Bezpečnostní rizika IS veřejné správy a zdravotnictví

Patrik Heiser

Bakalářská práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Patrik Heiser**
Osobní číslo:	**A12219**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnostní rizika informačních systémů veřejné správy a zdravotnictví**
Téma anglicky:	**The Security Risks of Public Administration and Healthcare Information Systems**

Zásady pro vypracování:

1. **Seznamte se s informačními systémy veřejné správy a zdravotnictví.**
2. **Popište vybrané informační systémy z hlediska jejich funkčnosti.**
3. **Analyzujte a srovnejte používané metody zabezpečení vybraných informačních systémů.**
4. **Zhodnoťte bezpečnostní rizika těchto informačních systémů.**
5. **Navrhněte snížení bezpečnostních rizik pro slabá místa informačních systémů.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **LIDINSKÝ, Vít, Ivana ŠVARCOVÁ a Petr BUDIŠ. EGovernment bezpečně. 1. Praha: Grada, 2008. ISBN 978-80-247-2462-1.**
2. **HEGER, Vladimír. Komunikace ve veřejné správě. 1. Praha 7: Grada, 2012. ISBN 978-80-247-3779-9.**
3. **SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 3. Praha: Grada, 2009. ISBN 978-80-247-3051-6.**
4. **KIM, David a Michael G. SOLOMON. Fundamentals Of Information Systems Security: Information Systems Security & Assurance. 2. Boston: Jones & Bartlett Learning, 2013. ISBN 1284031624.**
5. **SMITH, Richard E. Elementary Information Security: 2nd Edition. 2. Boston: Jones & Bartlett Learning, 2015. ISBN 978-1284055931.**

Vedoucí bakalářské práce: **Ing. Bronislav Chramcov, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **5. února 2016**

Termín odevzdání bakalářské práce: **1. června 2016**

Ve Zlíně dne 5. února 2016

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Tato bakalářská práce se zabývá informačními systémy veřejné správy a zdravotnictví a to z hlediska jejich bezpečnosti. Analyzuje jednotlivé systémy, programy a jejich základní prvky. Práce poukazuje na současný stav informačních systémů. Dále přináší pohled na zlepšení současné bezpečnostní situace na úřadech a dalších oficiálních místech. Dílčím cílem práce je popis chodu a cílů bezpečnostních agentur, které mají na starosti bezpečnost informačních sítí v České republice. V neposlední řadě je naznačeno možné využití G cloudu pro systémy veřejné správy.

Klíčová slova: veřejná správa, eGovernment, G cloud, informační systém, bezpečnost

ABSTRACT

This bachelor thesis deals of information systems in public administration and health in term of safety. It further analyse every single system or programes and they basic parts. The thesis explains present condition of information systems. Next the theisis brings view on beter security situation for offices and others official places. Part of point in this thesis is principe of work agentures of security whose take a care about security of information network in the Czech republic. On the other side describe posibility of using G cloud for systems in public administration.

Keywords: public administration, eGovernment, G cloud, information systém, security

Chtěl bych touto cestou poděkovat rodině, přítelkyni za trpělivost. Dále patří dík Ing. Otto Ďuricovi a také vedoucímu práce doc. Ing. Bc. Bronislavu Chramcovovi, Ph.D.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Informační bezpečnost dnes dávno není otázka nainstalování antivirových software a firewall proti případným attackům či průnikům z internetu nebo z jiných sítí. Bezpečnostní procesy jsou dnes v současných organizacích nastavovány v souladu s legislativou a bezpečnostními standardy, ke kterým se dostaneme později. Stanovování cílů v této oblasti se přitom musí odvíjet od cílů celé organizace, proto je nutné brát v potaz aspekty subjektů v našem případě veřejné správy a zdravotnictví.

Práce bezpečnostního manažéra zdravotnické organizace zahrnuje specifičtější rizika v porovnání s kolegy v soukromém sektoru. Při řešení otázky bezpečného zpracování informací je v tomto sektoru více než v jiných sektorech důležitá důvěrnost, dostupnost a integrita dat, protože zdravotnické organizace pracují se spoustou citlivých osobních dat pacientů. Na základě těchto dat se dějí rozhodnutí, která mohou být velmi citlivá či přímo zničující pro každého občana potažmo pacienta, a proto jakýkoliv přístup k informacím lékařského personálu musí být jednoznačně identifikovatelný a dohledatelný. Česká legislativa na tato specifika pamatuje tak že jsou bezpečnostní požadavky na zpracování informací ve zdravotnictví upraveny zákony, o kterých se zmíním v této práci.

Také práce bezpečnostního manažéra informačního systému veřejné správy není zcela bez rizik, protože i jeho software obsahuje data vysokého počtu uživatelů a tedy I vysokého počtu citlivých údajů. Dále takový software zajišťuje spoustu služeb, které musí stát svým občanům zajistit.

Narušení bezpečnosti by mohlo mít vysoký dopad vzhledem k tomu, že každý občan České republiky využívá více, či méně služeb státu, které jsou podporovány systémem ISVS.

Rizik je v tomto sektoru opravdu mnoho, proto budou mezi sebou porovnány a také popsány nejpoužívanější informační systémy s daných sektorů. V souvislosti s daným tématem bude provedena analýza rizik. V zápětí budou tato rizika popsána a eliminována. Po případě navržena a změna ať už na základě zjištěných informací, či budou implementována na již fungujících modelech ze zahraničí nebo ze systémů nadnárodních korporací ať už je zřizovatelem stát nebo soukromý sektor.

I. TEORETICKÁ ČÁST

1 BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ

Internet se od svých počátků dramaticky změnil. Rozrostl se z univerzit a vládních agentur do celého světa a dnes má tato síť přes dvě miliardy uživatelů.

Jak tato síť rostla, změnila komunikaci mezi lidmi nemluvě o jejich stylu podnikání. Internet lidem přinesl spoustu příležitostí, benefitů ale i rizik. Rozvinul se a expandoval do různých podob. Dnes internet nemá žádné hranice, neřídí ho žádná vláda nebo úřední orgán. Internet jak ho známe dnes má podle [1]str. 48 své kořeny v počítačové síti Advanced Research Projects Agency Network (ARPANET), který vytvořilo ministerstvo obrany ve Spojených státech Amerických již v roce 1969.

Dnes však lidé (uživatelé) používají tuto síť úplně jiným způsobem a za jiným účelem. Dnes se lidé pracující v kyberprostoru musí vypořádat s novými a neustále se vyvíjejícími hrozbami. Tím myslím kyber zločince (hackery), teroristy nové doby.

Připojením počítače nebo jiného zařízení k Internetu se okamžitě vystavujeme případnému útoku, který může mít za následek odcizení jak soukromých dokumentů či dat, tak pracovních dokumentů a citlivých dat občanů České republiky. Proto je za potřebí zvláště u státních institucí aby jednotlivé informační systémy obsluhovali pouze proškolení a poučení pracovníci. Aby byly eliminovány tzv. Lidské chyby neboli lidský faktor.

1.1 Definice bezpečnosti ISVS

Jedná se o souhrn informací nebo atributů, které stanovují jaké si pravidla pro dodržování správných postupů při manipulaci s daty. Provozovatelé jsou tedy povini pravidelně udržovat informace v bezpečí a tím pádem zajišťovat ochranu nad svým provozovaným systémem. Systém opatření se tvoří z bezpečnosti informačních, komunikačních a dalších systémů. Cílem těchto systémů je především zajištění důvěrnosti, integrity a postupnosti jednotlivých utajovaných informací. Za tento systém opatření vždy zodpovídá správa systému, popřípadě jejich uživatelé, kteří do těchto systémů vstupují. Bezpečnost ISVS bych rozdělil do dvou odvětví a to sice na dosáhnutí ideálního stavu, kdy se jedná o určitý cíl který by se měl uskutečnit/splnit. A za druhé za použití jakých nástrojů, lze daných cílů dosáhnout. Podíváme-li se na bezpečnost jako na cíl měli bychom postupovat podle nějaké veličiny či kritéria, které nám bude schopno říci, zda je daný systém bezpečný či nikoli. Dále od jakého okamžiku lze konkrétní systém ISVS brát jako za bezpečný a popřípadě jak

moc je jeho zabezpečení účinné. Tato úroveň zabezpečení se z pravidla řadí to tzv. tříd. Kdy daná norma stanovuje počet a úroveň různých zabezpečovacích systémů a podle jejich účinnosti posléze vyhodnocuje a zařazuje systémy do různých tříd bezpečnosti. Zbytku kapitoly dle [2]str. 48.

1.2 Ověření bezpečnosti ISVS

V předchozí kapitole jsem popisoval specifikaci požadavků pro jednotlivé systémy ISVS. Tyto požadavky by však nebyly příliš platné bez jejich ověřování či testování proti možným útokům či lidským chybám. K tomuto účelu slouží proces zvaný certifikace. Jedná se o postup kterým se řídí jednotlivé úřady při ověřování způsobilosti technických prostředků pro ochranu utajených dat. Dále ověření způsobu nakládání s utajenými daty a také způsobilost kryptografických prostředků, které slouží k ochraně dat. V neposlední řadě se ověřuje stínící komora, která má také za následek ochranu dat a utajených informací.

Dá se tedy říci že, k vybudování bezpečného systému pro veřejnou správu je za potřebí správně nejlépe optimálně nadstavit úroveň zabezpečení. Toho lze dosáhnout pouze kombinací správně nadstaveného systému bezpečnostní politiky, dále dodržením požadavků které jsou uvedeny v právních předpisech a v jiných technických normách, popřípadě je dobré přizvat k projektu odborníky z daného oboru.

1.3 Normy bezpečnosti IS

Tyto normy neboli standardy jsou pravidelně obměňovány. Děje se tak z jednoduchého důvodu a to sice proto, že se vývoj informačních systémů prudce vyvíjí a s ním i možná napadení. Tyto normy se dají rozdělit do čtyř skupin a to na základní bezpečnostní normy, které slouží k obecnému použití. Další skupinou jsou normy funkční, které udávají realizaci požadavků vyplývajících z norem pro IS. Třetí skupinou jsou normy hodnotící, které slouží k hodnocení bezpečnosti jednotlivých informačních systémů, příbuzných produktů a postupů. Z těchto norem stojí za zmínku ITSEC, ITSEM, TCSEC. Čtvrtou skupinou jsou speciální normy, které slouží pro různé specifické činnosti ať už telekomunikační či zpracování osobních údajů tedy citlivých dat.

1.4 Analyzování rizik u IS

Při používání jakéhokoli informačního systému je důležité zanalyzovat pokud možno všechna možná rizika, která mohou vznikat za provozu různého nebo různých systémů. Pro tyto účely se nejlépe jeví analýza rizik, tato analýza nám pomůže odhalit a pochopit různá rizika ať už se jedná o manipulaci s daty popřípadě jiné skryté hrozby. Dále tato analýza nabízí určitý pohled na to, jaké hrozby jsou v daném případě nejpravděpodobnější, nebo nejničivější. S tím je spojena pravděpodobnost rizika a také její možné následky. Můžu tedy říci, že se jedná o jakýsi proces, který poukáže na možná rizika v dané instituci nebo právě na úřadech a pracovištích veřejné správy a sektoru zdravotnictví. Tato analýza se skládá s identifikace aktiv, identifikace hrozeb a zjištění hodnoty aktiv. Aktivum je v tomto případě bráno jako hodnota ať už hmotná či nehmotná, mezi hmotné bych zařadil peníze nebo cenné papíry. V mé práci se však spíše zabývám nehmotnými aktivy, jakými jsou například informace, data či lidské zdroje a kvalita jejich práce při zpracování dat. Dále tato analýza určí pravděpodobnost výskytu hrozeb a zranitelnost (náchylnost) každého aktiva.

Budeme-li se bavit o hrozbách, myslím tím nějakou osobu, vytvořený program/aplikaci nebo určitou sílu. Za hrozbu tak můžeme považovat různé přírodní katastrofy či krádeže zařízení ale z pohledu této práce je nejdůležitější vypíchnout hrozbu neoprávněného přístupu k informacím. Dopad takových hrozeb závisí na jejich úrovni, které se dají kvantifikovat za pomocí metod analýzy rizik.

2 SYSTÉMY VEŘEJNÉ SPRÁVY A ZDRAVOTNICTVÍ

V této kapitole se budu zabývat systémy veřejné správy z hlediska vymezujícího a právního rámce. Zmíním se o principu ISVS, jaké formy může mít. Dále nastíním, co lze považovat za informační systémy veřejné správy a co naopak nikoli. V této kapitole se také zaměřím na formu činností veřejné správy a na informační koncepci, ve které budou zmíněny všechny základní neboli sdílené informační systémy, které jsou používány více či méně všemi institucemi, které spadají pod veřejnou správu.

2.1 Co není ISVS

Do ISVS nepatří tzv. provozní informační systémy mezi které se řadí Operační systém webový prohlížeč, e-mailový klient nebo tabulkové a textové editory.

2.2 Co je ISVS

Aby mohl být jakýkoli informační systém označen jako ISVS, musí splňovat naplnění materiálních a definičních znaků ISVS , které stanovuje zákon o ISVS.

2.2.1 Zákon o ISVS

ISVS jsou takovým souborem informačních systémů, které jsou zapojeny do procesů veřejné správy. § 3 odst. 1 zákona o ISVS. Veřejnou správu lze chápat jako správu veřejných záležitostí, sledování veřejných cílů za podpory veřejných zájmů. Můžeme to chápat jako jakýsi protipól zájmů soukromých. Soukromé zájmy hájí každá právnická nebo fyzická osoba, která sleduje své soukromé cíle.

2.3 Informační koncepce v ISVS

Jedná se o plán (koncepci) ve kterém si orgán veřejné správy stanovuje své cíle v oblasti řízení bezpečnosti a kvality v provozu ISVS. V této koncepci se také vymezují principy pořízení, tvorby a provozu ISVS. Na to pamatuje vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy, Tato informační koncepce se edituje (navrhuje) pro celý orgán veřejné správy a nikoliv jen pro jednotlivé ISVS.

3 INFORMAČNÍ SYSTÉMY VE SPRÁVĚ ORGÁNU VEŘEJNÉ SPRÁVY

V této části budou popsány informační systémy, které spadají pod správu orgánů veřejné správy. Celkově existuje deset systémů s označením ISVS, dále tři informační systémy PIS (Provozní informační systémy) s vazbami na ISVS a další tři PIS systémy, které nemají vazby na ISVS. Popíšeme si, s jakými daty pracují, jaké služby poskytují a jaké technické a programové požadavky jsou potřeba k provozu pro daný informační systém. Jedná se o systémy veřejné správy, na které má ministerstvo vnitra smlouvy s různými dodavateli, například s firmou Microsoft. Tyto systémy popíši, nastíním jejich funkce, základní informace a popřípadě jestli existuje vazba mezi jednotlivými systémy. Následující systémy jsou popsány dle [3]str. 48.

3.1 Informační systémy veřejné správy

3.1.1 Portál veřejné správy

Jedná se o portál se zkratkou PVS dle [4]str. 48. Spadá pod útvar odboru projektu E-governmentu. Řídí se zákony č. 365/2000 Sb., nař. vl. 495/2004 Sb., nař. vl. 408/2003 Sb. Jedná se o systém vytvořený pro veřejnost, která prostřednictvím tohoto softwaru komunikuje s veřejnou správou, či získává potřebné informace k různým životním situacím. Dále systém zveřejňuje metodické pokyny a publikační sbírky předpisů, tak zvané věstníky. Tyto věstníky mohou vydávat buď to ústřední správní orgány, popřípadě ostatní instituce. Věstníky jsou volně ke stažení ve formátu PDF. Přičemž každý věstník musí obsahovat informaci o tom, jaká instituce jej vytvořila a zveřejnila a kdy daný předpis nabyde účinnosti. Portál dále zpřístupňuje tzv. povinně zveřejňované informace, mohou to být různé informace, které zveřejňují jednotlivé orgány veřejné správy řídící se legislativními předpisy. Systém podává veřejnosti informace k různým životním situacím, které se týkají řešení úkonů ve vazbě ke státní správě. Jedná se tedy o strukturované manuály i s odkazy na elektronické formuláře a podobně. V současné době je tato služba je poskytována a zajišťována společností O2 v současné době probíhá nekonečné updatování dat, informací a služeb. Systém obsahuje prezentační část, která poskytuje automatickou konsolidaci zdrojů. Tento systém slouží také pro přístup k zákonům, které se týkají rozsahu a pravomocí veřejné správy, dále systém umožňuje přístup k různým životním situacím, které se mohou obča-

ům stát. Jako příklad uvedu úmrtí blízké osoby nebo ztráta OP (občanského průkazu). Systém dále slouží jako místo, kde mohou uživatelé/občané elektronicky podávat žádosti k veřejné správě. Systém poskytuje následující služby:

- zprostředkování doručení dokumentů na jiné úřady ,
- zveřejňování elektronických adres podatelen
- zveřejňování obchodního věstníku.

3.1.2 IS o datových prvcích

Tento systém nese zkratku ISDP a spadá pod odbor koncepce ISVS. Řídí se zákonem č. 365/2000 Sb. §4 odst. 1 písm. i. Do tohoto Informačního systému přispívají provozovatelé ISVS. CVOS jeho prostřednictvím vyhlašuje datové prvky. Tato aplikace poskytuje oficiální informace, které se týkají datových prvků informačních systémů veřejné správy. Systém vyhlašuje datové prvky a zveřejňuje číselníky. Aplikace seskupuje sémanticky podobné datové prvky do datových slovníků. Pro tyto datové slovníky je charakteristický formát XML. Každý datový slovní má pak přiřazena dokumentace ve formátu PDF. K bezpečnému provozu je za potřebí mít zakoupeny a nainstalovány Windows 2000 Server nebo novější verze, MS IIS, MS SQL server 2000, Java.

Systém zpracovává tato data

- jednoduché datové prvky
- složené datové prvky
- datové slovníky
- číselníky datových prvků

Zde si uvedeme potřebné údaje o jednoduchých a složených datových prvcích:

Jednoduché datové prvky

- základní identifikační údaje (název, kód, skupina DP),
- technické specifikace (datový typ, minimální a maximální délka znaků),
- popisné prvky (komentář, definice, zdroj hodnot),
- obsah datových prvků (číselník, správce číselníku),
- provozní parametry (provozovatel a správce datových prvků, datum platnosti)

Složené datové prvky

- základní identifikační údaje (název, kód, akronym, skupina DP)
- provozní parametry (správce datového prvku, zdroj hodnot)
- složení datových prvků (tabulky všech jednoduchých a složených datových prvků, ze kterých je složen)

Přispívání do IS

vkládání nových podmětů pro další datový prvek, úpravu stávajícího datového prvku, smazání stávajícího datového prvku.

Zveřejnění datových prvků

- Zobrazení jednoduchého datového prvku,
- Zobrazení složeného datového prvku,
- Skladba složeného datového prvku ,
- Výskyt jednoduchých datových typů, které se nacházejí v datových typech složených.

3.1.3 IS o informačních systémech veřejné správy

Používanou zkratkou je IS o ISVS. Útvarem, který zajišťuje správu tohoto IS je Odbor koncepce ISVS a upravuje ho zákon č. 365/2000 Sb. §4 odst. 1 písm. h. Tento informační systém slouží k poskytování základních informací o dostupnosti a obsahu informačních systémů veřejné správy, které jsou právě zpřístupněny. Systém umožňuje přístup k základním údajům o všech ISVS v České republice a také zobrazení údajů o dostupnosti všech ISVS na území České republiky. K provozu je za potřebí technologické vybavení, které zajistí provoz IS, jinak Microsoft Exel.

Poskytované služby

- vkládání různých záznamů o ISVS
- ukončování činností ISVS
- obnova záznamů o ISVS

- kontrola datových prvků při vytváření vazeb
- kvalifikované certifikáty na čipových kartách
- využití e-podpisu

3.1.4 Regionální statistika

Tento informační systém nese zkratku REGS a odbor elektronických komunikací je jeho správcem. Je řízen zákonem č. 127/2005 Sb. Tento software zajišťuje sběr statistických dat. Je veden ve spolupráci s ČTU (Český telekomunikační úřad).

Systém zpracovává tato data

- ukazatele, které se týkají slektronických komunikací ze všech regionů ČR,
- vybrané spravodajské jednotky kterých je zhruba 70.

Systém poskytuje tyto služby

Systém sbírá a následně sumarizuje data od všech zpravodajských jednotek v České republice.

3.1.5 Centrální podpora uživatelů

Používaná zkratka je CPU a je spravován odborem projektu E-governmentu. Tento systém se neřídí žádným speciálním právním předpisem. Jedná se o podpůrný systém PVS (porálu veřejné správy) Informační systém zpracovává problémy a záporné podněty stran, které obsahuje portál veřejné správy. Jedná se o tzv. poruchové lístky. Systém eviduje a následně řeší vzniklé problémy různého charakteru na portálu veřejné správy. V současné době je provozovatelem telekomunikační síť O2.

3.1.6 Statistiky

Tento software nese zkratku STA a je spravován taktéž odborem projektu E-governmentu. Také pro tento software neexistuje specielní právní předpis. Systém má za úkol sběr statistických dat různých druhů. Jedná se tedy o systém, který především poskytuje náhled do přehledně zpracovaných statistik (statistické výstupy). Tyto výstupy dále slouží k lepší kontrole a zobrazení různých údajů. Systém zpracovává následující data:

Zpracování dat

- vedení statistik o vydaných elektronických podpisech,
- vedení statistik o obchodu na elektronikém tržišti,
- vedení statistik o návštěvnosti elektronického portálu,
- statistiky týkající se mapových služeb,
- evidence ECDL (Mezinárodní standard pro digitální znalosti a dovednosti)

3.1.7 Elektronické tržiště

Systém nese zkratku ET. Spadá pod útvar odboru projektu E-governmentu. Řídí se usnesením vlády 683/2002 Sb. Systém především eviduje a vede licence COVS které jsou potřeba k obchodování na e-tržišti. Níže je nastíněn seznam poskytovaných služeb:

Poskytované služby

- příjem dokumentů od Evropské unie,
- distribuování hlaviček a dokumentů z Centra na jednotlivé Resorty,
- distribuování dokumentů dle požadavků od uživatelů ,
- předkešování ruzných dokumentů,
- distribuování již připojených dokumentů,
- přenos systémových informací,
- vyhledávání, čtení a ukládání dokumentů ,
- posílání požavků,
- administrace

3.1.8 EU Extranet ČR Distribuční agent

Systém nese zkratku EUXDA a je pod správou odboru evropské integrace a mezinárodní spolupráce, není zakotven žádným speciálním právním předpisem. Systém zprostředkovává komunikaci uživatelů s externímy systémy EU a distribuuje dokumenty z Evropské unie. Jedná se o jednotnou distribuovanou aplikaci, která má název distribuční agent. K zajištění pro komunikační bezpečnost slouží primárně Crypto Gateway, dále CSP II Microczech a také MS strong CSP. Mezi poskytované služby patří zejména přijímání a distribuce dokumentů z evropské unie úřadům a celkově uživatelům v české republice. Systém je rozdělen na dva resortní uzly. Jeden z nich je utajovaný a nese označení (V),

druhý uzel je neutajovaný a nese označení (N) dle [5] str. 48 se jedná o metodu generického řešení, kde existují dva vzdálené uzly, z nichž jeden je utajovaný.

3.1.9 E-podpis

Jako zkratka je používaná EPEV. Zakotvujícími právními předpisy jsou zákon č. 227/2000 Sb., vyhl. č. 366/2001 Sb., vyhl. č. 365/2000 Sb., nař. vlády č. 465/2004 Sb. Systém eviduje a zveřejňuje různé informace, které se týkají nebo souvisí s využitím elektronického podpisu. K bezpečnému provozu je za potřebí Windows 2000 Server ale spíše jeho novější verze, dále MS IIS a k zadávání údajů do tabulek MS Exel, popřípadě klasická verze MS office. Níže popisuji poskytované služby:

Poskytované služby

- Systém zveřejňuje a zpřístupňuje seznam akreditovaných poskytovatelů, kteří vlastní certifikační služby.
- Zveřejňuje výsledky ověřených a platných kvalifikovaných certifikátů.
- Dále zveřejňuje seznamy kde jsou vyhodnoceny nástroje elektronického podpisu.

3.1.10 Příprava návrhu pro výzkum a vývoj

Systém nese zkratku PNW a spadá pod odbor ekonomický, řídí se právním předpisem č. 130/2002 Sb. Co se týče charakteristiky, systém slouží především k podpoře pro návrh výdajů ze státního rozpočtu a také pro výzkum a vývoj v daných odvětvích. Systém vytváří jeden krát ročně předpokládaný vývoj výdajů ze státního rozpočtu pro vědu a výzkum na dva nastávající kalendářní roky. K provozu je za potřebí vytvoření jednoduché html stránky s java scriptem, který má výstup ve formátu XML.

3.2 Provozní informační systémy s vazbami na ISVS

3.2.1 IS-EKO účetnictví

Tento systém nese zkratku IS-EKO a zcela logicky spadá pod ekonomický odbor. Řídí se zákonem č. 563/1991 Sb. A vyhláškou č. 16/2001 Sb. Systém má na starosti vedení účetnictví správních center. Pro ISVS tento systém poskytuje různé závěrky ať už v elektronické či tištěné podobě. Dále systém zajišťuje účetní rozvahy a výsledovky. Mezi potřebné technologické vybavení patří MS Windows 2000 Server a také MS SQL Server 2000 nebo novější verze, pro klientské strany je za potřebí MS Windows XP, Vista, 7, 8 a další vše záleží na uvážení jednotlivých správních center a úřadů dle jejich uvážení. Níže uvádím heslovitě seznam poskytovaných služeb:

Poskytované služby

- správa účetnictví,
- evidence majetku
- správa skladů
- správa pokladen
- komunikace s bankou

3.2.2 UNICOS

Systém nese stejnou zkratku, jako je jeho název a spadá pod ekonomický odbor. Je zakotven v zákonech č. 143/1992 Sb., č. 217/2000 Sb. Dále se řídí nařízením vlády a to nařízením vlády č. 289/2002 Sb. ve znění nařízení vlády č. 514/2004 Sb. Systém má na starosti řízení prostředků, které jsou vynaloženy na platy zaměstnanců, dále na ostatní platby za činnosti které zaměstnanci vykonají. Systém také eviduje vnitřní rozpisy počtů zaměstnanců. Systém zajišťuje výstupy pro různé instituce, jakými jsou například Finanční úřady, Statistické úřady, zdravotní pojišťovny, OSSZ neboli Okresní správě sociálního zabezpečení, systém dále poskytuje informace o platech zaměstnanců. K plynulému provozu je potřeba mít zakoupen operační systém MS Windows Professional a také je zapotřebí mít zprovozněný účet e-mailového klienta. Z pohledu bezpečnosti se nejlépe jeví emailový klient od společnosti Mozzila a to Mozzila Thunderbird, popřípadě produkt společnosti Microsoft a to Windows Live Mail.

3.2.3 Statistika z účetnictví - el. sběr dat dle čísel výkazů

Systém nese zkratku STAESD a opět spadá pod ekonomický odbor. Systém má za úlohu odesílat pravidelné výkazy z účetnictví do systému statistiky, který je popsán výše v této práci. Systém poskytuje výstupy z výkazů z účetnictví a dále zajišťuje výkazy týkající se nákupu či prodeji služeb do zahraničních zemí po případě ze zahraničních zemí do České republiky.

3.3 Provozní informační systémy bez vazeb na ISVS

3.3.1 Mapy pokrytí - přístup vysokorychlostního internetu

Tento systém, který je bez vazeb na ISVS nese zkratku MAPP a spadá pod odbor elektronických komunikací. Systém je v zákoně zakotven požadavkem EK tedy evropské komise. Systém byl zřízen za účelem provádění a sběru statistických dat, které se týkají tzv. vysokorychlostního internetu. V současné době jej externě zajišťuje společnost TESTCOM. Systém zpracovává databáze všech obcí, které mají pověřený obecní úřad, především zjišťuje stav přístupnosti k vysokorychlostnímu připojení (internetu) napříč jednotlivými obcemi. Systém poskytuje přehledný seznam o situaci v jednotlivých regionech v České republice z hlediska dostupnosti technologií nutných k připojení pro vysokorychlostní síť, jedná se o přehledovou tabulku s orientačními mapami. K plynulému provozování je za potřebí program od společnosti Adobe a to Adobe Acrobat, který bych také doporučil, v současné situaci je však na každém úřadě jakou alternativu si zvolí pro svůj provoz.

3.3.2 Veřejný internet

Systém nese označení VEI a spadá pod Odbor projektu E-governmentu. Jediným zakotvujícím právním předpisem je dokument EU (Evropské unie). Na rozdíl od předešlého informačního systému MAPP tento systém eviduje místa (části) s přístupem k veřejnému internetu ne vysokorychlostního. Systém poskytuje náhled na seznam regionů s místy kde je dostupný internet plus zobrazuje přehledovou mapu.

3.3.3 CLAVIUS

Název systému je i zároveň jeho zkratkou a spravuje ho Referát knihovnicko-informačních služeb. Neexistuje žádný právní předpis, který by ho zakotvoval. Jedná se o systém, který vede evidenci knih v knihovnách, nebo, na jiných oficiálních lokacích. Do systému lze zadávat neomezenou délku vstupních polí, dále je systém schopen ukládat jednotlivé dokumenty do jedné báze. Tato aplikace podporuje MDI (Multi document interface). Výhodou je velmi intuitivní ovládání, jelikož jeho uživatelské prostředí je podobné jako u programů Microsoft Office. Další výhodou je dobrá kompatibilita se zmíněnými programy. Systém má předefinovány šablony jak pro vstup, tak pro výstup. Systém také podporuje technologii čárkových a QR kódů. Dále je podporován modul s názvem WWW, který umožňuje prezentaci dat/titulů na internetové síti, popřípadě na Intranetu dané instituce. V neposlední řadě bych vyzdvihl podporu všech používaných standardů pro knihovnictví. Systém poskytuje náhled na evidenci uživatelů, dále evidenci knih, a zároveň funguje jako software pro výpůjčku či objednávání titulů nebo li knih. K bezpečnému a plynulému provozu je za potřebí Windows 2000 Server, nebo jeho novější verze, MS IIS (Internet Information Services) a na straně klienta plně dostačuje operační systém MS Windows XP nebo novější verze, které bych doporučil především z hlediska zabezpečení, protože například pro Windows XP se již dnes nevydávají aktualizace. [6] str. 48

Obr.1. Ukázka grafického prostředí CLAVIUS

4 INFORMAČNÍ SYSTÉMY VE ZDRAVOTNICTVÍ

V současné době je rozdíl mezi využívání informačních technologií mezi zdravotnictvím a veřejnou správou markantní. Jak již bylo nastíněno, zatímco v ISVS je situace velmi nepřehledná až přehlcená u zdravotnictví je to přesně opačně. I v současné době některé nemocnice stále nevyužívají žádný informační komunikační systém pro evidenci a zasílání dat o pacientech. Některá pracoviště používají k tomuto účelu CD nosiče popřípadě flash disky, v horších případech klasické „papírové“ obálky a šanony. Poslední zmíněná situace se týká především malých ordinací například u praktických lékařů. Budeme-li se bavit o krajských a velkých nemocnic v okresních městech je zde situace o mnoho lepší. Následující kapitoly se řídí dle [7] str. 48.

4.1 Informační systémy zdravotnických středisek

Systém funguje na principu sdílené databáze, kde jednotlivá pracoviště jsou on-line připojená k vnitřní síti (intranet). Lékařské dokumentace jsou tedy uloženy v datové centrále, do které může personál nahlížet (číst), nebo vypisovat jednotlivé údaje (zápis). Pokud je pacient převezen na jiné pracoviště či oddělení a je zaevidován v systému, odpadá fyzické přeposílání celé dokumentace. Existuje zde velký výskyt využívání čárových kódů, které nedovolí jakoukoli záměnu při jednotlivých přesunech pacienta po odděleních.

Co se týče soukromých lékařů a jiných zdravotnických center, situace není standardizovaná. Jinými slovy neexistuje žádná jednotná platforma ani zákon, který by jednotlivým lékařům přikazoval jaké zařízení pro registraci a komunikaci mají používat. Důvodem je to že tito lékaři nespadají do systému nemocnic a poliklinik. Situaci si tak každý lékař řeší dle svého uvážení. Většina lékařů využívá internetové připojení v podobě klasické pevné linky či využívají ISDN linku. Menší procento lékařů pak investuje do rozsáhlejšího systému s názvem ADSL.

4.1.1 IS L-BIS

Tento systém vyvinula a provozuje společnost LAURYN. Systém je tvořen šesti subsystémy, které se skládají podle [8] str. 48 z agendy ubytovací, zdravotní, rehabilitační, stravovací a skladové a manažerského informačního systému, dále je možno systém integrovat a propojit s ostatními systémy jakými mohou být např. Ekonomický systém, či systém kartový.

Co se týče technologií, systém pracuje na platformě MS Windows XP až Windows 8. Systém pracuje jak na 32, tak na 64 bitové verzi. Jedná se o aplikaci s architekturou klient server. K provozu je za potřebí MS Word a MS Exel a také server MS SQL 2005 a jeho novější verze. Systém je určen jak k síťovému, tak k terminálovému provozu.

V současné době systém využívá 54 zdravotnických center na území České republiky a 14 center na území Slovenské republiky.

4.2 Střediska bez IS

I v dnešní informační době se najdou lékaři, kteří nevyužívají žádný zdravotnický informační systém. Jedná se především o služebně starší lékaře, kteří nemají důvěru k novým systémům. Lékařské zprávy tedy stále píší do papírových kartoték. Tím však značně komplikují a z dnešního pohledu i zpožďují chod celého systému, kdy musí kartotéku zaslat do nemocnice aby, při hospitalizaci pacienta zjistili, v jakém zdravotním stavu se pacient nachází, jaké medikamenty užívá a celkově celou historii pacienta.

Při hospitalizaci jsou nová data zaznamenávána do systému. Problém nastává, pokud pacient nemá kartu v systému zavedenou, musí se mu tedy zavést nová karta, která samozřejmě neobsahuje starší záznamy.

4.3 Propojení IS ve zdravotnictví s ISVS

Aby byl jakýkoli informační systém smysluplný, měl by být součástí nějakého většího celku, v našem případě se jedná o propojení zdravotnického systému se systémy veřejné správy nebo jinými institucemi např. (zdravotní pojišťovny, úřady práce a finanční úřady). Ta-

kový systém by měl sdílet společná data a mít odpovídající ochranu proti nedovoleným vniknutím do systému. Ale zároveň by měl umožnit k nahlédnutí určité informace, které se týkají jednotlivých občanu potažmo pacientů. Každý občan by měl mít možnost nahlédnout do svých záznamů a také by měl mít právo aktualizovat svá data, jakými jsou např. (trvalé bydliště, rodinný stav apod.)

5 BEZPEČNOSTNÍ RIZIKA ISVS A IS VE ZDRAVOTNICTVÍ

Úřad, který přijal informačně bezpečnostní politiku a provozuje ji ve svém systému, musí počítat s různými útoky, které mohou být vedeny jak zevnitř, tak zvenčí [9] str. 48. Útokem zevnitř budeme brát útok vedený osobou, která je v zaměstnaneckém poměru daného úřadu, nebo je vázána externí smlouvou s úřadem. S touto myšlenkou příliš nesouhlasím (většina útoků bude spíše prováděna z venčí), ale vyvrátit ji nelze. Daleko větším problémem jsou bezesporu útoky vedené zvenčí, čili osobami, které se snaží nabourat do systému, za účelem zisku informací/ financí či dat. Takovéto osoby můžeme nazvat „Crackery". Z důvodů které byly popsány blíže, jsou najímány různé bezpečnostní agentury, které zajišťují plynulý provoz. V České republice funguje nepřeberné množství takovýchto agentur, které mají různé kvality. Pro tuto práci jsem vybral ty, které se podílí na bezpečnosti ISVS a zdravotnických systému, kterými se tato práce zabývá.

5.1 NAKIT

Tento název je zkratkou pro nově vznikající agentury s názvem Národní agentura pro komunikační a informační technologie. Tento projekt vnikl 21. Prosince 2015 z usnesení vlády České republiky č. 1065, jedná se o nový státní podnik, který bude mít na starosti plnění ICT strategií zřizovatelů. Jedná se o servisní útvar pro Ministerstvo vnitra, které mu bude poskytovat koncepční rozvoj informačních technologií a celkově komunikační infrastruktury, která je vlastněna státem. [10] str. 48.

Cíle agentury NAKIT

Agentura bude především sledovat nové trendy týkající se informačních a komunikačních technologií jako jsou bez pochyby bezpečnost komunikačních sítí státu, dále, kapacity a celková dostupnost sítí. Požadovaným cílem je konsolidace znalostí a následné prosazení ucelené koncepce, kterou zajistí státní agentury s dalšími společnostmi. Dojde-li ke sdílení následně vybudované infrastruktury, ušetří se značný objem peněz ze státních zdrojů.

5.2 CSIRT

Jedná se o tým provozovaný sdružením CZ.NIC, který mimo jiné zajišťuje bezpečnost počítačových sítí a řeší bezpečnostní incidenty na sítích provozovaných na území České republiky. Podle [11] str. 48 je od 1. ledna 2011 CSIRT správcem české národní domény. Podílí se na kybernetické bezpečnosti na sítích v České republice. Tým dále přebral roli národního PoC neboli Point of Contact a tím se stal vzdělávacím centrem v oblasti kybernetické bezpečnosti.

Cíle CSIRT

Tým udržuje vztahy se zahraničními partnery zejména s nadnárodní komunitou CERT/CSIRT a s dalšími aliančními partnery. Dále spolupracuje se státní správou, bankami, bezpečnostními složkami a s ISP (informační systém o platech). Tým poskytuje služby z oblasti internetové bezpečnosti.

5.3 Hrozby pro IS

Úřad, který přijal informačně bezpečnostní politiku a provozuje ji ve svém systému, musí počítat s různými útoky, které mohou být vedeny jak zevnitř, tak zvenčí. Útokem zevnitř budeme brát útok vedený osobou, která je v zaměstnaneckém poměru daného úřadu, nebo je vázána externí smlouvou s úřadem. S touto myšlenkou příliš nesouhlasím (většina útoků bude spíše prováděna z venčí), ale vyvrátit ji nelze. Daleko větším problémem jsou bezesporu útoky vedené zvenčí, čili osobami, které se snaží nabourat do systému, za účelem zisku informací/ financí či dat. Takovéto osoby můžeme nazvat Crackery. [12] str. 48.

5.3.1 Vnitřní hrozby

V jednom českém rčení se dozvíme že, pod svícnem je největší tma. Častokrát se proto může stát, že osoby, bezpečnostní pracovníci či bezpečnostní instituce často opomenou variantu, že by pracovník ve firmě vynášel informace pryč. V této kapitole si tedy uvedeme nejčastější příklady tzv. vnitřních hrozeb.

Nespokojenost zaměstnanců

Jedná se o skupinu zaměstnanců, kteří nejsou spokojeni se svými pracovními podmínkami, nebo s platovým ohodnocením. Pro jiné osoby to zase může být špatná komunikace nebo tzv. chemie v kolektivu pracovníků. Takový typ zaměstnance se lehce může stát rizikovým co se týče bezpečnosti. Jako příklad uvádí [13] str. 49 správce sítě daného úřadu, který si po těžkém dni pohovoří nad sklenicí alkoholického nápoje svému známému či v nedbalosti jiným osobám, mezi kterými se mohou skrývat jedinci, kteří by k těmto utajovaným informacím mohli proniknout a využít jich. Tato představa je spíše méně pravděpodobná, ale do této práce jsem ji raději zahrnul, jako jednu z možných rizik.

Úřad by se měl tedy postarat o vytvoření bezpečnostní politiky, která bude respektovat důležitost dat. Například aby každé oddělení mělo možnost se připojit na samostatný server. Pokud ale instituce využívá centrální datový sklad, je za potřebí dlouhého a pečlivého procesu zkoušení a testování systému a také zkoušení práv pro přístup k serverům. Zkrátka je třeba zamezit přístup nepovolaným nebo nekompetentním osobám. Dále je zapotřebí vytvořit systém, který bude schopen monitorovat všechny aktivity v četně pokusů o průnik a následně je poslat správci systému.

Rozdělení pravomocí

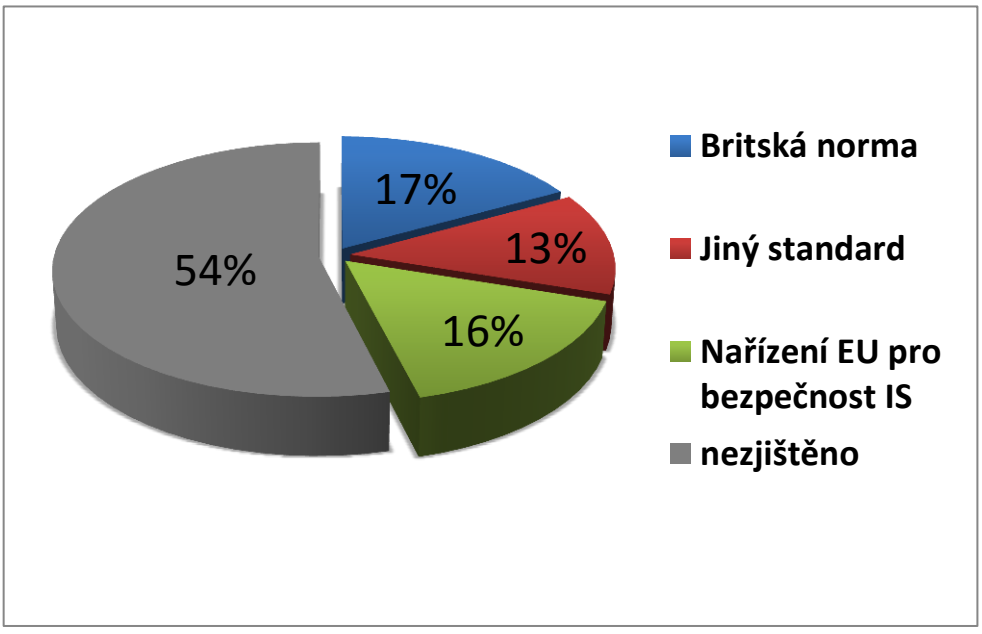
Vše začíná už při výběru zaměstnanců, ve státní správě a zdravotnictví sice existují tabulky na dané pozice, např. Dosažené vzdělání apod. Ale každá osoba je jiná a nikdy nelze vyloučit, že některé úkony zvládá bezpečně.

Proto je za potřebí provádět kontroly z vedení a také zaměstnance posílat na pravidelná školení. Je to sice investice, ale podle mého názoru ta nejlepší možná. Po takových to školeních je nejlepší zaměstnance podrobit testu, ze kterého by vyplynulo, jak kdo chápe danou problematiku. V případě splnění, by zaměstnance neměla minout odměna v podobě platového růstu, aby takto kvalifikovaný zaměstnanec neodešel k jiné instituci.

Outsourcing

Jedná se o firmy nebo týmy, které se živí vytvořením, zprovozněním a správou informačních systémů a přenosu dat. Jedná se tedy o externí firmy které mají také přístup k citlivým informacím od úřadů či jiných center. Zde je možné nebezpečí v tom že informace je třeba chránit nejenom před vlastními zaměstnanci, ale také před zaměstnanci dané externí firmy. Mezi těmito dvěma subjekty totiž proudí obrovské množství dat.

Z tohoto důvodu je zapotřebí uspořádat výběrové řízení na danou outsourcingovou společnost. Ze statistik [14] str. 49 pak vyplývá, že firmy s vyšším počtem zaměstnanců (100 a více) volí bezpečnostní firmy, které pracují s normou ISO/IEC 17799/BS 7799 jedná se o Britský standard. V české republice se jedná zhruba o 17% firem. Dalším zajímavým údajem pak je 13% firem, které si volí instituce, které se řídí nařízením evropské unie pro bezpečnost informačních systémů. Mezi poslední zmíněnou skupinu bych řadil i informační systémy veřejné správy. Následující graf zobrazuje jednotlivé procentuální rozložení podle použitých norem



Graf. 1. Procentuelní vyjádření podle používaných bezpečnostních norem.

Je třeba kontrolovat data to se dá zařídit dvěma způsoby. Prvním je umožnění přístupu outsourcingové firmě k datové základně daného úřadu. Jedná se ale o nedoporučovaný způsob, protože externí správce má přístup k veškerým informacím a tím i neomezenou

moc nad všemi daty. Druhý způsob je založen na principu schvalování každého toku dat, která jdou směrem ven. Sice se jedná o časově náročnější řešení, ale bezpečnost je o mnoho vyšší.

Správci systému

Jedná se o velice zapeklitý problém, který zní jak uhlídat/ kontrolovat zaměstnance, kteří jsou zároveň odpovědni za bezpečnost celého systému? Tito zaměstnanci se mohou hájit tím, že pro optimální vykonávání své práce zkrátka přístup ke všem informacím musejí mít. To je sice pravdou, ale v takovém případě neexistuje prakticky žádná kontrola těchto zaměstnanců.

V takových situacích hlavně záleží na výběru zaměstnance personalistou, doporučil bych kontaktovat předchozího zaměstnavatele, dále si myslím že není od věci si nechat vyjet výpis z trestního rejstříku a celkově si případného zaměstnance na této funkci tak zvaně „proklepnout". Také považuji za důležité zmínit tzv. rozdílnou politiku přístupu k datům. Nově zabudovaný správce sítě by neměl dostat přístup ke všem datům a měla by nad ním být kontrola ze strany zkušenějšího a prověřenějšího správce, který již má zkušenosti s daným systémem/ s danou sítí. Tímto krokem lze zamezit různým nechtěným ale samozřejmě také chtěným chybám ze strany tzv. junior administrator. [12] str. 48

5.3.2 Vnější hrozby

V této části se budeme zabývat různými potencionálními hrozbami, které mohou přijít z venčí. V této souvislosti se často vyskytuje označení „hacker". Toto označení je u veřejné vnímán jako něco negativního. Mohou za to především různé aktivity médií, které dokonce neváhají použít označení terorista.

Dle mého je toto označení poněkud zkreslené, protože jak víme, z historie za hackera se vždy považovali lidé, kteří se snaží co nejvíce rozšířit své znalosti a schopnosti v oblasti výpočetní techniky, a k tomu samozřejmě patří určité zkoumání různých zabezpečujících systémů, algoritmů a hesel. Pro již zmíněné označení terorista nebo také kyber terorista lépe sedí synonymum „cracker" tedy osoba, která se snaží s využitím svých znalostí proniknout do různých systémů za účelem co největšího poškození, či ovlivnění daného cíle.

Historie již několikrát zaznamenala útoky vedené za účelem zisku peněžních prostředků, nebo byly tyto útoky dokonce sponzorovány třetí stranou, většinou za účelem získání informací.

Sociotechnika

Pojem sociotechnika lze pojmenovat jako určitý způsob jak přesvědčit či ovlivnit vytipované osoby, které mají přístup ke kýženým informacím, které chce sociotechnik získat.

Sociotechnik je podle [15] str. 49 schopen předstírat osobnost s jinou totožností a prostřednictvím různých technik, je schopen manipulace a následného využití osob tak, aby se dostal k hledaným informacím i za následné pomoci různých technologických prostředků. Profesionální sociotechnik (ze slova sociální inženýrství) musí skvěle ovládat zákonitosti lidské psychiky, dále by měl být skvělým taktikem a v neposlední řadě brilantním hercem, při zvládnutí těchto třech faktorů dokáže zkušený sociotechnik vyloudit informaci z převážné většiny osob. Znalosti v oboru IS nejsou v prvotní fázi vůbec za potřebí. Lze říci, že podstatou sociálního inženýrství je zaměření se na nejslabší článek v řetězci, což je v dnešní době člověk.

Předmětem této kapitoly bude především tzv. sociohacking, budeme se zabývat významem, dále si uvedeme některé příklady použití a také si zodpovíme otázku obrany proti této technice.

Budeme-li se bavit o hrozbách síťových, všeobecně se tyto útoky na informační systémy rozdělují na:

- fyzické
- sémantické
- syntaktické

Do syntaktických útoků dle [12] str. 48 se řadí útoky na softwarové bázi. Jedná se především o různé viry, červy apod. Pod tuto kategorii dále spadá útok typu (D)DoS.

Co se týče útoků sémantických, jedná se o útoky vedené přes lidskou komunikaci. Vše je založeno na podávání nepravdivých informací a ty jsou podsouvány osobám, které jsou po té ovlivněny a jejich chování a rozhodování může být odlišné.

Dále je zapotřebí zmínit útoky autonomní a kognitivní. První zmíněný způsob útoku se vyznačuje tím, že není za potřebí žádné aktivity ze strany uživatele. Dá se tedy říci, že tento útok je realizován pouze za přispění výpočetní a komunikační struktury.

Infiltrace mezi pracovníky firmy

Tento druh hrozby je méně pravděpodobný avšak vyloučit jej nelze. Jeho použití je spíše proveditelné na větších pracovištích, kde se všichni zaměstnanci neznají dokonale. Jedná se o způsob, kdy si osoba zjistí o daném úřadě konexe mezi jednotlivými zaměstnanci, jména ostatních zaměstnanců apod. S těmito nabitými informacemi se obrátí na jednoho pracovníka s tím že u něho vyvolá dojem, že se jedná o jeho kolegu kupříkladu z jiné pobočky či města. Pokud se podaří osloveného pracovníka přesvědčit o tom, že ho kontaktoval jeho kolega, kýžené informace jsou většinou sděleny. Zaměstnanec, který takové informace sdělí si v mnoha případech ani neuvědomí komu, že danou informaci podal, například k vůli stresu, časovému tlaku apod. Dalším faktorem je fakt, že podvědomě si zaměstnanec může myslet že se jedná o test, popřípadě že se může informovaného dotázat příště až bude pomoc potřebovat zaměstnanec, který danou informaci poskytl.

Jediným efektivním řešením je ověření totožnosti volajícího „kolegy“, popřípadě vyžádání osobního čísla často označováno jako ID. Dalším krokem může být dotaz, ze které pobočky volá a kdo je jeho nadřízený. Pokud nejsou dotázané informace správné, v žádném případě by zaměstnanec neměl nic prozrazovat.

Falešná identita vlivné osoby

Metoda se zakládá na tom, že každá osoba má přirozeně v sobě zakódován respekt z autorit. Je to způsobeno především výchovou a respektem již od mládí k poslouchání druhých. Počínaje rodinnými příslušníky přes učitele a důležité osobě na telefonu konče. Člověk je tedy veden k tomu, aby pořád někoho poslouchal, jedná se tedy o patologický jev, který jen tak s koncem dětství nezmizí ba naopak. Právě na tomto kameni staví tato metoda, hacker se pomocí autoritativního vyjadřování a představení se za např. Generálního ředitele celé korporace pokouší o vytáhnutí vnitropodnikových informací či jiných dat. Při tomto stylu jednání většina zaměstnanců uposlechne zadané příkazy a ty následně splní, popřípadě poskytne kýžené informace.

Prevence je přitom téměř totožná jako u předchozí kapitoly. Princip spočívá v tom, že každý zaměstnanec je povinen řádně ověřit totožnost volajícího. I kdyby se mu představil jakkoli, tento postup je zásadní. Pokud by se skutečné jednalo a generálního ředitele nebo jinou osobu s vysokým postavením, zaměstnanci nic nehrozí, protože provedl standardní postup legitimace.

Phishing

Jedná se o metodu „hackingu“, která je velmi nebezpečnou pro tu část uživatelů, kteří nejsou příliš znalí v oblasti bezpečnosti internetu. Jeho použití je především u bankovních účtů, je to tedy nebezpečné, pokud zaměstnanec odesílá peněžní obnosy ze zařízení v práci pro různé účely. Název vznikl dle [16] str. 49 na hackerské konferenci roku 1996, kde každý napíchnutý účet nazývali rybou čili „the fish“ z tohoto pojmenování vzniklo pojnenování phish a následně nám již známý phishing. Phishing se může objevovat, jako e-mailová zpráva ve které je obsaženo oznámení nebo zpráva s pochybným příběhem například výhra v soutěži, či jiná atraktivní zpráva. V takovém e-mailu se po příjemci žádá vyplnění citlivých dat, jakými jsou například heslo do systému interbanking nebo do jiné aplikace na které se nacházejí peníze. Dále je požadováno kliknutí na odkaz, který uživatele odkáže na uměle vytvořené stránky většinou známé instituce se jménem. Jde však o pouhou napodobeninu oficiální stránky uvedené firmy.

5.3.3 Hygiena hesel

Všeobecně je doporučováno si hesla tvořit spíše s více znaky a s různou pestrostí znaků. Velká část uživatelů však tyto rady ignorují a tak podstupují riziko prolomení svého hesla a v práci obzvlášť. Nejhorší variantou je použití všeobecně známých slov jakými jsou např. „ahoj, 1234, mail“. Takto podobně postavená hesla dokážou prolomit programy, které mají svůj seznam neboli slovník, ze kterého dosadí často používaná slova či slovní spojení a pokouší se tak prolomit dané heslo. Jedná se například o programy Hackmail a Brutus A2.

Dnešní operační systémy ukládají zahashovaná či zašifrovaná hesla do souboru. K zašifrování hesel se dnes většinou používá tzv. symetrický klíč (DES). Problém ale spočívá v tom, že kdyby se zkušený hacker dokázal dostat na dostatečný čas k počítači, pravděpo-

dobně by se mu povedlo toto šifrování prolomit. Proto je lepší použít některou ze známých hashovacích funkcí kde je nejdříve porovnáno uložené heslo s heslem zadaným ze kterého se vzápětí vytvoří otisk. Výsledkem je že při zpětné kontrole nebude vydáno původní heslo zpět.

Mezi oblíbené funkce dnes patří podle [17] str. 49 MD5 a SHA-1, jedná se ale o funkce, které jsou již prolomeny (MD5 od srpna 2004, SHA-1 od února 2005). Proto bych doporučil používání funkce SHA-2 u které zatím nebyly zjištěny žádné bezpečnostní slabiny. Druhá metoda je tedy mnohem bezpečnější i když situace kdy se fyzicky útočník na úřadě ocitne u počítače sám je minimální, opomenout jsem ji však nemohl.

6 ELEKTRONICKÁ VÝMĚNA DAT EDI

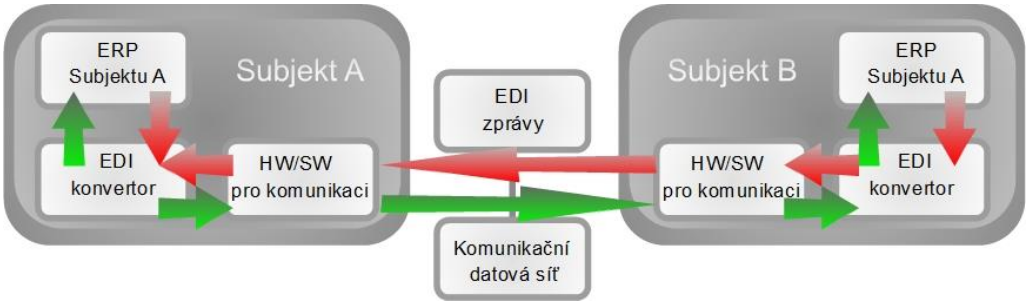
Jedná se o technologii, která slouží pro komunikaci mezi subjekty na sobě nezávislými. Při této komunikaci dochází k výměně či zasílání dokumentů v elektronické podobě, může se jednat o standardní dokumenty či strukturované popřípadě strukturované. Systém nese zkratku EDI (Electronic Data Interchange).

Dle [18] str. 49 Kompatibilitu při komunikaci zajišťuje systém EANCOM. Tento systém je schopen pracovat s většinou dokumentů, které jsou používány v obchodním prostředí. Cílem použití tohoto systému je přechod z papírových dokumentů na elektronické, což má za následek snížení nákladů a zároveň zvýšení efektivity, bezpečnosti a v neposlední řadě úspora času. Dále hlídá kompatibilitu mezinárodní standard s označením UN/EDIFACT, tento standard spravuje a dále vyvíjí organizace GS1 s globálním působením. Tato organizace také zajišťuje kontrolu nad celým procesem vývoje a na dodržování zásad při jeho používání.

Dá se tedy říci, že EDI komunikace umožňuje propojení informačních systémů od různých úřadů z různých krajů, které používají odlišné softarové či hardwarové platformy. K tomu jsou za potřebí EDI konvertory, jedná se o aplikaci, která dokáže zkonvertovat (přeměnit) data od poskytovatele do formátu EDI který systém používá pro přenos zpráv (informací). Pokud dojde k příjmu zpráv systém EDI opět zkonvertuje data do požadovaného formátu tak aby podnikové informační systémy příjemce dokázaly s těmito daty dále pracovat. Zbylé kapitoly se řídí dle [19] str. 49.

6.1 Průběh výměny zpráv mezi koncovými subjekty

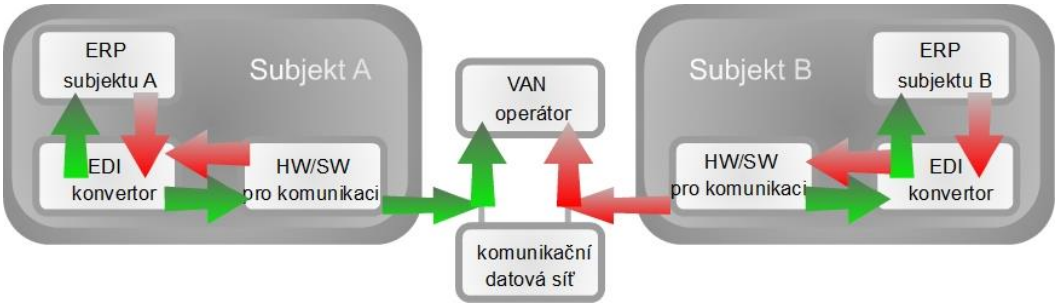
Každý subjekt, který chce využívat komunikaci EDI s používanou sítí x. 400 musí vlastnit software umožňující připojení do datové sítě. Dále je za potřebí vlastnit konvertor. Konvertorem myslím specializovaný software pro komunikaci s daty (zprávami). Jedná se však o velmi nákladnou cestu jak z hlediska nákupu, tak z hlediska správy, údržby a provozu všech systémů. Jelikož se toto odvětví neustále dynamicky vyvíjí, je potřeba počítat s častými aktualizacemi, které také nejsou levnou záležitostí.



Obr. 2. Výměna dat mezi koncovými subjekty

6.2 EDI se sítí VAN

Jedná se o tzv. síť, která nese přidanou hodnotu. Tato síť kromě toho že přenáší data, nabízí i rozšíření o další služby. Nejzajímavější službou je distribuce nezkreslených informací určenému adresátovi. Další změna o proti klasické EDI komunikace je existence VAN operátora, který zajišťuje část provozu a také správu systému přenosu. Jedná se tedy o určitou přidanou hodnotu. Tento VAN operátor slouží jako dodavatel softwaru, kterým je již zmíněný konvertor a také software pro komunikaci a napojení k síti VAN.

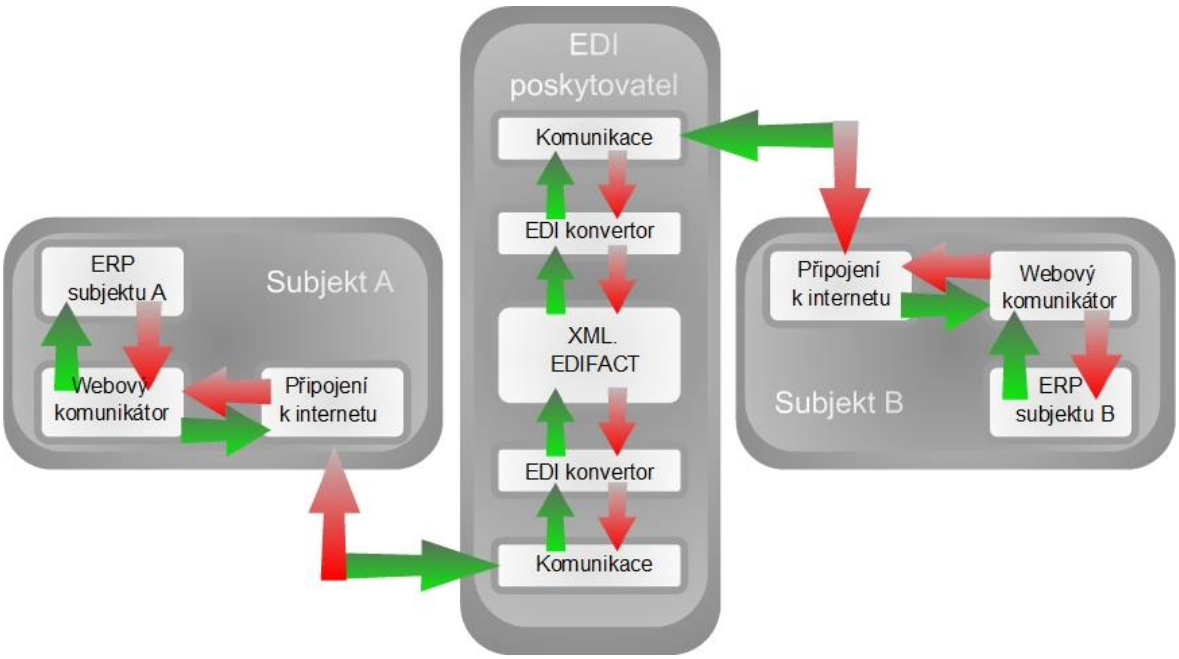


Obr. 3. Výměna zpráv s pomocí VAN operátora.

6.3 Elektronická výměna dat prostřednictvím EDI poskytovatele

Jedná se o další (propracovanější) stupeň komunikace. Tento systém vychází z již zmíněného systému EDI se správou a podporou VAN operátora. V tomto případě však poskytovatel VAN služeb provádí konverzi zasílaných zpráv. Podle [19] je výhodou tohoto systému že jak odesílatel, tak příjemce nepotřebují vlastnit zakoupený konvektor ani software který by změnil odesílaná či přijatá data, protože o to se postará již zmíněný VAN operátor. Uživatelům již pak stačí obyčejné připojení k internetové síti, která slouží jako základ-

ní platforma pro komunikaci. U toho to typu komunikace, také existuje systém s názvem EDI ORION. Tento systém je opět určitou inovací na předešlé komunikační systémy, jako u předešlých systémů EDI ORION zahrnuje poskytovatele, základní nástroje a napojení na datové sítě, dále je schopno komunikovat s ostatními poskytovateli. Tím odpadá určitá nekompatibilita a často složité transformování dat od adresáta ke koncovému příjemci. Dá se tedy říci, že při zvolené tohoto řešení nezáleží na tom, jaké EDI řešení komunikující strany používají. Tato metoda je poskytována za pomocí služby (software as a service) a také ASP čili (aplication service provider). Pro tyto služby je charakteristické to, že veškeré řešení, zpracování dat a dohled je zajištěno poskytovatelem. Myslím si, že nespornou výhodou jsou pořizovací náklady, které jsou o proti předchozím systémům velmi nízké až minimální. Celý systém je také nejmodernější, jelikož se jedná o systém s automatickým provozem. Myslím si, že právě poslední zmíněný systém by měl význam ve využití na úřadech veřejné správy a také ve zdravotnictví.



Obr. 4. Výměna a zpracování dat pomocí poskytovatele služeb EDI.

6.4 Elektronická výměna dat prostřednictvím webového portálu

Jedná se o další variantu pro využívání elektronické výměny dat. Tento systém pracuje za přítomnosti webového portálu od poskytovatele EDI, a však se nejedná o úplné řešení, tak jak jsme si jej popisovali výše. Oproti ostatním řešením je totiž propojen s externím informačním systémem. Což může mít za následky větší náchylnost k možným průlomům/ prů-

nikům od narušitelů či jiných hackerů. Na druhou stranu je tento systém daleko méně nákladný a však pro úřady veřejné správy či zdravotnictví mnou nedoporučovaný, protože veškeré příchozí zprávy je třeba ručně zpracovávat, což může mít za následky výskyt chyb při přepisu či únik citlivých dat. Ta samá situace nastane i za předpokladu odesílání dat, kdy uživatel musí přepsat všechny údaje ručně z informačního systému. Vzhledem k obrovskému objemu informací ve státní správě je tento systém neakceptovatelný.

7 CZECH POINT

Název tohoto terminálu je modifikovanou zkratkou, celým názvem pak je Český Podací Ověřovací Informační Národní Terminál. Tento projekt byl zřízen za účelem snížení osobní komunikace mezi občanem a úřadem. Občan při vyřizování určitého problému nemusí být přítomen na úřadě či více úřadech, ale může ho vyřešit pouze na jednom místě, čili na Czech POINT. Dá se tedy říci, že tak místo občana, který byl nucen obíhat různé úřady a pracoviště, dnes místo něho obíhají data.

Dle [20] str. 49 se jedná o garantovanou službu, s pomocí ní lze komunikovat se státem a jeho službami. Dají se zde ověřovat data z informačních systémů, které mohou být veřejné ale i neveřejné. Dále se na těchto místech dají úředně ověřit dokumenty a také se zde převádějí písemné dokumenty na dokumenty elektronické.

7.1 Czech POINT centrála

Tato centrála je za pomocí webového přístupu zpřístupněna ověřujícím úřadům. Každému ověřujícímu úřadu je přidělen jedinečný administrátorský přístup. Na tomto účtu si zřizovatel (úřad) může vytvořit uživatelské účty pro své pracovníky, kteří jsou pověřeni k vydávání ověřených výstupů. Pracovník, se pak jednoduše přihlásí do systému Czech POINT, ve kterém, nalezne vždy nejaktuálnější formuláře pro různé situace. Při přihlašování do systému musí zaměstnanec provést ověření identity, po té mu systém přidělí oprávnění, které slouží k přístupu pro pořizování různých výstupů z celého ISVS. Dá se říci, že jakékoli softwarové vybavení, které je označeno, jako klient CP může komunikovat s touto centrálou CP. Jedná se o velmi srozumitelné uživatelské prostředí, které je řešeno formulářově. [21] str. 49.

7.2 Software602 Form Filler

Jedná se o software používaný na zabezpečených počítačích ve správě Czech POINT. Jedná se o volně šiřitelný software, který se hojně využívá k elektronickému vyplňování formulářů. Tento software dokáže převést vyplněné dokumenty do formátu PDF, který je dobře přenositelný. Dále, sytém podporuje formáty ISDOC(X) a EDI, který je vhodný k elektronickému přenosu, jak jsem již zmínil v předchozí kapitole. [22] str. 49.

II. PRAKTICKÁ ČÁST

8 ÚROVEŇ ZABEZPEČENÍ VYBRANÝCH IS

V této kapitole budou porovnány vybrané informační systémy z pohledu odolnosti vůči již zmíněným rizikům pro účel porovnání byla vybrána následující rizika: Nespokojení zaměstnanci, zneužití pravomocí, outsourcing, správci systému, sociotechnika, infiltrace a phishing.

Cílem porovnání bude především zhodnotit nebezpečí vyplývající z chyb či nepozornosti zaměstnanců.

Z řad systémů byly ke zkoumání vybrány následující: Portál veřejné správy (PVS), IS o informačních systémech veřejné správy (IS o ISVS), Elektronické tržiště (ET), E-podpis (EPEV), UNICOS, CLAVIUS a IS L-BIS .

PVS byl vybrán z důvodu, že se jedná o primární a nejdůležitější IS pro veřejnou správu. IS o ISVS byl vybrán jako zástupce základních systémů ISVS. ET byl vybrán z důvodu příjmu dokumentů z Evropské unie. EPEV byl vybrán z důvodu jeho důležitosti při tvorbě e podpisů. UNICOS byl vybrán jako zástupce provozních informačních systémů, které mají vazby na ISVS. Systém CLAVIUS je zde zařazen jako zástupce provozních informačních systémů, které nemají vazby na ISVS. Systém IS L-BIS je zástupcem zdravotnických informačních systémů.

Výsledky budou vyobrazeny pomocí přehledné tabulky. Rizikovost vybraných IS bude vyjádřena na stupnici 1 až 10 přičemž číslo 1 značí nejnižší stupeň ochrany a číslo 10 stupeň nejvyšší.

8.1 Analýza vybraných IS

Analýza je provedena na již zmíněných informačních systémech. Každý systém je konfrontován se sedmi vybranými hrozbami. Následující tabulka ukazuje výsledky na stupnici od 1 do 10. Na konci každého řádku je vypočítán průměr, který značí rizikovost daného informačního systému.

Tab. 1. Rizikovost jednotlivých informačních systémů.

SYSTÉM/HROZBA	Nespokojení zaměstnanci	zneužití pravomocí	outsourcing	správce systému	sociotechnika	infiltrace	phishing	PRŮMĚR
Portál VS	10	7	10	8	10	10	10	**9,3**
IS o ISVS	7	9	10	8	9	9	9	**8,7**
Elektronické tržiště	5	5	7	7	7	7	6	**6,3**
E-podpis	5	7	9	8	6	7	6	**6,9**
UNICOS	4	6	5	5	4	4	5	**4,7**
CLAVIUS	7	9	10	6	8	5	10	**7,9**
IS L-BIS	8	7	5	5	4	5	9	**6,1**

8.2 Výsledky analýzy a shrnutí

Z výše uvedené tabulky vyplývá, že nejlépe zabezpečeným systémem je PVS s celkovým průměrem 9,3 „bodů“. Je to dáno především tím, že se jedná o systém, který poskytuje převážně informace dostupné všem občanům a uživatelům. U tohoto systému proto nehrozí únik zabezpečených informací.

Naopak nejhůře zabezpečeným systémem je systém UNICOS, který obdržel celkově pouhých 4,7 „bodů“. Je to dáno především proto, že se jedná o systém, který pracuje s peněžními toky a tak je u něho nejvyšší riziko možných útoků a pokusů o útoky.

V neposlední řadě je zmíněn IS L-BIS, který dostal konečné hodnocení 6,1 „bodů“ u tohoto systému lze čekat v příštích letech zlepšení, protože bude využíván stále více zdravotnickými středisky a tím se jeho ochrana bude muset posunout na vyšší úroveň.

9 NÁVRH NA SNÍŽENÍ RIZIK IS

9.1 G cloud

Jedná se o nový plán společně vypracovaný Ministerstvem financi a Ministerstvem vnitra. Jedná se o současný trend ze zahraničí, který je podporován Evropskou unií. Projekt je zřízen za účelem sjednocení nákupu ICT služeb pro všechny úřady v České republice. Dnes je situace taková, že si každý úřad nakupuje vlastní IT systémy a tím vzniká určitá nekompatibilita při komunikaci a tím vzniká vysoké riziko prolomení potažmo chyb v komunikaci mezi jednotlivými institucemi (úřady).

V současné době je dle [23] str. 49 registrováno 6 805 informačních systémů, které jsou v jednotlivých provozech a na jednotlivých úřadech či jiných státních institucích. Celkové náklady na provoz těchto systému činí 134,8 miliard korun. Na roční provoz všech informačních systémů je za potřebí 24,4 miliard korun.

Zavedení a zprovoznění G cloudu bude stát českou státní pokladnu něco kolem 13-ti miliard korun a více. Dle mého názoru se bude jednat o výhodnou inovaci, protože se předpokládá roční úspora kolem 20-ti procent nákladů což by činilo zhruba 2,5 miliardy korun.

Současný stav IT systémů

Jak je již zmíněno v předchozí kapitole, v současné době je evidováno téměř 7 tisíc IT systémů což má za následek vysoké náklady na nákup a také na jejich provoz. Dalším problémem v České republice jsou datová centra, kterých existuje 47.Tato centra nesplňují požadavky pro spolehlivost a bezpečnost ať už při zpracování či přenosu informací, což má za následek slabou ochranu vůči hrozbám napadení a prolomení ochrany z jiných stran.

9.1.1 Navrhovaná podoba G cloudu

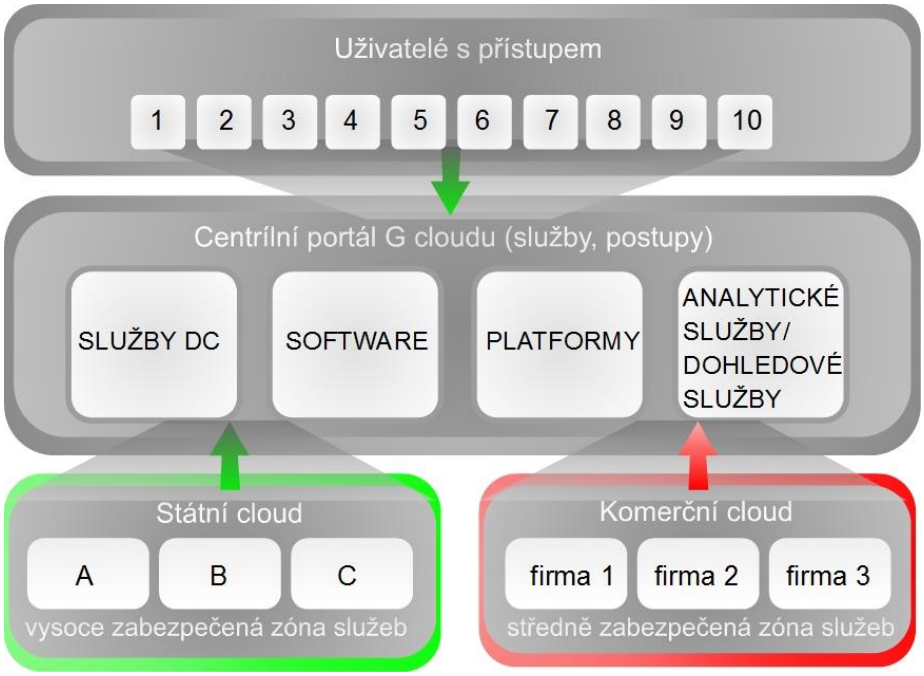
Cloud by měl být rozdělen na dvě části a to na státní cloud, který bude určen výhradně pro komunikaci mezi úřady a ostatními institucemi (nemocnice, univerzity) cloud bude mít na starosti kritickou infrastrukturu a data. Jako druhou část doporučuji tzv. komerční cloud do kterého se přesunou služby pro obyvatelstvo ze stávajících systémů.

Co se týče geografického rozdělení by měl být složen ze tří oddělených datacenter. Tato centra bych umístil do Hlavního města Prahy, dále do Brna a Ostravy logicky podle dopravní dostupnosti a nejrozvinutější infrastruktuře. Tato centra by bylo ideálním řešením využívat službu disaster recovery která slouží pro případ kdyby vypadla jedna lokalita. První dvě datacentra budou pod správou SPCSS, zbylý cloud bude spravovat buď státní podnik (Česká pošta), popřípadě již zmíněný NAKIT z kapitoly 5. V následujícím obrázku je naznačeno schéma navrhovaného G cloudu.

Legenda ke schématu:

1. Krajské úřady
2. Ministerstva
3. Obce I. až III. Typu
4. Magistráty statutárních měst
5. Orgány státní správy
6. Právnické osoby zřízené zákonem
7. Právnické osoby s datovou schránkou
8. Podnikatelé s datovou schránkou
9. Fyzické osoby s datovou schránkou
10. Ostatní orgány veřejné moci

A. Česká pošta
B. SPCSS
C. NAKIT



Obr. 6. Schéma navrhovaného G cloudu.

ZÁVĚR

V této bakalářské práci jsem se nejprve zaměřil na problematiku bezpečnosti informačních systémů obecně. Popsal jsem definice bezpečnosti informačních systémů a jejich certifikace. V neposlední řadě jsem popsal normy, kterými se řídí informační systémy a také různé analýzy rizik. V kapitole číslo 2. Je nejprve čtenář seznámen s tím co to vlastně ISVS je, co jej tvoří a co nikoliv a také právní rámec týkající se ISVS. Ve třetí kapitole je čtenář seznámen s vybranými informačními systémy, které spadají pod orgán veřejné správy. Tato kapitola informuje o právní úpravě jednotlivých IS ale také o jejich funkcích, parametrech, metodách zabezpečení a potřebného vybavení k jejich provozu. Ve čtvrté kapitole se čtenář doví o současné situaci IS ve zdravotnickém sektoru. Dále je zde popsán vybraný systém fungující ve zdravotnických zařízeních a také je zde nastíněno možné propojení systémů veřejné správy se systémy ve zdravotnictví.

Pátá kapitola je zaměřena především na hrozby, které číhají na IS, kterými se tato práce zabývá. Jsou zde popsány bezpečnostní agentury, které mají za úkol těmto hrozbám zamezit. V další části jsou popsány jednotlivé hrozby, které se týkají většinou lidského faktoru (zaměstnanců) jakožto nejslabšího článku systému. Šestá kapitola je věnována technologii pro výměnu elektronických dat, která je pro vybrané systémy klíčová. Jsou zde popsány možné varianty použití této technologie. V kapitole č. 7 se zmiňuji o kontaktním místě CZECH point a o jeho centrále a také o softwaru, který je zde využíván.

V osmé kapitole jsem se zaměřil na úroveň zabezpečení vybraných IS, tyto systémy byly konfrontovány s některými hrozbami a následně ohodnoceny v přiložené tabulce. V poslední podkapitole praktické části je nastíněn návrh na sjednocení nákupu informačních a komunikačních technologií pomocí G cloudu. Podobný systém již existuje v zahraničí a dle mého názoru se při správné implementaci může stát přehlednějším a levnějším řešením nákupu ICT než je tomu doposud.

SEZNAM POUŽITÉ LITERATURY

[1] KIM, David a Michael G. SOLOMON. *Fundamentals Of Information Systems Security: Information Systems Security & Assurance. 2. Boston: Jones & Bartlett Learning, 2013.* ISBN 1284031624.

[2] *Systémová integrace*. 2006, **13**(2). ISSN 1210-9479.

[3] Informační koncepce obce s pověřeným obecním úřadem. Mvcr.cz [online]. Ústí nad Orlicí: Konero, 2006 [cit. 2016-05-31]. Dostupné z: http://www.mvcr.cz/clanek/priklady-informacnich-koncepci.aspx

[4] PORTÁL VEŘEJNÉ SPRÁVY. *MVCR* [online]. Praha: Ministerstvo vnitra České republiky, 2016 [cit. 2016-04-25]. Dostupné z: http://www.mvcr.cz/clanek/portal-verejne-spravy.aspx

[5] Národní distribuce oficiálních dokumentů EU „IS EU Extranet ČR“. *Isss.cz*[online]. Hradec Králové: S.ICZ a.s., 2009 [cit. 2016-05-10]. Dostupné z: https://www.isss.cz/archiv/2009/download/prezentace/truxa_icz.pdf

[6] Clavius - základní informace. *Lanius.cz* [online]. Tábor: LANius s.r.o., 2012 [cit. 2016-05-09]. Dostupné z: http://www.lanius.cz/clavius/info.htm

[7] *KONTAKT* [online]. 2005, **2005**(7) [cit. 2016-05-29]. ISSN 1212-4117. Dostupné z: http://casopis-zsfju.zsf.jcu.cz/kontakt/administrace/clankyfile/20120321132235553463.pdf

[8] Subsystémy a moduly. *Lauryn* [online]. Pardubice: LAURYN v.o.s., 2011 [cit. 2016-05-27]. Dostupné z: http://lauryn.cz/subsystemy-a-moduly.html#zdravotni

[9] *Data security management* [online]. Praha: Tate International, 2004, **2004**(2) [cit. 2016-05-29]. ISSN 1211-8737.

[10] ISVS.cz. ISVS [online]. Třeboň: ADVICE.CZ, 2016 [cit. 2016-04-19]. Dostupné z: http://www.isvs.cz/vznika-narodni-agentura-pro-komunikacni-a-informacni-technologie/

[11] Vite-co-je-csirt. *ISVS* [online]. Třeboň: ADVICE.CZ, 2015 [cit. 2016-04-19]. Dostupné z: http://www.isvs.cz/vite-co-je-csirt/

[12] *Data security management* [online]. Praha: Tate International, 2002, **2002**(4) [cit. 2016-05-29]. ISSN 1211-8737.

[13] *Ernst & Young, DSM – Data Security Management: Průzkum stavu informační bezpečnosti* [online]. 2005, **2005**(3) [cit. 2016-05-29].

[14] *Data security management* [online]. Praha: Tate International, 2004, **2004**(2) [cit. 2016-05-29]. ISSN 1211-8737.

[15] EASTTOM II, William (Chuck). *Computer Security Fundamentals*. 3. Indianapolis: Pearson IT Certification., 2016. ISBN 978-0789757463.

[16] Nebezpečí jménem phishing. *Computerworld* [online]. Praha: SecurityWorld |, 2007 [cit. 2016-05-29]. Dostupné z: http://computerworld.cz/securityworld/nebezpeci-jmenem-phishing-46139

[17] [online]. krypto.krokonet, 2009 [cit. 2016-05-29]. Dostupné z: http://www.bezpecnost.estranky.cz/clanky/zpravodajske-techniky/uvod-do-kryptografie.html

[18] Reichel, D.: Jak na elektronickou výměnu dat? [online], září 2009 [cit. 2009-12-12], Dostupné na URL: http://data.businessworld.cz/file/elektronicka-vymena-dat.pdf

[19] *Http://data.businessworld.cz/* [online]. Brno: CVV informační systémy, 2009 [cit. 2016-04-28]. Dostupné z: http://data.businessworld.cz/file/elektronicka-vymena-dat.pdf

[20] Co je Czech POINT. *Czechpoint.cz* [online]. ČR: Ministerstvo vnitra ČR, 2016 [cit. 2016-05-12]. Dostupné z: http://www.czechpoint.cz/web/?q=node/22

[21] Dokumentace k projektu Czech POINT. *Czechpoint.cz* [online]. ČR: Software602, 2008[cit.2016-05-12]. Dostupné z: http://www.czechpoint.cz/web/files/Czech%20POINT_Dokumentace_k_projektu_Instalace_2-2-080619.pdf

[22] Software602 Form Filler. *602.cz* [online]. Praha 4: Software602, 2015 [cit. 2016-05-12]. Dostupné z: http://www.602.cz/produkty/form_filler

[23] Budeme mít státní cloud za 13 miliard? *ISVS* [online]. Třeboň: ADVICE.CZ, 2016 [cit. 2016-04-19]. Dostupné z: http://www.isvs.cz/budeme-mit-statni-cloud-za-13-miliard/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ISVS	Informační systémy veřejné správy.
IS	Informační systém.
PIS	Provozní informační systém
XML	Xtensible Markup Language
IIS	Internet Information Server
SQL	Structured Query Language (strukturovaný dotazovací jazyk)
CSP	Certified Systems Professional
CD	Compact disk
ISDN	Integrated Services Digital Network
ADSL	Asymetric Digital Subscriber Line
CERT	Computer Emergency Response Team Coordination Center
CSIRT	Computer Security Incident Response Team
ISO	International Organization for Standardization (mezinárodní organizace pro normalizaci)
IEC	International Electrotechnical Commision (mezinárodní úřad pro elektrotechniku)
DoS	Disc operating System
DES	Data Encryption Standard
SHA	Secure Hashing Algorithm (bezpečnostní hashovací algoritmus)
VAN	Value Added Network (síť)
PDF	Portable Document Format (přenosný formát dokumentu)
ISDOC	Information System Document
SPCSS	Státní pokladna centrum sdílených služeb

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Práce neobsahuje přílohy.