Metriky pro oblast bezpečnosti informací

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.

Integrita, dostupnost, důvěrnost

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.

Dostupnost

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

Důvěrnost

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

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.

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.

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.

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]

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.

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]

Systém řízení bezpečnosti informací

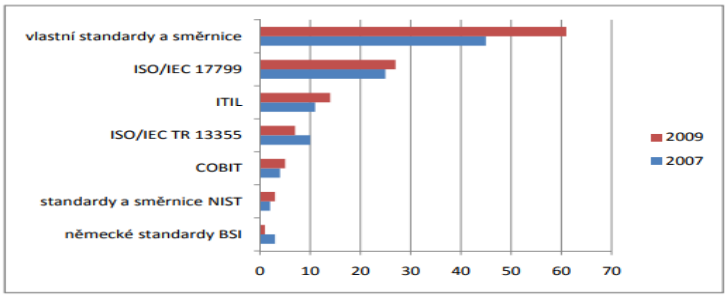
Zajištění bezpečnosti informací se na první pohled může zdát jako jednoduchá záležitost. Není tomu ovšem tak. Jedná se o důmyslný proces, který by měl být řízen. Měla by být jasně daná pravidla, postupy a zejména kontroly a měření, na jejichž základě lze vylepšit stávající bezpečnostní opatření a předejít 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

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.

ISMS

ISMS (Information Security Management System pro řízení bezpečnosti informací. řízení organizace. Podobn (po řadě systém řízení jakosti, systém a zdraví při práci) je založen na z předních statistiků 20. století složena z anglických slov P (jednej). PDCA cyklus pro 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 neusálým 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 jakkákoli organizace, ať už se jedná o státní instituce, nezisková organizace 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.

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.

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.

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.

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).

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

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.

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.

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.

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.

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.

Audit bezpečnosti

udit 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].

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.

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.

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.

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.

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)

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.

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.

Pojem metrika

Pavel Učeň v knize Metriky v informatice 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.

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 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

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.

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	Frekvence měření: 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

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.

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.

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.

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.

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).

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.

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).

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.

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]

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.

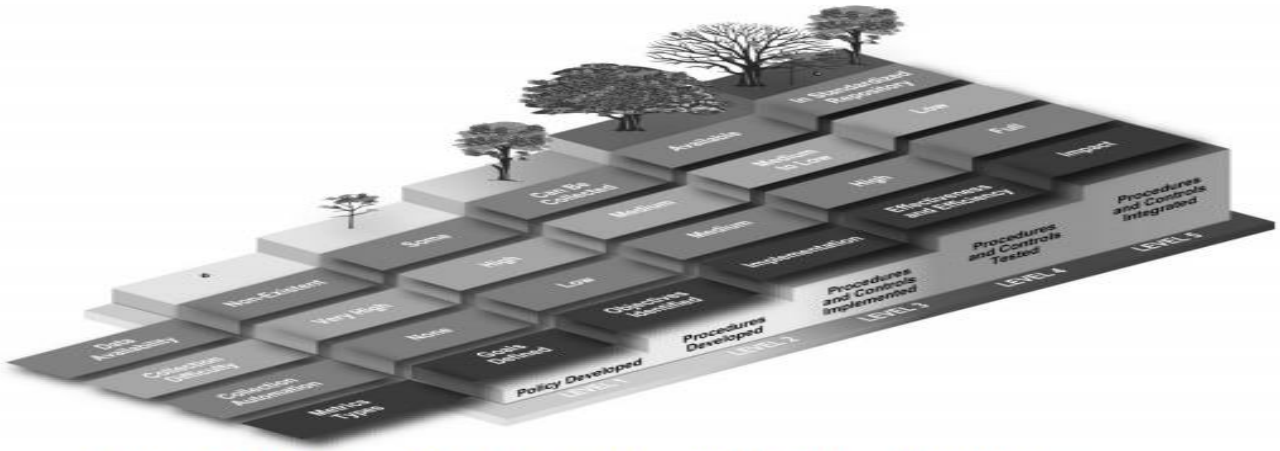
NIST rozděluje metriky v souvislosti s vyzrálostí bezpečnostního programu společnosti na metriky:

- 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

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]

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.

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

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]

Průzkum stavu bezpečnosti informací

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.

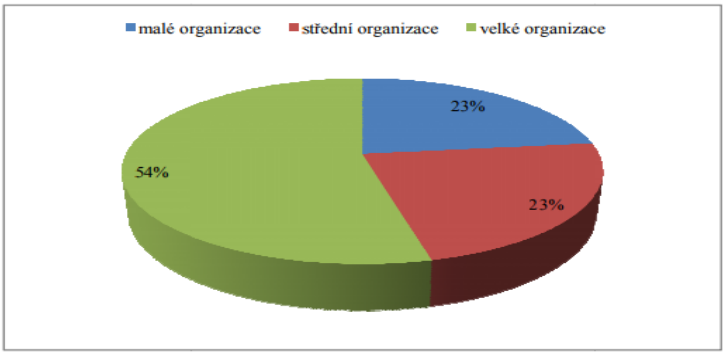
Metodika tvorby dotazníku

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:

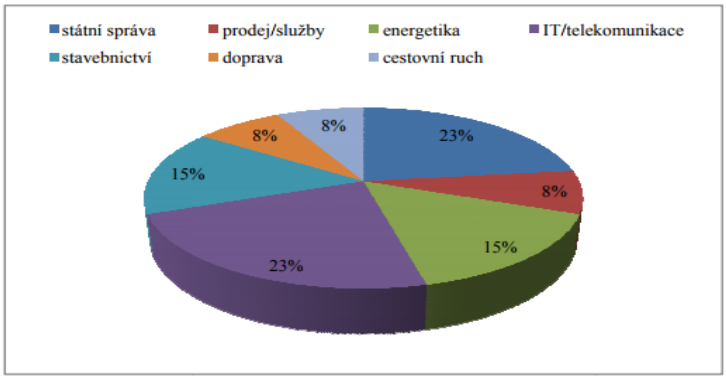
- organizaci bezpečnosti
- outsourcing
- standardy využívané pro řízení bezpečnosti
- metriky a nástroje využívané k řešení bezpečnosti • bezpečnostní audity
- penetrační testování
- fyzické zabezpečení – omezování přístupu
- školení zaměstnanců • analýzu rizik
- sledování činnosti zaměstnanců v pracovní 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). Dotazování organizace pak působí v šesti různých odvětvích. Podíl dotazovaných organizací dle velikosti je zobrazen obr.4



Podíl zastoupení organizací v 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×)

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.

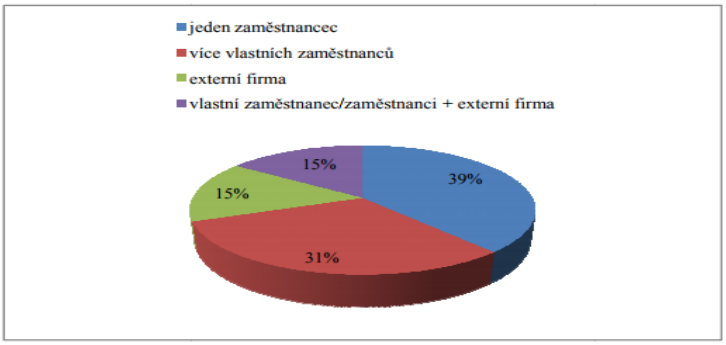
Cílem této oblasti je zjistit, kdo v organizacích zodpovídá za informační bezpečnost a zda se v organizaci nachází specializované oddělení bezpečnosti informací. Respondenti si mohli zvolit z několika nabízených možností tu, která je vyhovující. V případě, že se mezi nabízenými možnostmi žádná vhodná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

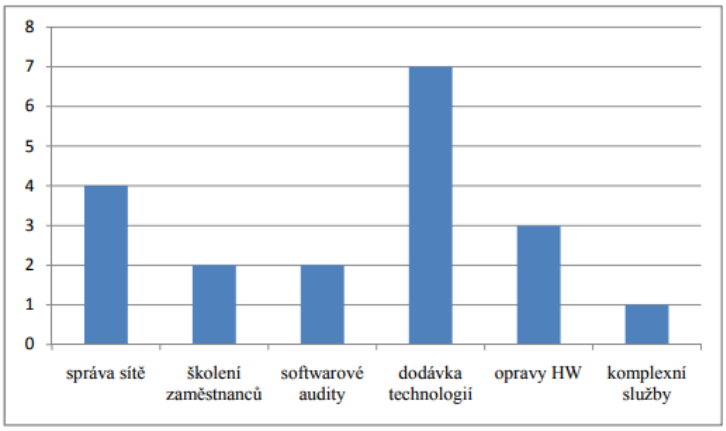


Obr. 6: Zodpovědnost za bezpečnost informací

Outsourcing

Již bylo řečeno v 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 dokaže zajistit. Existuje celá řada činností, které nabízejí firmy specializující se na outsourcing IT. Na základě prostudování spektra nabízených služeb několika oraganizací 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, nebyla vybrána žádná možnost. V případě, že se nekteté 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.

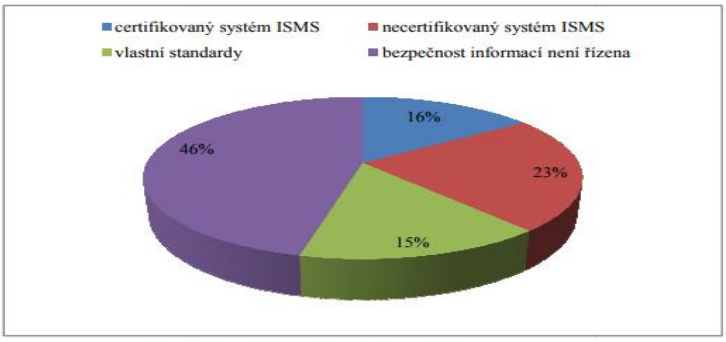
Standardy využívané pro řízení bezpečnosti

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

Metriky

Metriky jsou nástrojem pro hodnocení stávající úrovn opatření. Počátečním předpokladem bylo mít zavedena každá organizace. metrik nemusí pouze probíhat v bezpečnosti, ať už na základ přímo systému ISMS. M zaměstnanců, kteří mají na starosti informa by probíhalo pravidelně). správou IT od externích firem (formou outsourcingu), by m být zahrnuty ve smlouvě kolik z dotazovaných organizací používá často měřené jevy a respondenti mohli vybrat, které z v seznamu vhodné metriky nevyskytovaly varianty.