JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Pedagogická fakulta

Katedra informatiky

ANALÝZA RIZIK BEZPEČNOSTI IS STAG

Bakalářská práce

České Budějovice 2009 / 2010

Autor práce: Miloš Bučinský

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

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 27. prosince 2009 Miloš Bučinský

Anotace

Analýza rizik je nástroj pomáhající nám odhalit bezpečnostní rizika na systém a návrhu jeho bezpečnostních opatření. A právě analýza rizik bude hlavním tématem práce. V první, teoretické části budou popsány obecné pojmy bezpečnosti informačních systémů, teorie analýzy rizik a metody použitelné pro její měření. V druhé části budou vytvořeny dotazníky a tabulky samotné analýzy rizik, které budou vyplněny spolu se správci sítě Pedagogické fakulty Jihočeské univerzity. Z tabulek bude vypracováno závěrečné vyhodnocení a budou navržena vhodná opatření.

Abstract

Risk management is a tool, which helps to reveal the security risks to a system and proposal of its security action. And just a risk management will be a main part of work. In the first, theoretical part common definitions of IT security will be described, theory of risk analysis and a method usable for its measuring. In the second part question forms and tables of Risk analysis will be created, which will be filed with network managers of Pedagogical faculty of University of South Bohemia. From these tables final evaluation will be created and will be proposed useful action.

Poděkování

Rád bych poděkoval všem, kteří mi s mojí bakalářskou prací pomáhali, například s vyplňováním otázek či dotazníků, především pracovníkům Centra informačních technologií JU. Nejvíce bych ale chtěl poděkovat Ing. Ladislavu Beránkovi, CSc., MBA za cenné připomínky při vedení mé bakalářské práce.

Obsah

Seznam obrázků

Seznam tabulek

1. Úvod

Současný svět je plný rizik. Na rizika narazíme doslova na každém kroku. Také v informačních technologiích se rizika vyskytují a to dokonce ve velkém množství. Pod pojmem riziko si můžeme představit napadení počítače virem či trojským koněm, krádež dat zaměstnancem, popřípadě úplně cizí osobou, mechanickou závadou na harddisku a následnou ztrátu dat, ale také požár či jiné přírodní živly, které mohou znamenat pro společnost katastrofální následky. Informatika je v dnešní době základním kamenem fungování firem. Díky informatice jsou spolu navzájem propojeny různá oddělení firem, a to nejenom mezi sebou v rámci jedné budovy, ale i třeba z druhé strany světa. Proto je nezbytné mít systém pod kontrolou a nedopustit ani jedinou chybičku, která by jej mohla vyřadit z provozu.

Pro zjištění aktuální situace ve firmě či přímo v konkrétním systému je třeba mít dokonalý přehled a znát všechna potenciální nebezpečí. Znalost skutečného stavu bezpečnosti informací je základním předpokladem úspěšného a efektivního fungování a úspěšného rozvoje společnosti. A právě o poznání situace bezpečnosti je analýza rizik.

Ve větších firmách je důležité také získání certifikátu řízení bezpečnosti informačních systémů. To znamená, že náš systém splňuje všechny důležité normy v oblasti bezpečnosti a také legislativní normy České Republiky.

Tato práce představuje teorii analýzy rizik, představení norem bezpečnosti, základy řízení bezpečnosti informačních systémů a popis nejznámějších komerčních metod analýzy rizik. Druhá část mojí bakalářské práce bude věnována realizace analýzy rizik na informačním systému Pedagogické fakulty Jihočeské univerzity.

Jako nejvhodnější z používaných systémů jsem si vybral IS STAG, který slouží jako informační systém studijní agendy Jihočeské Univerzity. V systému jsou uchovávána veškeré informace ohledně našeho studia a jejich prozrazení, modifikace či dokonce ztráta by znamenala velký problém. K některým z těchto dat má navíc přístup velké množství uživatelů, což představuje potenciální riziko. A právě hodnocení bezpečnosti tohoto systému se budu věnovat ve druhé polovině mojí bakalářské práce.

2. Riziko, analýza rizik

2. 1. Riziko obecně

Riziko je výraz, který se poprvé objevil v 17. století v Itálii v souvislosti s mořeplavbou. Vyjadřoval úskalí, kterému se museli mořeplavci vyhnout. Dále se jimi vyjadřovalo vystavení nepříjemným okolnostem, nebezpečí, či že riskovat znamená „vážit si něčeho“. Později objevuje i význam ve smyslu možné ztráty a to především finanční. Dnes se rizikem rozumí nebezpečí vzniku škody, poškození, ztráty či zničení, případně nezdaru při podnikání.

- Pro pojem riziko se používají následující definice:
- Pravděpodobnost či možnost vzniku ztráty
- Pravděpodobnost možných výsledků či nejistota jejich dosažení
- Rozdíl skutečných a očekávaných výsledků
- Pravděpodobnost jiného výsledku, odlišného od výsledku předpokládaného
- Nebezpečí negativní odchylky od cíle
- Nebezpečí chybného rozhodnutí
- Možnost vzniku ztráty nebo zisku
- Neurčitost spojená s vývojem hodnoty aktiva (tzv. investiční riziko)
- Pravděpodobnost, že hrozba využije zranitelnosti systému

Riziko jako pojem se však nepoužívá pouze v oblasti počítačové bezpečnosti. Dalšími oblastmi jsou: politika, ekonomie, bezpečnost, ekologie, právní systém a mnoho dalších.

S rizikem jsou těsně spjaty dva pojmy:

- **Výsledek musí být nejistý** – Hovoříme-li o riziku, musí existovat dvě či více variant řešení. Víme-li s jistotou, že nastane ztráta, nelze hovořit o riziku.

- **Alespoň jeden z možných výsledků je nežádoucí** – Obecně lze říci, že jde o ztrátu, kdy jistá část majetku jednotlivce může být ztracena. Může však jít i o výnos, který je nižší než nejvyšší možný výnos.

Změna se nám může přihodit, vzniknout jako důsledek nenadálé události zvenčí, ale může být též dopředu plánována a řízena. A právě řízené změny jsou předpokladem správného chodu počítačové sítě. Pro řízení změny potřebujeme mít znalost technických požadavků a znalost postojů a motivací lidí.

Výjimečné výsledky, jak špatné, tak i dobré, by měly upoutat naši pozornost a dovést nás k otázkám, co je jejich příčinou.

Riziko hodnotíme ze dvou stránek, a to z:

- **Pozitivní stránky** – Možnost většího zisku a většího úspěchu
- **Negativní stránky** – Možnost horších výsledků a neúspěchu

Nežádoucí událost je událost, kterou můžeme definovat jako „nepříznivou odchylku od žádoucího výsledku, ve který doufáme nebo který očekáváme“. (1)

2. 2. Základní pojmy analýzy rizik

2. 2. 1. Aktivum

Aktivum (asset) je cokoliv, co má pro nás nějakou hodnotu. Tato hodnota však může být působením hrozeb zmenšena. Aktiva jsou hmotná (nemovitosti, elektronika, peníze) a nehmotná (autorská práva, informace, veškerá data na počítačích, kvalita zaměstnanců).

Při hodnocení aktiva se berou v úvahu tyto hlediska:

- Pořizovací náklady či cena
- Důležitost aktiva
- Velikost případné vzniklé škody aktiva
- Rychlost odstranění škody na aktivu
- Ostatní (specifická pro konkrétní případ) (1)

2. 2. 2. Hrozba

Hrozba (threat) je síla, událost, aktiva nebo osoba, mající vliv na bezpečnost, či dokonce může zapříčinit škodu. Hrozba může být například také požár, přírodní katastrofa, krádež, získání informací neoprávněnou osobou a další. Škoda, způsobená hrozbou se nazývá dopad hrozby. Do škody, kterou hrozba způsobí, se přičítají náklady na její obnovu. Úroveň hrozby se posuzuje dle následujících rysů:

- Nebezpečnost hrozby je schopnost způsobit škodu
- Přístup hrozby je pravděpodobnost, že se hrozba dostane k aktivu. Dalším parametrem je i frekvence výskytu hrozby.
- Motivace hrozby je zájem vyvolat hrozbu vůči aktivu. (1)

2. 2. 3. Zranitelnost

Zranitelnost (vulnerability) je nedostatek nebo slabina aktiva, který může hrozba využít pro uplatnění svého nežádoucího vlivu. Zranitelnost vyjadřuje citlivost aktiva na působení dané hrozby. Stejně jako u hrozby určujeme úroveň zranitelnosti, který se liší dle následujících faktorů:

- Citlivost zranitelnosti a náchylnost aktiva.
- Kritičnost a důležitost aktiva. (1)

2. 2. 4. Protiopatření

Protiopatření (control) je proces navržený pro zmírnění hrozby, eliminaci hrozby, snížení zranitelnosti nebo dopadu hrozby. Protiopatření navrhujeme s cílem předejít vzniklé škodě či usnadnit obnovu následků vzniklé škody. Všechna protiopatření musí být efektivní a musí mít co nejmenší náklady na realizaci. (1)

2. 2. 5. Riziko

Riziko (risk) z pohledu analýzy rizik je definováno jako míra ohrožení aktiva a následný vznik nebezpečí. Tím vzniká nežádoucí vliv a dochází ke vzniku škody. Lze říci, že riziko vzniká vzájemným působením hrozby a aktiva. Aktivum, na které nepůsobí ani jedna hrozba, není předmětem analýzy rizik. Úroveň rizika je určena

hodnotou aktiva, zranitelností aktiva a velikostí hrozby. Úroveň rizika lze také snížit a to pomocí protiopatření.

Zbytkové riziko je riziko, které je tak malé, že je pro nás přijatelné a není třeba aplikovat další protiopatření. (1)

2. 2. 6. Důvěrnost

Důvěrnost (confidentiality) je vlastnost, která je schopna zajistit ochranu informace (v libovolné formě) v okamžiku uložení, zpracování nebo přenosu před organizací nebo osobou, která není oprávněna tuto informaci získat. Jiným způsobem můžeme tuto vlastnost nazvat jako utajení informace.

2. 2. 7. Integrita

Integrita (integrity) je vlastnost, která zajišťuje, že informace (nebo jiné aktivum) je správně a úplně uložena nebo přenesena, že byla správně zpracována a nebyla pozměněna neoprávněným způsobem.

2. 2. 8. Dostupnost

Dostupnost (Availability) je vlastnost, která je schopna zajistit, že informace (nebo jiné aktivum) je dostupná tomu, kdo je oprávněn jí získat v jím požadovaném místě a čase.

2. 2. 9. Autentizace

Autentizace (Authentication) je proces pro jednoznačné ověření subjektu (člověka), vstupujícího do informačního systému. Autentizace rozlišujeme na několik druhů:

- Uživatelské jméno + heslo, šifrovací klíč
- Elektronický čip, například identifikační karta
- Biometrika – otisk prstu
- Bez autentizace

2. 2. 10. Autorizace

Autorizace (Authorization) je ověření práv. Uživatel může mít různá práva pro různé služby. K některým informacím může mít plný přístup, k jiným pouze částečný a jiné informace mu jsou nedostupné. Proces autorizace se skládá z:

- Autentizace subjektu (zjištění jeho identity)
- Vyhledání v seznamu oprávněných subjektů, jejich rolí a práv
- Udělení oprávnění nebo odepření přístupu

2. 3. Analýza rizik

2. 3. 1. Analýza rizik

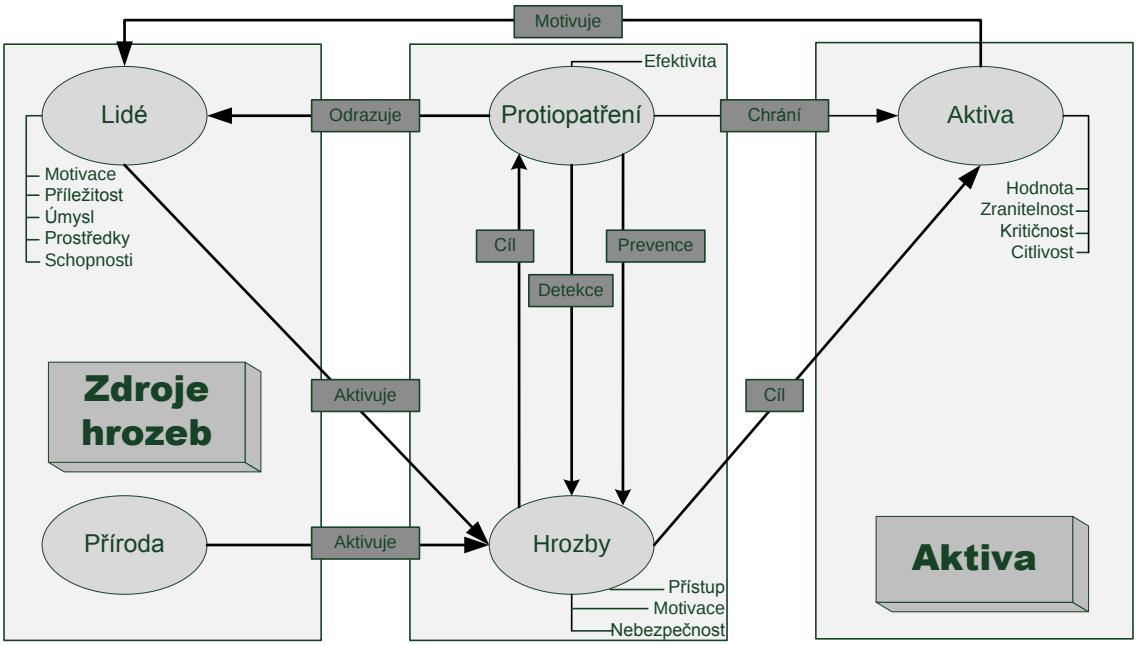
Analýza rizik (risk management) je proces, který identifikuje a hodnotí informační aktiva společnosti, zjišťuje možné hrozby, určí rizika a navrhne vhodné bezpečnostní protiopatření. Aktivy jsou myšleny zejména informace a data, která firma zpracovává. Analýza rizik přistupuje stejně k informacím v papírové i elektronické formě. Analýza rizik zahrnuje následující čtyři části:

- **Identifikace aktiv** – Stanovení a definování všech aktiv, které subjekt vlastní.
- **Stanovení hodnoty aktiv** – Určení hodnoty aktiv a jejich význam. Jejich hodnota se určuje podle velikosti ztráty v případě jejich ztráty, změny či poškození.
- **Identifikaci hrozeb a slabin** – Sepsání seznamu všech možných událostí, které by mohly nastat a mohly by mít negativní vliv na hodnotu aktiv. Druhou částí je sepsání všech potenciálně slabých míst v systému, které by se mohly stát možným cílem hrozeb.
- **Stanovení závažnosti hrozeb a míry zranitelnosti** - Určení pravděpodobnosti výskytu hrozby a míry zranitelnosti subjektu vůči dané hrozbě.

Výstupem analýzy rizik jsou popis informačního systému, stanovení úrovně hrozeb, odhad ztrát, stanovení protiopatření a určení zbytkových rizik. (2) (3)

2. 3. 2. Vztahy v analýze rizik

V analýze rizik jsou vztahy definovány podle následujícího schématu, uvedeného v knize Řízení rizik ve firmách a jiných organizacích od V. Smejkala.



Obrázek 1- Vztahy v analýze rizik

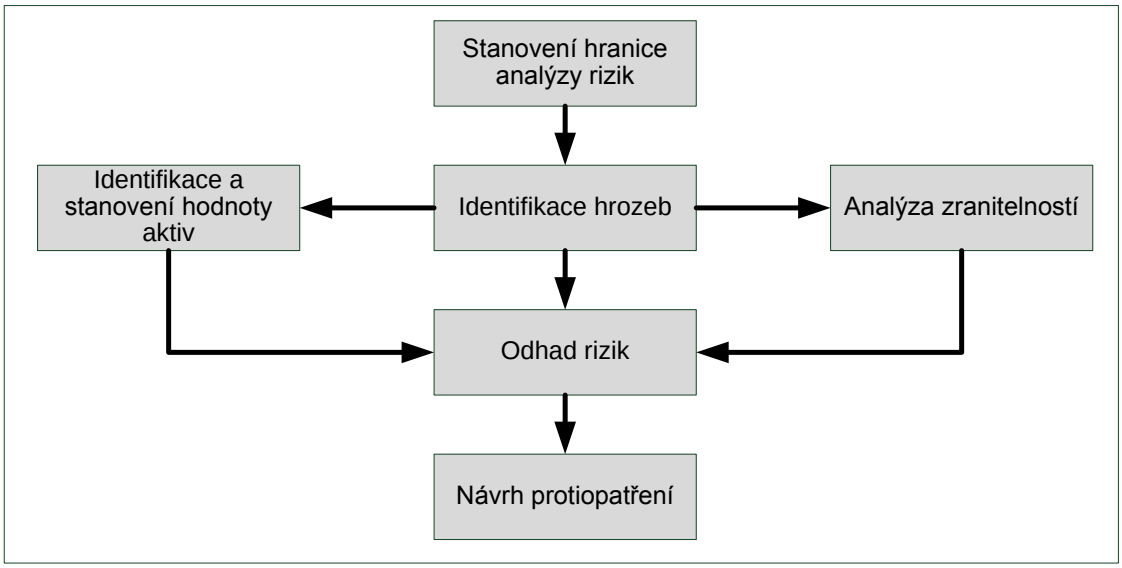
Mechanizmus uplatnění rizika probíhá následujícím způsobem:

- Hrozba využije zranitelnosti, překoná protiopatření a na aktivu způsobí škodu.
- Aktivum svou hodnotou motivuje útočníka k aktivaci hrozby. U každého aktiva můžeme určit úroveň zranitelnosti způsobené působením hrozby. Aktivum je třeba před hrozbami chránit.
- Protiopatření chrání aktiva, ruší hrozby a zabraňuje jim působit na aktiva.
- Hrozba působí na aktivum nebo na protiopatření, s cílem získat přístup přímo k aktivu. (1)

2. 3. 3. Obecný postup analýzy rizik

Při analýze rizik je potřeba vykonat následující kroky: (1)

- **Stanovení hranice** analýzy rizik, do které spadají veškerá aktiva, se kterými budeme dále pracovat.
- **Identifikace a stanovení hodnoty aktiv** systému spočívá v soupisu všech aktiv ležících uvnitř hranice analýzy rizik, se kterými budeme dále pracovat. Následně aktivům přiřadíme hodnotu, která se odvíjí od jejich reprodukční pořizovací ceny. Pokud je aktivum jedinečné a nenahraditelné, jeho cena stoupá.
- **Identifikace hrozeb** je, jak již název napovídá, o nalezení případných hrozeb, které mohou ohrozit naše aktiva. Pro jejich nalezení potřebujeme tzv. seznam hrozeb, který nalezneme v literatuře, či můžeme vycházet z našich zkušeností. Pro vytváření seznamu aktiv se nejčastěji používají metody jako brainstorming či metoda Delphi.
- **Analýza zranitelností** systému slouží k tomu, abychom si u jednotlivých aktiv určili úroveň hrozby (nebezpečnost, motivace, přístup…) a úroveň zranitelnosti (citlivost, kritičnost). Úroveň hrozeb i zranitelností můžeme snížit, díky aplikaci protiopatření.
- **Odhad rizik a pravděpodobnosti jeho uskutečnění** nám určí, jak často jev nastává. Především nám jde o to určit, zda je to jev náhodný či nikoliv. Také můžeme určit pravděpodobnost (z intervalu pravděpodobnosti tj. 0 až 100%), s jakou může nastat.
- **Návrh protiopatření** a vyhodnocení konkrétních závěrů.



Obrázek 2- Obecný postup analýzy rizik

2. 3.4. Přístupy provedení analýzy rizik IS

Přístupy, jak lze analýzu rizik provádět jsou tři. Každý z nich má své nesporné výhody, ale i nevýhody. Je však těžké organizaci doporučit jeden konkrétní přístup. Co někde funguje, jinde nemusí. Záleží tedy na velikosti organizace a složitosti informačního systému. (4)

- **Dodavatelský přístup** - Projekt analýzy rizik provádí dodavatel a nese za něj také odpovědnost.
- **Vlastní přístup** - Projekt analýzy provádí pracovníci organizace vlastními silami s pomocí zakoupené nebo vlastní metodiky, odpovědnost za provedení je na těchto pracovnících.
- **Partnerský přístup** - Projekt analýzy provádí pracovníci organizace pod metodickým i projektovým vedením dodavatelské nebo konzultační společnosti, odpovědnost je na dodavateli (konzultantovi). Tato varianta je nejméně častá.

	Dodavatelský přístup	Vlastní přístup	Partnerský přístup
Kdo provádí analýzu	Dodavatel	Pracovníci organizace	Pracovníci organizace pod vedením dodavatele (konzultanta)
Na kom je zodpovědnost	Dodavatel	Pracovníci organizace	Dodavatel (konzultant)
Kdo prezentuje výsledky	Dodavatel	Pracovníci organizace	Pracovníci organizace pod vedením dodavatele (konzultanta)
Výhody s nevýhody	+ Nezatěžuje organizaci (jen vyplnění dotazníků) + Není nutné mít vlastní odborníky + Odpovědnost je na straně dodavatele + Není nutné kupovat metodiku či nástroj - Nesrozumitelné výstupy - Vysoká cena	+ Všichni rozumí výstupům projektu + Nejnižší cena (i přes to že si musíme pořídit metodiku či nástroj) + Znalost interního prostředí + Větší ochota respondentů spolupracovat s kolegy než externisty - Velmi zatěžuje organizaci - Není jistota správného výsledku - „Vnitropodniková slepota“	+ Všichni rozumí výstupům projektu + Není nutné mít vlastní odborníky + Odpovědnost je na straně konzultanta + Odborné vedení a dohled ze strany konzultanta + Není nutné kupovat metodiku či nástroj - Velmi zatěžuje organizaci (ale efektivně) - Relativně vysoká cena - Pracovník se v rámci projektu vyškolí a odejde

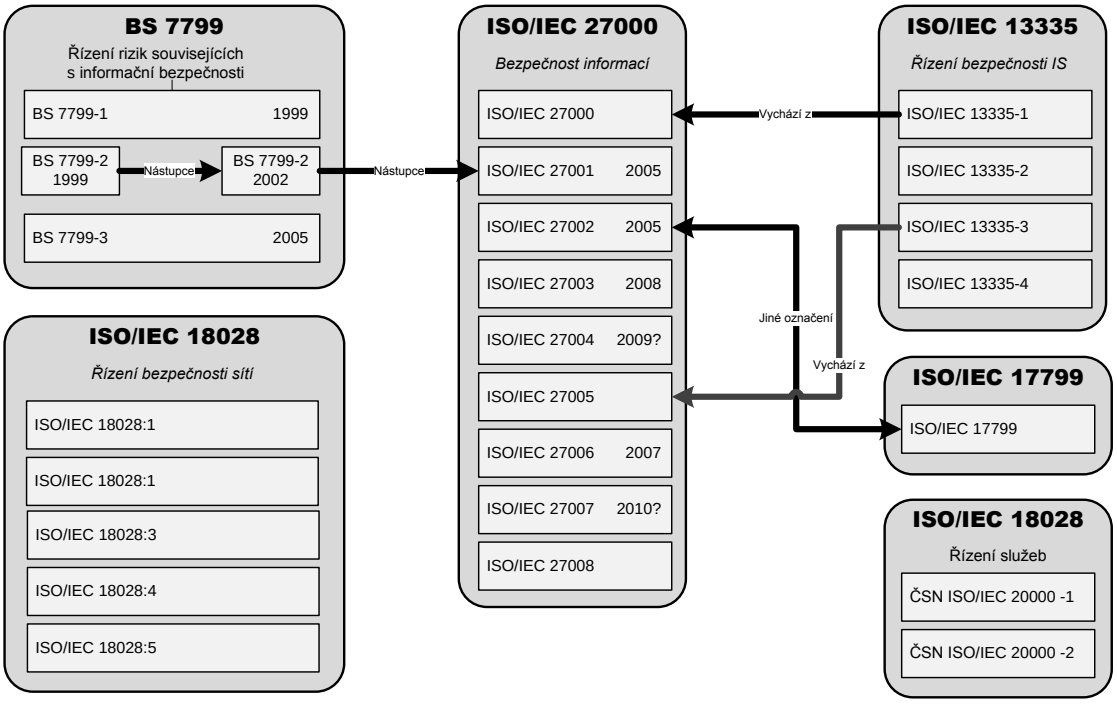
Tabulka 1- Přístupy provedení analýzy rizik IS

2. 4. Standarty bezpečnosti informačních systémů

Standarty neboli normy jsou požadavky na chování nebo vlastnosti předmětů, člověka, situace apod. Jsou buď závazně vyžadovány, či posuzovány jejich přijatelnosti nebo obvyklosti. Standardy pro bezpečnost informací jsou zaměřeny především na systémy řízení bezpečnosti informací, často označované jako ISMS (Information Safety Management System). Normy označované jako ČSN jsou k dispozici v českém jazyce.

2. 4. 1. Souhrnný přehled norem

V bezpečnosti informací se setkáváme s šesti normami, nejznámější a nejpoužívanější je však ISO/IEC 27001. Vztahy mezi normami jsou podle následujícího schématu. (2) (5)



Obrázek 3- Souhrnný přehled norem

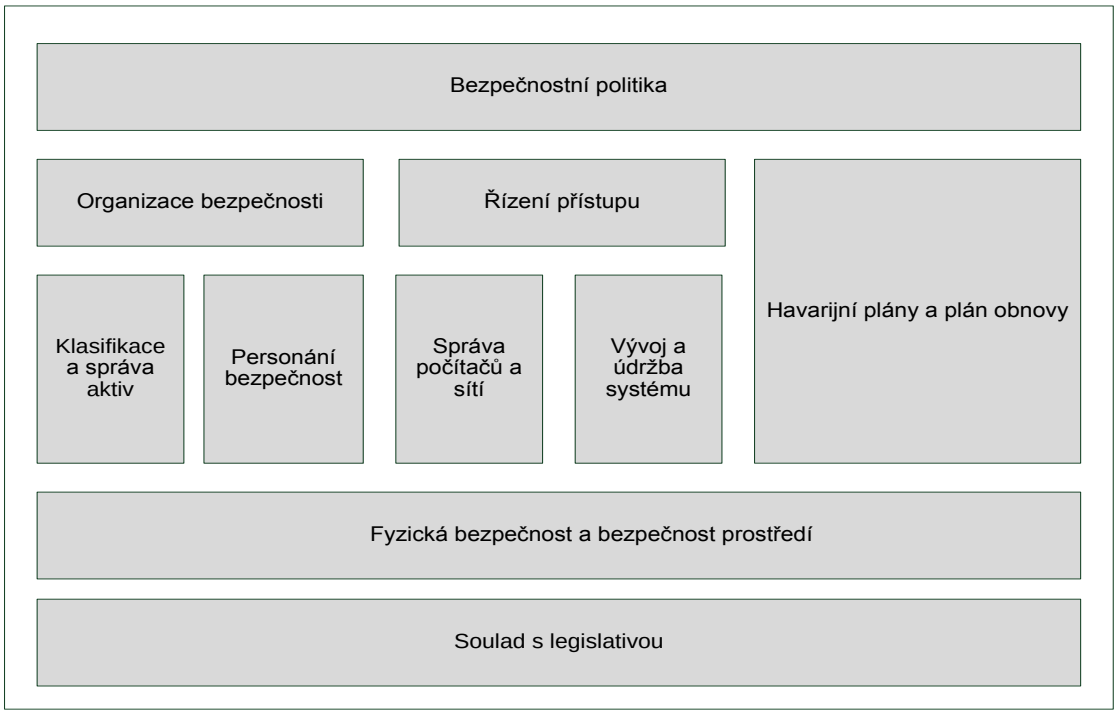
2. 4. 2. BS 7799

Standart BS 7799 je celosvětovým bezpečnostním standardem pro řízení rizik souvisejících s informační bezpečnosti. Jeho počátky se vyskytují již v roce 1995, v roce 2000 byl přijat jako standart a dnes se již nepoužívá. Byl nahrazen novějším ISO/IEC 27001.

BS 7799-1:1999 je jakýmsi katalogem bezpečnostních funkcí a bezpečnostních opatření, který definuje 127 bezpečnostních funkcí rozložených do 10 bezpečnostních zón:

- **Bezpečnostní politika** pojednává o řízení a podpoře řešení informační bezpečnosti ze strany vedení.
- **Organizace bezpečnosti** se zabývá organizačním zajištěním bezpečnosti, správou bezpečnosti v případech, kdy se k informacím dostávají osoby tzv. "třetí strany“.

- **Klasifikace a správa aktiv** určuje přidělení hodnoty určitým informacím podle síly dopadu na společnost při jejich ztrátě či nedostupnosti a o zajištění určitého stupně ochrany.
- **Personální bezpečnost** má za úkol omezení rizik od chyb lidí jako třeba zcizení nebo zneužití informace a to především díky pracovním smlouvám, směrnicím či školením.
- **Fyzická bezpečnost a bezpečnost prostředí** je fyzická ochrana zařízení, kde jsou informace uloženy.
- **Správa počítačů a sítí** jejichž cílem je:
    - Zajištění správnosti a bezpečnosti všech procesů, které přijdou do styku s informacemi
    - Minimalizace selhání systému
    - Ochrana integrity (celistvosti) dat
    - Správa integrity a dostupnosti zpracování informace
    - Bezpečnost dat v síti
    - Ochrana proti poškození, modifikaci či ztrátě dat
- **Řízení přístupu** slouží k zajištění řízeného přístupu k informaci a ochrana proti neoprávněnému přístupu.
- **Vývoj a údržba systému** určuje požadavky na bezpečnost systémů (ochrana důvěrnosti, autenticity a integrity dat při vývoji nových systémů, údržba bezpečnosti aplikací a dat).
- **Havarijní plány a plán obnovy** jsou protiopatření proti přerušení provozu podniku a kritických procesů v důsledku selhání informačního systému nebo katastrof.
- **Soulad s legislativou** a jinými bezpečnostními normami a předpisy podniku.



Obrázek 4- Schéma BS7799-1:1999

BS 7799-2:1999 je specifikací systému managementu bezpečnosti informací (ISMS). Obsahuje 6 kroků, po jejichž vykonání získáme sadu dokumentů definujících ISMS.

- Identifikace informačních aktiv.
- Definice rozsahu systému řízení informační bezpečnosti.
- Analýza rizik.
- Definice metod řízení rizik.
- Identifikace bezpečnostních kontrol.
- Sestavení kontrolního mechanismu pro správu bezpečnostního systému.

BS 7799-2:2002 je inovací předchozího standardu BS7799-2:1999. Oproti předešlé verzi obsahuje rady jak provozovat, udržovat a vylepšovat ISMS. Standart je založen na cyklu Plan – Do – Check – Act (viz. Kapitola 2. 6. 2.).

2. 4. 3. ISO/IEC 27000

V roce 2005 oznámila Mezinárodní organizace pro normalizaci (ISO) zavedla novou řadu norem týkajících se bezpečnosti informací. Normy ISO/IEC 27000, jak se nazývají, mají za úkol sjednotit doporučení, požadavky či návody, vyskytující se v různých normách. Její základ vychází z britské normy BS 7799 a z ISO/IEC 13335.

ISO/IEC 27000 je slovník a definice pravidel v oblasti ISMS. Navazují na něj další normy.

ISO/IEC 27001:2005 je základní normou používanou při certifikacích. Obsahuje požadavky na systém řízení bezpečnosti informací ISMS. Tato norma je nástupcem normy známou pod označením BS7799. Stejně jako tato norma obsahuje 4 základní fáze: Plan – Do – Check – Act (viz. Kapitola 2. 6. 2.), tj. celé schéma normy zůstává stejné.

ISO/IEC 27002 je sbírka nejlepších bezpečnostních praktik sloužících jako kontrolní seznam správnosti bezpečnosti informací. V současné době je často označována jako ISO/IEC 17799. Obsahuje 11 oddílů, které se dále dělí do 39 oddílů (číslo v závorce). Ty pak dále obsahují celkem 133 základních bezpečnostních opatření.

- Bezpečnostní politika (1)
- Organizace bezpečnosti (2)
- Klasifikace a řízení aktiv (2)
- Bezpečnost lidských zdrojů (3)
- Fyzická bezpečnost a bezpečnost prostředí (2)
- Řízení komunikací a řízení provozu (10)
- Řízení přístupu (7)
- Vývoj, údržba a rozšíření informačního systému (6)
- Zvládání bezpečnostních incidentů (2)
- Řízení kontinuity činností organizace (1)
- Soulad s požadavky (3)

Norma nepřikazuje, která opatření musí být bezpodmínečně aplikována, rozhodnutí nechá na organizaci. Vhodná opatření jsou vybírána podle výsledků analýzy rizik a jejich realizace je závislá na konkrétní situaci. Cílem není implementovat vše, co

norma popisuje, ale spíše naplnit všechny aplikovatelné cíle opatření. Norma je proto široce aplikovatelná a dává uživatelům volnost při implementaci.

ISO/IEC 27003 obsahuje návod k uskutečnění ISMS.

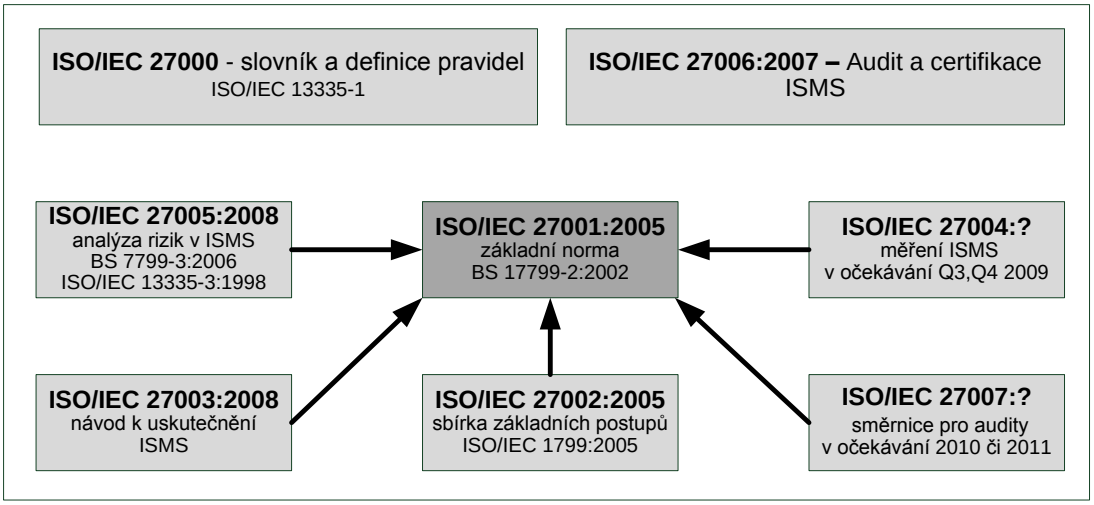
ISO/IEC 27004 popisuje management měření a metrik v ISMS. Poskytuje návod, jak uplatňovat metody měření, vhodné ukazatele (metriky) při implementaci.

ISO/IEC 27005 je norma, která popisuje principy analýzy rizik v ISMS.

ISO/IEC 27006 obsahuje požadavky na subjekty poskytující audit a certifikaci ISMS.

ISO/IEC 27007 je zatím neschválenou normou, která bude pojednávat o doporučení k provádění auditů ISMS podle ISO/IEC 27001.

ISO/IEC 27008 zatím také není schválenou normou. V platnost vejde v roce 2011 a bude obsahovat doporučení pro auditory, kteří kontrolují implementovaná ISMS opatření vycházejících z ISO/IEC 27002. (2) (5) (6) (7) (8) (9)



Obrázek 5- Vztahy mezi normami ISO/IEC 2700x

2. 4. 4. ČSN ISO/IEC TR 13335

Normy kategorie ČSN ISO/IEC TR 13335 jsou směrnicemi pro řízení bezpečnosti informačních systémů. Skládá ze čtyř základních částí:

ČSN ISO/IEC TR 13335-1 (Pojetí a modely bezpečnosti IT) popisuje pojmy a modely používané pro řízení bezpečnosti informačních systémů. Tato část je určena pro

členy bezpečnostní rady a pracovníky, zodpovídající se za bezpečnost informačního systému.

ČSN ISO/IEC TR 13335-2 (Řízení a plánování bezpečnosti IT) popisuje řídící a plánovací aspekty informačních technologií. Skládá se ze dvou částí, první určuje jednotlivé analýzy a přístupy k nim, druhá definuje role a zodpovědnosti jednotlivých pracovníků. Další oblasti, kterými se zabývá, jsou plánování bezpečnosti, zavádění nových bezpečnostních opatření, údržby, monitorování, kontroly plnění a řešení incidentů

ČSN ISO/IEC TR 13335-3 (Techniky pro řízení bezpečnosti IT) charakterizuje nejdůležitější bezpečnostní techniky a uvádí jejich strukturu a kategorizaci. Důležitým bodem je i definice samotné analýzy rizik včetně postupů a strategií k jejímu provedení. Tato část je určena pracovníkům, kteří mají na starosti plánování, návrhy, implementace, testování, pořizování a provoz systémů IT z hlediska jejich bezpečnosti.

ČSN ISO/IEC TR 13335-4 (Výběr bezpečnostních opatření) obsahuje doporučení pro výběr bezpečnostních protiopatření dle specifických potřeb organizace. (2) (5)

2.4.5. ČSN ISO/IEC 20000

ČSN ISO/IEC 20000 je normou zabývající se požadavky a řízením služeb. Jejím úkolem je zlepšování kvality, zvyšování efektivity a snížení nákladů u IT procesů. Skládá se ze dvou částí:

ČSN ISO/IEC 20000 -1 Informační technologie - Management služeb – část 1: Specifikace

ČSN ISO/IEC 20000 -2 Informační technologie - Management služeb – část 2: Soubor postupů (9)

2. 4. 6. ISO/IEC 18028

Norma zabývající se řízením bezpečnosti sítí. Skládá se ze dvou částí:

ISO/IEC 18028:1 – Řízení bezpečnosti sítí.

ISO/IEC 18028:2 – Architektura bezpečnosti sítí.

ISO/IEC 18028:3 – Bezpečná komunikace mezi sítěmi za použití bezpečnostních brán.

ISO/IEC 18028:4 – Bezpečný vzdálený přístup.

ISO/IEC 18028:5 – Bezpečná komunikace mezi sítěmi za použití virtuálních privátních sítí. (9)

2.4.7. ISO/IEC 27033

Tato norma vzešla z předchozí verze ISO/IEC 18028 a zabývá se doporučeními a implementací protiopatření, vztahujícími se k bezpečnosti sítí. Obsahuje 7 částí:

ISO/IEC 27033-1 - Celkový přehled principů a přístupů ostatních norem sady.

ISO/IEC 27033-2 - Bezpečnostní architekturu sítí.

ISO/IEC 27033-3 - Definuje rizika, techniky návrhu a řešení problému spjatých se správou sítí.

ISO/IEC 27033-4 - Definuje rizika, techniky návrhu a řešení problémů spjatých se zabezpečením datových toků mezi sítěmi.

ISO/IEC 27033-5 - Definuje rizika, techniky návrhu a řešení problémů spjatých se spojením pomocí VPN.

ISO/IEC 27033-6 - Zabezpečení IP konvergence.

ISO/IEC 27033-7 - Definuje rizika, techniky návrhu a řešení problémů spjatých se zabezpečením bezdrátových sítí. Zatím je tato norma ve vývoji. (7)

2. 4 8. Legislativa v České Republice

Normy jsou dále pozměněny pomocí zákonů. V České Republice jsou to právní normy připravené vládou ČR. Jedná se o tyto normy:

Zákon č. 148/1998 Sb. – Zákon o ochraně utajovaných skutečností (Dnes již z tohoto zákona téměř nic nezůstalo a byl nahrazen několika novými zákony.)

Zákon č. 227/2000 Sb. - Zákon o elektronickém podpisu

Zákon č. 365/2000 Sb. – Zákon o informačních systémech veřejné správy

Zákon č. 101/2000 Sb. - Zákon o ochraně osobních údajů

Zákon č. 480/2004 Sb. - Zákon o některých službách informační společnosti

Všechny zákony jsou k dispozici ke stažení na Portálu veřejné správy České Republiky na www.portal.gov.cz .

2. 5. Použití analýzy rizik

Analýzu rizik lze použít na jakýkoliv informační systém. Nejčastěji se používá v následujících případech:

- Zjištění aktuálního stavu bezpečnosti informačního systému
- Zavádění systému řízení informační bezpečnosti (ISMS) dle normy ISO/IEC 27001
- Restrukturalizace společnosti
- Pro uspokojení požadavků auditorských firem
- Před zavedením bezpečnostních protiopatření
- Legislativní důvody
- Pochyby o bezpečnosti informací (nedůvěra ve správce, administrátora či ostatní uživatele systému) (10)

2. 6. Standarty ISMS

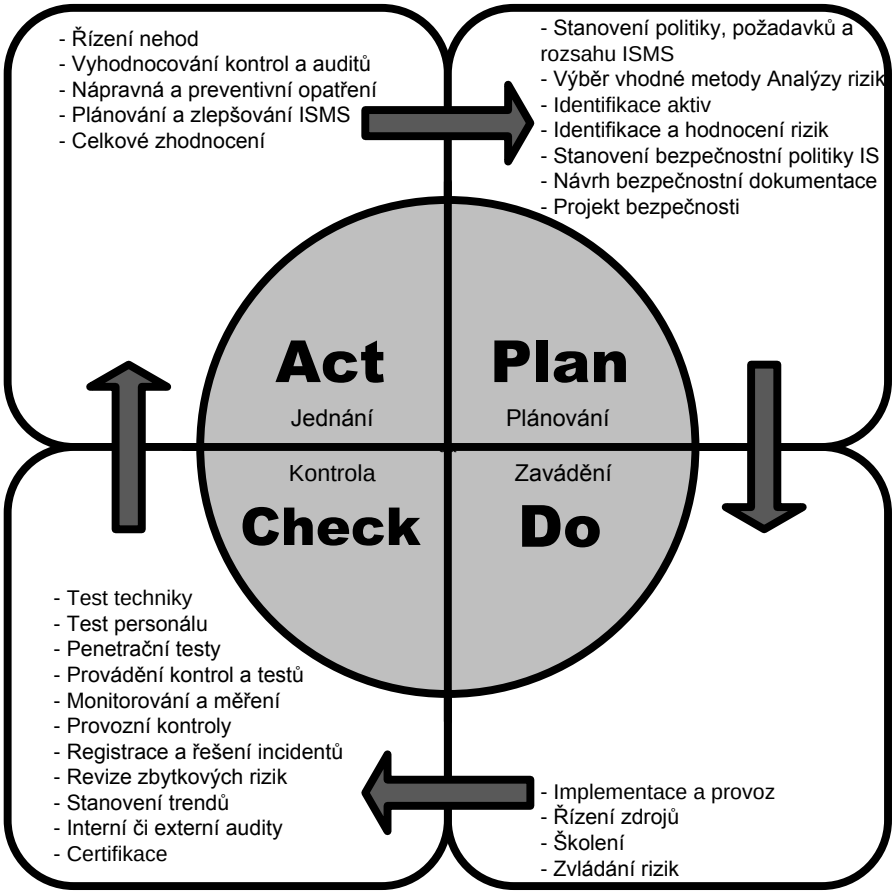
ISMS je nejčastěji používaným systémem pro řízení bezpečnosti informací. Dalšími známými systémy jsou ITIL či COBIT.

2. 6. 1. ISMS - Systém řízení bezpečnosti Informací

Systém řízení bezpečnosti informací neboli ISMS (Information Security Management System) je způsob, jak zajistit a regulovat bezpečnost informací a integrovat ji do stávajícího systému řízení organizace. ISMS je založený na mezinárodních normách ISO/IEC 27001, ISO/IEC 17799 (ISO/IEC 27002), ISO/IEC TR 13335, ISO/IEC 9001 (Systém řízení kvality) a několika dalších. Vlastní implementace systému se provádí pomocí postupu PDCA (Plánuj – Dělej - Kontroluj – Jednej, viz bod 2. 4. 3.). ISMS je otázkou na odpověď jak řídit bezpečnost informací. (11)

2. 6. 2. PDCA

PDCA je zkratkou 4 anglických slov (Plan-Do-Check-Act), podle kterých se řídí normy ISO/IEC 27001 a BS 7799‑2.



Obrázek 6- Schéma PDCA

2. 6. 3. PDCA – Plánování (plan)

Proces plánování se skládá z těchto kroků:

- Vyhotovení studie proveditelnosti zavedení ISMS je studie upozorňující na nejvýraznější nedostatky a poskytující souhrnný náhled na stav informační bezpečnosti organizace. Postup se skládá z:
    - Definování rozsahu působnosti informační bezpečnosti
    - Definování interních omezení (směrnice)
    - Definování externích omezení (legislativa, normy)

        - Zpracování získaných informací
        - Vypracování analýzy rizik
    - Zpracování bezpečnostní politiky definuje odpovědnosti, organizaci a řízení bezpečnosti, řízení aktiv, personální bezpečnost, fyzickou bezpečnost, bezpečnost prostředí, řízení komunikací a provozu, řízení přístupu, pořízení, vývoj a údržba informačních systémů, správa incidentů informační bezpečnosti, řízení kontinuity činností organizace a soulad s požadavky
    - Vypracování bezpečnostního projektu a výběr vhodných opatření
    - Zpracování bezpečnostní dokumentace jako například metodické pokyny, bezpečnostní příručky, směrnice, havarijní plány, plány zálohování a obnovy apod. (12)

2. 6. 4. PDCA – Zavádění (Do)

Ve fázi, kdy již máme vše naplánováno, přistoupíme k vlastnímu zavádění, například formou konzultací nebo realizací jednotlivých opatření. V této etapě se vytváří plán zvládání rizik, zavádějí doporučená opatření, zavádí se program zvyšování bezpečnostního povědomí, řízení dostupných zdrojů a řízení provozu. (12)

2. 6. 5. PDCA – Kontrola (Check)

V této etapě se provádí detekce bezpečnostních konfliktů a sledování účinnosti opatření, posuzování účinnosti opatření, revize zbytkových a akceptovaných rizik, provádění interních auditů, registrování událostí s dopadem na účinnost a efektivnost opatření informační bezpečnosti. (12)

2. 6. 6. PDCA - Jednání (Act)

Jednání je poslední etapou cyklu informační bezpečnosti. Jejím cílem je celkové zhodnocení výsledků informační bezpečnosti a vytyčení dalších cílů pro následující etapu. (12)

2. 6. 7. Úrovně zavedení ISMS

Dle společnosti Risk Analysis Consultants rozeznáváme 7 druhů úrovní bezpečnosti. (15)

Úroveň ISMS	Bezpečnost informací	Implementace provozu ISM	Rozsah bezpečnostní dokumentace
Re-certifikovaný ISMS	- Dlouhodobě řízena dle BS 7799-2	- Opakovaná certifikace - Opakovaná aktualizace opatření a dokumentace	- Pravidelná aktualizace dokumentace podle výsledků analýzy rizik
Certifikovaný ISMS	- Prokazatelně řízena dle norem BS 7799-2	- Organizace je certifikována ISMS - Realizace pre-certifikačního auditu a realizace chybějících opatření	- Zpráva o výsledcích pre-certifikačního auditu - Plán řízení zdrojů ISMS - Dokumentace ISMS - Zpráva o certifikaci - Certifikát ISMS dle BS 7799-2:2002
Implementovaný ISMS	- Bezpečnost informací je řízena a zlepšována. - Rizika jsou zvládána.	- Implementován a provozován ISMS dle normy ISO/IEC 17799:2000 - Rozsah ISMS, jeho řízení a procesy jsou definovány. - Jsou identifikována a zvládána všechna rizika a zavedena patřičná opatření. - Bezpečnostní dokumentace pokrývá všechny oblasti ISMS	- Plán zvládání rizik. - Prohlášeni o aplikovatelnosti opatření. - Základní dokumentace ISMS. - Záznamy o provozu, využívání a zlepšování ISMS. - Evidence bezpečnostních incidentů a následných reakcí a opatření. - Výsledky auditu a evidence nalezených neshod, nápravných a preventivních opatření.
Částečně implementovaný ISMS	- Koncepce bezpečnosti a plán zavedení ISMS jsou neúplné	- Je přijata koncepce bezpečnosti - Byla provedena analýza rizik a návrh opatření. - ISMS není řádně zdokumentován - Není prováděn audit ISMS	- Zpráva o aktivech a dopadech. - Zpráva o analýze rizik. - Návrh opatření a implementační plán, případně - Nekompletní ISMS - Dílčí projekty/plány implementace prioritních opatření.
Plánovaný ISMS	- Zavedení ISMS je ve fázi příprav a plánování	- Je přijata koncepce řízení bezpečnosti - Je vytvořen rámcový plán ISMS a případně delegován rozpočet na bezpečnost	- Strategie bezpečnosti. - Bezpečnostní politika informací. - Program zvyšování bezpečnostního povědomí. - Výsledky přehledové analýzy rizik. - Plán implementace ISMS a zvládání rizik
Ad-hoc ISM	- ISMS bez znalosti a zvládání bezpečnostních rizik	- Neexistuje systematická koncepce bezpečnosti - Částečné bezpečnostní povědomí některých pracovníků. - Zavedeny vybrané dílčí opatření a procesy	- Neexistuje řízená systematická bezpečnostní dokumentace. - Pouze dílčí interní dokumentace pokrývající určité oblasti nebo systémy. - Možný výskyt neprovázané dodavatelské dokumentace některých systémů
Nezavedený ISM	- Neprobíhá ISMS	- Neexistuje žádné bezpečnostní povědomí, řízení ani koncepce.	- Interní bezpečnostní dokumentace v oblasti bezpečnosti informací neexistuje.

Tabulka 2- Úrovně zavedení ISMS

2. 6. 8. COBIT

COBIT (Control Objectives for Information and related Technology) je univerzální metodika pro řízení bezpečnosti informací, vyvinutá americkou společností ISACA . COBIT je určen pro všechny, kdo nesou odpovědnost za spolehlivost informačních technologií, či těm, kdo poskytují služby v oblasti řízení kvality, kontroly a správy informačních technologií. Dle firmy Equica, specializující se na tuto metodu u nás, jsou základní myšlenky tyto:

- Cíle podnikové informatiky musí mít vazbu na cíle podniku. Jinými slovy informatika musí podporovat podnikové cíle.
- Informatika musí vytvářet přidanou hodnotu.
- Musí existovat systém řízení, který umožní minimalizovat rizika spojená s podnikovým IT.
- Systém řízení musí zaručovat šetrné nakládání s IT zdroji.
- Systém řízení informatiky by měl mít zabudován systém měření výkonnosti.

V současné době je aktuální ve verzi COBIT 4. 1. (14) (15)

2. 6. 9. ITIL

ITIL (Information Technology Infrastructure Library) vznikl jako veřejně dostupný rámec popisující způsoby řízení IT služeb. Je to knihovna spravovaná Office of Government Conference. Je to několik publikacích vycházejících z nejlepších praktických zkušeností, šířících se pomocí: knih, médií se softwarovými nástroji, školení, konzultace a certifikace. Součástí ITIL je těchto 5 základních knih:

- Podnikatelský pohled (Business Perspectives)
- Správa aplikací IT (Application Management)
- Dodávka IT služeb (IT Services Delivery)
- Podpora IT služeb (IT Services Support)
- Správa IT infrastruktury (IT Infrastructure Management)
- Řízení IT projektů (IT Project Management)

Dle brožury ze serveru www.itsmf.cz popisujících ITIL jsou největšími výhodami:

- Zvýšená spokojenost uživatelů a zákazníků se službami IT
- Zlepšená dostupnost služeb, což vede ke zvýšení zisků a obratu bussinesu
- Finanční úspory ze snížení opakovaných prací, ztraceného času, zlepšené správy a využití zdrojů
- Zkrácení času pro uvedení nových produktů a služeb na trh
- Zlepšení podkladů pro rozhodování a optimalizace rizik.

Aktuální vydání ITIL je již třetí verzí. (16)

2. 7. Místo analýzy rizik v systému řízení bezpečnosti ISMS

Pro správné fungování společnosti je třeba postupovat podle pravidel ISMS(systém řízení bezpečnosti informací) a to i u menších firem. ISMS nám pomáhá udržet informační systém ve funkčním, bezpečném stavu a zároveň splňuje všechny současné používané normy v oblasti bezpečnosti informací. Analýza rizik je nástroj, určený pro zhodnocení stavu bezpečnosti informací. Díky analýze získáme přehled o potenciálních nebezpečích, hrozbách či slabinách a navrhne vhodná opatření, aby jim bylo možné pro příště předcházet. Analýza rizik je tedy nezbytnou součástí ISMS a její provedení je nezbytně nutné v případě, že chceme získat certifikaci ISMS.

3. Metody analýzy rizik

Při vytváření analýzy rizik si můžeme zvolit komerční metodu s cenou již od 10 000Kč za základní verzi, nebo vybrat profesionální verzi programu za cenu i větší než 50 000 Kč, či si vymyslet vlastní metodu. Ta má tu výhodu, že je stavěna přímo pro naše potřeby. Nejznámějšími komerčními metodami jsou CRAMM, DELPHI a různé metody RISK.

3. 1. Komerční metody

3. 1. 1. CRAMM

CRAMM (CCTA Risk Analysis and Management Methodology) je dnes asi nejpoužívanější metoda, umožňující podle seznamu hrozeb a zranitelností zpracovat analýzu rizik a dále spravovat protiopatření, implementaci a audit. CRAMM byl původně vyvíjen britskou vládou, později byl uvolněn i pro komerční použití. Nejběžnějšími verzemi jsou CRAMM Express (výsledek během jednoho dne) a CRAMM Expert. V současné době se používá CRAMM verze 5.1 a je provozována i v českém jazyce.

Výhody metody CRAMM jsou:

- Rychlost provedení
- Určení přesné hodnoty dat v systému
- Stanovení nejrizikovějších částí systému
- Navržení protiopatření pro snížení rizik
- Certifikace podle bezpečnostní normy ISO/IEC 27001

CRAMM se nejčastěji používá pro:

- Zjištění vlivu nedostupnosti, prozrazení nebo modifikace dat na chod společnosti
- Jaké hrozby ohrožují systém
- Jaké má náš systém slabiny
- Výběr vhodné úrovně bezpečnosti tak aby byla levná a efektivní

- Výběr úrovně autentizace (ověřování pravosti)
- Výběr vhodných kryptografických služeb (šifrování)
- Fyzická bezpečnost zařízení
- Tvorba bezpečnostní dokumentace
- Expresní (analýza je hotová do 3 hodin) či detailní analýzy (doba několika měsíců) (7)

3. 1. 2. Cobra

COBRA je metodikou využívající expertní systém. Konzultant identifikuje hrozby, určí rizika a systém vypracuje návrh možných řešení. Cena programu se pohybuje od $ 1000 do $ 2000. (18)

3. 1. 3. Delphi

Metoda účelových interview, dotazníků neboli Delphi spočívá v řízeném kontakty mezi hodnotiteli a příslušníky hodnoceného subjektu. Metoda využívá souboru otázek, prodiskutovaných na pohovorech. První část je vždy stejná, druhá je variabilní a odvíjí se tedy podle předchozích odpovědí respondenta. Metoda Delphi je jednoduchá na provedení i na čas, neobsahuje bohužel přesné finanční vyjádření. Metoda určuje, co se může stát a za jakých podmínek. (1)

3. 1. 4. OCTAVE

Metoda Octave ® je sada nástrojů, technik a metod pro hodnocení a plánování bezpečnosti informací. Existují 3 základní metody Octave.

Standardní metoda OCTAVE je původní metodou, která tvoří základ následujících dvou metod. Je určena především pro velké organizace nad 300 pracovníků, avšak velikost není rozhodující. Obsahuje tři základní kroky:

- Identifikace a ohrožení jednotlivých kritických aktiv
- Identifikace zranitelností (organizačních, technologických)
- Strategie snižování rizik

OCTAVE-S je metodou určenou pro menší organizace do 100 osob, kterou provádí 3-5 lidí.

OCTAVE-Allegro je metodou vhodnou pro jednotlivce či velice malé skupiny osob. Skládá se ze 4 kroků:

- Odhad rizika a stanovení cílů
- Kontrola kritických informačních aktiv, stanovení hranic pro aktiva a identifikace bezpečnostních požadavků
- Identifikace hrozby pro každé aktivum
- Identifikace a analýza rizika (17)

3. 1. 5. Metoda RA2

RA2 neboli „Art of risk“ je nástroj vyvinutý společností AEXIS Security Consultants založený na standardech ISO/IEC 17799 a ISO/IEC 27001. RA2 není jen pouhým nástrojem, je to již hotový software, který nám pomáhá vedení organizace krok za krokem k navržení a implementaci systému managementu bezpečnosti informací.

RA2 zahrnuje:

- Vymezení rozsahu, politiky a cílů ISMS
- Vytvoření evidence aktiv
- Uskutečnění analýzy rizik
- Hodnocení rizik a zvážení vhodných opatření pro zvládání rizik
- Výběr systému kontrol a opatření
- Vytvoření dokumentace požadované v rámci ISMS (18)

3. 1. 6. @RISK

Metodika @RISK využívá k analýze rizik simulačních metod Monte Carlo. Typickou vlastností této metodiky je zpracování výsledků ve formě tabulek. Nejisté hodnoty jsou vyjádřeny v rozsahu možných hodnot. Nejdůležitějším faktorem této metody je návrh modelu, přičemž vytvořený model definuje danou situaci systému formou tabulek. (1)

3. 1. 7. RiskPAC

Metodika RiskPAC je systém, který nám zjednodušuje provádění analýzy rizik pomocí jednoduchých dotazníků. Uživatel vyplňuje právě tyto dotazníky a systém je

poté vyhodnocuje. Jedná o automatizaci stanovení jednotlivých rizik, podle odpovědí na dotazníky, nikoliv o expertní systém. (1)

3. 1. 8. RiskWatch

RiskWatch je software, který umožňuje metodický soubor pro zjištění, simulaci a následnou změnu parametrů jednotlivých rizik systému. Metoda je založena na vytvoření modelu, vytvořenému díky získaným datům, popřípadě simulační metodě Monte Carlo. Oba přístupy lze vhodně kombinovat a doplňovat. Jde o automatizaci zpracování výsledků, získaných na základě souborů otázek, strukturovaných podle definovaných bezpečnostních oblastí. (1)

3. 2. Vlastní metoda

Poslední možností, je vytvoření si vlastní metody. Tato metoda je velice vhodná v tom, že je připravena na přímo na míru dané situaci. Můžeme se inspirovat přímo jednou z již existujících metod, či si vytvořit metodu na míru dle uznávaných norem – nejčastěji to bývá norma ISO/IEC 17799 definující implementaci ISMS založené na bázi modelu PDCA.

4. Analýza rizik IS STAG

Hlavním cílem mé bakalářské práce je zpracování analýzy rizik pro informační systém STAG, který je využíván jako systém studijní agendy Jihočeské Univerzity. A právě o vypracování analýzy rizik bude tato kapitola.

Systém vznikl v Centru Informatizace a výpočetní techniky na Západočeské univerzitě v Plzni a to v roce 1993. O 6 let později, v roce 1999 byl systém poprvé použit i na Jihočeské Univerzitě. Nyní v roce 2009 je systém dostupný ve třetí verzi, která byla nasazena do ostrého provozu začátkem září. Kromě JČU a ZČU je používán na dalších 14 univerzitách a vysokých školách.

4.1 Popis IS STAG

IS STAG (**I**nformační **S**ystém **ST**udijní **AG**endy) je informační systém uchovávající informace o studentech a jejich studiu, přesněji řečeno obsahuje data o jednotlivých uživatelích (studenti a učitelé), předmětech (zkoušky, zápis). V kompletní verzi by obsahoval i informace o učebnách včetně rozvrhu, na Jihočeské Univerzitě však tato část není zprovozněna.

4. 1. 1. Přístupy k systému

K informačnímu systému lze přistupovat třemi způsoby:

- **Nativní klient** – Jde o program, který je nainstalován na PC pracující pod operačním systémem Microsoft Windows. Program používají uživatelé, používající složitější funkce, tedy například studijní referentky či sekretářky na katedrách. Tomuto programu se také často říká tlustý klient pro jeho nespočet funkcí. Aktualizace tohoto programu probíhá každý den, kdy si každá klientská aplikace stahuje aktualizaci ze serveru umístěného přímo na Jihočeské Univerzitě. Tento server získává aktualizace přímo z Plzně.
- **Webový klient** – Poskytuje základní funkce pro studenty a vyučující. Výhodou je, že je dostupné odkudkoliv na adrese

http://www.jcu.cz/education/stag. Klient obsahuje na 150 obrazovek a 120 tiskových sestav.

- **Webové služby** – Webové služby jsou rozhraní určené pro napojování na jiné informační systémy.

K systému lze přistupovat bez zadání hesla, kdy jsou dostupné základní informace o studijních programech, předmětech či katedrách. Při přihlášení pomocí hesla získá uživatel přístup ke všem částem systému, ke kterým má povolený přístup. IS STAG může definovat kolem 20 druhů uživatelských účtů. Jejich detailní popis včetně seznamu všech povolených funkcí je k dispozici v manuálu STAGu. Na JČU se používají pouze tyto typy účtů:

- **Administrátor** (přístup ke všem funkcím systému bez omezení)
- **Fakulta** (studijní plány, studijní programy, studijní obor, přijímací obor, informace o jednotlivých předmětech)
- **Katedra** (přístup k zadávání známek, k vypisování termínů zkoušek, diplomové práce a státnice)
- **Student** (předzápis, zapisování na zkoušky a výpisu informací o svém studiu)
- **Studijní referentka** (informace týkající se studentů, včetně osobních údajů)
- **Tajemník fakulty** (na JČU zastává tuto funkci proděkan, který má přístup ke všem funkcím systému s výjimkou rozvrhových a systémových funkcí)
- **Vyučující** (editace přiděleného předmětu, vypisování termínů zkoušek a zadávání známek)

Přihlašování do sítě je autorizováno pomocí dvou údajů. U studentů jimi jsou osobní číslo studenta, které je uvedené na první stránce v indexu (popřípadě jej lze zjistit na http://www.jcu.cz/education/stag/search_stag_num po zadání jména studenta) a heslo. To je v defaultním nastavení ve tvaru x a rodné číslo bez lomítka. Toto heslo se však dá velice lehce zjistit, například po vyžádání rodného čísla či ztrátě občanského průkazu studenta. Je nezbytné, aby si každý student změnil heslo na silnější (hůře prolomitelné). Nejvhodnější je kombinace velkých a malých písmen + čísla + nějaký speciální znak (ěščřžýáí@#$%^&…). Bezpečné heslo by mělo mít minimálně 8 znaků.

Více o vytváření silných hesel na http://www.microsoft.com/cze/athome/security/privacy/password.mspx.

- **Uživatelské jméno** – „P061111“ znamená P jako Pedagogická fakulta, 6 jako nástup v roce 2006 a 1111 znamená pořadové číslo studenta v daném roce.
- **Heslo** – x8612134567 v pro studenta s rodným číslem 861213/4567.

4. 1. 2. data v informačním systému STAG

IS STAG je nejdůležitějším systémem, fungujícím na univerzitě. Není však jediný. Na univerzitě souběžně běží desítky dalších systému, s některými z nich je STAG dokonce vzájemně provázán. Jde například následující systémy:

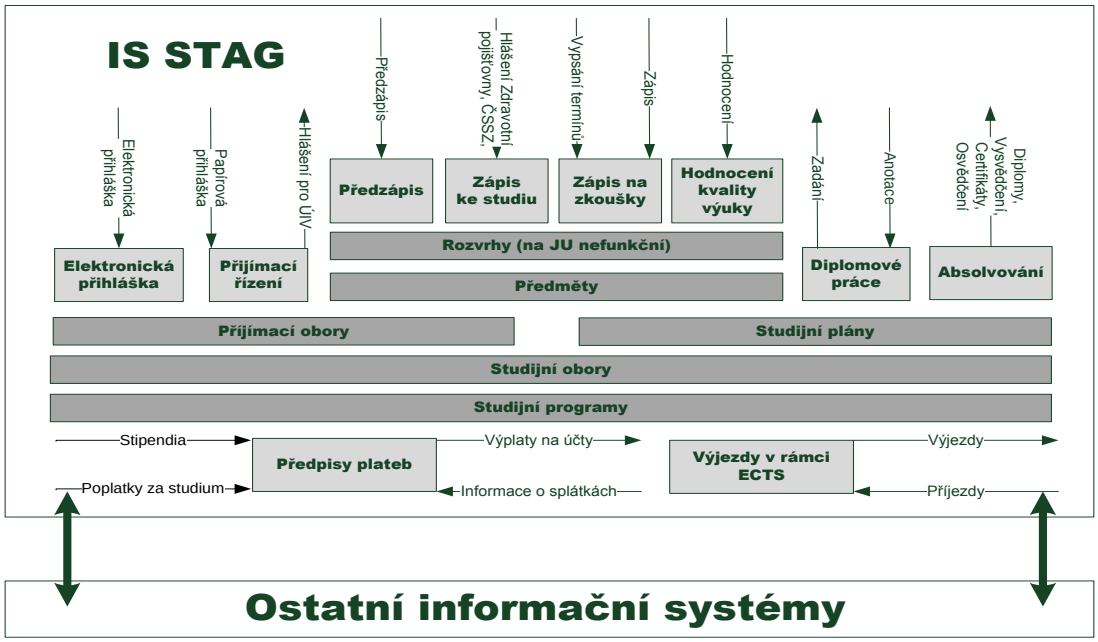
- **Systém FIS** - finance, účetnictví, majetek…
- **IPS** - identifikační a přístupový systém
- **IDM** - Správa uživatelských účtů na JU
- **Knihovní systém**
- **Menzovní systém**
- **Store.jcu.cz** - sdílený diskový prostor
- **SafeQ** - tiskové a kopírovací služby
- **Výukové systémy** – eamos, moodle…
- **Webové portály** JU
- **WiFi a eduroam** - bezdrátová síť na JU

Samotný informační systém STAG uchovává obrovské množství informací. Zde je jejich seznam některých z nich:

- **Evidence studenta** - osobní údaje, průběh studia
- **Předměty** - sylabus, vazby na podmiňující předměty, vylučující předměty, kapacita předmětu
- **Studijní programy** - vazba na studijní obory, kombinace studijních oborů, návaznost studijních programů
- **Studijní plány** - vazba na bloky předmětů
- **Rozvrh** - kolize, vyhledávání – na JU v současnosti nefunkční
- **Předzápis studentů** - individuální studijní plán pro každého studenta

- **Známky** - zapsání známek učiteli či katedrami
- **Zkoušky** - výpis termínů a zapisování se na ně
- **Podklady pro zápis** - splnění podmínek studia
- **Tiskové sestavy** - zahajovací výkaz, matrika studentů, výpis pro pojišťovny…
- **Výměna dat s kolejním systémem** - evidence ubytování
- **Přijímací řízení** - evidence uchazečů, nastavení parametrů pro přijetí, automatické vyhodnocení přijetí, korespondence
- **Elektronická přihláška ke studiu**
- **Absolvent** - evidence absolventů, zadání diplomové práce, vystavení dokladů ke státní závěrečné zkoušce, vysvědčení, certifikáty…
- **Výstup diplomových prací do knihovního systému**
- **Vizualizace studijního plánu** - obecně či konkrétního studenta
- **Program předmětu** - průběh semestru, požadavky k zápočtu či zkoušce

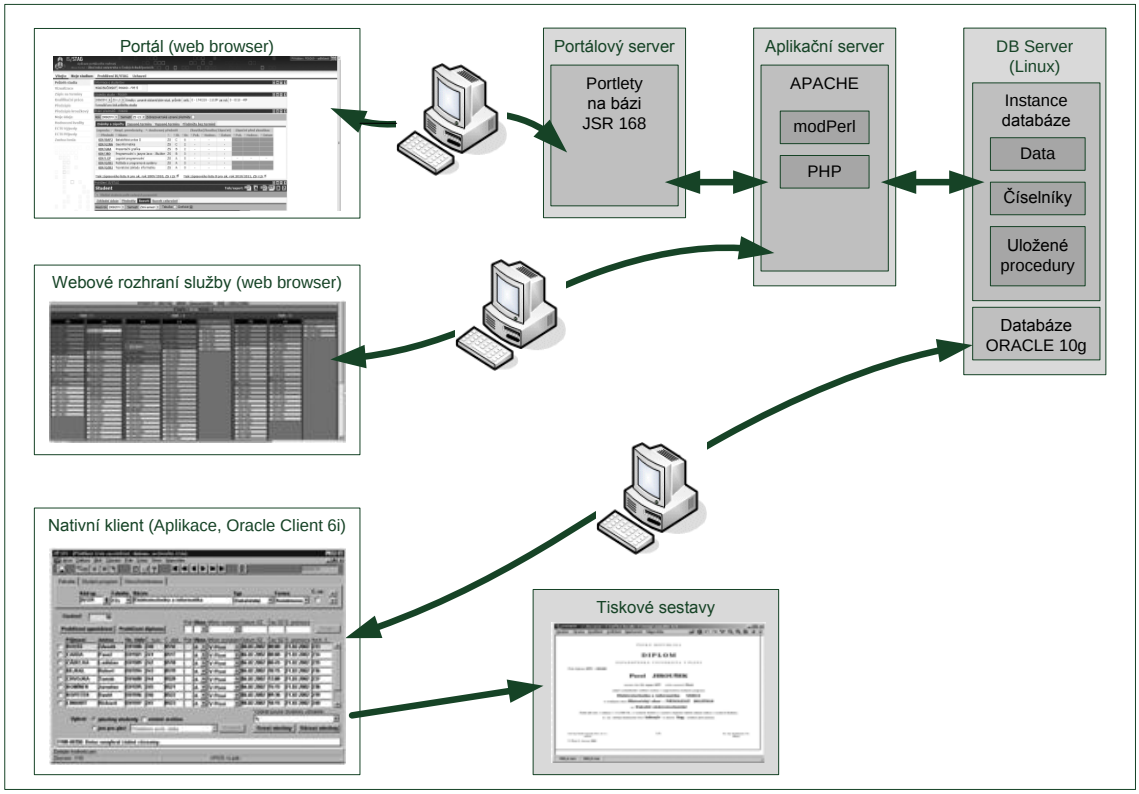
STAG tedy obsahuje například tyto informace. Systém se skládá ze samotného jádra programu, na které jsou napojeny návazné moduly. Jak celý systém funguje lze vidět na následujícím obrázku. (22)



Obrázek 7- Moduly informačního systému STAG

4. 1. 3. Technická specifikace serveru

Přesné informace o hardwaru, na kterém informační systém STAG na Jihočeské univerzitě nejsou k dispozici. Dle popisu systému ze Západočeské univerzity vše funguje podle následujícího schématu:



Obrázek 8- Schéma sítě a přístupu klientů

Jihočeská univerzita disponuje databázovým serverem s čtyřjádrovým procesorem 2,56 GHz, 64 GB RAM a několika terabajtovým polem (databáze obsahuje cca 1 TB dat). Na serveru běží dohromady asi 10 databází. Aplikační server běží na virtuálním stroji VMware pracujícím se 4 GB RAM. (22)

4.2 Návrh našeho postupu

Analýza rizik informačního systému STAG bude vypracována vlastním postupem, přizpůsobeným naším potřebám. Celý postup se bude skládat ze tří částí: vypracováním dotazníků, vyplnění dotazníků a zhodnocení dotazníků. Dotazníky musí být vypracovány v souladu s normami bezpečnosti podle standartu ISO/IEC 17799 a ISO/IEC 27001.

4. 2. 1. Postup analýzy rizik

Jako postup analýzy rizik byla zvolena standardní analýza rizik skládající se ze 4 částí: identifikace a stanovení hodnoty aktiv, identifikaci a ohodnocení hrozeb, identifikace zranitelností a návrh vhodných bezpečnostních protiopatření.

Pro zjištění odpovědí na tyto byly vytvořeny dva dotazníky. První dotazník byl určen pro správce systému a obsahoval otázky na zjištění hrozeb a zranitelností systému. Druhý dotazníček, určený pro běžné uživatele systému byl zaměřen na aktiva a jejich hodnoty.

První dotazník byl vytvořen pro správce sítě a následně odevzdán Ing. Janu Volfovi z Centra informačních technologií, který má IS STAG na starosti. Vyplnění dotazníku jako celku mi bylo nakonec zamítnuto manažerkou informační bezpečnosti paní Ing. J. Kolářovou a to z důvodu, že se jedná o příliš citlivé informace. Dále bylo tedy vycházeno bez těchto důležitých dat.

Druhý dotazník byl určen pro běžné uživatele, který měl za cíl identifikaci a ohodnocení jednotlivých aktiv byl rovněž vytvořen. Dotazník byl zaměřen na nejčastější možné problémy, se kterými se uživatelé mohou setkat: nedostupnost dat, zničení dat, prozrazení dat, modifikace dat, osobní bezpečnost, ochrana osobních údajů a zákonné povinnosti. Otázky byly vybrány tak, aby bylo možné dotazník použít pro široké spektrum uživatelů. Otázky byly následně položeny těmto uživatelům sítě:

- Sekretářka katedry (1x)
- Studijní referentka (1x)
- Oddělení IS STAGu a stipendií (1x)

- Vyučující (3x)
- Studenti (15x)

Výsledky všech otázek lze nalézt mezi přílohami. Dle těchto otázek byla identifikována aktiva, která jsou uvedena v následující kapitole věnované již samotné analýze rizik. Cena těchto aktiv byla vyhodnocena podle vodítek, která se zaměřují na jejich ztrátu, která by vznikla v případě nedostupnosti, prozrazení, modifikace či ztráty těchto aktiv.

Aktiva	**Integrita**	**Důvěrnost**	**Dostupnost**	**Hodnota aktiva**
Název aktiva	Hodnota aktiva z pohledu integrity	Hodnota aktiva z pohledu důvěrnosti	Hodnota aktiva z pohledu dostupnosti	Výsledná hodnota aktiva
…				
…				
				Nejvyšší hodnota aktiva

Tabulka 3 – Metodika (tabulka hodnoty aktiv)

Po vytipování nejhodnotnějších aktiv je potřeba dle vlastního odhadu vybrat hrozby, které systému hrozí. Vytipovaná aktiva byla zapsána do tabulky a porovnána s faktory realizací hrozeb. Těmito faktory jsou motivace, zdroje, schopnost provést, příležitost a počet uživatelů. Detailněji budou tyto faktory popsány přímo v analýze rizik včetně podrobných vodítek, podle kterých byla určována jejich hodnota.

	Faktor realizace hrozeb	**Motivace**	**Zdroje**	**Schopnost provést**	**Příležitost**	**Počet všech uživatelů**	**Výsledná míra hrozby**
Hrozby	Název hrozby	Motivace útočníka využití právě této hrozby	Zdroje útočníka potřebné k využití právě této hrozby	Schopnost útočníka provést útok s využitím této hrozby	Jak často se naskytne útočníkovi příležitost k útoku pomocí této hrozby	Počet uživatelů, kteří mohou této hrozby využít	
	…						
	…						
	…						
	…						
	…						
							Číslo nejvyšší míry hrozby

Tabulka 4 – Metodika (tabulka hrozeb I)

K hrozbám byla třeba vytvořit druhou, tentokráte o něco menší tabulku určující míru hrozby, zranitelnost a velikost rizika každé z hrozeb.

	Hrozba	**Míra hrozby**	**Zranitelnost**	**Riziko**
Hrozby	Název hrozby	Výsledná míra této hrozby	Úroveň zranitelnosti touto hrozbou	Velikost rizika této hrozby
	…			
	…	…	…	…
	…	…	…	…
		Číslo nejvyšší míry hrozby	Číslo nejvyšší zranitelnosti	Číslo nejvyššího rizika

Tabulka 5 - Metodika (tabulka hrozeb II)

Posledním bodem samotné analýzy rizik je vybrání aktiva s největší hodnotou. Toto nejcennější aktivum bude v tabulce porovnáno s konkrétními hrozbami a zranitelnostmi systému. Po dosazení čísel do tabulky (tabulka číslo 18) nám vznikne v místě průniku těchto tří hodnot číslo v rozmezí 1 až 7. Všechny hodnoty se dosadí do tabulky a nejvyšší výsledná hodnota, určuje velikost skutečného rizika.

Druhá část analýzy se zaměřuje na rizika a zranitelnosti informačního systému. Ty je třeba vyhodnotit na základě vlastních zkušeností s IS STAG, pomocí otázek s uživateli či správci sítě. Jedná se vlastně o seznam zranitelností, kterým je potřeba určit vhodná protiopatření.

Riziko hrozby	**Zdroj**	**Zranitelnost**	**Protiopatření**
Kategorie hrozby	Název zranitelnosti	Hodnota zranitelnosti	Návrh protiopatření
	…		
	…		

Tabulka 6 - Metodika (tabulka zranitelností)

4. 2. 2. Identifikace bezpečnostních požadavků

Bezpečnostní požadavky jsou definovány v dokumentech Politiky ISMS na JU. Cílem politiky je ochránit všechna aktiva Jihočeské univerzity proti možným interním a externím hrozbám, jejich zneužití prozrazení nebo zničení. Mezi hlavní dlouhodobé cíle patří

- Poskytnout usměrnění pro řízení a podporu informační bezpečnosti v souladu s požadavky, které jsou kladeny na provoz vysoké školy v souladu s relevantními zákony a vyhláškami, které tyto činnosti spravují
- Řídit informační bezpečnost na JU
- Dosáhnout a udržovat přiměřenou ochranu aktiv na JU
- Zabezpečit, aby zaměstnanci, studenti, smluvní partneři a uživatelé v pozici třetích stran rozuměli svým odpovědnostem
- Zabránit neautorizovanému fyzickému přístupu, poškození a ohrožování prostor a informací JU
- Zabezpečit správný a bezpečný provoz prostředků zpracovávajících informace
- Řídit přístup k informacím
- Zajistit, aby bezpečnost byla integrální součástí informačních systémů a odpovídajících procesů
- Vyhnout se porušení jakýkoliv zákonných, statutárních, regulačních nebo smluvních závazků a jakýkoliv bezpečnostních požadavků.

Více informací o bezpečnostních požadavcích lze nalézt na stránkách Systému řízení informační bezpečnosti na JU, na stránkách https://isms.jcu.cz/ . Dokumenty jsou rozděleny do tří skupin, podle toho, kdo k nim má přístup. Informace v mojí bakalářské práci jsem použil pouze z dokumentu typu „A“, tedy veřejných dokumentů. Poslední verze, z které jsem čerpal tyto informace, byla schválena 13. ledna 2009. (20)

Mezi požadavky na informační systém jsou dány také zákony a vyhláškami. Jde například o:

- Zákon o elektronických komunikacích
- Vysokoškolský zákon
- Vnitřní předpisy JU

4. 3. Dotazníky, otázky pro uživatele

Během vypracovávání analýzy rizik jsem provedl jeden průzkum mezi uživateli a několik konverzací se správci systému. Tato podkapitola tedy bude obsahovat základní

informace o dotaznících a schůzkách. Kompletní dotazníky jsou k dispozici mezi přílohami této bakalářské práce.

4. 3. 1. Otázky pro správce sítě

Jako první byl sestrojen dotazník pro správce sítě zjišťující nejčastější hrozby a zranitelnosti sítě. Pro jeho sestrojení jsem se inspiroval velmi často používaným dotazníkem CRAMM, který jsem ale přizpůsobil přímo pro naše požadavky. Systém vyhodnocování výsledků jsem zvolil vlastní. Celý dotazník se skládá z devíti kategorií a několika podkategorií. Ke každé z nich obsahuje dotazník několik otázek.

Obsah dotazníku

Přesné zadání otázek naleznete v příloze, zde je stručný seznam otázek:

- Falšování uživatelské identity
- Nesprávné používání software
- Komunikace
- Hardware a technické závady
- Další technické závady
- Software
- Personální problémy
- Přírodní katastrofy
- Personální problémy

Výsledek dotazníku

Tento dotazník byl určen správci informačního systému STAG, panu Ing. Janu Volfovi. Dotazník pan Ing. Volf projednával s ředitelem Centra informačních technologií JU RNDr. Josefem Milotou a manažerkou informační bezpečnosti paní Ing. Janou Kolářovou. Od správců mi však bylo sděleno, že dotazník obsahuje příliš choulostivé otázky a jedná se tedy pouze o interní informace. Výsledek dotazníku byl tedy nulový. Dále jsem se snažil sestrojit kratší dotazník. I ten nakonec nebyl vyplněn.

Odpovědi na ně jsem ale získal formou osobní či emailové komunikace s Ing. Volfem a RNDr. Milotou. Otázky se týkaly pouze obecných informací systému STAG, které jsou popsány na začátku čtvrté kapitoly a informace o některých ze zranitelností

systému, které jsem vytipoval. Výsledky diskuzí se správci jsou popsány v samotné práci.

4. 3. 2. Otázky pro uživatele sítě

Tyto otázky, jak již bylo řečeno v metodice, byly sestaveny tak, aby byly určeny pro všechny druhy uživatel od studijních referentek po studenty. Otázky byly probrány formou konzultací se sekretářkou katedry informatiky, studijními referentkami a oddělením IS STAGu a stipendií. Vyučující a studenti dostali otázky v papírové či elektronické formě a odpovídali na ně bez hlubších znalostí problematiky.

Obsah otázek

Přesné zadání otázek naleznete v příloze, zde je stručný seznam otázek:

- Nedostupnost informací
  - Kdy a na jak dlouho uživatelům nevadí nedostupnost systému
  - Období, kdy se bez systému neobejdou
  - Zkušenosti s nedostupností
- Zničení informací
  - Co by to pro uživatele znamenalo
  - Která data jsou důležitá z pohledu možné ztráty
- Prozrazení informací
  - Co by to pro uživatele znamenalo
  - Která data jsou důležitá z pohledu prozrazení
- Modifikace informací
  - Co by to pro uživatele znamenalo
  - Lze modifikaci nějak prokázat
  - Modifikace překlepy

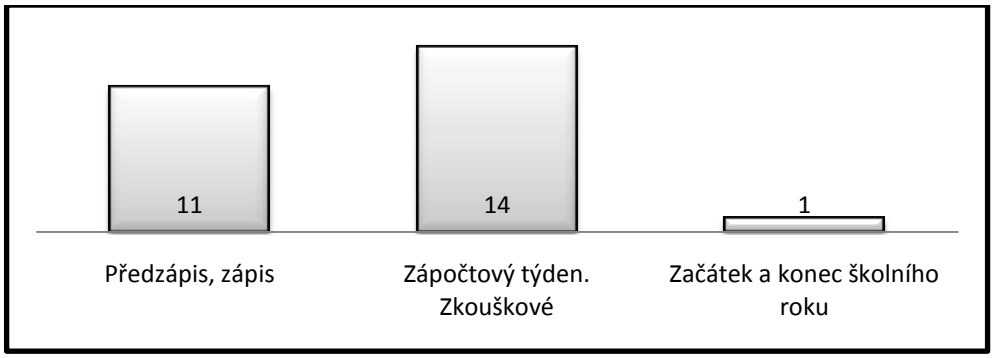
Výsledek

Výsledky těchto otázek jsem zapsal do přiloženého souboru a to včetně vyhodnocení pomocí grafů. Z těchto výsledků jsem určil aktiva, která jsou pro různé skupiny uživatelů různě cenná. Kromě určení aktiv jsem získal z dotazníku další zajímavé informace, které bych nyní ukázal na grafech. Světlé sloupečky značí běžné

uživatele (studenti, vyučující), tmavé sloupečky jsou každodenní pracovníci školy (studijní oddělení, oddělení stipendií a sekretářka katedry). Výsledky jsou v počtu hlasů, nikoliv v procentech. Na otázky odpovídali celkem: 3 každodenní pracovníci, 3 učitelé a 21 studentů Pedagogické a Ekonomické fakulty.

1. Období používání IS STAG – Kdy se bez systému nedokážu obejít?

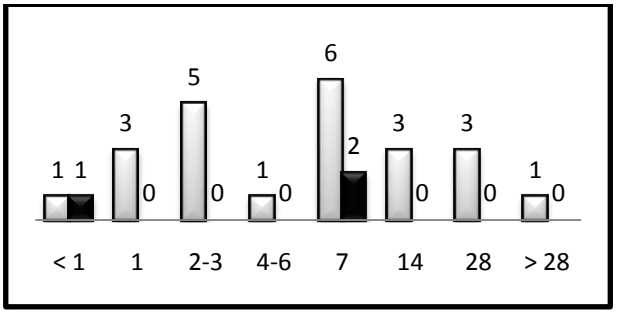
V grafu jsou zaznamenány údaje běžných uživatelů. U každodenních pracovníků je to u každého jiné. Sekretářka katedry STAG potřebuje v období státnic a přijících řízení, oddělení stipendií v období výplat a studijní oddělení prakticky neustále. Bez funkčního STAGu v úředních hodinách by ani nemohli fungovat.



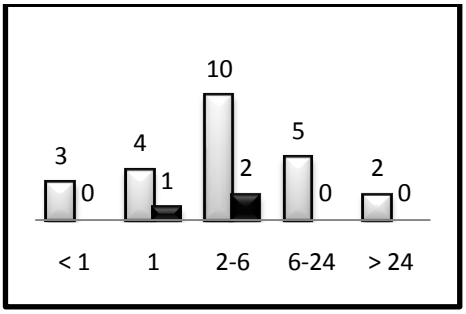
Obrázek 9- Používání IS STAG podle období.

2. Nedostupnost IS STAG – Jak dlouho se bez systému obejdu?

Tato otázka byla rozdělena na tzv. důležité a standardní období. Důležité období bylo specifikováno v minulé otázce.



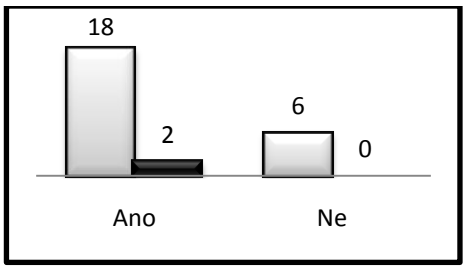
Obrázek 10- Nedostupnost ve standardním období (počet dnů)



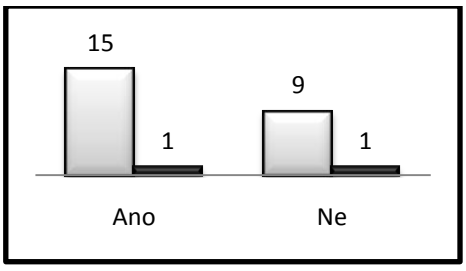
Obrázek 11- Nedostupnost v důležitém období (počet hodin)

3. Nedostupnost IS STAG – Stalo se mi někdy, že byl systém nedostupný?

Otázky byly směřovány, zda se někdy uživatelé setkali s nedostupností, popřípadě zda v ten okamžik STAG nezbytně potřebovali? Na obě otázky mnoho studentů odpovídalo, že ano. Důvodem je nedostupnost v období předzápisu. Pro každodenní pracovníky problém nedostupnosti není příliš častý, o plánovaných odstávkách jsou předem informováni.



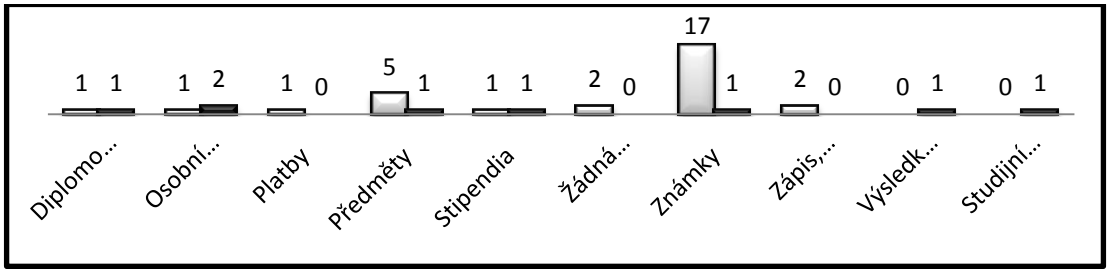
Obrázek 12- Nedostupnost STAGu, kolik uživatelů s ní již má zkušenosti



Obrázek 13- Nedostupnost STAGu v období, kdy jej bylo potřeba

4. U kterých dat nesmí dojít ke ztrátě?

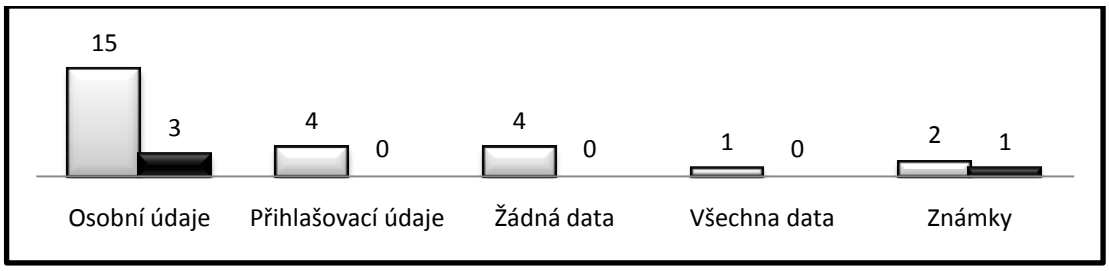
Zde tento bod dopadl zcela jasně. Nejdůležitější data, která se zde nachází, jsou pro studenty známky a pro každodenní pracovníky osobní údaje. Dle dalších otázek je zjištěno, že problém není příliš závažný. Informace by šlo dohledat v jiných dokladech (indexy, papírové podklady…). Krátkodobé ztráty dat nejsou pro uživatele vůbec žádný problém, jde jen o práci navíc. U dlouhodobých ztrát je problém větší. Data jsou ale zálohována a jejich ztráta se nepředpokládá. Každý z dotazovaných mohl zaškrtnout více položek.



Obrázek 14- Důležitost dat z pohledu ztráty

5. U kterých dat nesmí dojít k prozrazení?

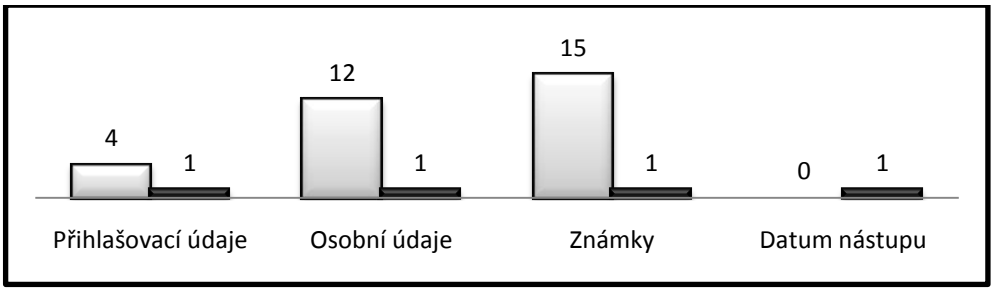
I tentokrát dopadly výsledky jednoznačně, ale pro jiná data. Informace, které nesmí být prozrazeny jak pro studenty, tak pro ostatní pracovníky, jsou osobní údaje uživatelů. Část uživatelů napsala i přihlašovací údaje, což je opět důležitá informace. Při jejím prozrazení by mohla osoba, ke které se tyto informace dostanou, nadělat dosti značné problémy.



Obrázek 15- Důležitost dat z pohledu prozrazení

6. U kterých dat nesmí dojít k modifikaci?

Data, která nesmí být modifikována, jsou více méně všechna ta, která jsem zjistil v minulých otázkách. Jde o přihlašovací údaje, osobní údaje, známky, ale také například den nástupu do školy. Student studující již pátým rokem bakalářské studium by se tak mohl vyhnout platbě za studium. Na modifikaci by se velice těžko přicházelo. Dle odpovědí od dotazovaných by na problém přišli jedině jednotliví studenti, ti by se ale ozvali jen, kdyby se jim to „hodilo“. Pokud by jim například vyučující zapsal lepší známku, neměli by důvod se ozývat. Jiné by to bylo například při zadání jiných osobních údajů, každý rok se to stává při zápisu několika lidem. Jako důkaz o modifikaci dat lze použít index, osobní doklady či různé papírové podklady uložené na škole jako například zápisový list.



Obrázek 16- Důležitost dat z pohledu modifikace

4. 4. Analýza rizik

Analýzu rizik informačního systému STAG byla provedena vlastní metodikou, která je inspirována metodikou CRAMM (CCTA Risk Analysis and Management Method). Analýza rizik byla provedena v období od 1. 9. 2009 až 30. 11. 2009. Postup včetně zpracování otázek, tabulek i celkového zpracování a ohodnocení byl vypracován podle vlastního návrhu, který byl přizpůsoben přímo pro informační systém STAG.

Informace byly získány při rozhovorech s:

- Sekretářkou katedry informatiky Soňou Juráskovou
- Pracovnicí oddělení IS STAGu a stipendií Zdeňkou Brychtovou
- Pracovnicemi studijního oddělení Petrou Opekarovou a Mgr. Zuzanou Svobodovou
- Správcem IS STAG Ing. Janem Volfem, se svolením jeho nadřízeného RNDr. Josefa Miloty

Druhou skupinou získávání informací, byly studenti a pedagogové. Ti dostali stejné otázky jako ostatní (stejné otázky jako třeba studijní oddělení), ale v papírové podobě.

Správci systému dostali otázky jiného charakteru, zaměřené především na systém samotný. Mnoho z těchto informací se mi tedy také nepodařilo získat, jelikož se jedná o citlivé informace. Podrobnějšími výsledky se zabývá pátá kapitola.

Jako hlavní cíl této analýzy rizik je stanovení míry rizika, vytipování zranitelností a návrh vhodných protiopatření k jejich eliminaci na akceptovatelnou úroveň.

4.4.1. Identifikace aktiv

Aktivem je třeba chápat všechna data, se kterými pracuje informační systém STAG na Jihočeské Univerzitě. Tyto aktiva mají pro univerzitu určitou hodnotu a jejich ztráta by znamenala možný problém. Druhou kategorií aktiv jsou zařízení, na kterém informační systém běží. Při jejich identifikaci bude každému aktivu přiřazena jeho hodnota podle vytvořených vodítek. Ta nebude vycházet z reálné ceny, ale pouze z jejího odhadu.

Aktiva byla vybrána na základě otázek, které jsem položil uživatelům sítě a dle vlastního odhadu doplnil i některá další, která by určitě neměla chybět. Výběr tedy padl na následující aktiva:

- **Přihlašovací údaje uživatelů** obsahující kromě uživatelského jména i heslo, pomocí kterého se lze do systému přihlásit.
- **Osobní údaje studentů**, včetně osobních údajů, čísla účtu, kontaktů, zapsaných předmětů a absolvovaných předmětů včetně získaných kreditů a známky.
- **Informace o studiu**, neboli absolvované předměty, známky ze zkoušek a získané kredity.
- **Informace o předmětech**, obsahující mimo jiné i popis předmětu, vyučujícího, semestr kdy je vypsán, kreditové ohodnocení, sylabus či kdo si může předmět zapsat.
- **Informace o stipendiích**, neboli seznamy se studenty dostávající stipendia.
- **Fyzická aktiva** neboli jinak řečeno vlastní hardware, na kterém informační systém běží. Jejich hodnota jsou veškeré náklady na jejich obnovu.
- **Zálohy**

Jednotlivá data jsme dále ohodnotili dle informací, které jsem získal při rozhovorech s uživateli. Aktiva byla hodnocena na základě citlivosti těchto dat z pohledu:

- Důvěrnost
- Integrity
- Dostupnosti

Vodítka pro stanovení hodnoty aktiv

Pro stanovení reálné hodnocení aktiv si je třeba nejprve vytvořit vodítka, která budou určovat jejich hodnotu podle různých aspektů, jako například finanční ztráty, negativní publicit, ohrožení zdraví osoby, pokuty a dalších kritérií. Stupeň hodnoty byl zaveden, abychom mohli následně odhadnout hodnotu aktiva. Inspirací pro tyto vodítka byly použity statistiky společnosti BITS. (24)

Hodnota aktiva	Vodítko hodnocení (nemusí splňovat všechny podmínky, stačí jedna)	Hodnota aktiva
Nízká	Finanční ztráta < 150 000 Kč Neefektivní fungování části organizace	1
Střední	Finanční ztráta 150 000 Kč až 1 000 000 Kč Malá újma na zdraví jedné osoby Negativní publicita v okolí Správní řízení, vedoucí k pokutě až 100 000 Kč	2-4
Vysoká	Finanční ztráta 1 000 000 Kč až 3 000 000 Kč Malá újma na zdraví několika osob Celostátní negativní publicita Správní řízení, vedoucí k pokutě 100 000 Kč až 1 000 000 Kč	5-7
Velmi vysoká	Finanční ztráta nad 3 000 000 Kč Ohrožení bezpečnosti jedné či více osob Nadnárodní negativní publicita Správní řízení, vedoucí k pokutě nad 1 000 000 Kč Ohrožení fungování organizace	8-10

Tabulka 7 – Vodítka pro stanovení hodnoty aktiv

Stanovení hodnoty aktiv

Tabulka obsahuje hodnoty aktiv z pohledu integrity, důvěrnosti a dostupnosti, které jsou určeny podle tabulky č. 7. Poslední sloupec určuje výslednou hodnotu každého z aktiv. Pro vyplnění tabulky se použijí informace, získané při rozhovorech se správci či uživateli sítí.

Aktiva	Integrita	Důvěrnost	Dostupnost	Hodnota aktiva
Přihlašovací údaje uživatelů	Vysoká	Vysoká	Střední	4
Osobní údaje studentů	Vysoká	Vysoká	Vysoká	5
informace o studiu	Střední	Střední	Střední	4
Informace o předmětech	Nízká	Nízká	Nízká	2
Informace o stipendiích	Vysoká	Nízká	Nízká	3
Fyzická aktiva	Nízká	Nízká	Nízká	1
Zálohy	Nízká	Nízká	Vysoká	2
				5

Tabulka 8 – Analýza rizik, stanovení hodnoty aktiv

Přihlašovací údaje

- **Integrita** – Vybrána hodnota vysoká. Důvodem je možné zneužití těchto údajů a následná nedovolená aktivita. Ta by vyvolala změnu dat a následné porušení jejich správnosti.
- **Důvěrnost** – Přihlašovací údaje by měli být utajené, a neměli by se dostat k jiné osobě, než které byly přiděleny. Hodnota aktiva z pohledu utajení je vysoká.
- **Dostupnost** – K těmto údajům mají standardně přístup pouze správci systému, ostatní nikoliv. Proto střední hodnota aktiva z pohledu dostupnosti.

Osobní údaje studentů

- **Integrita** – Změna osobních údajů studentů je velice závažná věc. Například při změně čísla bankovního účtu by finance vyplácená za stipendia studentům nedošla. Proto je hodnota aktiva z pohledu integrity vysoká.
- **Důvěrnost** - Při porušení utajení těchto dat hrozí porušení zákona č. 101/2000 Sb., o ochraně osobních údajů, proto jsem zvolil jako hodnotu vysokou.
- **Dostupnost** – Data o osobních údajích jsou dostupná jen studijnímu oddělení, které je nesmí dále rozšiřovat. Jsou vázáni zákonem č. 101/2000 Sb., o ochraně osobních údajů. S daty přijde do styku jen minimum lidí, proto je hodnota vysoká.

Informace o studiu

- **Integrita** – Informace o studiu obsahující hotové předměty, kredity a známky z předmětů zajisté musejí být správné. Jejich případná chyba by se ale dala zjistit, proto je hodnota aktiva z pohledu integrity pouze střední.
- **Důvěrnost** – Informace o studiu by měla být zajisté důvěrná, i když její prozrazení by nezpůsobilo příliš velkou škodu. Proto hodnota aktiva z pohledu důvěrnosti je střední.
- **Dostupnost** – Informace o studiu je privátní informace, ke které má kromě studenta přístup jen minimum lidí. Hodnota aktiva z pohledu dostupnosti je střední.

Informace o stipendiích

- **Integrita** – Data o stipendiích musí být v naprostém pořádku, stejně jako přihlašovací údaje či osobní údaje studentů. Proto jejich aktivum z pohledu integrity má vysokou hodnotu.

Zálohy

- **Dostupnost** – K těmto zálohám smí mít přístup pouze správci systému, proto je hodnota aktiv z pohledu dostupnosti vysoká.

Všechna ostatní aktiva byla ohodnocena jako nízká, jejich hodnota z pohledu integrity, důvěrnosti a dostupnosti je minimální.

Závěr hodnocení aktiv

Dle otázek položeným uživatelům sítě jsme ohodnotili aktiva a pro další postupy analýzy rizik bylo vybráno aktivum s nejvyšší hodnotou – tedy osobní údaje studentů. Na dalších místech se umístili přihlašovací údaje studentů a informace o studiu. S těmi i s dalšími aktivy se již dále pracovat nebude.

Aktivum osobních údajů bylo vybráno proto, že obsahuje nejcitlivější údaje v systému a nesmí být prozrazeny nepovolané osobě, ani nesmí být modifikován. Přístup k němu má však jen velice úzké spektrum uživatelů.

4. 4. 2. Identifikace a velikost hrozeb

Při identifikaci a ohodnocení aktiv bylo vybráno nejcennější aktivum, tedy přihlašovací údaje uživatelů. S ostatními aktivy se již dále pracovat nebude. Hrozby byly vybrány na základě expertního odhadu, nejedná se o všechny možné hrozby, které mohou nastat. Na konec byly vybrány tyto hrozby:

- **Vniknutí do systému a neoprávněná činnost** – může se jednat o autorizovaný či neautorizovaný přístup
- **Úmyslné poškození dat zaměstnanci** – poškození dat či hardwaru
- **Komunikace –** mezi serverem a klientem
- **Chyba software**
- **Chyba hardware**

- **Výpadky napájení či klimatizace**

Hrozby budou hodnoceny z pohledu faktorů hrozeb, tedy podle motivace útočníka, zdrojů potřebných k útoku, schopnosti provést útok, příležitosti jak často lze útok provést a počtu uživatelů, kteří mohou útok provést. Více o těchto faktorech si probereme v následujících vodítkách.

Vodítko pro stanovení vážnosti hrozby podle motivace

Motivace je nejdůležitějším prvkem, určujícím zájem útočníka využít jednotlivé hrozby.

Velikost hrozby	Velikost motivace
Zanedbatelná	Útočník nemá motivaci využít tuto hrozbu
Nízká	Útočník může této hrozby využít, ale nepředpokládáme to
Střední	Útočník může této hrozby využít
Vysoká	Vážná hrozba, takových míst je ale v systému několik
Velmi vysoká	Nejvážnější hrozba, útočník by si vybral právě tuto hrozbu

Tabulka 9 – Vodítko pro stanovení vážnosti hrozby podle motivace

Vodítko pro stanovení vážnosti hrozby podle zdrojů

Pod zdroji si představíme prostředky, které jsou třeba pro vykonání útoku. Může jít o zdroje technologické či finanční.

Velikost hrozby	Požadované velikosti zdrojů
Zanedbatelná	Bez technologických požadavků Bez finančních nákladů
Nízká	Nízké technologické požadavky Nízké finanční náklady
Střední	Střední technologické požadavky Střední finanční náklady
Vysoká	Vysoké technologické požadavky Vysoké finanční náklady
Velmi vysoká	Velmi vysoké technologické požadavky Velmi vysoké finanční náklady

Tabulka 10 – Vodítko pro stanovení vážnosti hrozeb podle zdrojů

Vodítko pro stanovení vážnosti hrozby podle schopnosti provést útok

Určuje, zda může útočník hrozby využít a jestli má k útoku předpoklady.

Velikost hrozby	Požadavek na znalosti
Zanedbatelná	Útok by mohl provést i laik
Nízká	Jsou potřeba nízké znalosti
Střední	Jsou potřeba střední znalosti
Vysoká	Jsou potřeba vysoké znalosti
Velmi vysoká	Velmi vysoké znalostní nároky

Tabulka 11 - Vodítko pro stanovení vážnosti hrozeb podle schopnosti provést útok

Vodítko pro stanovení vážnosti hrozby podle příležitosti

Příležitost určuje, jak často se útočníkovi může naskytnout příležitost využití hrozby konkrétní hrozby.

Velikost hrozby	Intenzita výskytu hrozby
Zanedbatelná	Jednou za rok a více
Nízká	Jednou za tři měsíce
Střední	Jednou za měsíc
Vysoká	Jednou týdně
Velmi vysoká	Jednou a vícekrát denně

Tabulka 12 - Vodítko pro stanovení vážnosti hrozeb podle příležitosti

Vodítko pro stanovení vážnosti hrozby podle počtu uživatelů

Určuje množství uživatelů, kteří mají přístup ke službám či místům, kde by mohli dané hrozby využít.

Velikost hrozby	Počet osob mající přístup k této oblasti
Zanedbatelná	1 osoba
Nízká	1 osoba až 10 osob
Střední	10 osob až 100 osob
Vysoká	100 osob až 1000 osob
Velmi vysoká	1000 a více osob

Tabulka 13 - Vodítka pro stanovení vážnosti hrozeb podle počtu uživatelů

Vodítko pro míru hrozby

Výsledná míra vycházející z faktorů realizace hrozeb má stejnou hodnotu jako nejvyšší z faktorů hrozeb.

Seznam hrozeb

Pro jednotlivé hrozby určíme podle vodítek jejich velikost vůči jednotlivým faktorům hrozeb. Z nich poté odhadneme výslednou míru hrozby a nejvyšší hodnotu z nich si zapíšeme dolů do tmavé buňky. S touto hodnotou budeme pracovat i nadále.

	Faktor realizace hrozeb	**Motivace**	**Zdroje**	**Schopnost provést**	**Příležitost**	**Počet uživatelů**	**Míra hrozby**
Hrozby	Vniknutí do systému a neoprávněná činnost v něm	Vysoká	Střední	Vysoká	Nízká	Střední	Vysoká
	Úmyslné poškození dat zaměstnanci	Střední	Střední	Střední	Vysoká	Nízká	Střední
	Komunikace	Nízká	Nízká	Nízká	S	S	Nízká
	Chyba software	Nízká	Nízká	Zanedbat.	Nízká	Nízká	Nízká
	Chyba hardware	Nízká	Nízká	Zanedbat.	Nízká	Nízká	Nízká
	Výpadky napájení či klimatizace	Nízká	Zanedbat.	Nízká	Nízká	Nízká	Nízká
							Vysoká

Tabulka 14 – Seznam hrozeb a jejich velikostí

Vniknutí do systému a neoprávněná činnost v něm

- **Motivace** – Motivace útočníka k využití této hrozby je největší ze všech. Právě díky této hrozbě by si mohl například student pozměnit známky, údaje a další uchovávané informace. Motivace útočníka k využití této hrozby je vysoká.
- **Zdroje** – Bez potřebné techniky by útočník nemohl útok uskutečnit. Není však potřeba speciálních prostředků. Zdroje útočníka k využití této hrozby jsou potřeba střední.
- **Schopnost provést** – Pro provedení útoku pomocí této hrozby jsou potřeba obrovské znalosti, jako například pokročilé znalosti programování či zkušenosti s hackováním systémů. Běžný uživatel by této hrozby nemohl využít. Schopnosti potřebné k provedení útoku jsou potřeba vysoké.

- **Počet uživatelů** – Je určitá skupina uživatelů, která by této hrozby mohla využít. Počet uživatelů, kteří mohou této hrozby využít je střední.

Úmyslné poškození dat zaměstnanci

- Motivace – Zaměstnanci nemají nějaký speciální důvod, proč by data pozměňovali či poškozovali. Vyloučit se to ale nedá. Proto je motivace zaměstnanců ohodnocena jako střední.
- **Zdroje** – Pro zaměstnance není problém nějaká data pozměnit či smazat. Potřebnou techniku mají v práci, proto není využití této hrozby problém.
- **Schopnost provést** – Tuto hodnotu jsem ohodnotil jako střední. Nepředpokládá se, že by zaměstnanci bezdůvodně pozměňovali či smazávali nějaká data. Příležitost – Příležitost mají zaměstnanci téměř kdykoliv. Proto velká příležitost.

Komunikace

- Přenos dat mezi uživateli a serverem může být narušen, avšak nepředpokládá se, že by si útočník využil právě této hrozby. Přesto počet uživatelů a příležitosti je vyšší než u ostatních hrozeb. Motivace jednotlivých hrozeb jsou nízké či zanedbatelné. Zabezpečení systému mají na starost autoři systému, kteří pravidelně provádějí aktualizace, splňující nejnovější požadavky bezpečnosti.

Chyba software

- K softwaru, na kterém informační systém běží, má přístup jen omezený počet uživatelů – správci. Kromě těchto uživatelů systému nikdo nerozumí. Potenciální útočník by musel mít velké znalosti. Motivace jednotlivých hrozeb jsou nízké či zanedbatelné.

Chyba hardware

- Chyba hardwaru je také minimální. Přístup k místu se servery mají jen správci a pracovníci Centra informačních technologií JČU. Ostatní uživatelé by museli provést násilné vniknutí a poškození hardwaru. Motivace jednotlivých hrozeb jsou nízké či zanedbatelné.

Výpadky napájení či klimatizace

- Napájení má rezervu v podobě záložního zdroje. Problém by mohl způsobit pouze dlouhodobý výpadek. V tomto případě by ale správci měli dostatek času servery odstavit. Motivace jednotlivých hrozeb jsou nízké či zanedbatelné.

4. 3. 3. Výsledná velikost rizika

Pro určení výsledné míry rizika již známe nejcennější aktivum, nejvyšší míru hrozby, chybí nám však velikost zranitelnosti jednotlivých rizik.

Vodítka pro ohodnocení hrozeb - zranitelnost

Velikost zranitelnosti	Popis zranitelnosti
Nízká	Systém není zranitelný na danou chybu, jsou zde implementována dostatečná protiopatření k snížení zranitelnosti.
Střední	Systém je zranitelný na danou chybu, jsou zde implementována protiopatření, avšak nedostatečná.
Vysoká	Systém je zranitelný na danou chybu, nejsou zde implementována žádná protiopatření jako například opravné patche, nejnovější verze software a další…

Tabulka 15 – Vodítko ohodnocení zranitelností

Vodítka pro ohodnocení hrozeb - riziko

Velikost rizika	Popis rizika	Číselná hodnota
Bezvýznamné riziko	Riziko je tak nízké, že pro nás nic nepředstavuje. Dále s ním již nepočítáme.	1
Akceptovatelné riziko	Riziko je pro nás akceptovatelné, přesto je však třeba ho i nadále sledovat.	2-3
Mírné riziko	Riziko je mírné, mělo by se s ním něco dělat při nejbližší příležitosti. Není však nezbytně nutné s aplikací protiopatření spěchat.	4
Nežádoucí riziko	Riziko je pro nás problém, který je potřeba co nejrychleji řešit a navrhnout vhodná protiopatření.	5-6
Nepřijatelné riziko	Nejvyšší úroveň rizika, musí se okamžitě přistoupit k nějakému protiopatření k minimalizování rizika.	7

Tabulka 16 – Vodítko ohodnocení rizik

Tabulka pro výpočet rizika

Po zadání všech nezbytných hodnot aktiv, hrozeb a zranitelností jsme provedli výpočet míry rizika. Výsledná míra má číselnou hodnotu od 1 do 7 s tím, že hodnota 1 znamená nízké riziko. Hodnota 7 znamená riziko nejvyšší a tedy vysoké požadavky na

zajištění bezpečnosti. Celkové výsledné hodnoty míry hrozeb a zranitelností z předchozích tabulek byly použity jako vstupy pro výpočet rizik v tabulce následující.

HODNOTA AKTIVA	**Míra hrozby**	**Z**	**Z**	**Z**	**N**	**N**	**N**	**S**	**S**	**S**	**V**	**V**	**V**	**VV**	**VV**	**VV**
	Zranitelnost	**N**	**S**	**V**	**N**	**S**	**V**	**N**	**S**	**V**	**N**	**S**	**V**	**N**	**S**	**V**
	1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
	2	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4
	3	1	2	2	2	2	2	2	3	3	3	3	4	3	4	4
	4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
	5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
	6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
	7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
	8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
	9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
	10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Tabulka 17 – Závěrečná tabulka pro výpočet rizika

Určení zranitelnosti a rizika pro jednotlivé hrozby

Do tabulky s ohodnocením hrozeb si opíšeme míru hrozby z předchozí tabulky a to včetně nejvyšší hodnoty. Druhou položkou je zranitelnost, kterou si opět určíme podle vodítek. Velikost rizika spočítáme z hodnoty nejhodnotnějšího aktiva, míry hrozby a zranitelnosti konkrétní hrozby. Tedy například vezmeme nejvyšší hodnotu aktiva 5, a pro každou z hrozeb dosadím do tabulky ještě její míru hrozby a zranitelnost. Výsledná hodnota je riziko, které hledáme. V poslední řádce jsou informace o nejvyšším riziku.

Hrozba	**Míra hrozby**	**Zranitelnost**	**Riziko**
Vniknutí do systému a neoprávněná činnost v něm	Vysoká	Střední	Mírné riziko (4)
Úmyslné poškození dat zaměstnanci	Střední	Střední	Mírné riziko (4)
Komunikace	Nízká	Nízká	Akceptovatelné riziko (3)
Chyba software	Nízká	Nízká	Akceptovatelné riziko (3)
Chyba hardware	Nízká	Nízká	Akceptovatelné riziko (3)
Výpadky napájení či klimatizace	Nízká	Nízká	Akceptovatelné riziko (3)
	Vysoká	Střední	Mírné riziko

Tabulka 18 – Zranitelnosti a rizika jednotlivých hrozeb

Závěr ohodnocení rizika

Z tabulky číslo 15, je zřejmé, že nejvyšší míra hrozby má hodnotu „vysoká“ a platí pro hrozbu „Vniknutí do systému a neoprávněná činnost v něm“. Nejvyšší zranitelnost těchto chyb vyšla jako „střední“ a to pro tuto stejnou hrozbu a také pro „Úmyslné poškození dat zaměstnanci“. Po dosazení míry rizika a zranitelností do tabulky pro nejcennější aktivum bylo získány hodnoty výsledného rizika pro konkrétní hrozby. Nejvyšší hodnota vyšla stejná pro dvě rizika – „Vniknutí do systému a neoprávněná činnost v něm“ a „Úmyslné poškození dat zaměstnanci“. Obě hodnoty vyšly na výsledné stupnici s hodnotou „4“, dle tabulky číslo 17 se tedy jedná o mírné riziko.

Velikost rizika tvoří propojení mezi analýzou rizik a zvládáním rizik v rámci provedené analýzy. Velikost rizika je rozhodujícím faktorem, který má následně vliv na výběr vhodných protiopatření. Dle výsledku, kterého bylo dosaženo, představují hrozby pro systém pouze mírné riziko. I přesto je potřeba identifikovat zranitelnosti systému a navrhnout vhodná protiopatření.

4. 4. 4. Podrobnější údaje o rizicích a výběr bezpečnostních protiopatření

Tabulka podrobnějších údajů o rizicích

Riziko hrozby je možnost realizace hrozby a s ním souvisejí i zranitelnosti. Nyní se soustředíme na podrobnější rozbor rizik. V následující tabulce je uveden seznam zranitelných míst ve vztahu ke zdroji a možné bezpečnostní protiopatření, které by snižovalo zranitelnost a riziko eliminovalo.

Riziko hrozby	Zdroj	Zranitelnost	Protiopatření
Úmyslné poškození dat zaměstnanci	Administrátor systému	Možnost čtení, modifikace či mazání dat.	Bez opatření
Úmyslné poškození dat zaměstnanci	Uživatelé	Počty uživatelů	Omezení
Vniknutí do systému a neoprávněná činnost v něm	Uživatelé	Dostatečné zabezpečení uživatelského účtu	Potřeba používat silné heslo
Vniknutí do systému a neoprávněná činnost v něm	Uživatelé	Dodržování základních pravidel bezpečnosti.	Odhlašovat se ze systému, nesdělovat nikomu přihlašovací údaje…
Chyba software	IS STAG	Úmyslné zablokování účtu	Upravit systém tak aby majitele účtu informoval o zablokování
Chyba software	IS STAG	Změna hesla	Vyžadovat původní heslo při změně hesla
Komunikace	Přenos dat	Šifrování přenosu	Bez opatření
Chyba hardware	Nedostupnost systému	Nedostupnost v době předzápisu	Výkonnější hardware
Chyba hardware	Nedostupnost systému	Nedostupnost v době jiné než je předzápis	Bez opatření
Chyba hardware	Zálohy dat	Intenzita zálohování	Replikované zálohy

Tabulka 19 – Seznam zranitelností

Administrátor systému – možnost čtení, modifikace či mazání dat

- Administrátoři mají přístup k tabulkám s daty, která mohou libovolně měnit či mazat. Administrátoři jsou velice úzká skupina lidí, k datům mají pouze 2 lidé s právy administrátora a několik desítek uživatelů se silnějšími právy (tajemník fakulty). Nikdy se však toto riziko vyloučit nedá, i když v současném stavu asi nemá smysl navrhovat nějaké protiopatření. Při změně dat se do databáze ukládá informace o změně (kdo a kdy změnu provedl a jaké informace změnil).

Uživatelé – Omezení počtu uživatelů

- V systému se nachází 6 druhů uživatelů: studenti (13 600 uživatelů), vyučující (1 300 uživatelů), katedry (190 uživatelů), studijní oddělení (58 uživatelů), tajemník fakulty (40 uživatelů) a administrátor (2 uživatelů). Počty uživatelů kateder a studijného oddělení jsou zbytečně vysoké. Je to dáno tím, že za

některé uživatele vykonávají jejich funkce sekretářky či jiní pracovníci. Takto vzrůstá počet uživatelů o několik desítek uživatelů. Ideální by bylo, aby bylo jen tolik uživatelů, kolik je potřeba.

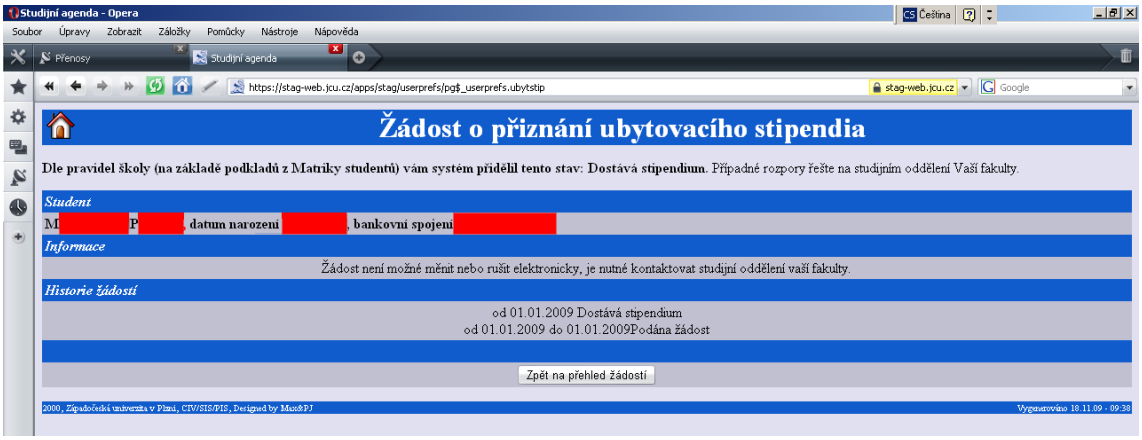
Uživatelé – Dostatečné zabezpečení uživatelského účtu

- Uživatelské účty studentů jsou zabezpečeny pomocí uživatelského jména a hesla. Uživatelské jméno se dá velice snadno zjistit, stačí do systému zadat jméno studenta a systém komukoliv vyhodí správné uživatelské jméno, které je zároveň i pořadovým číslem studenta. S heslem je to složitější. Defaultně je heslo nastaveno na x a rodné číslo bez lomítka (například x8510207777). A v tom by mohl být problém. Při prvním přihlášení do systému by měl být každý uživatel POVINEN si heslo změnit za nové, nejlépe co nejsilnější heslo obsahující písmena, číslice, popřípadě i speciální znaky. Dle mého průzkumu (ústní anketa – výsledky nejsou úplně přesné) více než 60% studentů stále používá výchozí heslo. Stačí si tedy od studentů zjistit rodné číslo a jsme na uživatelském účtu, kde si můžeme dělat, co chceme (odhlašovat z předmětů, odhlašovat z termínů, odhlašovat ze zkoušek, změnit osobní údaje, změnit uživatelovo číslo účtu na naše a další věci). V dnešní době rodné číslo sdělujeme cizím lidem celkem často, stačí, když dáme z ruky občanský průkaz.

Uživatelé – Dodržování základních pravidel bezpečnosti

- Do tohoto bodu bych zahrnul povinnosti uživatelů, především uživatelé nesmí heslo nikomu prozrazovat, neměli by si ho zapisovat pro případ možné ztráty a nesmí heslo ukládat do internetového prohlížeče a ihned po skončení práce se odhlásit, popřípadě raději ukončit prohlížeč. Možná se tento bod zdá jasný, opak je však pravdou. Dne 18. 11 2009 se mi podařilo využít zranitelnosti internetového prohlížeče Opera. Zranitelností je to, že si prohlížeč ukládá soubory (včetně cokies, hesel a dalších…) nikoliv na uživatelův síťový disk, ale přímo do konkrétního počítače. K těmto souborům se tedy dostane úplně každý uživatel tohoto počítače. V tento den se mi podařilo tedy přihlásit na

učebně číslo J242 přihlásit pod studentem s iniciály M. P. V tuto dobu jsem si mohl s jeho účtem dělat prakticky cokoliv, včetně změny hesla. Díky tomu, že se uživatel neodhlásil a navíc si i uložil heslo do systému, se pod ním nyní může přihlásit prakticky kdokoliv. Důkaz je na následujícím obrázku.



Obrázek 17- Cizí uživatelské údaje v IS STAG

IS STAG - Úmyslné zablokování účtu

- Další ze zranitelností, které může využít kterýkoliv ze studentů je úmyslné zablokování účtu. Jejím principem je to, že si útočník zjistí podle jména uživatelovo identifikační číslo a snaží se pod ním přihlásit. Systém však má ochranu proti brutal force technice (zkoušení všech možných variací hesel, jaké jen na světě existují), po desátém pokusu o přihlášení se účet zablokuje. V případě, že by se toto stalo den před zkouškou, ze které se chceme ještě na poslední chvíli odhlásit či na předzápis, mohlo by to pro uživatele znamenat velký problém. Největším problémem je také to, že majitel účtu vůbec o ničem nemá tušení, a ani STAG nevyhodí patřičnou hlášku o překročení počtu přihlášení. Prostě jen nabídne uživateli přihlášení, ale nepřihlásí se. Uživatel je tedy zmaten a neví, co se děje. Účet mu bude odblokován poté, co kontaktuje Zdeňku Brychtovou z oddělení IS STAG na pedagogické fakultě či někoho ze správců systému. Ideální protiopatření by bylo vytvoření chybové hlášky o překročení počtu přístupů popřípadě i zaslání emailu uživateli s oznámením o blokaci jeho účtu.

IS STAG - Změna hesla

- Tento problém se týká pouze starší verze portálu STAG. Při změně hesla není vyžadováno současné heslo. Komukoliv kdo se dostane k účtu, jehož uživatel zůstal přihlášen či se cizí osobě podařilo na účet dostat si tak může jednoduše heslo změnit. V horším případě a v kombinaci se zranitelností Uživatelé / Dodržování základních pravidel bezpečnosti můžeme heslo jednoduše změnit a dotyčný to ani nezjistí. Bude se snažit do systému přihlásit a sám si účet tak maximálně zablokuje. Po odblokování, které lze provést u správců by stále nebylo možno se do systému přihlásit. Po čase by se na změnu určitě přišlo. Tento problém bude definitivně vyřešen až kompletní náhradou za novou verzi informačního systému STAG, který však zatím používá naprosté minimum uživatelů.

Přenos dat – Šifrování přenosu

- Přenos dat v novém, i starém portále zajišťují protokoly http a http. Ve staré verzi probíhá šifrování pomocí TLS, v novějším portále je vše řešeno pomocí SSL. V současné době je zabezpečení přenosu dat dostačující.

Nedostupnost systému - Nedostupnost v době předzápisu

- V období předzápisu bývá nápor na systém největší. V jeden okamžik se snaží přihlásit několik tisíc uživatelů. Maximální počet přítomných uživatelů je 300, což je jakýmsi kompromisem mezi maximálním počtem uživatelů a dostatečnou rychlostí pro každého uživatele. Předzápisy probíhají na všech fakultách najednou (až na drobné výjimky – např. Přírodovědecká fakulta) a kapacita je tak rychle obsazena. V dnešní době, kdy jsou některé předměty přístupné pro studenty různých kateder, není možné předzápis rozdělit na více termínů. Limit 300 uživatelů je nastaven na portálovém serveru, uživatelé přihlašující se pomocí tlustého klienta se do systému dostanou i při překročení limitu. Počty uživatelů se každoročně zvyšují cca o 20% v případě, že předchozí rok nebyl server příliš vytěžován. V následujícím roce bude možný předzápis pouze pomocí nového portálového rozhraní, které by mělo být méně

náročné na výkon serverů. Tento problém přetížení serverů je každoroční a vše je jen otázkou peněz investovaných do hardwaru.

Nedostupnost systému - Nedostupnost v době jiné než je předzápis

- Tyto plánované odstávky serverů jsou předem uveřejňovány na stránkách IT portálu (http://itportal.jcu.cz/). Plánované odstávky se vyskytují pouze několikrát do roka v přijatelných hodinách. Dle odpovědí uživatelů se s krátkodobými výpadky setkají čas od času, nebývají však dlouhodobého charakteru. Většinou je to otázkou několika málo minut a stávají se například při restartu serverů.

Zálohy dat - Intenzita zálohování

- Frekvence zálohování databázového serveru Oracle je jednou za den v podobě malé zálohy na server, který je umístěný v jiné budově Jihočeské Univerzity a na pásky. Velká záloha se provádí každých 60 dní a navíc každých čtvrt roku rovněž na pásky. Dle informací na požadavky zálohování od autorů STAGu je ideální provádět zálohování častěji, konkrétně 7x denně a 3x za měsíc. Navíc však data bývají jednou denně zálohována do tzv. Testovací zálohy, což je záloha s pravdivými daty, která jsou ale přiřazena jiným uživatelům než ve skutečnosti. Chybná data by se tedy dala dohledat i tady. Do budoucna se zálohy ještě zlepší a to díky replikovaným zálohám, což budou zálohy prováděné přes síť na úplně jiné místo a navíc v reálném čase. Data ze záloh se vrací pouze ve výjimečných případech, například při provádění radikálnějších změn v databázi či přechodech na novější verze.

Závěr a shrnutí zranitelností a výběru bezpečnostních protiopatření

V informačním systému STAG nebyly odhaleny žádné mimořádné zranitelnosti. Spíše se však jedná o chyby systému, některé z nich již byly opraveny přechodem na novou verzi portálového rozhraní. Mezi nejzávažnější zjištěné zranitelnosti bych zařadil nedostupnost systému v době předzápisu a dodržování základních bezpečnostních pravidel. To se stává z používání dostatečně silného hesla a odhlašování se po skončení

práce se systémem. Závažnou chybou v samotném systému je neinformování uživatele o zablokování účtu a tváření se systému, jako by byl systém pouze nedostupný.

5. Závěr

Analýza rizik byla vytvořena a aplikována na informační systém. Byly identifikovány aktiva a hrozby, které byly ohodnoceny. Z těchto hodnot byla sestavena výsledná míra rizika, která byla ohodnocena jako mírné riziko. Informační systém STAG je velice dobře zabezpečen, mimo jiné je implementován systém řízení informační bezpečnosti (ISMS), který zaručuje splnění nejnovější bezpečností normy ISO/IEC 27001 a je pravidelně bývá také prováděna externími pracovníky detailní analýza rizik. Pro svou analýzu rizik jsem si vybral vlastní metodu, kterou jsem navrhl. Informace jsem získal při interview s uživateli sítě především se správci systému a s uživateli. Vycházel jsem pouze z dostupných informací, které mi byly sděleny.

Analýza rizik byla prováděna na informačním systému STAG, na kterém právě probíhal přechod na novější verzi portálového přístupu. Přechodem na novější verzi bylo odstraněno velké množství chyb a prostředí se také stalo uživatelsky přívětivější. Nicméně pár chyb se vyskytuje i nadále, jako například při zablokování účtu se systém tváří jako by jen nebyl dostupný a uživatel se o blokaci nijak nedozví. V období předzápisu či zkoušek by tak mohly vzniknout studentům drobnější komplikace. Bezpečnost osobních údajů a dalších informací, které systém obsahuje, nejvíce závisí na samotných uživatelích – na studentech. Dle zjištění více než polovina z nich používá defaultní heslo, skládající se z rodného čísla. Při zjištění rodného čísla se tedy kdokoliv dostane do studentského účtu. Zjistit osobní číslo již není problém, k tomu nám stačí znát jméno. Studenti také musí dodržovat základní pravidla bezpečnosti, jako nesdělování svého hesla cizím osobám a při ukončení své práce se odhlásit. Druhé pravidlo všichni uživatelé nedodržují, a není proto problém se ze školních počítačů se přihlásit pod cizím jménem. Stačí k tomu projít si jakoukoliv učebnu a někdo takový se najde. Při dodržování základních pravidel bezpečnosti, tedy změněného dostatečně silného hesla, odhlašování se po skončení a nesdělování hesla komukoliv jsou naše údaje v bezpečí.

Cíle bakalářské práce, které jsem si zvolil, byly splněny. Byla odhadnuta míra rizika a vytipovány některé ze zranitelností systému.

Reference

1. **Smejkal, Vladimír a Rais, Karel.** *Řízení rizik ve firmách a jiných organizacích.* Praha : Grada, 2006.

2. **Kunderová, Ing. Ludmila.** Bezpečnost IS/IT. *Ústav informatiky, PEF MZLU v Brně.* [Online] 21. 2 2009. [Citace: 23. 3 2009.] https://akela.mendelu.cz/~lidak/bis/.

3. **DCID.** Analýza rizik - Rizika existují, poznejte je všechny. [Online] 2004. [Citace: 20. 9 2009.] http://www.dcit.cz/files/bezpecnost/info/DCIT_analyza_rizik.pdf.

4. **Risk Analysis Consultants, s.r.o.** Přístupy k provedení analýzy rizik IS. *Risk Analysis Consultants.* [Online] 2004. [Citace: 9. 27 2009.] http://www.rac.cz/rac/homepage.nsf/CZ/Download/$FILE/PristupyAR.pdf.

5. **Kostiha, František.** Bezpečnost informací. *Ikaros - Elektronický časopis o informační společnosti.* [Online] 2006. [Citace: 20. 9 2009.] http://www.ikaros.cz/node/3332.

6. **TATE International s.r.o.** Nová série bezpečnostních norem. *Bezpečnost a normy.* [Online] 2005. [Citace: 20. 9 2009.] http://www.dsm.tate.cz/picture/clanky/clanek_1.pdf.

7. **Risk Analysis Consultants, s. r.o.** Risk Analysis Consultants. *RAC.* [Online] 2009. [Citace: 20. 9 2009.] http://www.rac.cz.

8. **ISO 27001 Security.** About the ISO27k standart. *ISO 27001 Security.* [Online] 2009. [Citace: 23. 3 2009.] http://www.iso27001security.com/html/iso27000.html.

9. **IsecT Ltd.** *ISO/IEC 27000-family of information security standards.* [Online] 2009. [Citace: 20. 9 2009.] http://www.iso27001security.com/.

10. **MBK Consulting, s.r.o.** Systém managementu služeb IT dle ISO/IEC 20000:2005. *MBK Consulting.* [Online] 2008. [Citace: 20. 9 2009.] http://www.mbk.cz/iso-iec-20000-2005.

11. **Novák, Luděk.** Přehled a možnosti využití norem voblasti bezpečnosti. *Anect.* [Online] 2008. [Citace: 7. 10 2009.] http://domino.cni.cz/np/notesportalcni.nsf/6f28e376f4ef9ed1c1256f8200606d97/f0decdebd6ace568c12571fd003f5297/$FILE/02870192.pdf/Přehled%20a%20možnosti%20využití%20norem%20v%20oblasti%20bezpečnosti.pdf.

12. **AEC, spol. s r.o.** Analýza rizik IS. *AEC.* [Online] 2009. [Citace: 20. 9 2009.] http://www.google.com/url?sa=t&source=web&ct=res&cd=3&url=http%3A%2F%2Fwww.aec.cz%2Fdownload.php%3F69844bb44a8cb2fc906b53b090d1d219&ei=xkZSSp32MczJ_gbT17isBQ&usg=AFQjCNHiUnwAMUOBqIJ7p87sVVMBXwLQ5w&sig2=F8UpQKDmb9_h9Fv1NsANqw.

13. **Pro IT, a. s.** ISMS - Systém managementu bezpecnosti informací. *Pro IT.* [Online] 2007. [Citace: 17. 10 2009.] http://www.proit.cz/doc/I_ProIT_info_ISMS_norma.pdf.

14. **YOUR SYSTEM, spol. s r.o.** Model PDCA. *Your System.* [Online] [Citace: 20. 9 2009.] http://www.yoursystem.cz/wps/wcm/connect/yoursystem/katalogvyrobkuasluzeb/bezpecnostIS/model_pdca/.

15. **Risk Analysis Consultants.** RAC - Řešení. *RAC - Risk Analysis Consultants.* [Online] 2008. [Citace: 23. 3 2009.] http://www.rac.cz/rac/homepage.nsf/CZ/Reseni.

16. **Equica a.s.** Řízení ICT. *Equica.* [Online] 2009. [Citace: 20. 9 2009.] http://www.equica.cz/rizeni-ict.

17. **IT Governance Institute.** Obtain COBIT. *ISACA.org.* [Online] 2009. [Citace: 20. 9 2009.] http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/Obtain_COBIT.htm.

18. **itSMF.** Úvodní přehled ITIL® V3. *itSMF Česká Republika.* [Online] 4. Duben 2008. [Citace: 20. 9 2009.] http://www.itsmf.cz/webset/y_download.asp?soubor=ITILbrozuraV3CZ13365.pdf&adr=D:\web\DB\webset\katalog_000\itsmf\&pu_lo=6E6570F869686CE19A656E203132313032353339.

19. **Dušátko, Jan.** Analýza rizik. *dusatko.org.* [Online] 2007. [Citace: 20. 9 2009.] http://www.dusatko.org/cs/node/13.

20. **Carnegie Mellon University.** OCTAVE. *CERT.* [Online] 2008. [Citace: 20. 9 2009.] http://www.cert.org/octave/.

21. **ÆXIS Security Consultants.** About RA2 art of risk. *ÆXIS Security Consultants.* [Online] 2009. [Citace: 20. 9 2009.] http://www.aexis.de/index.php?site=static&staticID=4.

22. **Západočeská univerzita.** Informační systém studijní agendy. *IS STAG.* [Online] 31. 10 2009. [Citace: 31. 10 2009.] http://stag.zcu.cz/dokumenty/IS_STAG_uvodni_prezentace.ppt.

23. **Jihočeská univerzita.** ISMS dokumenty. *ISMS portál.* [Online] 1. 11 2009. [Citace: 1. 11 2009.] https://isms.jcu.cz/.

24. **BITS.** Bits Publications. *BITS.* [Online] 25. 11 2009. [Citace: 25. 11 2009.] http://www.bitsinfo.org/p_publications.html#SRA.

Rejstřík

Seznam příloh

Součástí této práce je médium, na kterém jsou přiloženy následující soubory:

- Příloha I - Dotazník pro správce sítě v prvním návrhu
- Příloha II - Otázky pro uživatele
- Příloha III - Výsledky otázek s uživateli včetně kompletního vyhodnocení formou grafů.
- Příloha IV - Dotazník pro správce sítě ve druhé verzi