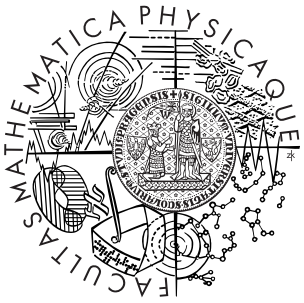
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



František Princ

Systém managementu bezpečnosti informací pro malou počítačovou síť

Středisko informatické sítě a laboratoří

Vedoucí bakalářské práce: RNDr. Libor Forst
Studijní program: Informatika - správa počítačových systémů

2009

Na tomto místě bych rád poděkoval RNDr. Liboru Forstovi za cenné rady a konzultace během psaní této práce. Dále chci poděkovat také zástupci ředitele Mgr. Miloši Maxovi a správci sítě Bc. Martinu Kukačkovi z Gymnázia Vítězslava Nováka v Jindřichově Hradci, kteří mi umožnili neomezený přístup ke školní počítačové síti a tím také napsání této práce.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne 29. května 2009 František Princ

Obsah

Název práce: Systém managementu bezpečnosti informací pro malou počítačovou síť
Autor: František Princ
Katedra (ústav): Středisko informatické sítě a laboratoří
Vedoucí bakalářské práce: RNDr. Libor Forst
e-mail vedoucího: forst@ms.mff.cuni.cz

Abstrakt: V předložené práci studujeme aspekty vývoje bezpečnostní politiky pro konkrétní počítačovou síť. Práce dokumentuje kompletní průběh tvorby bezpečnostní politiky, což zahrnuje analýzu celého prostředí, návrh bezpečnostního záměru a následné sepsání vlastní bezpečnostní politiky. Součástí práce jsou i návrhy na zlepšení infrastruktury sítě, které vyplynuly z výsledků práce.
Klíčová slova: bezpečnostní politika, systém řízení bezpečnosti informací, počítačová síť, ČSN ISO/IEC 27001

Title: Information Security Management System for Small Network
Author: František Princ
Department: Network and Labs Management Center
Supervisor: RNDr. Libor Forst
Supervisor's e-mail address: forst@ms.mff.cuni.cz

Abstract: In the present work we study aspects of the security policy development for the specific computer network. The work documents complete development of the security policy. It includes complete analysis of the environment, where is the network located, the draft of security statement and formation of security policy as a document. The work includes also some tips to improve the network infrastructure. These tips are results of the work.
Keywords: security policy, information security management system, computer network, ISO/IEC 27001

Kapitola 1

Úvod do problematiky

Definice pojmu *bezpečnostní politika* se vyskytuje na Internetu v mnoha různých mutacích. Vybral jsem definici z [3] : *Systémová bezpečnostní politika je závazný dokument organizace (interní předpis) regulující bezpečné používání a správu určitého informačního systému nebo systému ICT.* Popis tvorby a provozování bezpečnostní politiky pokrývá norma [1]. Bezpečnostní politiku jako dokument je vhodné rozčlenit do několika částí.

- Bezpečnostní záměr - přibližně 1-2 strany A4 textu, schválené vedením organizace.
- Politika a principy bezpečnosti - dokument, který obsahuje komplexní informace o bezpečnostní politice včetně konkrétních bezpečnostních opatření. Je vhodné rozdělit dokument na více částí, vzhledem k různosti uživatelů systému. Uživatelé by se měli seznámit pouze s opatřeními, která se jich týkají. Například bankovní úředník za přepážkou nemusí znát části, které se týkají správy celého systému nebo instalace softwarových produktů.
- Přílohou bezpečnostní politiky bývá velmi často také dokument, se kterým se povinně seznamují všichni uživatelé systému. Tato příloha obsahuje závazná pravidla pro chování každého uživatele. Pravidla musí důsledně korespondovat s bezpečnostní politikou. Důvodem pro vznik samostatného dokumentu je především srozumitelnost a jednoduchost pro obyčejného uživatele.

Část *Principy a politika bezpečnosti* by podle normy [1] měla obsahovat následující součásti:

- **Popis aktiv** je kompletní seznam všeho, co má pro danou organizaci nějakou cenu (hardware, software, data, administrátoři a další). Pro každou organizaci je tento soupis specifický, nicméně pro organizace podobného zaměření se příliš neliší.
- **Vymezení zodpovědnosti** rozděluje práva a povinnosti pro jednotlivce i skupiny. Tato součást je z právního hlediska velmi podstatná v případě bezpečnostního incidentu.
- **Plán na udržování bezpečnosti** určuje například počet pracovníků vyčleněných na udržování bezpečnosti nebo minimální výdaje do oblasti bezpečnosti.Také obsahuje popis kontrolních mechanismů.

Bezpečnostní politika by měla být neustále se vyvíjející dokument, který zohledňuje vývoj informačních technologií, nových hrozeb nebo legislativní změny. Je nutné zavést systém kontroly dodržování politiky a řešit její porušování. Je také velmi vhodné komunikovat se všemi uživateli a přizpůsobovat politiku jejich potřebám v souvislosti s výkonem jejich pracovních úkolů (např. časté vynucení změny hesla vede k tomu, že uživatelé volí jednoduchá hesla nebo, pokud je implementován mechanismus na kontrolu složitosti hesla, píší si je na papírky a ukládají pod klávesnici nebo lepí na monitor).

1.1 Bezpečnostní politika pro počítačovou síť

Použiji definici z [3]: *Systémová bezpečnostní politika počítačové sítě, resp. intranetu by měla být zpracována v každé organizaci. Pokrývá specifické oblasti správy sítí LAN a WAN, jejich spolehlivosti a řízení přístupu. Obecně jde o jeden z nejrizikovějších segmentů informačního systému každé organizace, zejména díky prudce se zvyšující míře závislosti celého informačního systému na počítačové síti, integraci velkého množství informačních zdrojů dostupných prostřednictvím počítačové sítě, v neposlední řadě pak díky obvykle rychlému rozvoji a častým změnám.*

1.2 Cíl práce

Tato práce ukazuje kompletní postup tvorby bezpečnostní politiky pro síť menšího rozsahu od analýzy až po sepsání samotné bezpečnostní politiky. Cílem této práce je pokusit se zmapovat praktický dopad dokumentu jakým je bezpečnostní politika. Za tímto účelem jsem si vybral konkrétní počítačovou síť. Zde jsem provedl analýzu a následně se pokusil navrhnout bezpečnostní politiku. Důraz byl kladen především na analýzu rizik, což je stežejní část celé práce. Vzhledem k současné situaci nebylo možné politiku uvést do praxe, a proto chybí pozorování dopadů bezpečnostní politiky na celou organizaci.

Kapitola 2

Analýza konkrétní sítě

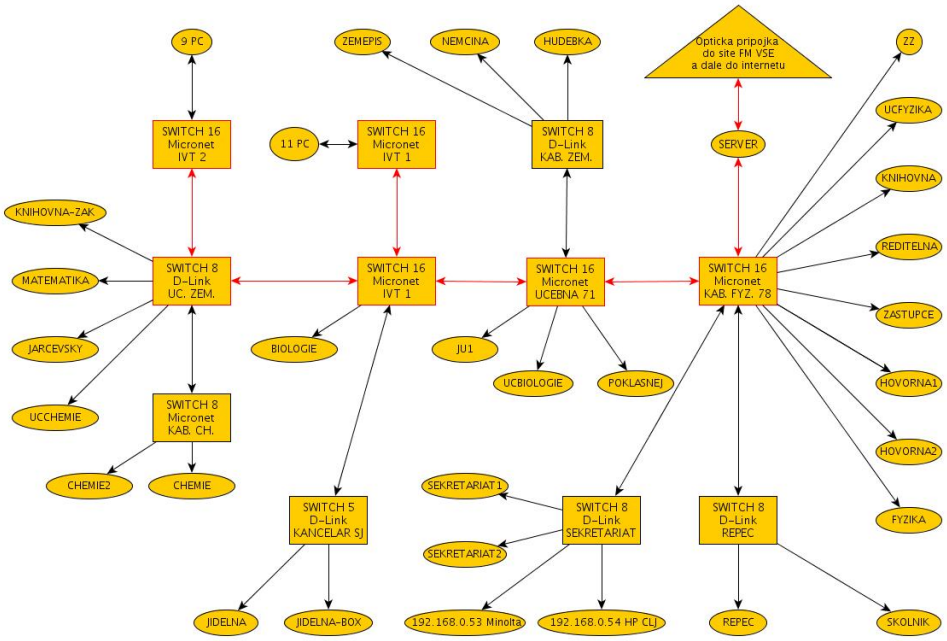
Předmětem zkoumání je školní počítačová síť Gymnázia Vítězslava Nováka v Jindřichově Hradci (dále jen GVN). Tato síť primárně slouží ke vzdělávání studentů a přípravě vyučujících, ale i k vedení agend s citlivými údaji (finanční a mzdové účetnictví, komunikace se státní správou, zpracování klasifikačních dat studentů, přijímací řízení). Hned na začátku je třeba zmínit, že ve školní budově probíhají rozsáhlé stavební práce při budování půdní vestavby, kde má mimo jiné vzniknout i nová (kapacitně větší) počítačová laboratoř. Dále se díky stavbě změní umístění serveru a některých síťových prvků. V případě potřeby se po dokončení stavebních prací bezpečnostní politika novému prostředí přizpůsobí.

2.1 Hardware

Prvním krokem zkoumání byla fyzická prohlídka celé budovy s cílem zaznamenat veškerá zařízení, která jsou připojena do sítě. V době, kdy byla prohlídka provedena, byl stav následující:

- Počítačová síť GVN je postavena kabeláži UTP cat. 5e, jejíž teoretická rychlost je až 100 Mbit/s.
- Síť obsluhuje celkem 11 přepínačů propojených pomocí výše uvedené kabeláže. Je použita stromová topologie, která je schématicky znázorněna na obrázku 2.1.

  Vzhledem k poruchovosti starších přepínačů značky Micronet uvažuje vedení školy o zakoupení nových přepínačů, které již podporují rychlost 1 Gbit/s.



Obrázek 2.1: Schéma sítě GVN na linkové vrstvě

Obrázek 2.2: Schéma sítě GVN na síťové vrstvě

- Síťové kabely jsou vyvedeny skoro do všech učeben a kabinetů. V učebnách bez stálého počítače jsou kabely schovány v instalační krabičce ve zdi.

- Síť není nijak softwarově chráněna proti neoprávněnému připojení stanic. Neoprávněně připojená stanice má přístup do Internetu, ale pro přístup ke sdíleným síťovým prostředkům je třeba autorizace pomocí uživatelského účtu. Na serveru běží démon Samba, který zajišťuje připojení stanic do domény. Stále však existuje několik strojů, které nejsou z různých důvodů do domény zapojené.

- Připojení do Internetu je realizováno pomocí optického kabelu prostřednictvím sítě CESNET2. V současné době má přípojka rychlost 8 Mbit/s. Propojení vnitřní sítě se sítí poskytovatele je ilustrováno obrázekem 2.2

- Propojení sítě GVN a Internetu zajišťuje server, který běží na operačním systému Gentoo Linux a je spravován externistou. Tento server slouží zároveň jako Domain Controller (Samba server) pro stanice s operačním systémem Microsoft Windows.

- Do sítě jsou přímo (bez počítače) připojeny dvě tiskárny a to HP Color LaserJet 2600n a Konica Minolta Di2510. Obě tiskárny se nachází v sekretariátu školy.

- Dále je do sítě připojeno celkem 47 stálých pracovních stanic.

  - Dvě počítačové laboratoře čítají celkem 20 počítačů.
  - Pět odborných učeben je vybaveno počítačem s audiovizuální prezentační technikou (projektor, reproduktory).
  - Dvě stanice jsou k dispozici učitelům ve sborovně.
  - Jeden počítač slouží k objednávání stravy v blízkosti školní jídelny.
  - Zbytek počítačů je v kancelářích, kabinetech atd. Tyto počítače jsou využívány jen určitými uživateli a jen výjimečně se k nim přihlásí jiný uživatel.

- Navíc škola vlastní dva notebooky, které se do sítě též připojují.

- Při fyzické prohlídce bylo objeveno značné množství hardwaru, který by měl být vyřazen. Evidence hardwarového vybavení není v pořádku a bude nutné provést kompletní inventuru a zavést určitá pravidla pro evidenci, nákup a vyřazování hardware. Pravidla by měla zahrnovat i mechanismy pro pravidelné kontroly počítačů jak z hlediska hardware, tak i z hlediska obsahu pevných disků.

2.2 Software

- Školní server je postaven na operačním systému Gentoo Linux a je na něm nainstalovaný pouze software pod licencí GNU/GPL.
- Uživatelské stanice jsou postaveny na operačním systému Microsoft Windows XP Professional CZ. Na všech strojích s OS Windows je nainstalovaný kancelářský balík Microsoft Office 2003 CZ a bezpečnostní program AVG 8.5 (antivirus, antirootkit, antispyware, osobní firewall). Programové vybavení uvedené v tomto bodě je řádně licencováno.
- Škola dále vlastní licenci na následující programy: Relax KEŠ (studijní agenda - především vysvědčení), Vema s moduly PAM, RNP a ELD (evidence zaměstnanců i studentů, mzdové účetnictví, zdravotní pojištění a komunikace s portálem veřejné správy), Fenix (finanční účetnictví, evidence majetku), Zoner Callisto (grafický software), ASC Rozvrhy.
- Ostatní programy nainstalované správou sítě jsou šířeny pod licencí GNU/GPL.
- Bohužel bylo zjištěno, že někteří uživatelé mají nainstalované různé programy bez patřičné licence, což správce sítě okamžitě řešil odstraněním programu a upozorněním uživatele.

2.3 Uživatelské účty

- Všichni zaměstnanci a studenti mají svůj osobní uživatelský účet na serveru. Nárok na uživatelský účet má každý pouze po dobu svého působení na škole. U studentů tedy účet funguje po dobu jejich studia a u zaměstnanců po dobu pracovního poměru.

- Uživatel získává prostřednictvím svého účtu přístup ke školním počítačům a svému domovskému adresáři. Bez platného uživatelského účtu nemůže nikdo využívat většinu počítačů. Cílem je, aby všechny počítače byly chráněny před neoprávněným přístupem.

- Domovský adresář každého uživatele je umístěn na serveru. Mapuje se při přihlášení k libovolnému počítači jako disk X: (v prostředí Microsoft Windows). Na počítačích s Linuxem není přihlašování uživatelů do sítě nijak ošetřeno. Studenti se při seminářích s Linuxem seznamují a přihlašují se na přímo účtem uživatele `root`. Díky podpoře protokolu SMB si mohou uživatelé domovské adresáře namapovat sami i v prostředí Linuxu. Velikost domovského adresáře není nijak softwarově ošetřena. Z prostředí Internetu mohou všichni uživatelé přistupovat ke svému domovskému adresáři na server pomocí protokolu FTP.

- Dále má každý uživatel zřízenou e-mailovou schránku, jejíž adresa má tvar *uzivatelske-jmeno@gvn.cz*. E-mailové schránky jsou umístěny na serveru webhostingové firmy, která provozuje také webové stránky školy. K e-mailovým schránkám mají uživatelé přístup přes webové rozhraní nebo protokolem POP3 či IMAP.

- Uživatelské jméno pro zaměstnance je jeho příjmení psané malými písmeny bez diakritiky. Účty zaměstnanců jsou zakládány individuálně. Případné kolize nového uživatelského jména s již existujícím se řeší také individuálně.

- Studentské uživatelské jméno má tvar **JPRRMMDD** (JP - iniciály studenta, RRMMDD - číst rodného čísla před lomítkem). Není nijak explicitně ošetřen výskyt dvou studentů se stejnými iniciály a datem narození. Takové případy se řeší individuálně, vzhledem k jejich vzácnému výskytu. Studentské účty jsou generovány automaticky vždy na začátku školního roku.

- V uživatelských jménech jsou použity jen číslice a malá písmena. Na hesla jsou již nyní kladeny vysoké nároky z hlediska jejich složitosti. Změna hesla je možná pouze přes zapezpečené webové rozhraní (protokol HTTPS), kde se složitost a opakování hesla kontroluje.

2.4 Současný stav z hlediska bezpečnosti

- Fyzické zabezpečení serveru je na dobré úrovni. Server je umístěn v nejvyšším patře budovy v kabinetu. Jeho umístění se změní po dokončení půdní vestavby, kde vznikne prostor pro bezpečné umístění serveru v nové počítačové laboratoři. S tím souvisí i nezbytné přeložení optického kabelu.

- Softwarové zabezpečení serveru je dostačující. Správce pravidelně aktualizuje operační systém a má k dispozici logy. Analýza logů není pravidelně prováděna. Se softwarovým zabezpečením souvisí také síťová bezpečnost. Server je samozřejmě vybaven firewallem. Existuje několik portů, které jsou otevřené i směrem do Internetu, což představuje potencionální slabinu v zabezpečení. Příkladem je port 21 s protokolem FTP, který je rizikový díky nešifrované komunikace (včetně přenosu hesel).

- Velkou slabinu serveru představuje absence zálohovacího mechanismu. Škola však počítá s nutností nasazení nějakého zálohování.

- Pracovní stanice s Windows XP jsou většinou připojeny k doménovému řadiči. Uživatelé se musí k takové stanici vždy přihlásit svým uživatelským účtem. Tím je dostatečně eliminováno riziko zneužití počítače neoprávněnou osobou.

- Žádným způsobem není omezeno připojení neautorizovaných počítačů ani jiných síťových zařízení do sítě.

- Naprosto chybí kontrolní mechanismy ze strany odpovědných osob. Žádný zaměstnanec není v současné době odpovědný za kontrolu softwarového vybavení ani za kontrolu hardwaru, což se v minulosti projevilo pokusem o krádež.

2.5 Odhad rizik

Nejdůležitější součástí analýzy je identifikace rizik. Pro školní počítačovou síť nejsou rizika příliš vysoká, nicméně je nutné je prozkoumat. Bezpečnostní politika má za úkol tato rizika eliminovat, případně je snížit. Následující seznam zahrnuje stručný výčet zjištěných rizik, která se však s postupem času

a změnami v síti neustále vyvíjí. Je tedy třeba bezpečnostní politiku neustále rizikům přizpůsobovat. Podrobnější rozbory a návrhy eliminace rizik jsou pro svou obsáhlost umístěny v samostatné kapitole.

- **Výpadek serveru** by měl za následek nemožnost připojení celé sítě do Internetu. Uživatelé tím ztrácí přístup ke svým domovským a dalším sdíleným adresářům. Dále není možné přihlašování uživatelů na pracovní stanice po dobu výpadku serveru. Uživatelé, kteří byli přihlášeni již před výpadkem, by měli problém při ukládání svého profilu během odhlášení.

- **Nedostupnost výpočetní techniky při výuce** způsobí nemožnost kvalitního průběhu výuky informatiky. Běžná hodina informatiky probíhá tak, že studenti si veškeré poznatky zkouší přímo u počítače a tudíž absence techniky z jakéhokoli důvodu znamená vážný problém.

- **Ztráta důležitých a citlivých dat** je riziko způsobené nedostatečným zálohováním. Ztrátou se myslí nedostupnost dat v případě poruchy datového úložiště.

- **Únik citlivých dat** je bezpečnostním incidentem a v mnoha případech zároveň i porušením platných zákonů ČR. Data mohou uniknout přímo z počítačů, ze záložních médií nebo odposlechem síťové komunikace.

- **Přerušení připojení do sítě Internet** není rizikem, které by výrazně narušilo fungování sítě samotné, ale představuje jisté omezení práce.

- **Nedostupnost správce sítě** v případě technických potíží je problematické zejména během výuky, kdy jsou v provozu obě počítačové laboratoře.

- **Zneužití počítačové sítě** ze strany uživatelů je rizikem, jak pro počítačovou síť samotnou, tak i pro dobré jméno školy.

- **Průnik do sítě z vnějšího prostředí** znamená riziko spočívající v ohrožení dat a také ve zneužití sítě pro získání počítačů k nelegálním činnostem.

- **Připojení neautorizovaného počítače do sítě** není nijak ošetřeno. Přípojná místa (zásuvky) jsou většinou volně přístupná (v učebnách). Kdokoli má možnost připojit počítač k síti. Tím získá potencionální útočník přístup k vnitřní síti i do Internetu. Sdílené zdroje na serveru tímto rizikem nejsou dotčeny, protože přístup k nim je umožněn pouze autorizovaným uživatelům.
- **Výpadek síťové infrastruktury** způsobí přerušení komunikace mezi síťovými uzly a tedy výrazně naruší fungování sítě jako celku.

Kapitola 3

Rozbor analyzovaných rizik

Nyní máme identifikovaná rizika. Pro každé riziko musí být popsán způsob jeho eliminace, případně zdůvodnění ponechání rizika jako zbytkového. Po vytvoření návrhu eliminace rizik je nezbytné prověřit, zda nevznikla rizika nová. Takto vzniklá rizika je třeba opět ošetřit. Další možností je změna způsobu eliminace původního rizika tak, aby nové riziko nevzniklo. V následujícím výčtu se nachází návrhy na eliminaci identifikovaných rizik.

- **Výpadek serveru:** Server je centrální prvek celé sítě a jeho zabezpečení musí být věnována maximální pozornost. Výpadek může být způsoben hned několika faktory. Prvním faktorem je výpadek napájení serveru, což je nepředvídatelný jev, ale dá se mu velmi účinně zabránit použitím záložního napájení typu UPS[1]. Záložní napájení poskytuje dostatečnou časovou rezervu pro bezpečné vypnutí serveru a jeho automatické zapnutí po obnovení dodávky proudu z elektrické sítě. V kombinaci se zálohováním napájení přípojky do sítě Internet může správce dostat varování o výpadku proudu do své e-mailové schránky nebo na mobilní telefon. Další příčinou výpadku serveru může být porucha hardwaru. Pro takovou situaci je vhodné mít připravený seznam náhradních dílů, případně záložní počítač, který by mohl zajistit alespoň částečné fungování sítě. Z finančního hlediska se škole nevyplatí mít náhradní server, který by byl po většinu času nevyužitý a vypnutý. Ke zvážení je možnost svěření péče o hardware serveru specializované firmě, která může garantovat výměnu dílů (případně opravu) ve stanoveném časovém limitu (např. do 24 hodin), což ale

[1] Uninterruptible power supply

opět vyžaduje určité finance. Výpadek serveru může být samozřejmě zapříčiněn i úmyslně, čemuž se dá zabránit uzamčením serveru ve vyhrazené místnosti, případně ve standardní serverové skříni. Kromě technických příčin může být výpadek způsoben selháním softwaru. Takovým problémům se dá předcházet pečlivou konfigurací systému i jednotlivých programů a pravidelnou aktualizací. Výběru programů by měla být věnována patřičná pozornost. Samostatnou kapitolou je zneužití bezpečnostní chyby v softwaru serveru, což může být příčinou nejen výpadku, ale i úniku nebo zneužití uživatelských dat, průniku do sítě apod. Tyto problémy pokrývají další rizika. Malé riziko vznikne nasazením UPS. Jedná se o poruchu samotného UPS nebo jeho baterie. Poruše se dá zabránit pravidelnou údržbou a monitorováním stavu. Baterie by měla být měněna v intervalech stanovených výrobcem. S těmito opatřeními dostaneme velmi malé zbytkové riziko, které je přijatelné.

- **Nedostupnost výpočetní techniky při výuce:** Výpočetní technika je využívána nejen v počítačových laboratořích, ale také v některých odborných učebnách. Případná porucha v počítačové laboratoři znamená vzhledem k malému počtu pracovních stanic poměrně citelné narušení vyučovací hodiny. Náprava musí být zjednána v co nejkratší době a správce laboratoře by tedy měl být přítomen ve škole po celou dobu výuky v laboratořích. V odborných učebnách, kde počítač slouží především k promítání prezentací a dalším podobným činnostem, není případná porucha tolik závažná. Zde tedy stačí poruchu řešit během dne, výjimečně během více dnů.

- **Ztráta důležitých a citlivých dat:** Ztrátou dat se pro tento případ myslí jejich vymazání (omylem, záměrně, . . .) nebo porucha na zařízení pro uchování dat. Nejvíce dat se vyskytuje na pevném disku serveru. Bohužel v současné době nemá server žádný zálohovací mechanismus, což představuje velmi vážné riziko. Zálohování se dá zajistit několika způsoby.

  – Ruční zálohování na přenosná média. Toto řešení je sice možné, ale časově náročné. Navíc při současném objemu dat na serveru by byl problém se zálohovacími médii. Ruční zálohování by se muselo provádět velmi často, protože data se mění prakticky neustále.

– Zálohování pevného disku technologií RAID se jeví jako nejschůdnější řešení z hlediska finančních možností školy. Konkrétně to znamená zakoupit další pevný disk a zapojit ho do serveru pomocí technologie RAID, kterou server podporuje. Vzhledem ke stupni důležitosti dat na serveru uložených by toto řešení bylo dostačující. Případnou poruchu serveru s poškozením všech disků ponecháváme jako zbytkové riziko.

– Další možností je využití nezávislého počítače, který by byl určen výhradně pro zálohu dat. Toto řešení představuje jednak investici do dalšího počítače, ale také zde vzniká nové nezanedbatelné riziko poruchy tohoto zálohovacího stroje.

– Rozvedením předchozího řešení se objevuje ještě možnost využití služeb nějaké specializované firmy. Podstatou je, že zálohování probíhá na stroj, který leží fyzicky i logicky mimo síť školy. Riziko poruchy takového stroje leží v tomto případě na poskytovateli služby. Slabinou je v tomto případě spojení obou strojů skrz síť Internet, což znamená, že data se musí při přenosu přes Internet šifrovat. Dlouhodobější výpadek připojení k Internetu znamená nemožnost zálohování. Z finančních důvodů toto řešení také určitě nebude vybráno.

Po zvážení výše uvedených variant bude riziko ztráty dat z důvodu poruchy datového nosiče na serveru sníženo pomocí technologie RAID a zůstane zbytkové riziko (porucha více disků zapojených do RAID). Konkrétní varianta RAID bude zvolena podle možností řadiče RAID na serveru a především podle kritéria bezpečnosti. To znamená, že bude zvolena varianta s vyšší redundancí na úkor celkové kapacity. Pro potřeby školy bude vyhovovat konkrétně varianta RAID1. Server má hardwarovou podporu technologie RAID1, a proto budou finanční nároky pro nasazení omezeny pouze na nákup pevných disků. Použití technologie RAID klade vyšší nároky na náhradní díly v případě poruchy nějakého disku zapojeného do RAID. Pro případ RAID1 (mirroring) to znamená mít připraven náhradní pevný disk se stejnou kapacitou (ideálně stejného typu) nebo větší kapacitou. Nasazení technologie RAID však řeší pouze poruchu datového úložiště, nikoli riziko smazání dat.

Smazání dat na serveru je velmi rizikové a rozlišujeme několik situací.

– Neúmyslné smazání důležitých dat může způsobit pouze osoba přihlášená s právy superuživatele `root`. Ostatní uživatelé mají přístup pro zápis pouze do svých domovských adresářů a někteří učitelé také do sdíleného adresáře, který se připojuje všem uživatelům po přihlášení ke stanicím s OS Windows. Ve sdíleném adresáři učitelé publikují především studijní materiály k výuce informatiky. Za zálohování těchto dat jsou zodpovědni sami učitelé. Zálohování domovských adresářů je při současných poměrech a zvyklostech ve škole zbytečné. Největším problémem je tedy smazání důležitých dat na serveru uživatelem `root`. Správce serveru by měl zajistit bezpečné zálohování konfiguračních souborů, přihlašovacích údajů uživatelů a dalších podstatných dat na přenosná média po zásadních změnách konfigurace nebo manipulaci s uživatelskými účty. Zálohy by se měly v ideálním případě uchovávat v trezoru školy a přístup k nim by měl mít pouze správce serveru. Ztráta těchto dat z trezoru je ponechána jako zbytkové riziko.
– Úmyslně mohou být data na serveru smazána při neoprávněném získání hesla uživatele `root` nebo například při přístupu ke konzoli, kde je `root` přihlášen, čemuž však může zabránit pouze správce důsledným odhlašováním. Na heslo superuživatele je nezbytné klást vysoké nároky na bezpečnost z hlediska jeho složitosti, pravidelné obměny a také pro případ jeho zapomenutí. Tomuto tématu se bude věnovat některý z dalších odstavců. Data mohou být úmyslně smazána také útočníkem, který by prolomil softwarovou ochranu serveru na síťové úrovni. Zde je na místě pečlivá konfigurace firewallu a pravidelná instalace bezpečnostních aktualizací softwaru, který je na serveru provozován. To je náplň práce pro správce serveru. Při důsledném nastavení zůstane přijatelné zbytkové riziko.

Dále zbývají ještě data v jednotlivých pracovních stanicích. Zde je třeba se zaměřit především na počítače, ve kterých jsou instalovány programy na vedení různých agend (účetnictví, evidence studentů, školní jídelna, ...). Takových počítačů je v síti připojeno několik:

– Finanční účetnictví zpracovává zaměstnankyně školy na počítači, který využívá sama. Je řádně poučena a pravidelně zálohuje data na přenosná média. V případě absence zaměstnankyně z různých

důvodů musí vedení školy zajistit náhradní pracovní sílu, která bude řádně proškolena, nejlépe výrobcem softwaru. O pravidelnou údržbu programu se stará výrobce. Riziko ztráty dat při pravidelném zálohování je v tomto případě přijatelné jako zbytkové.

- Mzdové účetnictví zpracovává další zaměstnankyně školy na počítači, který opět využívá sama. Zálohování probíhá automaticky na server výrobce programu přes Internet. Výrobce program také vzdáleně spravuje a aktualizuje. Rizikem nemožnosti zálohování, které v tomto případě ponecháváme jako zbytkové, je výpadek připojení do Internetu. Mzdová účetní je řádně proškolována na pravidelných školeních pořádaných výrobcem softwaru.
- Evidenci studentů (klasifikace, matrika, ...) má na starost jedna z učitelek. K dispozici má počítač, na kterém zpracovává data (pololetně) a tiskne vysvědčení. Vzhledem k frekvenci využití softwaru na evidenci studentů stačí zálohovat data po každém pololetí na přenosná média. Pololetní zálohy by měly být uloženy alespoň dvě nejnovější. S ohledem na citlivost dat by bylo vhodné uschovat zálohy v trezoru školy. Samozřejmostí jsou dílčí zálohy v průběhu zpracování jednoho pololetí, které si obsluha pořizuje a ukládá na server. V tomto směru je tedy zálohování také zajištěno dostatečně a v případě problémů při pořizování dat je riziko ztráty sníženo pouze na data pořízená během práce. Záleží na zaměstnankyni samotné, jak často pořizuje dílčí zálohy, protože v případě ztráty dat by byla nucena pořizovat je od poslední zálohy znova.
- Poslední důležitou agendou je školní jídelna. Obědy se dají objednávat u terminálu v budově školy, případně přes Internet. Internetové objednávky zajišťuje výrobce programu. Při výpadku připojení do Internetu mají studenti stále možnost objednat oběd u terminálu ve škole. Nejrizikovější je počítač v kanceláři jídelny, kde aktuálně nefunguje žádné zálohování dat. Zde je třeba poučit vedoucí školní jídelny, aby zálohovala data alespoň na přenosná média nebo na server. Software pro provoz školní jídelny možností zálohování nabízí. Žádné další pokročilejší zálohovací techniky nejsou nutné.

V ostatních počítačích mají už data jednotliví uživatelé. Každý uživatel má možnost zálohovat svá data na přenosná média, případně na ser-

ver (až bude zprovozněno zálohování). Riziko ztráty těchto dat nesou uživatelé sami. U záloh na přenosná média vzniká riziko nečitelnosti média. V současnosti se důležité agendy zapisují na optická média, kde je riziko nečitelnosti výrazně nižší než u dříve používaných disket.

- **Únik citlivých dat:** Za citlivá data považujeme veškerá data, která mohou být zneužita k různým účelům. Příkladem mohou být osobní údaje studentů (především klasifikační data), dále osobní údaje zaměstnanců (např. mzdové podklady), ale také data z domovských adresářů jednotlivých uživatelů nebo jejich e-mailových schránek.

  Agendy jako finanční a mzdové účetnictví, klasifikace studentů zpracovávají pověření zaměstnanci školy, kteří mají k tomuto účelu vyhrazené počítače. Každý z těchto počítačů je uzamčen v nějaké kanceláři a je k němu tedy omezen přístup. Riziko neoprávněného fyzického přístupu k takovému počítači je tedy přijatelné a ponecháváme ho jako zbytkové. Složitější je riziko neoprávněného vzdáleného přístupu pomocí počítačové sítě. Zde se nabízí instalace kvalitního osobního firewallu, který zabrání pokusům o přístup k počítači po síti. Toto řešení je již ve velké míře využíváno, protože škola vlastní licenci na bezpečnostní software AVG, jehož součástí je i zmiňovaný firewall. Činnost firewallu může nevhodně narušit i obsluha počítače (např. zavirováním). Pro tyto případy by obsluha měla mít pouze nezbytná uživatelská práva, která nesmí zahrnovat nastavení firewallu apod. Únik dat přes přenosná média ponecháváme jako zbytkové riziko, protože fyzický přístup k počítači je dostatečně omezen. Únik dat z pracovní stanice může být také způsoben vědomou instalací různého softwaru nebo změnou konfigurace softwaru a operačního systému. Změny konfigurace operačního systému smí provádět pouze administrátor[2], ale konfigurace různého softwaru je v mnoha případech přístupná jeho uživatelům a nelze tomu účinně zabránit (uživatel potřebuje daný software spustit a používat). Administrátor systému by tedy měl zajistit pečlivou konfiguraci operačního systému při jeho instalaci (např. implicitně je po instalaci zapnuto sdílení celého disku) a tím co nejvíce snížit riziko vzdáleného přístupu k počítači. Také by měl uživatelům nastavit co nejstriktnější uživatelská práva tak, aby nemohli instalovat žádný software a měnit konfiguraci operačního systému.

[2] terminologie MS Windows

Další citlivá data se vyskytují na serveru v domovských adresářích uživatelů. Přístup k domovským adresářům má pouze uživatel sám a správce serveru. Domovské adresáře jsou chráněny uživatelským jménem a heslem, které zná výhradně uživatel. Každý uživatel musí být při zřízení uživatelského účtu vhodnou formou poučen, že má své heslo udržovat v tajnosti. Za správce serveru se považuje osoba, která zná heslo uživatele `root`. Vzhledem k neomezeným uživatelským právům toho uživatele musí být striktně určeno, kdo smí heslo znát. V současnosti zná heslo pouze jediný člověk, který server spravuje. Tím vzniká riziko, že v případě zapomenutí hesla bude server bez možnosti správy. Tomuto riziku se budeme podrobněji věnovat níže.

Uživatel `root` má jako jediný přístup i k autentizačním údajům uživatelů na serveru. Hesla uživatelů nejsou uložena v textové podobě, ale jsou zašifrovaná. Tedy nikdo kromě uživatele samotného nezná jeho přístupové heslo a v případě jeho ztráty musí být vygenerováno heslo nové. Z výše uvedených skutečností vyplývá, že heslo uživatele root musí být dostatečně složité a velmi dobře chráněné.

Prostor pro únik citlivých dat je ještě v komunikaci pracovních stanic se serverem. Komunikace není až na výjimky nijak šifrována a tudíž může být velmi jednoduše odposlouchávána. Odposlechu dat se věnuje riziko připojení neautorizovaného počítače. Uživatel `root` se k serveru nikdy vzdáleně nepřihlašuje. Správce serveru musí vždy použít svůj osobní účet, jehož přostřednictvím se připojí pomocí protokolu SSH a teprve pak se přepne do superuživatelského režimu. Protokol SSH je šifrovaný, a proto je riziko napadení této komunikace přijatelné.

Citlivá data mohou uniknout také ze záložních médií. Aktuální zálohy by měly být umístěny v trezoru školy. Neaktuální zálohy musí být spolehlivě zlikvidovány. U přenosných médií (v našem případě především optických) to znamená jejich fyzickou likvidaci. Firmy, které se zabývají likvidací citlivých materiálů dnes už standardně nabízí kromě skartace papírových dokumentů také likvidaci různých dalších médií.

- **Přerušení připojení do sítě Internet:** Výpadek připojení do sítě Internet může být způsoben ze strany poskytovatele. V takovém případě je vhodné mít ve smlouvě s poskytovatelem dohodnutý postup pro tyto případy. Výpadek na straně školy je svázán většinou s výpadkem serveru. Přípojka je vyvedena přímo k serveru a proti úmyslnému

narušení funkcionality platí podobná opatření jako u ochrany serveru. Napájení koncového zařízení je vhodné zálohovat pomocí UPS stejně jako server. Postup řešení výpadku připojení začíná kontrolou na straně školy a v případě neúspěchu následuje kontaktování poskytovatele a řešení poruchy v součinnosti s poskytovatelem.

- **Nedostupnost správců sítě:** Správce sítě by měl být dostupný během celé provozní doby školy tak, aby byl schopen operativně řešit vzniklé problémy. Vzhledem k současné situaci, kdy má škola správce celkem 3, je víceméně zajištěno, že alespoň jeden ze správců bude přítomen. Dva správci jsou externisté, ale jsou schopni řešit problémy telefonicky, případně vzdáleně přes Internet. Jeden externí správce se stará o server, uživatelské účty, e-mailové schránky a připojení do Internetu. Druhý externista má na starosti celou vnitřní síť kromě počítačových laboratoří. Bylo by vhodné zajistit, aby byl externista schopen se v případě potřeby dostavit do budovy školy do rozumně stanovené doby. Třetí ze správců je z řad vyučujících a stará se především o počítačové laboratoře. Během výuky v laboratořích je ve škole přítomen a tedy schopen řešit poruchy menšího rozsahu v průběhu dne.

  Situace se správci není v současné době uspokojivá. V ideálním případě by mohla mít škola v pracovním poměru jednoho stálého správce místo dvou externistů, který by měl na starost celou počítačovou síť včetně serveru. Tento správce by mohl mít zástupce z řad učitelů informatiky. Tímto opatřením by se vyřešil problém s nedostupností externistů a se zaneprázdněním správce - učitele v době výuky. Riziko nedostupnosti správce se tím sníží na přijatelnou úroveň a zůstane jako zbytkové pro případ, kdy by nebyl dostupný ani jeden správce.

- **Zneužití počítačové sítě:** Zde máme na mysli zneužití sítě k činnostem, které narušují fungování sítě, neoprávněně získávají cizí data, jsou v rozporu s platnými zákony ČR a dalšími předpisy.

  - Činnostmi, které narušují fungování sítě, se myslí neúměrné zatěžování síťové infrastruktury datovým provozem, připojování neautorizovaných počítačů, neoprávněná manipulace se síťovými prvky atd. Pro tyto činnosti mámě zpracovaná další samostatná rizika.
  - Neoprávněné získávání dat se může konat více způsoby. Neautorizovaný počítač může odposlouchávat, případně i pozměňovat data

putující po síti. Připojení neautorizovaného počítače je řešeno v rámci samostatného rizika.

Získáním hesla nějakého uživatele se útočník může dostat k jeho datům. V nejhorším případě může získat i heslo uživatele `root` při nedbalosti správců, kteří ho znají. K tomu, aby útočník heslo uživatele `root` mohl zneužít, musí znát ještě osobní uživatelský účet správce. Toto riziko existuje vždy a bránit se mu dá jedině tak, že uživatelé budou držet svá hesla v tajnosti, pravidelně je měnit a dodržovat zásady pro tvorbu bezpečného hesla (nároky na složitost).

Získání citlivých dat z počítačů, kde jsou zpracována, reší riziko zabývající se únikem citlivých dat.

– Činnosti v rozporu s různými předpisy zahrnují publikování nevhodného obsahu na osobní stránce uživatele, neoprávněnou instalaci licencovaného softwaru, provozování programů, které mohou vést k porušování autorských práv apod.

Pravidla pro publikování na osobní webové stránce na serveru školy stanoví pravidla pro uživatele (kapitola 7). V případě zjištění nevhodného obsahu může správce webový prostor uživateli zrušit, případně pouze smazat nevhodný obsah. Řešení takových problémů je v kompetenci vedení školy.

Správce sítě má v kompetenci kontrolu všech pracovních stanic. Při kontrole zjištuje, zda v počítačích není instalován nelegální software a další nepovolené programy. Správce takové programy z počítače odstraní a informuje vedení školy.

Riziko instalace nevhodného softwaru se dá snížit nastavením minimálních uživatelských práv. Problém je v počítačových laboratořích, kde se studenti seznamují s ovládáním operačního systému, s jeho základní konfigurací a také s instalací softwaru. Proto zde potřebují mít vyšší uživatelská práva. Existuje software, který dovoluje vytvářet obrazy pevných disků a poměrně rychle je nahrát do počítače. Tím je zajištěno, že v počítačové laboratoři budou naistalované pracovní stanice v definovaném výchozím stavu.

- **Průnik do sítě z vnějšího prostředí:** Vnitřní síť je chráněna firewallem, který je nainstalován na serveru (tedy chrání i samotný server). Konfiguraci firewallu by měla být věnována velká pozornost. Nej-

lepším řešením je striktní politika, kdy se veškerý provoz zablokuje a povolí se pouze potřebné služby (FTP, SSH, HTTP apod.). Firewall musí také zapisovat v rozumném rozsahu do logů pokusy o průnik a podezřelý provoz. Správce serveru je pak povinen tyto logy pravidelně číst, aby mohl pružně reagovat na vzniklé situace. Dále musí správce sledovat a instalovat bezpečnostní aktualizace operačního systému i dalších programů, které na serveru provozuje. Všemi výše uvedenými opatřeními se snažíme chránit server a tím i celou síť před útokem z Internetu. Firewall by měl filtrovat nejen příchozí, ale i odchozí spojení.

Útok může být proveden i díky pracovní stanici, na které se podaří spustit škodlivý kód, který naváže spojení mimo lokální síť a potenciálně tím může zpřístupnit celou síť, aniž by firewall zasáhl. Proti tomu se lze bránit tak, že na všech pracovních stanicích bude instalován bezpečnostní software, který musí být velmi často aktualizován. Dále musí být uživatelům nastavena pouze nezbytná přístupová práva, aby se riziko škodlivého kódu co nejvíce snížilo.

- **Připojení neautorizovaného počítače do sítě:** Aktuálně není nijak ošetřeno připojení cizího počítače do místní sítě. Skoro v každé místnosti je ethernetová zásuvka. Každý připojený počítač dostává IP adresu prostřednictvím protokolu DHCP a server nijak neověřuje, komu tuto IP adresu přiděluje. V této fázi může daný počítač nekontrolovaně přistupovat do sítě Internet. Pro přístup ke sdíleným zdrojům na serveru je však vyžadováno uživatelské jméno a heslo. Tedy při eliminaci tohoto rizika chceme dosáhnout znemožnění (případně znesnadnění) připojení cizího počítače do sítě a tím se mu snažit zabránit v komunikaci se sítí Internet. Nejjednodušším opatřením je nastavení DHCP serveru tak, aby přiděloval IP adresu pouze známým MAC adresám. Toto řešení není bezpečné, protože potenciální útočník může odposlouchávat provoz a poté si MAC adresu jednoduše změnit. Další variantou je statické přidělení IP adres jednotlivým počítačům a nastavení firewallu tak, aby propouštěl provoz pouze z povolených IP adres. Tato varianta má analogickou slabinu jako kontrola MAC adres. Škola momentálně nemá finanční prostředky na to, aby zajistila moderní a inteligetní síťové prvky, schopné kontrolovat připojené počítače. Dále se při velikosti sítě nevyplatí implementovat pokročilejší techniky autorizace počítačů (například protokol 802.1x). Ze zmíněných důvodů

se využije varianta přidělování IP adres pouze známým MAC adresám a zůstane zbytkové riziko, které se ještě zmenší odpojením dlouhodobě nevyužívaných zásuvek od switchů.

V předchozím odstavci se řešilo riziko připojení neutorizovaného počítače za účelem využití sítě (přístupu do Internetu). Existuje však daleko větší riziko a to připojení neautorizovaného počítače s úmyslem narušit fungování sítě nebo se dostat k citlivým datům. Útočník, kterému by se povedlo připojit svůj počítač do lokální sítě může způsobit poměrně rozsáhlé škody.

- V nejhorším případě může dojít až ke kolapsu lokální sítě. Stačí, když si útočník nastaví nevhodnou IP adresu a tím naruší komunikaci některých počítačů, v krajním případě i se serverem. Ve chvíli, kdy nefunguje komunikace se serverem, je síť prakticky nepoužitelná. Kolaps může být také způsoben přetížením sítě nebo některé její části, což je podstatou DoS[3] útoku.
- Dále může dojít k odposlouchávání komunikace a tím se zde opět objevuje riziko úniku citlivých dat. Komunikace po síti není až na výjimky šifrována. Pokud tedy útočník dokáže přesměrovat veškerou síťovou komunikaci na sebe, může velmi jednoduše odposlouchávat data včetně různých hesel. Přesměrování veškeré komunikace je až překvapivě jednoduché. Stačí, aby si útočník na svém stroji zprovoznil DHCP server, čímž má možnost nastavit svůj počítač jako default router. Všechny počítače v síti potom směřují komunikaci na tento stroj, na kterém je možné data bez problému odposlechnout. Uživatelé nemají šanci nic poznat, protože komunikace funguje standardním způsobem. Únik citlivých dat je velmi nebezpečný a v případě bezpečnostního incidentu se mohou o celou situaci zajímat různé instituce (např. Úřad na ochranu osobních údajů). Dalším způsobem neoprávněného přesměrování komunikace je tzv. *ARP spoofing*. Podstatou tohoto útoku je, že útočník ze svého stroje odešle falešné ARP pakety na počítače, jejichž komunikaci chce odposlouchávat. Obě strany si tedy upraví svoje ARP tabulky tak, že k IP adrese protistrany mají přiřazenou MAC adresu útočníka. Z toho vyplývá, že veškerá komunikace jde přes útočníka. Obranou proti

[3]Denial of Service

ARP spoofingu je statické nastavení ARP tabulek, což velmi znepříjemní práci správce při zapojování nebo odpojování jednotlivých síťových uzlů. Další obranou je nasazení protokolu 802.1x, což současná infrastruktura školní sítě neumožňuje.

Riziko DoS útoku a odposlechu dat není zcela jednoduše odstranitelné. Z finančního hlediska pravděpodobně nebude v silách školy zařídit eliminaci těchto rizik. Vzhledem k existenci počítačů s citlivými daty by stálo za zvážení alespoň oddělit tyto počítače od zbytku sítě. Všechny dotčené počítače se nacházejí poměrně blízko (fyzicky) u sebe. Bylo by tedy celkem jednoduché zřídit pro tyto stroje vlastní síť, která by mohla být připojena přímo na server. Investice jsou v tomto případě zanedbatelné a riziko úniku citlivých dat se tím snižuje. Riziko výpadku serveru bude mít nezměněné dopady.

- **Výpadek síťové infrastruktury** znamená poruchu některého aktivního síťového prvku (v tomto případě přepínače) nebo přerušení kabelového spojení mezi jednotlivými síťovými uzly.

  Většina přepínačů je v součastnosti volně přístupná. To znamená, že každý může takový přepínač vypnout, poškodit nebo odpojit některý síťový kabel. Připojení vlastního počítače přímo k přepínači je obecně řešeno jako riziko *připojení neautorizovaného počítače*. Proti tomuto riziku existuje účinná ochrana, která spočívá v umístění všech přepínačů do uzamykatelných skříněk (nejlépe včetně přívodu elektrické energie). Zbytkové riziko je pouze vniknutí do uzamčené skříňky, což je přijatelné.

  Síťové kabely jsou aktuálně zmapovány pouze schematicky a v některých částech školní budovy není zřejmé kudy vedou. Tím vzniká riziko neúmyslného poškození. Proto by měla být co nejdříve zpracována přesná dokumentace veškerého síťového vedení, aby se takovému poškození předešlo. Riziko úmyslného přerušení hrozí především u těch kabelů, které nejsou umístěny ve zdech. V nejmírnějším případě může být kabel pouze přerušen. Pokud by však útočník přerušil kabel na vhodném místě (např. mezi serverem a nejbližším přepínačem) a poté připojil svůj počítač do místa přerušení, mohl by odposlouchávat veškerou komunikaci. Tím se dostáváme k riziku *připojení neautorizovaného počítače* a dalším rizikům, které z něj vyplývají. Pro kabely ve zdech je riziko nízké a ponecháváme ho jako zbytkové. Pro ostatní

kabely je nutné provést opatření, aby se odstranilo zmiňované riziko. Příkladem takového opatření je přemístění kabelů do zdi (pokud je to možné) nebo alespoň do chrániček. Vzhledem k tomu, že v budově probíhají rozsáhlé stavební práce, pak je vhodná doba i pro přeložení nejrizikovějších kabelů. Správce sítě by měl také pravidelně kontrolovat volné části kabeláže. Každý kabel od přepínače ke stanici by měl být ukončen zásuvkou.

Z výše uvedeného rozboru vyplývají nová rizika, která je třeba řešit.

- Heslo uživatele `root` na serveru je velmi citlivý údaj. Při jeho vyzrazení může potenciální útočník totálně odstavit celou počítačovou síť. Dále může být heslo zapomenuto. Proti zapomenutí hesla může sloužit zapečetěná obálka uložená v trezoru školy, do které se heslo vloží. Při každém otevření obálky se musí heslo změnit a poté se zapečetí nová obálka s novým heslem. Aktuální heslo zná pouze správce serveru. Při sebemenším podezření na vyzrazení hesla je povinen toto heslo okamžitě změnit a uložit ho opět do obálky v trezoru místo původního. Změnu hesla je vhodné provádět pravidelně.

  Dále s heslem superuživatele `root` souvisí riziko nefunkčnosti tohoto uživatelského účtu. Není podstatné, jakým způsobem tako nefunkčnost nastane, ale důsledkem je nemožnost správy serveru. V takovém případě nezbývá správci jiná možnost než reinstalace operačního systému. Pokud pevný disk není šifrovaný, tak je tu alespoň možnost odzálohovat data. Jinak mohou uživatelé přistupovat pouze ke svým datům, ale nikdo není schopen konfigurovat systém, spravovat uživatelské účty. Nefunkčnost uživatele `root` je tedy velmi vážným rizikem. V praxi se proto zavádí záložní uživatel (např. `toor`) s UID 0, jehož heslo nezná žádná osoba a je uloženo v trezoru školy v zapečetěné obálce pro případ nouze. Pravidla pro manipulaci se zapečetěnou obálkou jsou zde stejná jako s heslem superuživatele `root`.

  Pokud má škola více správců, kteří mají mít superuživatelský přístup na server, pak je velmi vhodné, aby měl každý z nich vlastní superuživatelský účet. Svázání účtu s konkrétní osobou je důležité proto, aby se dalo snadno zjistit, kdo jaké změny prováděl. Dále je to výhodné proto, aby jednotliví správci nemuseli sdílet jedno heslo. Aktuálně má škola pouze jednoho správce, ale toto opatření se může v budoucnu uplatnit.

- Může se vyskytnou nefungující záložní médium. Z těchto důvodů se vyplatí ponechat více po sobě jdoucích nejnovějších záloh. Dále je možné uchovávat jednu zálohu ve více kopiích, ale v prostředí zkoumané sítě je to zbytečné. Snížení rizika můžeme dosáhnout tím, že zálohu po vytvoření okamžitě otestujeme. V současnosti se na zálohování používají jednorázově zapisovatelná optická média (CD), u nichž je riziko nečitelnosti menší než u dříve používaných disket. Nečitelnost optických médií je nejčastěji způsobena vystavením daného média dlouhodobému slunčenímu záření. Výše je uvedeno, že zálohy by se měly ukládat do trezoru, takže sluneční záření můžeme vyloučit.

V několika bodech se zmiňuje školní trezor jako bezpečné úložiště. Pro potřeby bezpečnostní politiky je vhodné zmínit, kdo má do trezoru přístup a za jakých podmínek. Klíč od trezoru mají pouze dvě osoby (ředitel a finanční účetní). Nikdo jiný se bez jejich přítomnosti do trezoru nedostane. V praxi trezor obsluhuje pouze finanční účetní a je jasně stanoveno, komu smí vydávat jednotlivé uložené věci. Z hlediska bezpečnosti počítačové sítě a výpočetní techniky nás zajímají pouze instalační média, licenční kódy k softwaru a zapečetěná obálka s heslem uživatele `root` na serveru. Instalační média a licenční kódy si smí vyžádat pouze správce sítě. Heslo uživatele `root` smí žádat pouze správce serveru, který je zodpovědný za opětovné zapečetění obálky po jejím otevření a také za aktuálnost hesla v obálce.

Kapitola 4

Bezpečnostní záměr

- Vzhledem k neustálému rozšiřování informačních technologií do všech myslitelných oblastí je nutné přijmout soubor opatření a mechanismů pro zajištění bezpečnosti místní počítačové sítě, efektivního využívání všech dostupných prostředků, ale i pro zamezení zneužívání těchto prostředků.
- V prostředí školy jsou tři druhy uživatelů, kteří mají velmi odlišné potřeby při práci s počítačem a sítí.

  1. **Studenti** mají k dispozici výpočetní techniku ve dvou laboratořích. Primárním využitím techniky pro studenty je výuka. Ve volných hodinách mají přístup do laboratoří za přítomnosti studentského dozoru. Škola takto umožňuje studentům přístup k Internetu a k počítači především pro studijní účely a pro osobní komunikaci.
  2. **Učitelé** mají možnost se připravovat na výuku s pomocí výpočetní techniky a Internetu. Ve vybraných učebnách mají možnost pomocí audiovizuální techniky promítat prezentace a další materiály týkající se vzdělávání. Jakožto zaměstnanci však učitelé nesmí využívat služební počítače k činnostem, které nesouvisí s výkonem jejich funkce.
  3. **Ostatní zaměstnanci** mají velmi rozdílné potřeby pro využití výpočetní techniky. Tyto potřeby jsou řešeny individuálně pro každé pracovní zařazení. Stále však platí, že je nutné zamezit využívání výpočetní techniky pro činnosti, které nesouvisí s výkonem jejich funkce.

- Všichni uživatelé musí být seznámeni se zásadami využívání výpočetní techniky (příloha bezpečnostní politiky - kapitola 7). U počítačů v kabinetech je nutné přenést část odpovědnosti za počítač na zaměstnance, pokud požaduje vyšší uživatelská práva a využívá počítač sám.

- V oblasti evidence hardwaru je nezbytné provést kompletní inventuru veškerého vybavení a dále přijmout taková opatření, aby nákup nového a likvidace starého vybavení byly průhlednější. Tuto agendu dostane na starost konkrétní zaměstnanec.

- Všichni uživatelé mají právo na soukromí. Každý má k dispozici domovský adresář, který není přístupný nikomu jinému, a také svoji mailovou schránku.

- Uživatelé potřebují velmi často sdílet data a to z několika důvodů. Skupina uživatelů (typicky studenti) potřebuje data od jiného uživatele (učitel). Není příliš praktické tato data distribuovat jednotlivě, protože je to časově náročné, případná aktualizace není příliš dobře realizovatelná a navíc uložení dat na jednom místě vede k úspoře diskové kapacity. Sdílení dat je umožněno více způsoby, ale ne každý uživatel má k dispozici všechny.

  1. V domovském adresáři má každý uživatel adresář `public_html`. Tento adresář je přístupný přes protokol HTTP komukoliv. Původně je tento prostor určen pro osobní webové stránky studentů, ale je možné takto sdílet cokoli.
  2. Server poskytuje sdílený adresář `shared`, který se připojí každému uživateli prostřednictvím Samby pouze s právy pro čtení. Zápis je umožněn pouze vybraným uživatelům pomocí tzv. symlinku, který mají ve svém domovském adresáři.
  3. V rámci stanic s Windows mají uživatelé možnost sdílet nejen adresáře s daty, ale například tiskárny nebo vyměnitelná média. Sdílení tímto způsobem je regulováno pomocí přístupových práv na obou stranách. To znamená, že na straně sdílejícího není možné přidávat či rušit libovolné sdílení. Sdílející však může v rámci svých práv sdílení omezovat jen pro určité uživatele.

- V případě zneužívání poskytnutých prostředků může dojít k omezení nebo zrušení přístupu a to dočasně nebo trvale. U zaměstnanců může

být zneužívání výpočetní techniky k činnostem nesouvisejícím s jejich pracovní činností posuzováno jako porušení pracovní kázně.

- Vzhledem ke zvyšování počtu pracovních stanic s operačním systémem Gentoo Linux (popř. další distribuce Linuxu) je nutné vyřešit autorizaci uživatelů těchto stanic. Možné jsou dvě varianty:

  1. Stávající systém přihlašování ke sdíleným prostředkům na serveru pomocí Samby je použitelný i pro jiné operační systémy než MS Windows. Výhodou tohoto řešení je, že by nebylo nutné provádět žádné citelné zásahy do konfigurace serveru. Systém je odzkoušený a bez problémů slouží několik let. Na jednotlivé stanice by se musel nainstalovat klient Samby a pečlivě nakonfigurovat systém tak, aby bylo možné přihlašování pomocí protokolu Samby. Nevýhodou ovšem je, že Samba je určena především k připojení stanicí s MS Windows k serveru běžícím na systému unixového typu. Na připojení unixových stanic k unixovému serveru se toto řešení příliš často nepoužívá.
  2. Další variantou je zprovoznění NIS (Network Information System), což je čistě unixové řešení využívající NFS (Network File System). Toto řešení je velmi elegantní v případě připojení unixových stanic, ale není použitelné pro připojení stanic s Windows. Jeho zavedení by představovalo instalaci nových služeb na straně serveru a pečlivou konfiguraci. To je vyváženo velmi jednoduchou konfigurací klientských stanic.
  3. Ještě existuje možnost kombinace obou výše uvedených možností. To sebou přináší určité problémy spočívající v nutnosti synchronizace uživatelských účtů apod. Na druhou stranu by se pro každou platformu používalo řešení, které je pro ni přirozené.

  Konečné rozhodnutí je ponecháno ke zvážení správcům sítě, kteří budou zvolené řešení realizovat.

Kapitola 5

Závěr

Vedení GVN se staví kladně k vytvoření bezpečnostní politiky, nicméně v současné době nepřistoupí na její nasazení. Důvodem je provádění rozsáhlých stavebních prací na půdní vestavbě v budově školy. Po dokončení půdní vestavby vznikne v budově nové patro, kde bude mimo jiné i nová počítačová laboratoř. Do této nové laboratoře bude umístěn i server, který bude uzamčen v serverové skříni spolu s přípojkou k síti Internet. V novém patře budou zřízeny rozvody počítačové sítě pomocí gigabitového ethernetu a poté se bude modernizovat i zbytek počítačové sítě (aktivní prvky, kabeláž). Díky existenci bezpečnostní politiky může GVN výše uvedené akce podřizovat konkrétním pravidlům.

I bez zavedení kompletní bezpečnostní politiky je možno alepoň některé partie uvést do provozu. Jedná se především o přílohu politiky, se kterou by se měli na začátku školního roku seznámit všichni uživatelé.

Při tvorbě bezpečnostní politiky byly zjištěny nedostatky v evidenci hardwaru a licencí. Správce sítě byl pověřen provedením komplexní inventury hardwaru, díky čemuž se povedlo zlikvidovat mnoho starých a nefunkčních počítačů. Vedení školy také řeší dokoupení licencí na software tak, aby bylo možné rozšířit počet pracovních stanic, které budou umístěné v nové počítačové laboratoři.

Správce serveru se na základě této práce rozhodl, že provede kompletní reinstalaci a zcela novou konfiguraci serveru. Důvodem je, že z dřívějších dob je nainstalováno množství nepoužitých programů a existence starých uživatelských účtů, které je potřeba zrušit. Před reinstalací budou do serveru zakoupeny kvalitní pevné disky, které se zapojí pomocí technologie RAID1. Tato akce se uskuteční o letních prázdninách, kdy je provoz na síti minimální.

Cílem práce bylo zdokumentovat průběh tvorby bezpečnostní politiky a následně sepsat její finální podobu, která je v kapitole 6. Dále byl vytvořen dokument s pravidly pro uživatele (kapitola 7), který vznikl přepracováním dokumentu [2].

Kapitola 6

Příloha - Politika a principy bezpečnosti

6.1 Popis aktiv

6.1.1 Fyzická aktiva

Mezi fyzická aktiva řadíme veškerý hmotný majetek, který je součástí počítačové sítě GVN. Tento majetek je evidován v tzv. Sbírce informatiky, za kterou zodpovídá jeden určený pracovník. Sbírka musí být kontrolována vedením školy podle platných předpisů.

Mezi nejdůležitější a nejcennější fyzická aktiva patří:

- **Server** je nejkritičtější součástí celé sítě. Jeho zabezpečení musí být věnována zvláštní pozornost. Musí být bezpodmínečně umístěn v uzamykatelné místnosti a všechny osoby s přístupem do takové místnosti jsou poučeni, že nesmí se serverem nijak manipulovat. Výjimku tvoří pouze správci sítě, kteří mají oficiálně přístup k serveru povolen. Ideálně by taková místnost měla být přístupná výhradně správcům. V případě poruchy je každý povinen neprodleně informovat vedení GVN nebo správce sítě.

  Napájení serveru je zálohováno zařízením UPS, které je na server napojeno také datovým kabelem. Díky tomu je možné monitorovat stav baterií. Při výpadku napájení se server pokusí odeslat e-mailem varování správci. Pokud není napájení včas obnoveno (tj. baterie se dostane na kritickou hranici výdrže), server odešle e-mail správci a automaticky

se vypne. Po obnovení napájení zařízení UPS zajistí opětovné nastartování serveru. Pro zajištění spolehlivosti UPS musí být kontrolována a případně vyměněna baterie dle pokynů výrobce UPS.

Při poruše hardwaru serveru musí být zajištěna výměna nefunkčního dílu v co nejkratší době. Je vhodné mít připravené především záložní pevné disky, protože na serveru je provozována technologie RAID1 pro zajištění ochrany dat. Dále je vhodné mít v zásobě náhradní zdroj. Ostatní díly nevykazují tak častou poruchovost jako pevné disky a zdroje.

Na serveru musí bezpodmínečně fungovat zálohovací mechanismus postavený na technologii RAID1 (mirroring), aby se předešlo ztrátě dat na disku v případě poruchy pevného disku.

Server má také funkci brány do sítě Internet. Veškerá komunikace pracovních stanic s vnějším prostředím probíhá přes server. Na serveru proto musí být instalován a řádně nakonfigurován firewall, aby se předešlo průniku do sítě z prostředí Internetu.

Konfiguraci serveru, instalaci softwaru a další činnosti ovlivňující chod serveru smí provádět pouze superuživatel `root`. Heslo superuživatele `root` musí být dostatečně složité a řádně zabezpečené proti vyzrazení. Toto heslo zná pouze správce serveru a je také uloženo v zapečetěné obálce v trezoru školy. Obálka smí být vydána pouze správci serveru nebo řediteli školy. Po otevření obálky musí být heslo neprodleně změněno a opět zapečetěno do obálky. Pro případ nefunkčnostni uživatelského účtu `root` je vhodné zavést ještě záložního uživatele (např. `toor`) se superuživatelskými právy. Jeho heslo nesmí znát žádná osoba. Heslo je uloženo opět v trezoru školy v zapečetěné obálce. Pro manipulaci s obálkou platí stejná pravidla jako pro uživatele `root`.

- **Přípojka do sítě Internet** je řešena pomocí optického kabelu, který je v celé své délce umístěn ve zdi, kromě jeho ukončení v místnosti se serverem. Optický kabel až k zařízení, jež převádí optické signály na elektrické, je v majetku poskytovatele připojení a tudíž není nikomu bez výjimky dovoleno s ním manipulovat. Vedení kabelu ve zdi je zaneseno ve stavební dokumentaci školy. Každý mechanický zásah v okolí kabelu musí podléhat souhlasu vedení školy, aby nedošlo k jeho poškození.

  Koncové zařízení, které převádí optické signály na elektrické (a na-

opak) je závislé na elektrickém proudu. Toto zařízení by mělo být umístěno v bezprostřední blízkosti serveru a napojeno na zařízení UPS, aby server mohl komunikovat do Internetu (e-mailová varování pro správce) i v případě výpadku napájení.

- **Přepínače** zajišťují propojení všech pracovních stanic se serverem i mezi sebou navzájem. Výpadek libovolného přepínače způsobí odříznutí určité části sítě a v nejhorším případě celé vnitřní sítě od serveru. Z těchto důvodů je nutné, aby každý přepínač byl umístěn v uzamykatelné skříňce, aby nikdo nemohl odpojovat či připojovat síťové kabely ani manipulovat s přívodem elektrického proudu.

- **Síťová kabeláž** slouží k propojení jednotlivých uzlů v síti. Kabeláž je z větší části umístěna ve zdech budovy, ale existují místa, kde jsou kabely volně přístupné (např. konce kabelů v učebnách a kabinetech). Veškeré vedení síťových kabelů musí být pečlivě zmapováno, aby nehrozilo poškození (např. při stavebních úpravách). Volné části kabelů by měly být umístěny v instalačních lištách nebo chráničkách a ukončeny zásuvkou. Připojení stanice do zásuvky se pak realizuje volným kabelem. Správce sítě musí pravidelně kontrolovat, zda jsou volně přístupné kabely neporušené. S tím také souvisí kontrola, zda není do sítě připojen neautorizovaný počítač.

- **Pracovní stanice** je každý počítač kromě serveru, který je připojen do sítě GVN. Připojení pracovní stanice do sítě musí schválit správce sítě. Všechny pracovní stanice musí být umístěny uzamykatelných místnostech. Pro každou pracovní stanici musí být jednoznačně určena odpovědná osoba. Všechny stanice se po ukončení pracovní doby vypínají. Pracovní stanice v laboratořích se vypínají po skončení výuky v daný den. Jakékoli mechanické zásahy jsou povoleny pouze pověřeným pracovníkům školy, případně zaměstnancům servisní organizace.

  Všechny pracovní stanice musí být provozuschopné. Správce sítě je zodpovědný za fungování stanic. V pravidelných intervalech musí provádět kontrolu funkčnosti. U stanic v počítačových laboratořích je vhodné zálohovat obrazy pevných disků a pravidelně je aktualizovat, pro případ rychlé reinstalace. Uživatelé jsou povinni správci sítě hlásit jakékoli poruchy, aby mohla být včas zjednána náprava.

- **Síťové tiskárny** podléhají kontrole ze strany správy sítě. Jsou umístěny v uzamykatelných místnostech. Tiskárny musí být vždy po ukon-

čení pracovní doby vypnuty. Každá tiskárna musí být pod kontrolou odpovědné osoby, aby nedocházelo k jejímu zneužívání a používala se pouze k tisku materiálů souvisejících s provozem školy a studijních materiálů.

- **Záznamové zařízení kamerového systému** je umístěno v sekretariátu školy a je centrálním prvkem tohoto systému. Kamerový systém slouží k zajištění bezpečnosti ve vnějších prostorách školy a je v provozu nepřetržitě. Přístup k záznamovému zařízení je omezen. Navíc je k němu připojen jeden monitor, který zprostředkovává obraz ze všech kamer. Tento monitor by měl být během pracovní doby sledován pracovnicemi sekretariátu školy. Záznamové zařízení je připojeno do počítačové sítě GVN a pověření zaměstnanci k němu mají přístup přes webové rozhraní, které je chráněno heslem.

- **Náhradní díly a servisní technika** slouží k rychlé opravě běžných technických problémů. Jedná se například o náhradní zdroje, pevné disky apod. Tyto díly jsou umístěny v jedné uzamykatelné místnosti. Zásoby dílů je třeba kontrolovat, protože se mohou stát předmětem krádeže jednodušeji než např. pracovní stanice. Dále do této kategorie patří nářadí (šroubováky, konektorovací kleště, měřící zařízení apod.) sloužící pro jednoduché opravy a instalace, které není nutné provádět v odborném servisu.

  Pro spolehlivý provoz serveru je nezbytné mít v zásobě náhradní pevný disk stejné nebo mírně větší kapacity (ideálně stejný typ disku), než mají aktuálně nasazené disky v RAID poli na serveru. V případě poruchy musí být zajištěna okamžitá výměna, jinak hrozí ztráta dat.

- **Datové nosiče** by měly být uloženy na bezpečném místě. Originální instalační disky zakoupeného softwaru se ukládají do školního trezoru. Ostatní datové nosiče jsou v kompetenci jednotlivých zaměstnanců, kteří je využívají pro ukládání a zálohování svých prací a dokumentů. Pouze pro tyto účely poskytuje škola zaměstnancům prázdná zapisovatelná média. Zneužívání médií pro soukromé a jiné účely se posuzuje jako zneužívání školního majetku. O tato média se zaměstnanci starají sami.

  Zálohovací média s citlivými údaji (zálohy klasifikace, finančního a mzdového účetnictví a dalších agend) musí být uschována v trezoru školy, aby se předešlo jejich ztrátě, zničení nebo zneužití. Zastaralé

zálohy a další média s citlivými údaji se musí zlikvidovat podle platných právních předpisů.

6.1.2 Informace

V prostřední GVN se vyskytují informace s různými požadavky na autenticitu, integritu a utajení. Jedná se především o osobní údaje studentů a zaměstnanců, dále účetní údaje, klasifikační data apod. Z hlediska bezpečnostní politiky počítačové sítě nás zajímají informace udržované v elektronické podobě.

- **Osobní údaje studentů** jsou citlivé údaje, které v elektronické podobě zpracovává sekretariát školy pro vedení zákonem stanovených agend a také je využívá pracovník pověřený zpracováním klasifikačních dat na konci pololetí za účelem tisku vysvědčení. Každý pracovník, který přichází do styku s údaji studentů v elektronické podobě, nesmí taková data poskytovat žádné třetí osobě jakoukoli formou. Tedy žádná třetí osoba si takové údaje nesmí ani prohlížet na obrazovce počítače nebo je tisknout. Pro osobní údaje vedené v papírové podobě existují zvláštní směrnice a tato politika se jimi nezabývá.

- **Osobní údaje zaměstnanců** jsou citlivé údaje, které využívá výhradně sekretariát a vedení školy. Mezi tyto údaje patří také mzdové účetnictví. Platí přísný zákaz poskytování jakýchkoli údajů o zaměstnancích mimo případů vymezených zákonem a dalšími právními předpisy.

- **Informace nezbytné pro provoz školy** zahrnují finanční účetnictví, evidenci hmotného i nehmotného majetku a různé oficiální dokumenty. S těmito údaji nakládá výhradně vedení školy a sekretariát. Nikomu dalšímu nesmí být údaje přístupné. Počítače, v nichž se tyto informace vyskytují, nejsou volně přístupné.

Všechny důležité informace využívané v elektronické podobě musí být pravidelně zálohované. Záložní média se ukládají do trezoru školy a je nutné ponechat nejméně 3 po sobě jdoucí nejnovější zálohy. Starší zálohy je nutné zlikvidovat bezpečným způsobem. Při případném přenosu citlivých informací po síti, případně i mimo síť, je nezbytně nutné použít šifrování, aby se zabránilo odposlechu přenášených dat. Vhodným nastavením uživatelských

práv je třeba ochránit data před smazáním. Obsah pevného disku serveru se zálohuje pomocí technologie RAID1 na druhý pevný disk.

Veškeré citlivé informace musí být patřičně chráněny. Na počítačích, kde se takové informace zpracovávají, musí být instalován a řádně nakonfigurován osobní firewall a antivirový software. Zaměstnanci, kteří tyto počítače obsluhují, by měli mít co nejnižší uživatelská práva, aby se předešlo nechtěné nebo úmyslné instalaci nebezpečného softwaru nebo změně konfigurace operačního systému a bezpečnostního softwaru. Dále zaměstnanci nesmí žádným způsobem kopírovat citlivá data s výjimkou řádného zálohování.

Zaměstnancům, kteří obsluhují programy pro zpracování citlivých dat, musí být umožněna účast na pravidelných školeních výrobců softwaru, kde se zaměstnanci seznamují s obsluhou programu včetně zálohování. Zálohování musí probíhat pravidelně a dostatečně často (s ohledem na frekvenci změn v datech). Za zálohování je zodpovědná obsluha programu. Vytvořené zálohy ukládají zaměstnanci na přenosná média a uschovávají je v trezoru školy. Vždy je třeba ponechat alespoň tři po sobě jdoucí nejnovější zálohy. Ostatní mohou být bezpečně zlikvidovány.

6.1.3 Software

V této kategorii je zahrnut veškerý software potřebný pro běžný provoz školy. V následujícím seznamu je vyjmenován software spolu s účelem jeho využití a také údaje o instalačních médiích a licenci.

- **Microsoft Windows XP Professional CZ** je operační systém, který je instalován na všech pracovních stanicích. Instalační disk je uložen v trezoru školy stejně jako licenční kód. GVN vlastní multilicenci na 50 instalací. Za dodržení počtu licencovaných instalací zodpovídá správa sítě.

- **Microsoft Office 2003 CZ** je kancelářský balík využívaný pro běžnou práci zaměstnanců i pro výuku studentů. Instalační disk je uložen v trezoru školy stejně jako licenční kód. GVN vlastní multilicenci na 50 instalací. Za dodržení počtu licencovaných instalací zodpovídá správa sítě.

- **AVG 8 Network Edition** je bezpečnostní software zahrnující moduly proti škodlivému softwaru, firewall atd. Škola vlastní multilicenci na 50 instalací. Instalační disk je zastaralý a proto byl zlikvidován.

Licenční kód, který je každé dva roky obnovován, je uložen v trezoru školy. Instalační soubory se v případě potřeby vždy stahují z webových stránek výrobce z důvodu jejich nezbytné aktuálnosti.

- **Relax KEŠ** slouží ke zpracování osobních a klasifikačních dat studentů a s tím souvisejících činností. GVN vlastní licenci pro jednu instalaci. Instalační disk je uložen v trezoru školy, nicméně je zastaralý a v případě nové instalace programu musí být stažena aktuální verze instalačních souborů z webových stránek výrobce programu. Licenční kód je uložen v trezoru školy.

- Rozvrhovací software využívá k práci zástupce ředitele školy. Instalační program je volně stažitelný z webových stránek výrobce a licenční kód je uložen v trezoru školy.

- Účetní programy, evidence majetku a další podobné programy jsou využívány v sekretariátu školy. O jejich údržbu se stará z velké části výrobce daného programu. Součástí této kategorie je i komunikační program, který slouží pro ovládání telefonní ústředny školy. O provoz telefonní ústředny včetně obslužného softwaru se stará telekomunikační operátor.

- **Gentoo Linux** je operační systém, který se používá na serveru a dále na některých stanicích v počítačových laboratořích. Instalační média se speciálně upravenou verzí systému pro server má u sebe správce serveru, který je zároveň dodavatelem této instalace. Pro instalaci na pracovní stanice se používá standardní verze, která je volně ke stažení z Internetu.

- **Programy určené pro výuku** jsou potřebné pro kvalitní a moderní výuku. Instalační média a případné licenční kódy jsou uloženy v trezoru školy.

6.1.4 Pracovníci

Pro bezpečný a spolehlivý chod počítačové sítě GVN a zařízení do ní zapojených je nezbytný dohled odborných pracovníků. Tito pracovníci mají na starosti instalaci a připojování nových prvků do sítě. Dále se starají o údržbu veškeré techniky a také o řešení problémů a poskytování odborné pomoci ostatním uživatelům sítě. V následujícím seznamu jsou vyjmenovány

pracovní pozice, o jejichž konkrétním obsazení rozhodne vedení školy. Není vhodné obsadit všechny jmenované pozice jedním zaměstnancem, protože v případě jeho absence vzniká problém s řešením krizových situací. Pokud budou všechny pozice správce obsazeny jedním zaměstnancem, je třeba aby měl tento pracovník alespoň jednoho zástupce.

- **Správce serveru** se stará o nepřetržitý a spolehlivý běh serveru. Náplní jeho práce je udržovat aktuální uživatelské účty (zakládat nové a rušit staré). Dále musí monitorovat logy a v případě zjištění jakýchkoli podezřelých aktivit podniknout příslušné kroky nutné k zamezení těchto aktivit. V případě závažných zjištění je povinen informovat vedení školy a ve spolupráci se správcem sítě těmto aktivitám zamezit. Důležitou součástí pracovní náplně správce serveru je péče o připojení do sítě Internet. Tento pracovník zná jako jediný heslo uživatele *root* na serveru.

- **Správce sítě** zajišťuje všechny úkony související s provozem počítačové sítě a stanic do ní připojených. Stará se o instalaci software do počítačů, opravu běžných závad a řešení problémů uživatelů. V neposlední řadě je povinen kontrolovat, zda uživatelé nepoužívají a neinstalují nelegální software, nešíří neoprávněně data podléhající autorským právům apod. V případě zjištění nějaké takové aktivity musí tuto skutečnost oznámit vedení školy. Každý správce sítě vlastní uživatelský účet s oprávněním *Domain Administrator* (terminologie Microsoft Windows). Správce sítě zná heslo lokálního uživatele *Administrator* na stanicích s Windows a heslo uživatele *root* na stanicích s Linuxem.

- **Správce laboratoře** má stejný rozsah práv a povinností jako správce sítě, ale navíc zná specifika údržby a provozu počítačové laboratoře. Tato pracovní pozice je v ideálním případě obsazena učitelem informatiky, který je plně obeznámen s potřebami vyučujících pro kvalitní průběh výuky. Laboratoř vyžaduje vyšší frekvenci údržby než kancelářské počítače. Pro potřeby snadné a rychlé údržby, reinstalace a zálohování by měla škola zakoupit vhodný software, který ve vybavení správy sítě chybí.

- **Zaměstnanci obsluhující software potřebný pro provoz školy:** Škola využívá několik programů, na kterých je závislý bezproblémový chod školy. Pro každý takový program je nutné zajistit nejméně dva

pracovníky, kteří umí daný program obsluhovat. Každý program primárně obsluhuje jeden zaměstnanec v rámci své pracovní náplně. Druhý (záložní) pracovník musí být s daným programen obeznámen tak, aby byl schopen kdykoli obsluhu programu zastoupit. Škola musí zajistit pravidelné proškolování pracovníků u výrobců jednotlivých programů.

6.2 Vymezení odpovědnosti

6.2.1 Provoz sítě

O provoz počítačové sítě GVN se stará více zaměstnanců či externích pracovníků. Je proto nutné vymezit odpovědnost pro konkrétní pracovníky. Tato část by měla korespondovat s pracovními smlouvami jednotlivých pracovníků. V následujícím seznamu jsou uvedeny klíčové činnosti pro bezproblémové fungování sítě. Provozem se pro tyto účely myslí instalace operačního systému a dalších programů, běžná údržba, funkčnost, spolehlivost, dostupnost a případné opravy hardwarového charakteru.

činnost	**odpovědná osoba**
připojení do sítě Internet	správce serveru
provoz a dostupnost serveru	správce serveru
provoz počítačových laboratoří	správce laboratoře
provoz počítačů mimo laboratoře do sítě	správce sítě
provoz a připojování ostatních zařízení do sítě	správce sítě

6.2.2 Užívání sítě

Každý uživatel bez výjimky je sám osobně zodpovědný za veškerou činnost, kterou provozuje pod svým uživatelským účtem. Z tohoto důvodu se požaduje, aby každý uživatelský účet byl striktně osobní. Komplexní vymezení práv a povinností uživatelů ale i správců sítě vymezuje dokument[1] *Zásady pro provozování a používání výpočetní techniky zapojené do počítačové sítě GVN*, který je k této bezpečnostní politice přiložen.

[1] Vznikl přepracováním dokumentu [2].

6.3 Plán na udržování bezpečnosti

Vedení GVN má zájem na tom, aby školní síť fungovala spolehlivě a sloužila ke vzdělávání studentů, odborné přípravě vyučujících a také aby usnadnila práci při zpracování dat ostatním zaměstnancům.

6.3.1 Kontrola uživatelů

S rozvojem výpočetní techniky se vyvíjí i nová rizika při práci s počítačem, při přístupu na Internet atd. Vedení GVN vyjádřilo potřebu více kontrolovat činnosti uživatelů. Tím by se mělo zlepšit využití pracovní doby zaměstnanců a usměrnit mimoškolní činnost studentů v laboratořích. Školní síť nesmí studentům sloužit pro získávání nelegálního softwaru prostřednictvím Internetu, ke hraní počítačových her a v neposlední řadě k prohlížení webových stránek s nevhodným obsahem. Správce sítě má právo kontrolovat činnost všech uživatelů. Počítačová síť může být monitorována za účelem optimalizace nebo odhalování zakázaných činností.

6.3.2 Mechanismy pro kontrolu licencí

Evidence softwaru je vedena v rámci tzv. Sbírky informatiky, kam se veškerý software zařazuje. Tuto evidenci udržuje pověřený pracovník, který má povinnost informovat správce sítě.

Správce sítě si vede na základě poskytnutých informací vlastní evidenci, která zahrnuje údaje o počtu zakoupených licencí pro daný software a případně i o době platnosti licence, je-li omezena.

Správce sítě je povinen pravidelně kontrolovat jednotlivé pracovní stanice a zjišťovat stav instalovaného software. V rámci této kontroly také správce zjišťuje, zda není nainstalován software bez patřičné licence, případně i software, který není povolen správou sítě. Jesliže je takový program objeven, správce prošetří okolnosti instalace a poté program z počítače odstraní. Dále informuje uživatele o provedeném zásahu. V případě opakovaného prohřešku informuje také vedení školy.

Správce také pravidelně na základě kontrol informuje vedení školy o stavu využití zakoupených licencí. Nákup licencovaného software představuje finanční zátěž, a proto je třeba, aby vedení mělo přehled a mohlo plánovat investice nákupu software.

6.3.3 Obnova technického vybavení

Škola se snaží poskytovat svým uživatelům kvalitní výpočetní techniku podle svých finančních možností. Odvětví informačních technologií se velmi rychle vyvíjí a stoupají hardwarové nároky nového softwaru.

- Škola uvažuje o zkvalitnění počítačové sítě z hlediska její přenosové rychlosti. K tomu je nutné zakoupit nové síťové přepínače podporující rychlost $1Gbit/s$ a v některých případech i obnovit kabeláž. Dále se musí server osadit kvalitní síťovou kartou a tím bude dokončeno zrychlení páteřní sítě (mezi přepínači a serverem). V dalším kroku se mohou stávající počítače osadit novými síťovými kartami, což není nezbytně nutné. U nově nakupovaných počítačů se bude požadovat vybavení gigabitovou síťovou kartou.

- Počítače v laboratořích podléhají rychlému stárnutí. Správce laboratoře musí pravidelně informovat vedení školy o stavu laboratoře, aby se včas zajistily finance na obnovu laboratoře. Původní počítače vyřazené z laboratoří lze většinou po drobných opravách využít v kancelářích a kabinetech.

- Počítače v kabinetech, kancelářích a dalších místech zastarávají pomaleji. Požadavky zaměstnanců na novou techniku je nutné posuzovat přísněji. Mnohdy mají zaměstnanci k dispozici výpočetní výkon, ze kterého využijí jen zlomek pro svou pracovní činnost. Starší počítače lze většinou bez problému nahradit použitým počítačem z laboratoře.

6.3.4 Ochrana sítě před připojováním neautorizových počítačů

Je velmi nebezpečné ponechat komukoli možnost připojit si vlastní počítač do vnitřní sítě školy. Takové jednání přináší nezanedbatelná rizika (odposlech komunikace, úmyslné i neúmyslné přetížení sítě nebo narušení fungování sítě). V rámci finančních možností je žádoucí, co nejvíce ztížit připojení neautorizovaných počítačů do sítě. Správce serveru by měl zajistit konfiguraci DHCP serveru tak, aby přidělovat IP adresy pouze známým počítačům (dle MAC adres). Dále by měl správce sítě pravidelně kontrolovat všechna místa, kde je možné připojit neautorizovaný počítač. Všechny dlouhodobě nepoužívané síťové kabely je možné odpojit od přepínačů.

6.4 Kontrola správy sítě

Činnost správců podléhá přímé kontrole ze strany vedení školy. Správce sítě musí vedení školy poskytovat veškeré dostupné informace o stavu školní sítě, což činí formou pravidelných zpráv o změnách v síti a o využívání sítě. Správce laboratoří je podřízen správci sítě (pokud obě funkce nezastává jeden pracovník). Vedení školy má právo kdykoli zkontrolovat stav sítě s výjimkou osobních dat uživatelů v jejich domovských adresářích a e-mailových schránkách. Stav domovských adresářů může vedení kontrolovat pouze v přítomnosti vlastníka a správce serveru, který má jako jediný přístupová práva ke všem domovským adresářům. Tato kontrola může být provedena pouze na základě důvodného podezření, nikoli namátkově.

Kapitola 7

Příloha - Zásady pro provozování a používání výpočetní techniky zapojené do počítačové sítě GVN

7.1 Základní ustanovení

a) Síť Gymnázia Vítězslava Nováka (dále jen GVN) je soubor technických prostředků (tj. kabeláž, síťové prvky, počítače a další příslušenství), umožňující zaměstnancům a studentům přístup do sítě Internet. Tyto zásady vymezují základní práva a povinnosti správců i uživatelů sítě.

b) Uživatelem je pro potřeby těchto pravidel zaměstnanec, student a případně další osoba schválená správou sítě, užívající výpočetní techniku na GVN.

c) Správou sítě jsou pověřeni zaměstnanci školy, kteří mají právo svěřit určité pravomoci vybraným studentům. Těmto studentům mohou být svěřeny pouze pravomoci, které nezasahují do soukromí ostatních uživatelů.

7.2 Správa sítě

a) zajišťuje provoz základní infrastruktury sítě GVN a funkčnost pracovních stanic.

b) schvaluje připojení každého nového zařízení do sítě a přiděluje mu doménové jméno (případně IP adresu).

c) zodpovídá za konfiguraci síťových prvků a za provoz serveru.

d) má v závažných případech právo odpojit segment nebo koncové zařízení, které způsobuje problémy (např. šíří virovou nákazu), na dobu nezbytně nutnou, aby byla zachována funkčnost a bezpečnost sítě.

7.3 Pravidla pro uživatele

a) Každý uživatel musí být registrován a musí být známa jeho identita. Uživatelský účet musí být striktně osobní s výjimkou dočasných účtů pro návštěvy (kurzy, maturitní komise, krátkodové výměnné pobyty). Uživatel je povinen volit bezpečné (dostatečně složité) přístupové heslo a udržovat ho v tajnosti. Pokud uživatel umožní zneužití své identity, je zodpovědný za způsobené škody. Pokud uživatel zjistí zneužití svého účtu, musí tuto skutečnost neprodleně oznámit správě sítě (např. prostřednictvím kanceláře školy, e-mailem, osobně). Ukončením pracovního poměru, ukončením studia uživatelská práva zanikají.

b) Výpočetní technika, která je majetkem GVN, a síť GVN může být použita pouze pro aktivity související s výkonem práce (zaměstnanci) nebo se studiem (studenti).

c) Každý uživatel má k dispozici e-mailový účet. Pro používání elektronické pošty platí stejná etika jako pro poštu klasickou. Odesílatel se nesmí vydávat za jinou osobu (platí i pro vyplňování WWW formulářů) ani nesmí svou korespondencí obtěžovat ostatní uživatele (řetězové zprávy, spam). Elektronický dopis je nutno považovat za otevřenou zásilku (v případě důvěrných informací je nutné zprávu šifrovat).

d) Na počítačích zapojených do sítě GVN je zakázáno získávání, šíření, instalace a používání takového softwaru, k jehož šíření, instalaci nebo

užívání nemá uživatel právo. Uživatel nesmí používat ani volně šiřitelné programy, které nejsou správou sítě povoleny.

e) Jsou zakázány pokusy o získání neoprávněného přístupu k programům, informacím a datům jiných uživatelů. Nastane-li takovýto přístup nebo stav neúmyslně, je uživatel povinen informovat správu sítě a tento stav okamžitě ukončit.

f) Uživatel nesmí vědomě přetěžovat síť (např. zasíláním nevyžádaných e-mailových zpráv, přesunováním neúměrného objemu dat).

g) Uživatel nesmí šířit informace, které jsou v rozporu se zákonem nebo které by mohly poškodit dobré jméno GVN.

h) Uživatel je povinen dodržovat další specifická pravidla pro používání počítačů, s nimiž pracuje (např. řád počítačových laboratoří).

i) Provoz sítě může být monitorován za účelem optimalizace, předcházení abnormálním stavům a pokusům o neoprávněný přístup. Uživatel při získání svého účtu souhlasí s tím, že jeho aktivity mohou být správou sítě monitorovány. Takto získané informace mají důvěrný charakter. Správa sítě ani GVN nenesou žádnou právní odpovědnost za případné nedoručení, opoždění nebo jiný defekt v přenosu informací.

j) Každému uživateli je na serveru přidělen tzv. domovský adresář, což je prostor pro ukládání dat. Za obsah svého domovského adresáře má odpovědnost každý uživatel samostatně. Uživatel nesmí tento prostor neúměrně zaplňovat na úkor ostatních uživatelů. Pro uživatele z řad studentů je maximální objem domovského adresáře stanoven na 50 MB. Pro zaměstnance toto omezení neplatí, ale ani jim není dovoleno neúměrně zaplňovat svůj domovský adresář a tím omezovat ostatní uživatele.

7.4 Závěrečná ustanovení

a) Porušení uvedených pravidel bude řešeno vedením školy. Závažné nebo opakované porušení pravidel může mít za následek zrušení nebo omezení uživatelského účtu.

b) Tato pravidla nabývají platnosti dnem vydání.

Literatura

[1] ČSN ISO/IEC 27001 (Bezpečnostní techniky - Systémy managementu bezpečnosti informací)

[2] Příkaz děkana MFF UK č. 4/1998 (Zásady pro provozování a používání výpočetní techniky zapojené do sítě MFF UK)

[3] Webové stránky společnosti Infosec (http://www.infosec.cz)