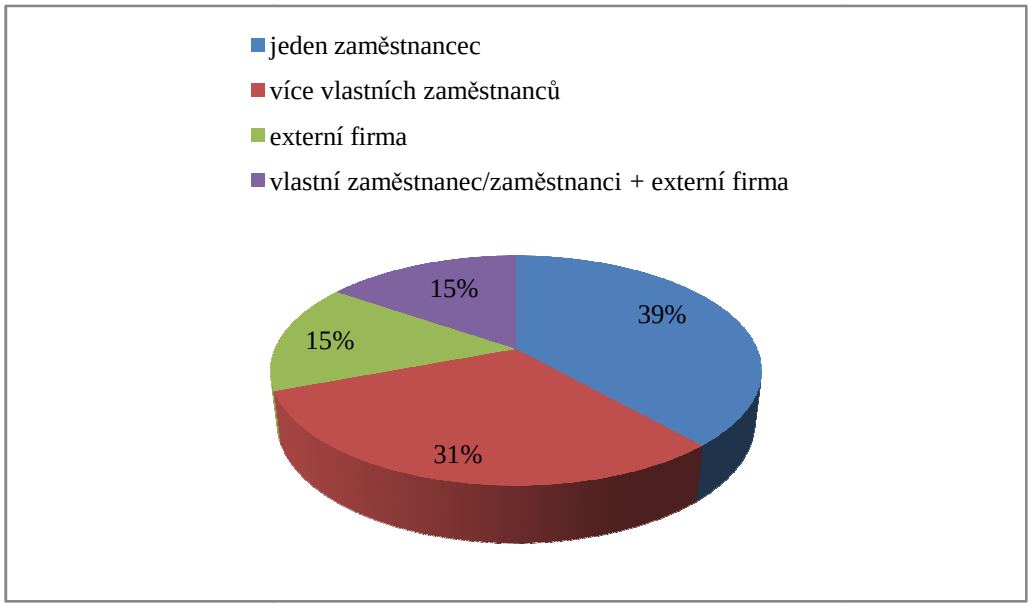
Z výsledku průzkumu vyplývají následující skutečnosti:

- Specializované oddělení bezpečnosti informací se nachází pouze v jedné organizaci.
- Zodpovědnost za bezpečnost informací se v jednotlivých organizacích různí. Z celkového počtu třinácti respondentů čtyři

uvedli, že bezpečnost organizace má na starosti jedna osoba – správce sítě a v jednom případě pak správce sítě plus externí firma. V tomto případě se jednalo o státní instituci, kde jednodušší incidenty a problémy, které jsou v silách samotného správce sítě, se řeší bez pomoci. Vyskytnou-li se nějaké závažnější problémy, je zajištěna podpora od externí firmy (outsourcing). Dvě organizace pak řeší bezpečnost informací čistě cestou outsourcingu. Ve čtyřech organizacích je bezpečnost informací zajišťována prostřednictvím skupiny vlastních zaměstnanců - to znamená pomocí více osob. V tomto případě jeden z respondentů přímo uvedl, že za bezpečnost odpovídá bezpečnostní manažer a bezpečnostní tým ve složení správce budovy, vedoucí IT, technici. V jednom případě, v závislosti na velké rozsáhlosti IT, zodpovídá za bezpečnost jednak skupina pracovníků, jednak externí firma. Poslední z respondentů uvedl, že za bezpečnost informací v jeho organizaci zodpovídá obchodní ředitel.

Pro lepší srozumitelnost je výsledné zjištění zobrazeno na obrázku Obr. 6. Výčet možností byl nakonec upraven do čtyř kategorií. Těmito kategoriemi jsou:

- jeden zaměstnanec
- více vlastních zaměstnanců
- vlastní zaměstnanec/zaměstnanci + externí firma
- externí firma

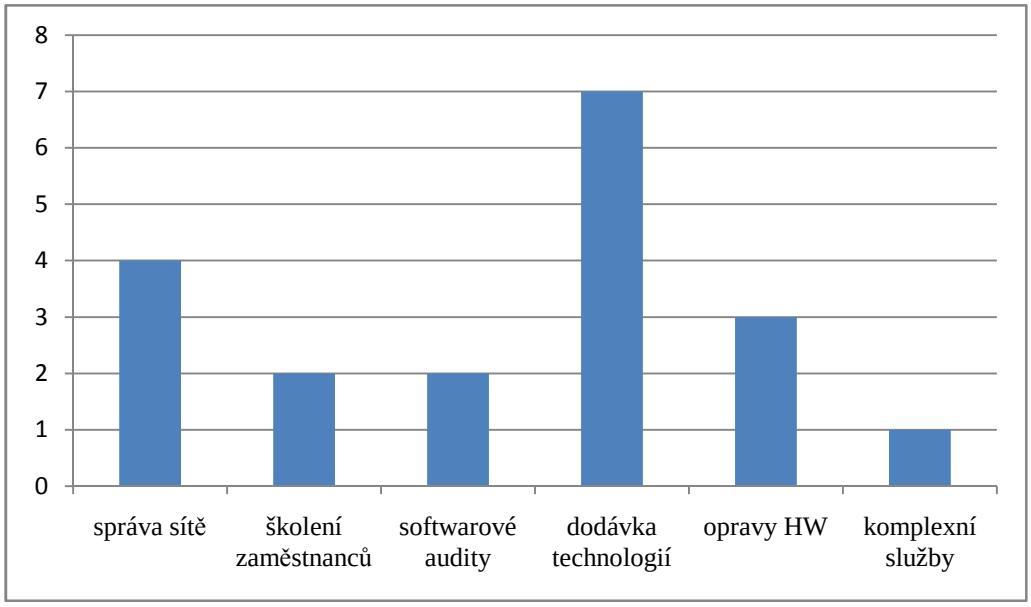


Obr. 6: Zodpovědnost za bezpečnost informací

5.4 Outsourcing

Již bylo řečeno v bodě 4.4 (Metriky v oblasti outsourcingu), že jednou z možností, jak řešit různé služby spojené s provozováním a užíváním IS/ICT, je přenesení na nějakou externí firmu, která tyto služby dokáže zajistit. Existuje celá řada činností, které nabízejí firmy specializující se na outsourcing IT. Na základě prostudování spektra nabízených služeb několika organizací zabývajících se outsourcingem IT byly vybrány možnosti, z kterých měl respondent vybrat ty služby, které si nechávají outsourcovat. Pokud outsourcing nevyužívají, nebyla vybrána žádná možnost. V případě, že se některá varianta v nabízených odpovědích nenacházela, byla respondentovi ponechána možnost doplnit vlastní odpověď. Z odpovědí respondentů vyplývá, že externí firmy jsou nejčastěji využívány k dodávce nových technologií, to znamená při přechodu na modernější techniku, k opravám HW a ke správě sítě (včetně zálohování dat). Dvě organizace si nechávají provádět softwarové audity. Jeden z dotazovaných respondentů uvedl, že externí firmu využívají

k zajištění komplexních služeb týkajících se IT. Výsledky zjištění jsou zobrazeny na obrázku Obr. 7.



Obr. 7: Služby zajišťované externími firmami

K výsledkům je ještě nutné dodat, že tři z dotazovaných organizací nevyužívají externí firmy k žádným činnostem, které by byly spjaty s informačními technologiemi.

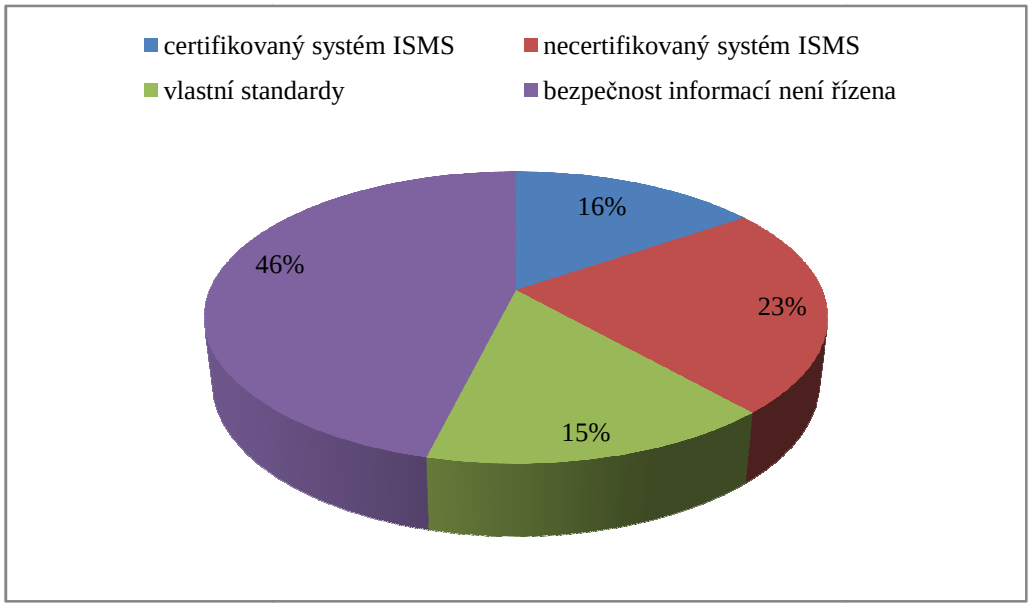
5.5 Standardy využívané pro řízení bezpečnosti

Další oblastí vhodnou k prozkoumání je rozšířenost bezpečnostních standardů. Tedy jestli se organizace řídí určitými psanými pravidly, ať už se jedná o vlastní standardy a směrnice organizace či obecně uznávané standardy, ze kterých vychází systém řízení bezpečnosti ISMS nebo jiné systémy řízení. Zjištěné skutečnosti jsou následující:

- Dvě z dotazovaných organizací mají certifikovaný systém ISMS.
- Tři respondenti odpověděli, že používají systém ISMS, ale certifikát nemají.

- Ve dvou organizacích mají stanovena vlastní pravidla (interní standardy), podle kterých je řízena bezpečnost informací.
- Zbylých šest respondentů uvedlo, že informační bezpečnost není v jejich organizaci nikterak systematicky řízena, tedy že žádná přesná pravidla stanovena nemají.

Dále byli respondenti dotázáni na to, co vedlo jejich organizaci k zavedení systému řízení bezpečnosti ISMS (pokud systém mají zaveden). Nejčastější odpovědí byla shoda s legislativou – zejména vyhovění zákonu č. 101/2000 Sb. (ochrana osobních údajů), neboť právě tyto organizace zpracovávají velké množství osobních údajů. Dalšími podněty k zavedení systému řízení bezpečnosti informací byly pak zejména vůle samotných vlastníků organizace, požadavky obchodních partnerů a nebezpečí negativní medializace, která by mohla vyplynout z úniku soukromých informací na veřejnost. Respondenti byli ještě poptáni, zda si myslí, že by zavedení ISMS s následnou certifikací mohlo mít vliv na obchodní styky a důvěru zákazníků. Deset z třinácti dotazovaných respondentů si myslí, že certifikovaný systém ISMS by pro jejich organizaci z pohledu obchodních styků mohl mít určitý přínos. Z pohledu zvýšené důvěry ze strany zákazníků pak devět respondentů odpovědělo ano. To znamená, že určitý přínos by zavedení a následná certifikace mít mohly. Nutno podotknout, že organizace, pro které by z těchto hledisek certifikace ISMS valný smysl neměla, jsou státní instituce - tedy organizace, které přímo obchodní partnery či zákazníky nemají. Je tedy pochopitelné, že v tomto případě byly odpovědi negativní. Aby mohla stoupnout důvěra zákazníka v danou organizaci v důsledku certifikace dle normy ISO 27001, by však musela být veřejnost dostatečně seznámena s tím, čeho se daný certifikát týká, co vše musela společnost splnit, aby ho získala, a jaké výhody pro samotného zákazníka může představovat (např. určitá záruka, že osobní data firmě svěřená jsou v relativním bezpečí). Rozšíření bezpečnostních standardů, které bylo zjištěno během průzkumu, je zachyceno na obrázku Obr. 8.



Obr. 8: Standardy pro řízení informační bezpečnosti

5.6 Metriky

Metriky jsou nástrojem pro hodnocení stávající úrovně bezpečnostních opatření. Počátečním předpokladem bylo, že alespoň základní metriky by měla mít zavedena každá organizace. Návrh, zaznamenávání a vyhodnocování metrik nemusí pouze probíhat v souvislosti se zavedeným systémem řízení bezpečnosti, ať už na základě nějakých interních standardů a směrnic nebo přímo systému ISMS. Měření by mohlo vycházet čistě z vlastní iniciativy zaměstnanců, kteří mají na starosti informační bezpečnost (za předpokladu, že by probíhalo pravidelně). U organizací, které mají zajištěny služby spojené se správou IT od externích firem (formou outsourcingu), by měly určité metriky být zahrnuty ve smlouvě o poskytování služeb SLA. Cílem bylo tedy zjistit, kolik z dotazovaných organizací používá metriky. Následně pak byly vybrány často měřené jevy a respondenti mohli vybrat, které z nich měří. Pokud se v seznamu vhodné metriky nevyskytovaly, byli vyzváni, aby doplnili vhodné varianty.

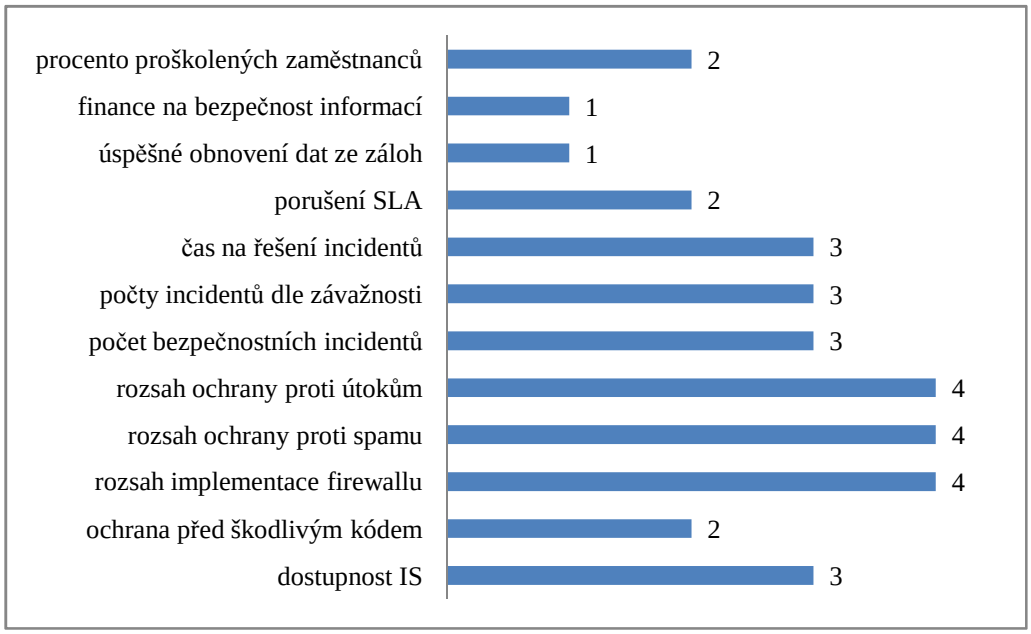
Další zkoumanou oblastí bylo používání standardních bezpečnostních prostředků. Respondenti byli dotázáni, zda používají prostředky a nástroje, jako IDS (zařízení či aplikace, které monitorují síť nebo systémové činnosti jako porušení zásad, počet útoků atd.), spamové filtry, antivirové ochrany či firewally. Logy z těchto nástrojů by mohly být použity pro metriky. Dále pak bylo zjišťováno, zda organizace používají i nějaké vlastními silami navržené nástroje.

Zjištěné skutečnosti jsou následující:

- Metriky mají zavedeny pouze čtyři organizace. Zbylé organizace žádné metriky nemají stanoveny. Dokonce bylo zjištěno, že dvě z organizací, které si nechávají správu IT a s tím spojené služby realizovat externí firmou, tedy prostřednictvím outsourcingu, žádné metriky stanoveny taktéž nemají. Bližší informace však ani po opakovaném dotázání nebyly poskytnuty. Tedy se lze jen domnívat, jakým způsobem je podpora řešena (zda se jedná o nějakou ústní dohodu typu oznámení problému – příjezd odpovědného pracovníka – domluva na finančním vyrovnání nebo nějakou neúplnou smlouvu o poskytování služeb).
- Běžná bezpečnostní opatření se v dotazovaných organizacích vyskytují. Firewall používá deset, antivirové ochrany dvanáct, spamové filtry deset a IDS čtyři z celkového počtu třinácti dotazovaných respondentů. Logy z těchto zařízení pak jsou ve většině případů prohlíženy čistě z osobního zájmu odpovědných zaměstnanců nebo v případě vzniku bezpečnostních incidentů. Ve většině případů se však vysledované hodnoty nikterak nezaznamenávají. To samozřejmě souvisí zpětně s tím, že pouze čtyři respondenti uvedli, že mají zavedeny metriky.
- Některé vlastními silami navržené nástroje pak využívají tři z celkového počtu třinácti dotazovaných organizací.

Zajímavý je výrok, který uvedl jeden z respondentů, který byl přímo účasten vyplňování dotazníku. Na dotaz, zda mají zavedeny metriky a které jevy měří, odpověděl doslova: „My tady nejsme od toho, abychom řešili IT – jsme tu od toho, abychom vyráběli věci, to nás živí.“ Následující odpovědi se odvíjely od tohoto faktu. Tato organizace nemá zavedena bezpečnostní opatření, neboť se specializuje na jiné činnosti a IT je pro ni vedlejší. Jiný respondent zase uvedl, že zavádění metrik je zbytečná administrativa navíc. Práce má prý velmi mnoho a další úkony by nestíhal. Přijetí dalšího zaměstnance, který by měl metriky na starosti, by se však dané organizaci z finančního hlediska nevyplatilo. Krom toho nepřisuzuje metrikám nějaký valný význam.

Zastoupení nejčastěji měřených jevů je znázorněno na obrázku Obr. 9.



Obr. 9: Nejčastěji měřené jevy v dotazovaných organizacích

Krom již uvedených faktů bylo též zjištěno, kdo zodpovídá za realizaci metrik a reporting zjištěných výsledků. Ve třech případech za realizaci metrik zodpovídá vlastní pověřený zaměstnanec. V jednom případě pak externí firma, která kompletně zajišťuje správu IT. Vyhodnocování pak probíhá jak ručně, tak

i automatizovaně. Jednou za rok je vedení organizace předkládána zpráva o zjištěných výsledcích.

5.7 Audity bezpečnosti

Krom metrik je bezpečnostní audit dalším prostředkem pro zjištění stavu bezpečnosti informací. Audity jsou prováděny jak interně, tak i externě. Tedy prostřednictvím vlastních zaměstnanců (interní audit prováděný vedením organizace) nebo prostřednictvím externí nezávislé organizace (spojené např. s bezpečnostním poradenstvím). Respondenti byli dotázáni, jestli jsou u nich v organizaci prováděny interní audity, jak často (s jakou periodou) a zda si nechává organizace dělat externí audity od specializovaných firem. Přitom externími audity byly myšleny i například audity předcertifikační, tedy takové audity, které jsou prováděny nezávislou organizací předtím, než je přizván certifikační orgán pro certifikaci systému ISMS.

Z průzkumu vyplynulo, že interní audity probíhají v pěti z celkového počtu třinácti dotazovaných organizací, a to zpravidla jedenkrát do roka. Externí audity si nechává dělat taktéž pouze pět organizací.

5.8 Penetrační testování

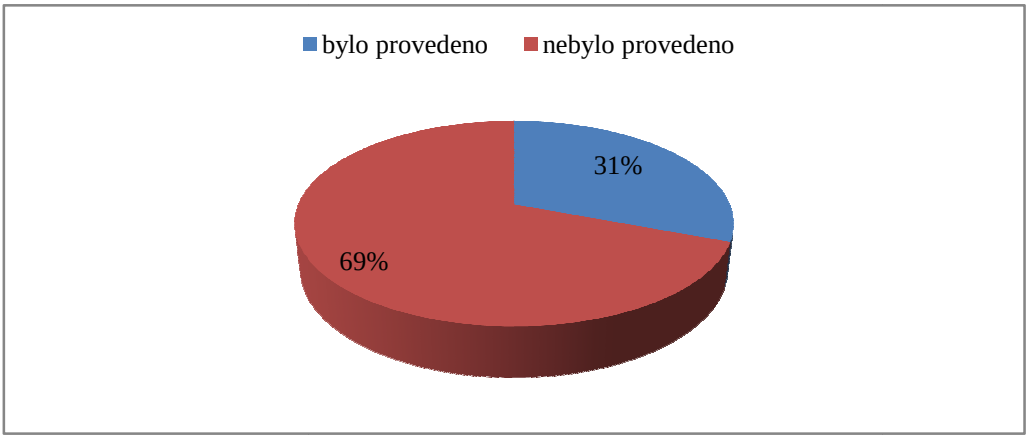
Penetrační testování je moderní metodou, jak zjistit odolnost systému vůči útokům. Jedná se o jakýsi předstíraný hackerský útok s cílem pokusu o průnik do vnitřní sítě a získat tak kontrolu nad testovanými zařízeními. Testy mohou být prováděny jednak prostřednictvím vlastních zaměstnanců, jednak přizváním specializované firmy, která se na provádění penetračního testování přímo specializuje. V případě specializované firmy pak může celý proces testování probíhat různými způsoby. Tato firma může být předem seznámena s prostředím, ve kterém bude probíhat testování, nebo také nemusí – pak je úloha fingovaného hackera reálnější. Personál, který má v prověřované organizaci na starosti bezpečnost IT pak o tom, že se bude provádět penetrační

testování, vědět může, ale také nemusí. Pokud personál není obeznámen, může to mít jistý přínos v tom, že současně se samotným prověřením zařízení jsou prověřeni i tito zaměstnanci. Tím je myšleno jejich reagování – zda si všimli nějakých zvláštních událostí a jakým způsobem na ně reagovali. Penetrační testování často nabízejí specializované firmy společně s prováděním bezpečnostních auditů. [29]

Respondenti byli dotázáni, zda bylo v jejich organizaci někdy provedeno penetrační testování a jestli si myslí, že by pro jejich organizaci mohlo mít nějaký význam. Zjištěna byla tato fakta:

- Penetrační testování bylo provedeno ve čtyřech z dotazovaných třinácti organizací.
- Deset respondentů si myslí, že pro jejich organizaci by bylo penetrační testování užitečné. Jeden respondent uvedl, že nespatřuje v takovémto způsoby prověření žádný velký význam. Dva respondenti nedokázali odpovědět přesně, tedy uvedli, že neví, zda by bylo penetrační testování pro organizaci, kterou zastupují, nějak přínosné.

Jak respondenti odpovídali lze spatřit na obrázku Obr. 10.



Obr. 10: Provedení penetračního testování v dotazovaných organizacích

5.9 Fyzické zabezpečení

Další oblastí, kterou bylo vhodné prozkoumat, je omezení přístupů do určitých lokalit, ať už se jedná o specializované místnosti či přímo samotné budovy. Existuje více možností, jak přístup umožnit pouze oprávněným osobám. V současnosti se nabízejí zejména biometrická zařízení, která jsou založena na rozpoznávání jedinečných znaků každého lidského jedince. Tato zařízení mohou sloužit i k evidenci docházky jednotlivých zaměstnanců (např. na základě otisku prstu) [30]. Jiným způsobem zabezpečení mohou být např. čipové karty (např. karty ISIC, které jsou využívány i na JČU).

Respondenti měli odpovědět na otázku, zda se v jejich organizaci využívají nějaké biometrické přístupové terminály nebo zda využívají nějaké jiné formy přístupu (čipové karty).

Zjištěno bylo:

- Čipové karty jsou využívány v devíti ze třinácti dotázaných organizací.
- Biometrické přístupy využívá pouze jediná organizace, která ale zároveň využívá i čipové karty.

5.10 Školení zaměstnanců

Školení zaměstnanců v oblasti bezpečnosti informací může hrát důležitou roli. Každý zaměstnanec, který pracuje s informacemi, a to v jakékoli podobě, by měl vědět, co má a nemá dělat, co si může a nemůže dovolit a zejména pak pracuje-li s výpočetní technikou, jakým způsobem se chovat a čeho se vyvarovat, aby nedošlo ke zbytečným bezpečnostním incidentům. Je mnoho variant, jak může probíhat školení. Může být prováděno vlastními zaměstnanci, externími školiteli nebo například formou e-learningu (zaměstnanec si přečte nějaký článek či projde nějaký elektronický kurz). Samotné školení pak může, ale i nemusí být zakončeno nějakým testem – ověřením nabytých znalostí či

toho, zda dávali během školení pozor nebo porozuměli e-learningovému kurzu. Stejně tak je potřeba zaškolit zaměstnance po zavedení nějakých nových technologií (např. nový software). Krom řádného školení by měli zaměstnanci, kteří zodpovídají za bezpečnost informací, sledovat současné trendy a hrozby. Velké nebezpečí může představovat phishing, tedy rozesílání emailů s odkazy na podvodné internetové stránky za účelem zjištění citlivých údajů (například přihlašovacích hesel pro přístup k bankovním kontům) či pochybné emaily s různými viry či trojskými koni ukrytými v přílohách. Pokud pověřené osoby zaregistrují nějakou vážnou a rychle se šířící hrozbu, měli by na ni upozornit ostatní zaměstnance a případně je poučit, jak se zachovat, pokud s touto hrozbou přijdou do styku.

Respondenti byli dotázáni, zda v jejich organizaci probíhá školení v oblasti bezpečnosti IT, jak často, jakou formou a zda bývá zakončeno nějakým testem (ověřením).

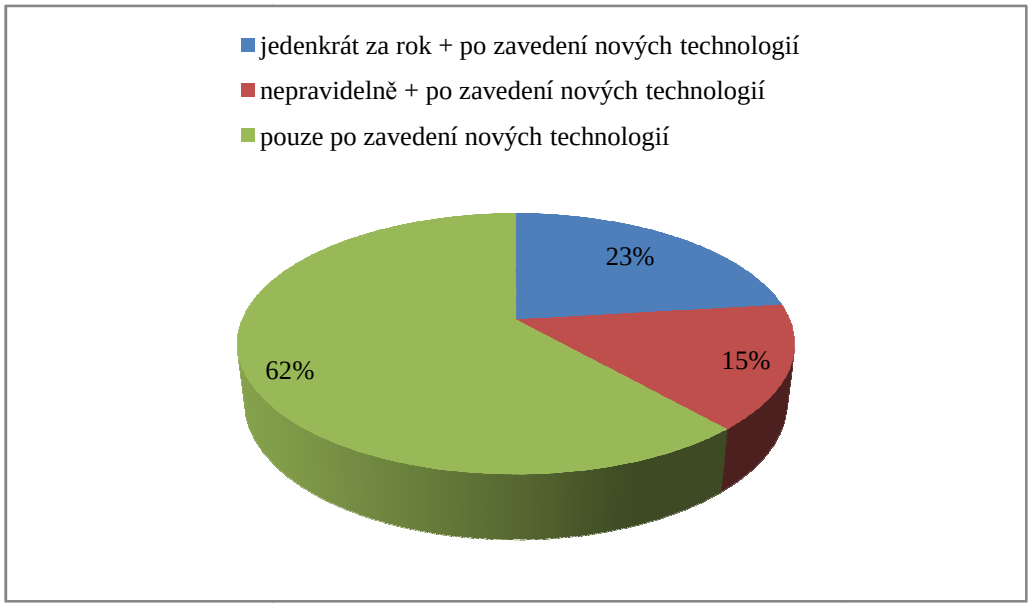
Zjištěno bylo následující:

- Školení v oblasti bezpečnosti informací probíhá ve třech organizacích pravidelně jedenkrát do roka, ve dvou organizacích probíhá kvůli odlišné pracovní době zaměstnanců nepravidelně a ve zbylých osmi organizacích neprobíhá vůbec. Jediné, co je pro všechny organizace společné, je potřeba proškolení zaměstnanců v případě zavedení nějakých nových technologií.
- Školením (zaškolením) bývá pověřen nejčastěji vlastní zaměstnanec (celkem šest odpovědí). Ve dvou případech byla odpověď externí školitel a ve dvou organizacích je školení řešeno formou e-learningu. Otázka však byla položena obecněji, a tak mohli odpovídat i zástupci organizací, ve kterých probíhá školení pouze po zavedení nějakých nových technologií (vybrat, kdo v takovém případě seznámí zaměstnance s danou problematikou – zaškolí je). V několika případech bylo vybráno více odpovědí. Z toho lze

usoudit, že školení neprobíhá vždy stejným způsobem. Například byla zvolena kombinace vlastního pověřeného zaměstnance a elektronického kurzu.

- Školení pak je zakončeno nějakým testem (ověřením znalostí) pouze u dvou z dotazovaných organizací.

Na obrázku Obr. 11 je zobrazeno, jak často a v jakých případech probíhá školení v oblasti IT. Získané odpovědi byly nakonec rozčleněny do třech kategorií.



Obr. 11: Školení zaměstnanců v oblasti IT

5.11 Analýza rizik

Následující otázka byla zaměřena na analýzu rizik. Respondenti byli dotázáni, kdy naposledy byla v jejich organizaci provedena analýza rizik.

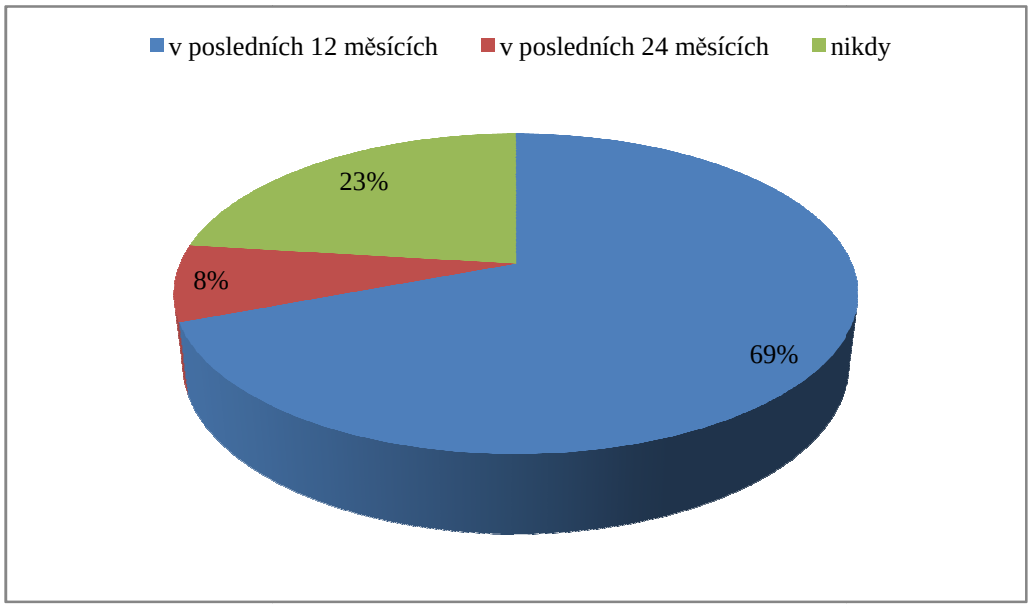
Bylo zjištěno, že:

- Ve třech organizacích analýza rizik nikdy provedena nebyla, v jedné organizaci byla provedena v posledních 24 měsících, ve zbylých

devíti organizacích pak byla provedena v období posledních dvanácti měsíců.

- Počet organizací s provedenou analýzou rizik je větší, než počet organizací, ve kterých je řízena bezpečnost. Z toho vyplývá, že analýza rizik může být provedena nezávisle v podobě nárazové akce.

Výsledek zjištění je zachycen na obrázku Obr. 12.



Obr. 12: Kdy byla provedena analýza rizik v dotazovaných organizacích

5.12 Monitoring činnosti zaměstnanců, kamerové systémy

Poslední zkoumanou oblastí je používání kamerových systémů a monitoring skutečných aktivit zaměstnanců v průběhu jejich pracovní doby. Kamerové systémy lze používat kupříkladu k monitoringu areálu či pracoviště. Je však nutné řídit se příslušnými zákony. Mělo by být jasně a zřetelně oznámeno, že oblast je monitorována kamerovými systémy a způsob, jakým se zpracovávají záznamy, po jakou dobu jsou uchovávány a k jakým účelům slouží [33]. Monitoring činnosti zaměstnanců je pak také vhodným prostředkem pro zvyšování a zefektivňování kvality odvedené práce. Monitorovací software umožňuje zjistit, jaké internetové stránky zaměstnanci nejčastěji navštěvují,

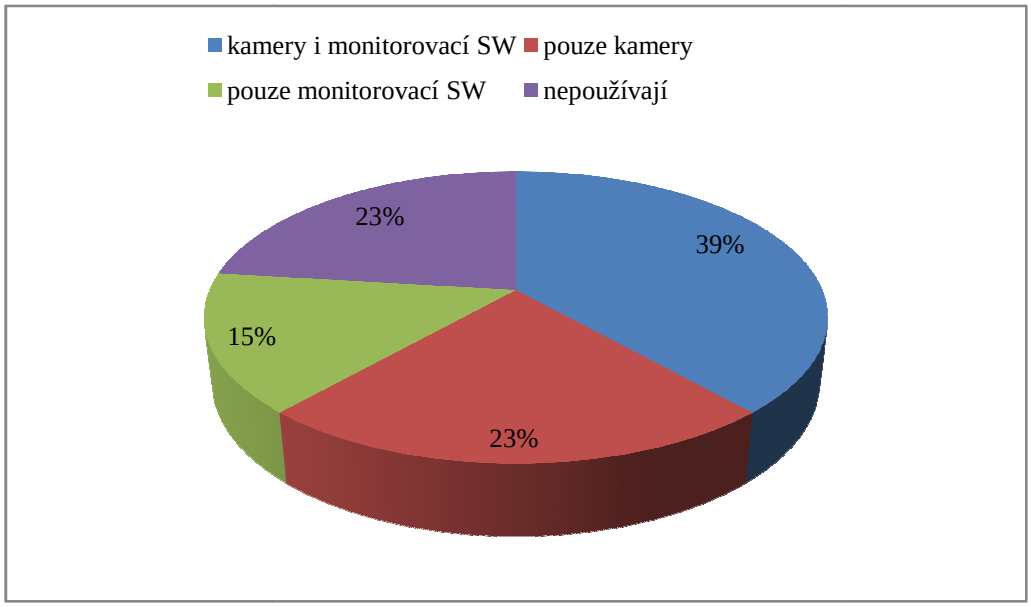
kolik času tráví na internetu a v rámci jakých aktivit (chat, prohlížení osobních emailů, stahování dat, hraní her atd.). Toto sledování přitom lze provádět tak, že to zaměstnanci nezareagují (nevědí o tom). Monitoring činnosti zaměstnanců může hrát důležitou roli například v období hospodářské krize, kdy na každé pracovní místo čeká mnoho uchazečů a nevyplatí se proto zaměstnávat člověka, který se plně nevěnuje svým pracovním povinnostem. [31] [32]

Zástupcům organizací byly položeny otázky, zda k nějakým účelům používají kamerové systémy a jestli provádí monitoring činnosti zaměstnanců během pracovní doby.

Závěry vyplývající z odpovědí jsou následující:

- Kamerové systémy využívá osm z dotazovaných třinácti organizací. Způsob a doba uchovávání a přesný účel, ke kterému jsou kamerové systémy využívány, se však nepodařilo zjistit u všech organizací. Někteří respondenti uvedli, že kamerové systémy využívají k monitoringu areálu závodu, dále pak k činnosti v místnostech s výpočetní technikou (škola – nepořizují se záznamy).
- Monitorovací software využívá sedm z třinácti dotazovaných organizací. Jeden z respondentů upřesnil, že činnost je sice monitorována, ale není nějak pravidelně vyhodnocována. Získaná data by však mohla sloužit jako záminka pro propuštění zaměstnance či alespoň pro nějaké sankce v podobě snížení platu či prémií. Je to tedy prostředek, který může být užitečný při redukování počtu zaměstnanců (zaměstnávat osobu, která řádně neplní své pracovní povinnosti, je pro organizaci zbytečným luxusem).

Na obrázku Obr. 13 je zobrazen počet organizací, které využívají zmiňované nástroje.



Obr. 13: Využívání kamerových systémů a monitorovacího SW

5.13 Závěrečné shrnutí

Na začátek je nutno konstatovat, že počáteční předpoklady se nenaplnily. Bylo očekáváno, že bezpečnost informací bude v převážné většině organizací řízena na základě nějakých pravidel a směrnic. Průzkum však tento předpoklad vyvrátil. Šest ze třinácti dotázaných uvedlo, že žádná pravidla stanovena nemají, natož pak zaveden nějaký celistvý systém řízení bezpečnosti informací. Metriky jsou taktéž zavedeny pouze v malém množství dotazovaných organizací. Tedy přesně řečeno ve čtyřech z nich. Proč nejsou zavedeny i v ostatních organizacích, bylo zřejmé z dodatečných odpovědí. Hlavními důvody je náročnost sběru dat a související administrace nebo to, že zaměstnanci, kteří mají informační bezpečnost na starosti a zároveň tak vedení organizace, nepřisuzují nějakému soustavnému zjišťování a zaznamenávání určitých jevů velkou důležitost. Celkem potěšujícím zjištěním je, že většina organizací alespoň provedla analýzu rizik, tedy má ohodnocena aktiva. Mají proto povědomí o hrozbách, kterým jsou vystaveny. Penetrační testování bylo provedeno pouze ve čtyřech organizacích, ale z názoru většiny respondentů, že

pro jejich organizaci by mohlo být penetrační testování prospěšné (odstranění slabin a nedostatků), lze očekávat, že v budoucnu by mohlo být provedeno právě i v jejich organizaci. Co se týče školení v oblasti IT a bezpečnosti informací, bylo zejména zjištěno, že ve většině organizací pravidelné školení neprobíhá. Zaměstnanci jsou spíše průběžně upozorňováni na nově se objevující hrozby v podobě nových počítačových virů či podvodných webových stránek a o způsobech, jak se zachovat, pokud se s těmito nebezpečími dostanou do styku. Prostředky pro monitorování činnosti zaměstnanců v pracovní době a kamerové systémy pak využívá více než polovina z dotazovaných organizací.

Na závěr je nutné k provedenému průzkumu dodat, že respondenti s průzkumem souhlasili pouze po přislíbení anonymity. Názvy organizací tedy nemohly být uvedeny ani zmiňovány.

6 ISMS a metriky na Jihočeské univerzitě

Vhodně zavedený systém řízení bezpečnosti informací ISMS, tedy myšleno takový systém, který je v souladu s normou ČSN ISO/IEC 27001, je pro organizace určitou zárukou toho, že jejich informační bezpečnost je řízena a je zabezpečena integrita, dostupnost a důvěrnost informací. Jak již bylo v kapitole 3 uvedeno, systém řízení bezpečnosti informací ISMS je vhodný pro všechny typy organizací. Zejména pak v prostředích, ve kterých se zpracovává mnoho osobních a citlivých údajů a kde je proto nutné dbát na dodržení patřičných zákonů.

Tohoto faktu jsou si vědomi i lidé z vedení Jihočeské univerzity v Českých Budějovicích, kteří se rozhodli pro zavedení systému ISMS. Dle Opatření rektora o zavádění Systému řízení bezpečnosti – ISMS, které bylo vydáno 23. února 2009, je podstatou ISMS zejména splnění požadavků, které předepisuje zákon č. 101/2000 Sb., o ochraně osobních údajů a zákon č. 127/2005 Sb., o elektronických komunikacích. Těmto zákonům je potřeba vyhovět z důvodu zpracovávání osobních údajů o zaměstnancích a studentech univerzity. [34]

6.1 Současný stav ISMS na JČU

V popisu současného stavu ISMS na Jihočeské univerzitě bylo vycházeno zejména z rozhovoru s paní manažerkou informační bezpečnosti JU. Původní záměr byl popsat podrobněji celkovou bezpečnostní politiku JU na základě informací, které jsou přístupny na ISMS portálu [35]. Na portálu ISMS se nacházejí tři typy dokumentů. Veřejné dokumenty (typ A) jsou k dispozici široké veřejnosti. V současnosti je jediným veřejným dokumentem Politika ISMS JU. Interní dokumenty (typ B) jsou k dispozici pouze studentům a zaměstnancům univerzity po jejich přihlášení (autentizaci). Interním dokumentem je již zmiňovaná Celková bezpečnostní politika JU. U informací

typu B však platí omezení, že nemohou být přenášené a distribuované mimo Jihočeskou univerzitu. Nelze tedy uvádět nějaké detailnější informace. Poslední kategorií jsou pak důvěrné dokumenty (typ C), které jsou přístupny pouze odpovědným zaměstnancům. Fakta, která lze uvést jsou následující:

- ISMS je v současnosti ve stádiu naplňování norem ISO/IEC 27001 a příbuzné ISO/IEC 27002. Je potřeba vytvořit sadu směrnic pro bezpečnostní audity.
- Politika ISMS je rozpracována do Celkové bezpečnostní politiky Jihočeské univerzity.
- Bylo ustanoveno Fórum bezpečnosti, což je skupina lidí, která zastřešuje informační bezpečnost.
- Aktiva IT jsou ohodnocena, dokumentována a mají své vlastníky – zejména fakulty.
- Analýza rizik byla provedena specializovanou firmou na třech vybraných součástech instituce.
- Jsou stanovena bezpečnostní pravidla (např. pro zálohování a zabezpečení).
- Co se týče metrik, tak momentálně žádné zavedeny nejsou.
- Do budoucna je potřeba připravit havarijní plány (např. pro systém STAG). Až budou plány hotové, měl by následovat interní audit, který by prověřil bezpečnost (fyzickou, personální,…) a na základě jeho výsledků by měly být odstraněny případné nedostatky.
- Momentálně není systém ISMS v takovém stádiu, aby mohl být certifikován (fáze Do – dělej v PDCA modelu). Již v této fázi by však mělo dojít k navržení vhodných ukazatelů (alespoň základních), které by měly sloužit ke kontrolám stavu ISMS v další fázi cyklu PDCA, tedy ve fázi Check – kontroluj (monitorování a přezkoumávání ISMS). V budoucnu, tedy až se systém ISMS více rozvine, by mohl být eventuelně certifikován, avšak není to

prioritou. Podmínkou pro certifikaci musí být zejména řádné zdokumentování zásadních kroků.

Jelikož ještě nebyly navrženy a zavedeny žádné metriky, bylo by vhodné pokusit se navrhnout několik kandidátních metrik, které by v prostředí Jihočeské univerzity eventuelně mohly být v budoucnu použity.

6.2 Návrh vlastních metrik

Při návrhu metrik je potřeba pamatovat na důležité zásady, podle kterých je vhodné se řídit. Metrika musí poskytovat kvantifikovatelné informace (tedy procenta, průměry, čísla). Data by měla být rychle a co možná nejsnadněji získatelná. Měřeny by měly být opakovatelné bezpečnostní procesy a metriky by měly být užitečné, tedy měly by měřit podstatné jevy. Postupy pro návrh a implementaci metrik jsou pak v různých standardech, které se týkají bezpečnostních metrik, obdobné. Metriky by měly být schváleny vysoce postavenými zaměstnanci (nejlépe vedením organizace). Mělo by být stanoveno, co má metrika sledovat, zdroj dat a jak mají být data vyhodnocována, pro koho jsou výsledky určeny a osoba zodpovědná za shromažďování dat, jejich vyhodnocování a reporting. Dále by mělo být stanoveno, s jakou frekvencí bude měření probíhat (denně, týdně, měsíčně, čtvrtletně, atd.) a jak často budou zjištění oznamována (např. jednou za rok předložena detailní zpráva vedení organizace). Pro naše potřeby byla zvolena šablona z dokumentu ISO/IEC 27004 (draft). Tato šablona obsahuje všechny potřebné náležitosti a je vhodná pro svoji přehlednost. Šablony však nejsou závazné – lze si je upravit dle vlastních potřeb. Některá pole je možno vynechat, popřípadě přidat vlastní. Vše záleží jen na osobních potřebách organizace. Stejně tak by bylo možné použít například šablonu ze směrnice NIST 800-55.

6.2.1 Šablona

Šablona byla upravena dle vlastních požadavků. Pro naše potřeby byla některá pole nepodstatná. Z tohoto důvodu došlo k jejich vynechání. Finální podobu navrženého formuláře zobrazuje následující tabulka (Tab. 5).

Identifikace měření			
Název měření			
Účel měření			
Objekt měření a atributy			
Objekt měření			
Atributy			
Specifika základního měření			
Základní měření			
Metoda měření			
Specifika odvozeného měření			
Odvozené měření			
Metoda měření			
Specifika indikátoru			
Popis indikátoru			
Analytický model			
Rozhodovací kritéria			
Efekty/dopady			
Příčiny odchylek			
Formát reportingu			
Procedura sběru dat			
Frekvence sběru		Kolektor	
Nástroje pro sběr		Datum sběru	
Procedura analýzy dat			
Frekvence reportingu		Analytik a reportér	
Nástroje pro analýzu		Příjemce analýzy	

Tab. 5: Šablona pro metriky [27], úprava autora

6.2.2 Celková bezpečnostní politika

Celková bezpečnostní politika JU je jedním z klíčových dokumentů, se kterým se dle pravidel uvedených na portálu ISMS Jihočeské univerzity musí seznámit každý student a zaměstnanec JU. Pro zpřístupnění tohoto dokumentu se uživatel musí přihlásit do systému a následným potvrzením dává najevo, že si dokument pročetl a zároveň s tím se zavazuje k tomu, že bude dodržovat pravidla a zásady, které tento dokument obsahuje. Jako vhodná se tedy nabízí metrika, která bude sledovat počet (procento) osob, které potvrdily seznámení s tímto dokumentem.

Identifikace měření	
Název měření	Seznámení s dokumentem Celková bezpečnostní politika JU
Účel měření	Ověřit, do jaké míry probíhá seznamování s dokumentem Celková bezpečnostní politika JU.
Objekt měření a atributy	
Objekt měření	databáze údajů o uživatelích
Atributy	osoby seznámené s Celkovou bezpečnostní politikou JU
Specifika základního měření	
Základní měření	Počet záznamů s hodnotou pole „Přečtení CBP“ = „Přečteno“.
Metoda měření	součet počtu polí
Specifika odvozeného měření	
Odvozené měření	Počet seznámených členů vůči celkovému počtu všech členů.
Metoda měření	Seznámení členové/všichni členové * 100
Specifika indikátoru	
Popis indikátoru	kruhový diagram
Analytický model	zelená výseč – procento seznámených s CBP JU červená výseč – procento neseznámených s CBP JU
Rozhodovací kritéria	zelená výseč < 75% - informace vedení s následným opatřením zelená výseč < 90% - více informací na univerzitní web zelená výseč nad 90% - žádná akce
Efekty/dopady	Celková bezpečnostní politika je základním dokumentem. Všichni by s ní měli být seznámeni. Pokud nejsou seznámeni, bezpečnost nemůže řádně fungovat.
Příčiny odchylek	Malá informovanost – informace na webu nestačí. Možná nápravná

	opatření – např. informační cedule/brožury v prostorách studijních oddělení a počítačových učeben. Další příčiny – lhostejnost a nezodpovědný přístup ze strany zaměstnanců a studentů.		
Formát reportingu	zpráva obsahující graf s číselnými údaji		
Procedura sběru dat			
Frekvence sběru	půlroční	Kolektor	správce databáze
Nástroje pro sběr	databázové nástroje	Datum sběru	říjen, březen
Procedura analýzy dat			
Frekvence reportingu	půlroční	Analytik a reportér	manažer bezpečnosti
Nástroje pro analýzu	tabulkový procesor	Příjemce analýzy	Fórum bezpečnosti

Tab. 6: Metrika „Seznámení s dokumentem Celková bezpečnostní politika“

K této metrice by se ještě hodilo dodat, že pro lepší kontrolu by bylo vhodné platnost potvrzení daného dokumentu omezit do konce akademického roku, popřípadě do vydání aktualizované verze Celkové bezpečnostní politiky JU.

6.2.3 Školení o ochraně osobních údajů a nakládání s nimi

Na Jihočeskou univerzitu se stejně jako na ostatní organizace, ve kterých se zpracovávají osobní údaje, vztahují příslušné zákony. Zejména pak zákon č. 101/2000 Sb., o ochraně osobních údajů. Personál, který tato data zpracovává, by se měl účastnit pravidelných školení nebo seminářů, kde by měl být seznámen s obecnými zásadami, podmínkami pro zpracovávání osobních údajů a případnými sankcemi, které mohou vyplynout ze zanedbání nebo porušení povinností. Nabízí se tedy navržení takové metriky, jejímž účelem by bylo sledování počtu odpovědných osob, které byly proškoleny (účastnily se semináře).

Identifikace měření	
Název měření	Školení ochrany osobních údajů
Účel měření	Zjistit, jaký je podíl zaměstnanců zpracovávajících osobní údaje, kteří absolvovali příslušné školení (seminář).
Objekt měření a atributy	
Objekt měření	Databáze zaměstnanců, kteří pracují s osobními údaji.
Atributy	Záznamy o zaměstnancích.

Specifika základního měření			
Základní měření	Počet záznamů s hodnotou pole „Proškolen“ = „ANO“.		
Metoda měření	součet počtu polí		
Specifika odvozeného měření			
Odvozené měření	Počet proškolených zaměstnanců vůči všem zaměstnancům.		
Metoda měření	Proškolení zaměstnanci/všichni zaměstnanci zpracovávající osobní údaje * 100		
Specifika indikátoru			
Popis indikátoru	kruhový diagram		
Analytický model	zelená výseč – procento proškolených pracovníků červená výseč – procento neproškolených pracovníků		
Rozhodovací kritéria	Výsledek (zelená výseč) < 100% - zpráva vedoucímu daného zaměstnance, že je nutno absolvovat školení.		
Efekty/dopady	Pokud nejsou všichni zaměstnanci pracující s osobními informacemi proškoleni, existuje riziko zanedbání povinností z důvodu neznalosti. Krom toho by mohly následovat i sankce a kárná opatření ze strany kontrolních orgánů.		
Příčiny odchylek	Pracovní neschopnost, nově příchozí zaměstnanec – nutno proškolit.		
Formát reportingu	Zpráva obsahující grafy s číselnými údaji.		
Procedura sběru dat			
Frekvence sběru	půlroční	Kolektor	manažer bezpečnosti
Nástroje pro sběr	databázové nástroje (tabulkový procesor – např. Excel)	Datum sběru	říjen, březen
Procedura analýzy dat			
Frekvence reportingu	půlroční	Analytik a reportér	manažer bezpečnosti
Nástroje pro analýzu	tabulkový procesor	Příjemce analýzy	Fórum bezpečnosti

Tab. 7: Metrika „Školení ochrany osobních údajů“

6.2.4 Školení v oblasti bezpečnosti informací

Mimo školení v rámci zpracovávání osobních údajů, které je určeno pro úzký okruh zaměstnanců, by bylo vhodné provádět školení, která by se týkala zaměstnanců a studentů. Předmětem takovýchto školení by byly základní zásady při práci s výpočetní technikou a poučení o nejvážnějších hrozbách a jejich možných dopadech na informační aktiva. Vhodnou formou školení je

přečtení nějakého článku či průchod jednoduchého e-learningového kurzu s následným potvrzením přečtení. Kurz může být zakončen testem, avšak není to podmínkou.

Identifikace měření			
Název měření	Školení v oblasti bezpečnosti informací		
Účel měření	Zjistit, jaké množství studentů a zaměstnanců JU absolvovalo kurz bezpečnosti informací.		
Objekt měření a atributy			
Objekt měření	E-learningový kurz „Bezpečnost informací“		
Atributy	Záznamy o účastnících kurzu.		
Specifika základního měření			
Základní měření	Počet absolventů kurzu.		
Metoda měření	Součet absolventů kurzu.		
Specifika odvozeného měření			
Odvozené měření	Podíl proškolených osob k počtu všech osob, které by měly absolvovat kurz.		
Metoda měření	počet proškolených osob/počet všech osob * 100		
Specifika indikátoru			
Popis indikátoru	kruhový diagram		
Analytický model	zelená výseč – procento absolventů kurzu červená výseč – procento těch, kteří ještě kurz neabsolvovali (zbytek)		
Rozhodovací kritéria	procento proškolených (zelená výseč) < 90% - nápravná opatření – např. výzva prostřednictvím vyučujících k absolvování kurzu procento proškolených nad 90% - žádná akce		
Efekty/dopady	Nedostatečné povědomí o možných rizikách a základních pravidlech zacházení s PC může mít za následek vznik bezpečnostních incidentů.		
Příčiny odchylek	Nedostatečná informovanost o kurzu, ignorování ze strany studentů.		
Formát reportingu	Zpráva obsahující grafy s číselnými údaji.		
Procedura sběru dat			
Frekvence sběru	půlročně	Kolektor	správce kurzu
Nástroje pro sběr	databázové nástroje	Datum sběru	začátek semestrů
Procedura analýzy dat			
Frekvence reportingu	půlročně	Analytik a reportér	manažer bezpečnosti
Nástroje pro analýzu	tabulkový procesor	Příjemce analýzy	Fórum bezpečnosti

Tab. 8: Metrika „Školení v oblasti bezpečnosti informací“

6.2.5 Počet bezpečnostních incidentů

Dalším z jevů, které jsou často sledovány, je počet bezpečnostních incidentů. Bezpečnostními incidenty přitom rozumíme veškeré události, které mohou narušit integritu, důvěrnost a dostupnost a porušení pravidel a směrnic (vyzrazení hesel, krádež dat či zcizení zařízení…). Jako zdroj dat pro tuto metriku mohou sloužit jednak logy z používaných bezpečnostních aplikací či zařízení (např. antivirové programy, firewally), jednak hlášení incidentu samotnými uživateli (např. student nahlásí incident bezpečnostnímu správci).

Identifikace měření			
Název měření	Počet bezpečnostních incidentů na JU		
Účel měření	Zjistit počet bezpečnostních incidentů. Cílem je zjistit trendy výskytu bezpečnostních incidentů (porovnání s předchozími výsledky).		
Objekt měření a atributy			
Objekt měření	servery, pracovní stanice, síťové prvky		
Atributy	bezpečnostní logy (IDS, antiviry, firewall…), hlášení o incidentech		
Specifika základního měření			
Základní měření	Počet bezpečnostních incidentů.		
Metoda měření	Součet počtu bezpečnostních incidentů z různých zdrojů.		
Specifika odvozeného měření			
Odvozené měření	aktuální stav vůči předchozímu měření		
Metoda měření	(aktuální počet/počet z předchozího měření) * 100		
Specifika indikátoru			
Popis indikátoru	graf (spojnicový)		
Analytický model	graf + procenta		
Rozhodovací kritéria	nárůst počtu incidentů vůči předchozímu období > 5% - hlášení Fóru bezpečnosti, navržení opatření (koupě nového firewallu, zkvalitnit a rozšířit školení…)		
Efekty/dopady	Zvyšující se počet bezpečnostních incidentů signalizuje, že stávající opatření nejsou dostatečná. Může dojít k vážnějším incidentům.		
Příčiny odchylek	Malá informovanost uživatelů, zastaralé technologie, špatná implementace bezpečnostních opatření.		
Formát reportingu	zpráva obsahující grafy s číselnými údaji		
Procedura sběru dat			
Frekvence sběru	denní	Kolektor	IT manažeři

			jednotlivých součástí (fakulty…)
Nástroje pro sběr	systémové nástroje, IDS, antiviry, antispamy, hlášení uživatelů (Pozn. data uložena v databázi incidentů)	Datum sběru	
Procedura analýzy dat			
Frekvence reportingu	měsíční	Analytik a reportér	manažer bezpečnosti
Nástroje pro analýzu	tabulkový procesor, databáze incidentů	Příjemce analýzy	Fórum bezpečnosti

Tab. 9: Metrika „Počet bezpečnostních incidentů na JU“

6.2.6 Shrnutí

Pro naše potřeby byly navrženy čtyři metriky, které by eventuelně mohly být použity v univerzitním prostředí. Na tomto místě je vhodné znovu zdůraznit, že tyto metriky jsou pouze kandidátní, tedy mohou posloužit jako inspirace při návrhu konkrétních metrik. Konkrétní metriky však budou muset být navrženy odpovědnou osobou, která je zároveň dokonale znalá prostředí Jihočeské univerzity. Tedy nejlépe manažerem bezpečnosti. Zároveň je potřeba, aby metriky byly schváleny nadřízeným orgánem. Tímto orgánem by mělo být Fórum bezpečnosti.

7 Závěr

Cílem bakalářské práce bylo podat přehled oblasti metrik bezpečnosti informací, dále pak popsat systém řízení bezpečnosti informací ISMS, jehož součástí je i měření účinnosti zavedených opatření a technologií. Nedílnou součástí práce je i zjištění stavu bezpečnosti informací v několika organizacích.

Systém řízení bezpečnosti ISMS byl podrobněji popsán. Důraz byl přitom kladen na monitorování a přezkoumávání a zejména pak na bezpečnostní metriky, kterým je věnována celá kapitola 4. Bylo vysvětleno, co si lze představit pod pojmem metrika, jaké znaky by měla mít dobrá metrika, jak lze metriky klasifikovat a jakou roli hrají v řízení bezpečnosti informací a ve speciálních případech - např. v situacích, kdy je část úkonů souvisejících s IT svěřena někomu zvenčí (outsourcing).

V praktické části byl proveden průzkum. Cílem průzkumu bylo podat přehled o tom, jak se v praxi řeší a hodnotí bezpečnost informací. S vyplněním dotazníku nakonec souhlasilo třináct respondentů – zástupců organizací. Otázky byly směřovány zejména na řízení bezpečnosti. Tedy zda se organizace řídí nějakými známými normami, používají vlastní směrnice a pravidla či bezpečnost nikterak neřídí. S tím souvisí i používání metrik jako prostředku pro sledování aktuálního stavu a vývoje (např. zda vzrůstá počet bezpečnostních incidentů). Další otázky pak směřovaly například na outsourcing IT, monitoring zaměstnanců či školení v oblasti bezpečnosti informací. Z výsledků průzkumu, kterého se zúčastnily organizace různých zaměření a velikostí, vyplynulo, že systematické řízení bezpečnosti informací není zdaleka samozřejmostí. Ve většině organizací žádná jasně daná pravidla neexistují. Metriky jako kontrolní nástroj jsou pak využívány také minimálně (pouze ve čtyřech případech).

Samostatnou část pak představuje průzkum stavu ISMS na Jihočeské univerzitě. Získané informace však byly pouze obecnějšího charakteru –

detailnější informace JU tají, což je celkem pochopitelné. Důležitou informací, kterou se však podařilo získat je, že žádné metriky zatím nebyly navrženy. Proto jsem se rozhodl navrhnout několik kandidátních metrik, které by do budoucna mohly posloužit jako inspirace při návrhu metrik konkrétních.

Cíle bakalářské práce, které jsem si předem stanovil, byly splněny. Problematika metrik oblasti bezpečnosti informací byla rozebrána a průzkum stavu informační bezpečnosti byl proveden.

Literatura

[1] ČERMÁK, Miroslav. *Clever and Smart* [online]. 2010 [cit. 2010-02-15]. Dostupné z WWW: <http://www.cleverandsmart.cz>.

[2] DOUCEK, Petr; NOVÁK, Luděk; SVATÁ, Vlasta. *Řízení bezpečnosti informací*. První vydání. Praha: Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7.

[3] ERNST & YOUNG; NBÚ; DSM - DATA SECURITY MANAGEMENT. Průzkum stavu informační bezpečnosti v ČR 2007. [online]. 2007, [cit. 2010-03-02]. Dostupný z WWW: <http://www.dsm.tate.cz/files/download/PSIB_CR_2007.pdf>. ISSN 978-80-86813-13-4.

[4] ERNST & YOUNG; NBÚ; DSM - DATA SECURITY MANAGEMENT. Průzkum stavu informační bezpečnosti v ČR 2009. [online]. 2009, [cit. 2010-03-02]. Dostupný z WWW: <http://www.dsm.tate.cz/files/download/PSIB_CR_2009.pdf>. ISSN 978-80-86813-19-6.

[5] MIKULECKÝ, Jan; SKALICKÝ, Marek. ISMS v malých a středních firmách. *Data Security Management* [online]. 2004, 03/2004 až 06/2004, [cit. 2010-03-02]. Dostupný z WWW: <http://www.rac.cz/rac/homepage.nsf/CZ/Download/$FILE/ISMS%20pro%20SME%20051129.pdf>.

[6] SEKERKA, Vladimír. ISMS ve státní správě a samosprávě. 2008, [cit. 2010-03-02]. Dostupný z WWW: <www.isss.cz/archiv/2008/download/prezentace/sekerka_icz.ppt>.

[7] *Gity : Bezpečnost v kostce* [online]. 2008 [cit. 2010-03-02]. Dostupné z WWW: <http://www.chrantesidata.cz/> siemens

[8] BERÁNEK, Ladislav Standard ISO/IEC 27001 a oblast vývoje a pořizování software. In *Celostátní konference TVORBA SOFTWARU 2008*. Ostrava : VŠB-TU Ostrava, Ekonomická fakulta, 2008 [cit. 2010-03-02]. Dostupné z WWW: <formular-ekf.vsb.cz/formulare/F01/tsw/getfile.php?prispevekid=915>. ISBN 80-248-1765-1.

[9] JANĎOUREK, Jiří. *Eset : Chráníme vaše digitální světy* [online]. 2010 [cit. 2010-03-02]. Bezpečnostní audit. Dostupné z WWW: <http://www.eset.cz/bezpecnostni-audit>.

[10] *International Register of ISMS Certificates* [online]. 2010 [cit. 2010-03-02]. Dostupné z WWW: <http://www.iso27001certificates.com/>.

[11] *ISO : International Organization for Standardization* [online]. c2010 [cit. 2010-03-05]. Dostupné z WWW: <http://www.iso.org/iso/home.htm>.

[12] *ISO 27001 Security* [online]. c2010 [cit. 2010-03-05]. Dostupné z WWW: <http://www.iso27001security.com/index.html>.

[13] *ISACA : Trust in, and value from, information systems* [online]. c2010 [cit. 2010-03-06]. Dostupné z WWW: <http://www.isaca.org/>.

[14] *ITIL* [online]. c2007-10 [cit. 2010-03-06]. Dostupné z WWW: <http://www.itil-officialsite.com/home/home.asp>.

[15] UČEŇ, Pavel, et al. *Metriky v informatice : Jak objektivně zjistit přínosy informačního systému*. První vydání. Praha : Grada Publishing, 2001. 139 s. ISBN 80-247-0080-8.

[16] JAQUITH, Andrew. *Security Metrics : Replacing Fear, Uncertainty, and Doubt*. Indianapolis : Addison-Wesley Professional , 2007. 335 s. ISBN 0-32-134998-9.

[17] WRIGHT, Steve. *IWS : The Information Warfare Site* [online]. 01.08.2006 [cit. 2010-03-08]. Measuring the Effectiveness of Security using ISO 27001. Dostupné z WWW: <http://www.iwar.org.uk/comsec/resources/iso-27001/measuring-effectiveness.pdf>.

[18] *BSI* [online]. British Standards Institution, c2010 [cit. 2010-03-08]. About BSI British Standards. Dostupné z WWW: <http://www.bsigroup.com/en/Standards-and-Publications/About-BSI-British-Standards/>.

[19] *National Institute of Standards and Technology* [online]. NIST, 10.07.2000, Last updated: March 1, 2010 [cit. 2010-03-09]. Dostupné z WWW: <http://www.nist.gov/index.html>.

[20] CHEW, Elizabeth, et al. *NIST Special Publication 800-55 Revision 1 : Performance Measurement Guide for Information Security* [online].

Gaithersburg : National Institute of Standards and Technology, July 2008 [cit. 2010-03-10]. Dostupné z WWW: <http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf>.

[21] SWANSON, Marianne. *NIST Special Publication 800-26 : Security Self-Assesment Guide for Information Technology Systems* [online]. Washington : National Institute of Standards and Technology, November 2001 [cit. 2010-03-10]. Dostupné z WWW: <http://www.worldcat.org/arcviewer/1/OCC/2007/08/08/0000070511/viewer/file3526.pdf>.

[22] CHEW, Elizabeth, et al. *NIST Special Publication 800-80 Initial Public Draft : Guide for Developing Performance Metrics for Information Security* [online]. Gaithersburg : National Institute of Standards and Technology, May 2006 [cit. 2010-03-10]. Dostupné z WWW: <http://permanent.access.gpo.gov/lps72067/draft-sp800-80-ipd.pdf>.

[23] *Cobit 4.1*. Rolling Meadows : IT Governance Institute, 2007. 196 s. ISBN 1-933284-72-2.

[24] *ITIL version 3 : Continual Service Improvement*. Edinburgh : Office of Government Commerce, 2007. 221 s. ISBN 978-0-11-331049-4.

[25] HOFRICHTER, Kamil; JURČA, Radomír. Základní aspekty outsourcingu IT. *SystemOnLine : Zpravodajský portál časopisu IT Systems* [online]. 2005, [cit. 2010-03-12]. Dostupný z WWW: <http://www.systemonline.cz/outsourcing-ict/zakladni-aspekty-outsourcingu-it-1.htm>.

[26] ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements.

[27] ISO/IEC 27004 (draft), Information technology – Security techniques – Information security management systems - Requirements.

[28] *Enterasys : Secure Networks* [online].Enterasys, 2010 [cit. 2010-03-18]. Security Information & Event Manager (SIEM). Dostupné z WWW: <http://www.enterasys.com/company/literature/siem-ds.pdf>.

[29] *DCIT, a.s. : konzultační a auditorské služby v oblasti IT a vývoj software PROVYS* [online].DCIT, c2008 [cit. 2010-03-19]. Hackeři ve vašich službách. Dostupné z WWW:

<http://www.dcit.cz/files/bezpecnost/info/DCIT_penetracni_testy.pdf>.

[30] *DIGITUS s.r.o. : identifikační systémy, biometrie* [online]. Digitus, c1999 - 2009 [cit. 2010-03-20]. Dostupné z WWW: <http://www.digitus.cz/produkty.php>.

[31] *Monitorovací systém Asistent : Monitorovat zaměstnance je legální!* [online]. Azprostor, c2009 [cit. 2010-03-21]. Dostupné z WWW: <http://www.monitorovat.cz/>.

[32] *Cyclope Series : Software pro monitoring využití lidských zdrojů* [online]. Amenit, 2010 [cit. 2010-03-21]. Dostupné z WWW: <http://www.cyclope-series.cz/default.aspx>.

[33] NĚMEC, Igor. *Úřad pro ochranu osobních údajů* [online]. c2000 - 2010, 20.03.2010 [cit. 2010-03-22]. Kamerové systémy a ochrana soukromí. Dostupné z WWW: <http://www.uoou.cz/files/med_0626_medtrib.pdf>.

[34] KOLÁŘOVÁ, Jana. *Opatření rektora o zavádění Systému řízení informační bezpečnosti - ISMS* [online]. České Budějovice : Jihočeská univerzita, 23. února 2009 [cit. 2010-03-26]. Dostupné z WWW: <http://www.jcu.cz/documents/rectors_proceedings/platna-opatreni/2009/>.

[35] MILOTA, Josef. *ISMS : Systém řízení informační bezpečnosti na JU* [online]. Jihočeská univerzita, 2009, 06.04.2009 [cit. 2010-03-27]. Dostupné z WWW: <http://isms.jcu.cz/>.

[36] ADAMEC, Zdeněk. *Hodnocení úrovně informační bezpečnosti banky*. Praha, 2009. 80 s. Diplomová práce. Bankovní institut vysoká škola Praha, Katedra informačních technologií a elektronického obchodování. Dostupné z WWW: <http://is.bivs.cz/th/6918/bivs_m/DP-Adamec.pdf>.

Seznam příloh

Příloha A – CD obsahující dotazník, který byl použit při průzkumu stavu informační bezpečnosti.