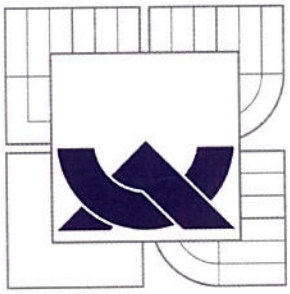
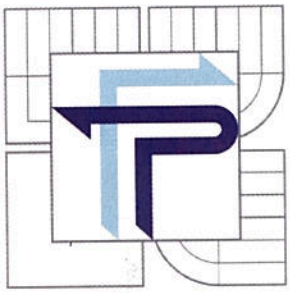


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

ZAVEDENÍ MANAGEMENTU BEZPEČNOSTI ICT NA STŘEDNÍ ŠKOLE

IMPLEMENTATION OF ICT SECURITY MANAGEMENT IN HIGHSCHOOL

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — JAN MATUSÍK
AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.
SUPERVISOR

BRNO 2013

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2012/13
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jan Matusík

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských, magisterských a doktorských studijních programů zadává bakalářskou práci s názvem:

Zavedení managementu bezpečnosti ICT na střední škole

v anglickém jazyce:

Implementation of ICT Security Management in Highschool

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

HORÁK, J. a M. KERŠLÁGER. Počítačové sítě pro začínající správce. 1. vydání. Brno: Computer Press, 2006. 304 s. ISBN80□251-0892-9.
ISO/IEC. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements. Švýcarsko, 2005. 42 p.
SELECKÝ, M. Penetrační testy a exploitace. 1. vydání. Brno: Computer Press, 2012. 304 s. ISBN978-80-251-3752-9.
SOSINSKY, B. Mistrovství – počítačové sítě. 1. vydání. Brno: Computer Press, 2010. 840 s. ISBN978-80-251-3363-7.
UNBS. DUS ISO/IEC 27007:2011: Information technology – Sucurity techniques – Guidelines for information security management systems auditing. Kampala: Uganda National Bureau of Standards, 2012. 37 p.

Vedoucí bakalářské práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2012/13.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ

L.S.

B. Půže

doc. RNDr. Bedřich Půža, CSc.
Ředitel ústavu

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Děkan

V Brně, dne 28.2.2013

Abstrakt

Obsahem této bakalářské práce je návrh zavedení managementu bezpečnosti ICT na konkrétní střední škole v Moravskoslezském kraji. Úvodní část popisuje objekt školy a dosavadní management bezpečnosti. V praktické části této práce jsou poté rozebrány nedostatky. Především z hlediska používaných bezpečnostních mechanismů, chování uživatelů, správců. Součástí práce jsou také návrhy na řešení dané situace.

Abstract

The aim of this bachelor's thesis is proposal of implementation of the ICT Security Management to the specific Highschool in the Moravian-Silesian region. Introduction part describes the school building and current Security Management. In the practical part of this thesis are then discussed the shortages in the Highschool. This is done mainly from the perspective of security mechanisms used and the behavior of users and administrators. There are also proposals how to deal with this situation in this work.

Klíčová slova

Management bezpečnosti, bezpečnost, ICT, ISO/IEC 27000

Key Words

Security management, security, ICT, ISO/IEC 27000

Bibliografická citace mé práce

MATUSÍK, J. *Zavedení managementu bezpečnosti ICT na střední škole*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2013. 55 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D..

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 31. května 2013

……..

Jan Matusík

Poděkování

Na tomto místě bych rád poděkoval vedoucímu své bakalářské práce panu Ing. Viktoru Ondrákovi, Ph.D., za jeho cenné rady, čas, který mi věnoval a ochotu při vedení mé práce. Také bych rád poděkoval panu Mgr. Pavlu Královi za poskytnutí podkladů a za cenné rady.

Obsah

ÚVOD

Počítačová kriminalita se spojuje v mnoha odvětvích a stává se součástí našeho života. Setkáváme se s ní denně na internetu, v práci, nebo jiných aspektech našeho života. Typicky se jedná o krádež našich soukromých, nebo osobních údajů. Ať už pomocí lidí, nebo počítačových virů.

Jedním z důvodů, proč se počítačová kriminalita v dnešní době rozšiřuje, je bezesporu životní styl lidí, kteří díky potřebě komunikovat co nejrychleji a nejefektivněji se svými osobními počítači, tablety či chytrými telefony zanedbávají základní bezpečnostní upozornění a pravidla. Tyto věci se bohužel staly nutnou součástí této doby a našeho života. Je tedy zapotřebí je přijmout a akceptovat. Bylo by ovšem vhodné se občas nad věcmi pozastavit a přemýšlet nad tím, proti čemu a jak se lze bránit a není-li hloupé zanedbávat to či ono bezpečnostní pravidlo.

VYMEZENÍ PROBLÉMU A CÍLE PROBLÉMU

Cílem této práce je návrh zavedení managementu bezpečnosti ICT na střední škole. Tato práce si dále bere za cíl obeznámit o problematice bezpečnosti a zabezpečení z pohledu používaných bezpečnostních mechanismů, chování uživatelů a správců.

1 ANALÝZA SOUČASNÉHO STAVU

V rámci této práce bude provedena analýza, která je nezbytná pro vytvoření managementu bezpečnosti. Budou popsány pouze prvky, týkající se zavedení managementu bezpečnosti ICT na střední škole a to pouze u subjektů, které poskytly podklady k analýze. Mezi tyto prvky patří počítačová síť, software, hardware a dokumentace zabezpečení ICT. V této části bude také obsažena kapitola týkající se činnosti uživatelů sítě, zálohování, autentizace a organizační struktury

1.1 Obecná charakteristika organizace

Škola je příspěvková organice a jejím zřizovatelem je Moravskoslezský kraj. To znamená, že všechna zodpovědnost za chod školy padá na hlavu ředitele. Ve škole sídlí 4 subjekty. Dva subjekty jsou spojeny v jednu státní veřejnou střední školu (gymnázium a střední odborná škola), další subjekt je soukromá škola a poslední subjekt obstarává chod jídelny.

1.2 Organizační hierarchie

Na vrcholu organizační hierarchie stojí ředitel školy, který zodpovídá za její chod. Jako druhá v pořadí se zde řadí zástupkyně ředitele, poté vedoucí pracovníci, kterým se zodpovídají řadoví zaměstnanci. Dále jsou řadoví zaměstnanci a studenti.

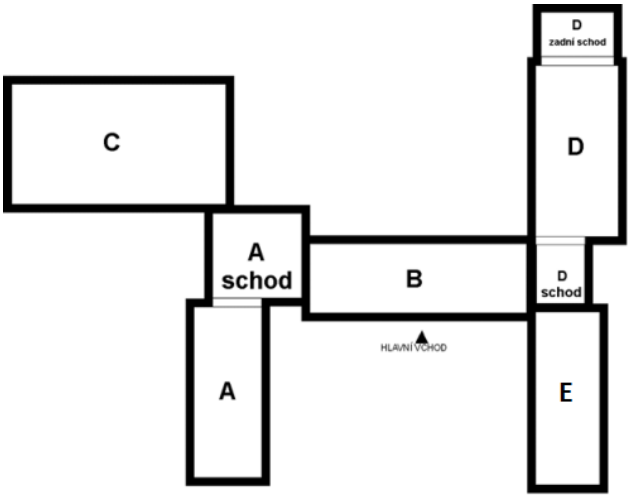
Obr. 1: Grafické zobrazení Hierarchie ve škole (Zdroj: Vlastní zpracování)

1.3 Obecná charakteristika analyzované oblasti a budovy

Analyzovaná škola, slouží pro středoškolskou výuku a je situována při okraji města. V této lokalitě, se nenachází jiné budovy s podobnou infrastrukturou. Škola je obklopena pouze panelovými domy, odkud do objektu zasahuje signál domácích Wi-Fi sítí, které se nachází na standardních kanálech 1 až 9 v pásmu 2,4 GHz.

Škola je rozdělena do pěti bloků, které jsou popsány písmeny A až E. Bloky A a D mají tři podlaží, bloky B, C a E mají dvě podlaží. Ve všech podlažích je síť

realizována pomocí síťové kabeláže. V některých také pomocí Wi-Fi přístupových bodů. Konkrétní plány místností, jejich rozměry a způsob využití jsou uvedeny v přílohách. Ve škole aktuálně pracuje 46 členů učitelského sboru, 13 technických a úklidových pracovníků a studuje zde 563 studentů.



Obr. 2: Schéma budovy (Zdroj: Vlastní zpracování)

1.4 Analýza počítačové sítě

V této kapitole bude popsán stav sítě, včetně stavu jednotlivých zařízení.

1.4.1 Pasivní síťové prvky

V této kapitole budou uvedeny prvky nezbytné k provozu školní sítě. Tyto prvky, se na komunikaci podílejí pouze pasivně (tj. nevyžadují stálý zdroj napájení).

1.4.1.1 Síťové uzly

Ve škole jsou strategicky rozmístěny 3 hlavní síťové uzly, ze kterých je rozvedena kabeláž. Jednotlivé uzly jsou popsány níže.

PRVNÍ SÍŤOVÝ UZEL tvoří RACK skříň, která je umístěna v prostoru volně přístupné chodby A 207 ve výšce zhruba 2 metry. Tato skříň je umístěna za sloupem. Skříň je uzamčená a klíče má pouze vyučující výpočetní techniky, který se stará o síťovou infrastrukturu školy. Skříň není nijak monitorována. Skříň obsahuje vlastní záložní zdroj napájení ve formě UPS SMART 650.

DRUHÝ SÍŤOVÝ UZEL je tvořen RACK skříní, která je umístěna v místnosti B 207. Tato místnost slouží jako učebna výpočetní techniky. Tato skříň je uzamčená a klíče má pouze vyučující výpočetní techniky, který se stará o síťovou infrastrukturu školy. Skříň není nijak monitorována. Skříň obsahuje vlastní záložní zdroj napájení ve formě UPS SMART 500.

TŘETÍ SÍŤOVÝ UZEL je místnost B 217. Tato místnost zde hraje klíčovou roli, je využívána jako serverovna. Místnost je obdélníkového tvaru a má rozlohu 9,7 m^2. Vstupuje se do ní přímo z chodby přes jediný přístupový bod a to dveře, uzamčené a opatřené bezpečnostní klikou. V této místnosti nejsou žádná okna. Je zde pouze malý otvor v pravém horním rohu místnosti, který je kryt plastovou mřížkou. Tato místnost je vybavena klimatizací. Klimatizace je umístěna na stěně naproti dveří. Jsou zde umístěny 2 obyčejné dřevěné stoly situované na levé straně místnosti a dvě police, které jsou na pravé straně. Na stolech jsou umístěny servery a v policích nepotřebný materiál.

V místnosti je pod klimatizací umístěna RACK skříň. Tato skříň obsahuje vlastní záložní zdroj napájení ve formě UPS SMART 500. Je opatřena zámkem, který však není využíván. Přístup do této místnosti je omezen a klíče má pouze údržbář, vyučující informatiky, uklízečka a jedny záložní klíče jsou umístěny v ředitelně. Místnost ani přístupy do ní nejsou nijak monitorovány. Není zde umístěno hasicí zařízení. Není zde umístěno ani čidlo, které by upozorňovalo požár či jiné nebezpečí.

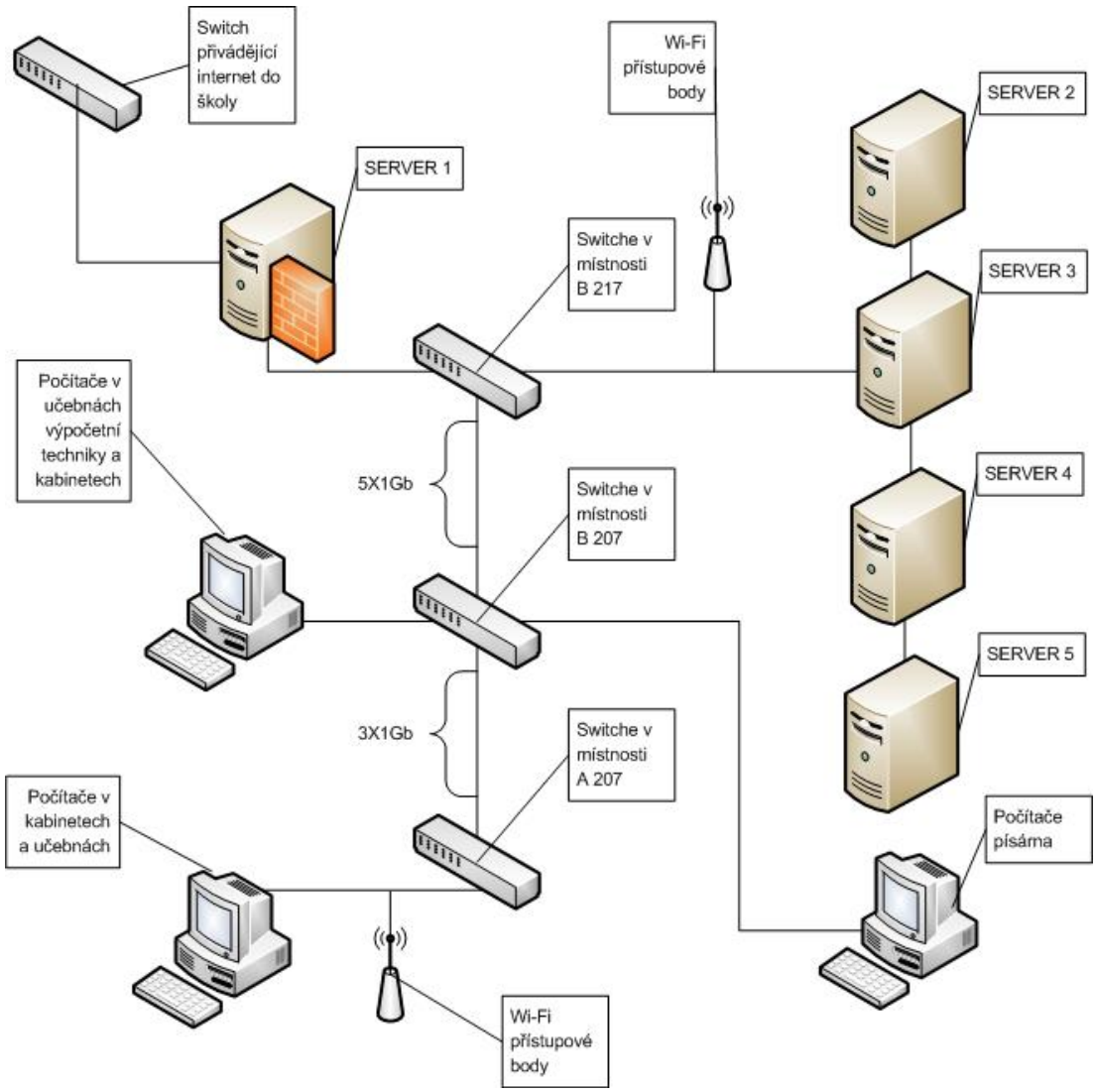
1.4.1.2 Kabeláž

Celá datová síť je řešena pomocí nestíněných UTP kabelů minimálně kategorie 5e. Podle předložené dokumentace se nejedná o certifikovaný kabelážní systém se systémovou zárukou výrobce.

Kabely jsou po trasách vedeny v chráničkách přímo ve zdi, nebo jsou umístěny v lištách sloužících k tomuto účelu. Pokud jsou kabely vedeny v lištách, jsou na většině míst dobře ukryty v podhledech, parapetech, nebo jsou umístěny u stropu, kde se bez žebříku nelze dostat. Najdeme zde však i místa, která jsou bez větších problémů přístupná uživatelskému zásahu. Jelikož lišty neobsahují žádné čidlo, které by upozorňovalo na narušení strukturované kabeláže, mohou tvořit jednu z možných hrozeb zabezpečení. Kabely jsou sváděny k datovým zásuvkám, kde je ve většině případů funkční pouze jeden port.

1.4.2 Aktivní síťové prvky

V budově se vyskytuje celá řada aktivních prvků. Z tohoto důvodu budu při popisu postupovat systematicky podle typu zařízení a jejich umístění v jednotlivých blocích a patrech budov.



Obr. 3: Logické schéma topologie prvků sítě (Zdroj: Vlastní zpracování)

1.4.2.1 Uzly rozvaděčů

Školní síťová infrastruktura má 3 hlavní uzly rozvaděčů, které jsou umístěny v hlavních síťových uzlech. O tyto aktivní prvky se stará převážně jediný člověk, který na této škole učí a který se také stará o ostatní informační technologie školy. Tyto uzly jsou schopny mezi sebou komunikovat rychlostí až 5 Gb/s. Všechny uzly rozvaděčů jsou zde připojeny ve VLAN1. Uzly rozvaděčů budou dále popsány podle umístění v hlavních síťových uzlech.

PRVNÍ UZEL ROZVADĚČŮ je tvořen prvním síťovým uzlem, ve kterém jsou umístěny následující switche:

- SMC Tiger switch 10/100 6724AL2
- Zyxel ES-2024
- SMC Network 8126PL2F

Výše popsané aktivní prvky mohou být spravovány pouze z jednoho PC, které je umístěno v místnosti B 204. PC je připojeno ve VLAN1 ve které má statickou IP, která zaručuje správu těchto prvků. Kontrolu IP a následné povolení správy obstarává SERVER 1. Výše zmíněné prvky mohou být spravovány pouze přes webové rozhraní. Ostatní možnosti správy jsou zakázány.

DRUHÝ UZEL ROZVADĚČŮ je tvořen druhým síťovým uzlem, ve kterém jsou umístěny následující switche:

- SMC Tiger switch 6724AL2 10/100
- SMC Tiger switch 6724AL2 10/100
- Cisco SG200-50 10/100/1000
- SMC Tiger switch 6724AL2 10/100

Výše popsané aktivní prvky mohou být spravovány pouze z jednoho PC, které je umístěno v místnosti B 204. PC je připojeno ve VLAN1 ve které má statickou IP, která zaručuje správu těchto prvků. Kontrolu IP a následné povolení správy obstarává SERVER 1. Výše zmíněné prvky mohou být spravovány pouze přes webové rozhraní. Ostatní možnosti správy jsou zakázány.

TŘETÍ UZEL ROZVADĚČŮ je tvořen třetím síťovým uzlem RACK skříní, ve kterém jsou umístěny následující switche:

- Edge-Core ES3528M
- SMC Network 8126PL2F 10/100/1000
- Cisko Small Bussines SG200-50 10/100/1000
- SMC Tiger Stark 8824M 10/100/1000

Tři z těchto switchů patří škole a jeden patří poskytovateli internetu. Switch patřící poskytovateli internetu je značky Edge-Core ES3528M. Tento switch je spravován samotným poskytovatelem internetu. Přivádí do školy internet po optickém kabelu a vyvádí jej jako kroucený dvoupár do SERVERU 1. Ze SERVERU 1 je dále veden

kroucený dvoupár do switchů a ostatních koncových zařízení, která jsou již spravována buďto správcem školní sítě nebo externí firmou.

Výše popsané aktivní prvky SMC a Cisco mohou být spravovány pouze z jednoho PC, který je umístěn v místnosti B 204. Je připojen ve VLAN1 a má statickou IP, která zaručuje správu těchto prvků. Kontrolu IP a následné povolení správy obstarává SERVER 1. Výše zmíněné prvky mohou být spravovány pouze přes prohlížeč. Ostatní možnosti správy jsou zakázány.

1.4.2.2 Wi-fi přístupové body

V budově je umístěno osm Wi-Fi přístupových bodů ve vlastnictví školy a dva které si zakoupili studenti. Všechny přístupové body jsou spravovány centrálně přes webové rozhraní, správu proto bez problémů zvládá jeden zaměstnanec. Všechna tato zařízení byla nakonfigurována velice podobně vyučujícím, který se stará nejen o Wi-Fi síť, ale o celou síťovou infrastrukturu školy. Nastavení Wi-Fi přístupových bodů není zdokumentováno a síťový provoz u těchto prvků není nijak kontrolován. Nyní budou popsány jednotlivé SSID, které školní zařízení vysílají. Následně budou popsány jednotlivé typy přístupových bodů.

- ***SSID PUBLIC***

SSID tohoto typu je ve škole používáno nejčastěji. K této síti se může připojit jakýkoliv student, nebo návštěva školy vlastnící zařízení s technologií Wi-Fi. Síť je zabezpečena šifrováním WPA2-PSK. Heslo je pro všechny uživatele jednotné a lze jej získat na školní nástěnce u učeben výpočetní techniky, které jsou volně přístupné. Uživatel připojený v této síti, nemůže vidět ostatní aktivní prvky školní infrastruktury z důvodu přístupu z VLAN2.

- ***SSID EMAN***

Tato síť slouží pouze pro připojení zařízení IPAD, které škola vlastní. Síť je zabezpečena šifrováním WPA2-PSK. Heslo znají pouze pověření zaměstnanci školy. Z této sítě se není možno připojit do LAN, odkud by bylo možné vidět všechny stolní počítače a servery připojené přímo ve školní síti. Důvodem je přístup z VLAN3.

- ***SSID SECURITY***

Tato síť je chráněna šifrovacím algoritmem WPA2-PSK, je však využívána minimálně. Důvodem je nedávné zavedení a připojení do VLAN1, ve které jsou

připojeny servery a ostatní stolní počítače školní infrastruktury. Heslo zná pouze správce sítě.

- ***Přístupový bod Zyxel NWA3166***

Ve škole se nachází celkem 6 kusů zařízení tohoto typu. Tyto přístupové body jsou strategicky rozmístěny ve škole v blocích budov A, B a C. První z Wi-Fi přístupových bodů lze najít ukrytý v podhledu chodby A 123. Druhý se nachází naproti vchodu do místnosti A 215, je připevněn přibližně 15 cm pod 3,3 m vysokým stropem. Třetí zařízení se nachází naproti vchodu do místnosti A 310 a je umístěno přibližně 15 cm pod stropem. Čtvrté zařízení je umístěno v místnosti A 312 ve vzdálenosti přibližně 20 cm od reproduktoru rozhlasu. Stejným způsobem je umístěno páté zařízení v místnosti C 209. Poslední zařízení je umístěno v místnosti B 212 asi 15 cm pod stropem nad dveřmi.

Přístupové body tohoto typu spadající do kategorie bussines. Jsou schopny pracovat jak v 2,4 GHz, tak v 5 GHz pásmu. Podporují standard 802.11 a/b/g/n. Splňují mnohé certifikace týkající se bezpečnosti. V tuto chvíli jsou tyto Wi-Fi přístupové body nastaveny tak, že signál nezasahuje do přilehlých obydlí. Tato zařízení vysílají SSID typu PUBLIC, EMAN a SECURITY.

- ***Přístupový bod TP-LINK TL-WR741ND***

Ve škole se nachází celkem 2 kusy tohoto zařízení. Tato zařízení mohou sloužit také jako router, ke kterému lze připojit další zařízení kabelem. Zařízení si pořídili sami žáci. Hesla pro přístup k administraci těchto zařízení byla nastavena správcem sítě, žáci tedy k administraci nemají přístup. Je zde však možnost restartu zařízení, protože obě dvě zařízení jsou umístěny v místnostech na parapetu poblíž síťové zásuvky. Tato zařízení jsou umístěny v místnostech A 313 a A 203. Zařízení vysílají pouze SSID typu PUBLIC

Tato zařízení splňují standard 802.11 a/b/g/n a umí pracovat 2,4 GHz pásmu. Navíc podporují funkci WPS, která je povolena. Signál z těchto zařízení sahá až do přilehlých obydlí, kde je možnost se na něj připojit.

- ***Přístupový bod Zyxel NBG5715***

Toto zařízení je ve škole jediné. Kombinuje vlastnosti přístupového bodu s multimediálním routerem. Je umístěno v místnosti C 149 na parapetu vedle počítače, je k němu tedy volný přístup. Zařízení vysílá pouze jeden SSID a tím je PUBLIC.

Tato zařízení splňují standard 802.11a/b/g/n a umí pracovat jak 2,4 GHz pásmu tak 5 GHz pásmu. Signál z tohoto zařízení zasahuje pouze do jednoho rodinného domu poblíž školy.

1.4.3 Servery

Všechny servery, které jsou ve škole k dispozici, jsou umístěny v třetím síťovém uzlu a jsou připojeny do VLAN1. U každého z nich je umístěn záložní zdroj napájení ve formě UPS. Dále budou popsány jednotlivé servery.

Server pro připojení na internet „SERVER 1“

Na tomto serveru je nainstalován operační systém Debian 7. Server slouží primárně jako router pro celou školu. Tento server je pod správou externího pracovníka, se kterým má škola řádně sepsanou smlouvu. Tento externí zaměstnanec nebyl nijak proškolen. Správce má možnost připojit se a pracovat vzdáleně. Přihlašuje se pomocí kryptografického klíče o velikosti 4096 b. Na tomto serveru je pouze jeden účet, který má práva root. Na tomto serveru má administrátor virtuální PC, které slouží k jeho vlastní potřebě a testování. Jsou zde nainstalovány různé aplikace, které plní tyto konkrétní specifické služby:

- DHCP – aplikace ISC's DHCP,
- DNS – aplikace Bind9,
- Firewall – definováno v systému a řízen pravidly, která přibližuje encyklopedie Common Vulnerabilities and Exposures neboli CVE,
- Proxy server,
- FTP server- WSDTPD,
- SSH,
- Webový server – Lighttpd.

Server pro správu vnitřní sítě „SERVER 2“

Na tomto serveru je nainstalován operační systém VMware, který pracuje na bázi operačního systému Linux RedHat. Je zde vytvořeno více uživatelských účtů s odlišnými právy. Pravidla pro hesla k těmto účtům nejsou nijak specifikována. Jsou tedy zadávána a užívána bez předem definovaných bezpečnostních požadavků. Na serveru je vytvořen jeden účet pro externího zaměstnance, který se stará o stránky školy. Tento zaměstnanec má se školou řádně uzavřenou smlouvu. Zaměstnanec nebyl nijak proškolen. Na serveru jsou nainstalovány tyto aplikace:

- Novel – aplikace sloužící jako uživatelská databáze k ověřování uživatelů v síti, úložiště dat a také tiskový server.
- Moodle – softwarový balík určený pro podporu prezenční i distanční výuky prostřednictvím online kurzů dostupných na internetových stránkách.
- Bakaláři – aplikace sloužící pro ukládání údajů o žácích, elektronické třídní knize, záznamů o suplování, hodnocení žáků a sdílení databází učitelů.
- Virtuální OS.

Server pro správu vnitřní sítě „SERVER 3“:

Na tomto serveru je nainstalován operační systém VMware, který pracuje na bázi operačního systému Linux RedHat. Na tomto serveru probíhá replikace databáze, která je tvořena Novelem na „SERVERU 2“. Je zde vytvořeno více uživatelských účtů s odlišnými právy. Pravidla pro hesla k těmto účtům nejsou nijak specifikována, hesla jsou zadávána a užívána bez předem definovaných bezpečnostních požadavků. Na serveru běží tyto aplikace:

- Novel,
- Virtuální OS,
- Zálohování.

Server pro správu vnitřní sítě „SERVER 4“:

Na tomto serveru je nainstalován operační systém Windows Server 2008 R2. Server je používán především pro virtualizaci operačního systému Windows 7, ke kterému žáci přistupují z učebny, kde tento operační systém není na PC nainstalován. Na tomto serveru je vytvořeno více uživatelských účtů s odlišnými uživatelskými právy. Je zde vytvořen také učet pro externího pracovníka, který se stará o VMware

spravující virtuální počítač s Windows 7, na který se připojují uživatelé z prostoru písárny, kde tento systém není nainstalován. Tento zaměstnanec má se školou řádně uzavřenou smlouvu. Zaměstnanec není nijak proškolován. Systémové účty mají obyčejná hesla, která se řídí podle pravidel systému. Nejsou zde tedy téměř žádné požadavky na sílu hesla. Dále se na serveru nacházejí tyto aplikace:

- Terminálový Win server,
- Virtualizované Windows 7 a jiné operační systému určené pro testování.

Server „STREAM“

Na tomto serveru je nainstalován operační systém VMware, který pracuje na bázi operačního systému Linux RedHat. Je zde vytvořeno více uživatelských účtů s odlišnými právy. Probíhají zde ještě tyto činnosti:

- Streamování a práce s videem.
- Virtualizace operačních systémů.
- Testování.
- Zálohování.

Server Regulace „SERVER 5“

Na tomto serveru je nainstalován operační systém Windows 7 Professional. Server má jediný účel a tím je regulace topení pro celou budovu. Škola není vlastníkem tohoto serveru. Má jej pouze umístěn v serverovně a připojen do sítě. Tento server nelze vzdáleně spravovat.

1.4.4 Pracovní stanice

Pracovní stanice jsou rozmístěny v celé škole. V kabinetech se nachází vždy jeden stolní počítač a v některých případech také notebook, využívají je členové učitelského sboru. V učebnách a třídách se obvykle nachází jeden stolní počítač, který využívají převážně žáci. Výjimkou jsou 2 učebny výpočetní techniky a učebna B 215 sloužící k výuce „psaní všemi deseti“. V učebnách výpočetní techniky je umístěno 18 a 16 počítačů pro žáky a jeden pro učitele. V učebně B 215 je 20 počítačů pro žáky a jeden pro učitele. Pravidla týkající se používání pracovních stanic, jsou sepsána pouze pro učebny výpočetní techniky a učebnu B 215. Dokumenty s pravidly lze nalézt v přílohách. Chybí zde dokumentace pro užívání

PC, které jsou v učebnách a třídách, a které má k dispozici učitelský sbor. Pracovní stanice jsou aktualizovány manuálně přes server vždy, když jsou vydány kritické aktualizace. Jediná automatická aktualizace je pro program AVG. Firewall zabudovaný ve Windows je vypnut z důvodu nekompatibility s AVG.

Pracovní stanice, které jsou ve školním prostředí používány, nejsou postaveny na jednotné platformě a mají také různý výkon. Používají se zde dva druhy systémů.

WINDOWS XP – v tomto okamžiku již značně zastaralý operační systém, kterému v příštím roce oficiálně končí podpora a pro který budou zastaveny aktualizace. Ve škole je používán většinou kvůli nedostatečnému výkonu staršího hardwaru, na kterém by novější systém měl problém s rychlostí.

WINDOWS 7 – v tuto chvíli je nástupce Windows XP. Tento systém zaručuje dlouhou podporu ze strany Microsoftu, avšak škola již nyní přemýšlí o zakoupení licencí pro Windows 8, nejnovějšího produktu od firmy Microsoft.

Aplikační software

Počítače jsou při předání do užívání vybaveny běžným softwarem, který je licenčně v pořádku. Licence jsou kontrolovány jednou ročně pověřeným pracovníkem, který zodpovídá za jejich správu. Licence pro systémy a kancelářské balíky jsou kupovány jako multilicence. Počítače obsahují následující software.

- Novel klient – aplikace sloužící jako uživatelská databáze k ověřování uživatelů v síti, úložiště dat a také tiskový server GIMP.
- Bakaláři – aplikace sloužící pro ukládání údajů o žácích, elektronické třídní knize, záznamů o suplování, hodnocení žáků a sdílení databází učitelů.
- Winrar 4.11 – aplikace sloužící pro kompresi a dekompresi dat.
- MS Office 2010 – kancelářský balík.
- Poštovní klient Microsoft Outlook 2010.
- Antivirová ochrana AVG.
- Internet Explorer 9 – webový prohlížeč.
- Firefox – webový prohlížeč.
- Windows Mediaplayer – přehrávač médií.

Dodatečné softwarové vybavení počítače mzdové účetní:

- MZDY 2000 UNICOS,
- Acronics True Image 10.0 (zálohování).

Dodatečné softwarové vybavení ekonomické účetní:

- Fenix,
- Acronics True Image 10.0 (zálohování).

1.5 Analýza uživatelů

Uživatelem je člověk vedený jako student nebo zaměstnanec školy. Uživatel má přístup do školní sítě, ke školním aplikacím a především k počítačům. Můžeme zde rozlišit 5 druhů přístupů podle pravomocí a postavení ve školní infrastruktuře.

Student

Tento typ uživatelů a přístupu je nejběžnější. Tento přístup zahrnuje možnost přihlášení uživatele na školním PC pomocí aplikace Novel. Dále se může uživatel přihlásit do aplikace Moodle a do školní pošty. Tyto aplikace jsou však umístěny volně na webu, tudíž uživatel k jejich použití nepotřebuje být připojen v intranetu. Uživatelé nemají přístup k žádnému ze síťových uzlů.

Učitelský sbor

Běžný zaměstnanec učitelského sboru disponuje podobnými přístupy, kterými disponuje uživatel typu student. Má přístup na školní počítače, do aplikací Novel, školního e-mailu a aplikace Moodle. Navíc však má přístup do aplikace Bakaláři a někdy také do administrace modulu Moodle. Zaměstnanci nemají přístup k žádnému ze síťových uzlů.

Technický pracovník

Mají stejné možnosti přístupů jako studenti s tím rozdílem že mají možnost dostat se k jednomu ze síťových uzlů a to do místnosti B 217.

Správce

Správci mají mít stejné možnosti přístupů do systémů jako učitelský sbor. Především však mají přístup k některému ze síťových prvků školy ať je jím server, switch, nebo

jiný prvek sítě. Většinou využívají přístup pomocí remote desktop. Mají však možnost dostat se k hardwaru i fyzicky.

Ředitel

Ředitel má přístupy jako běžný člen učitelského sboru. Má však také přístup do serverovny, a to v případě, že použije náhradní klíče umístěné v kanceláři u ředitelny.

1.6 Autentizace

Ve školním prostředí probíhá autentizace pouze za pomoci uživatelských přihlašovacích údajů. Autentizace je zde zajišťována pomocí eDirectory, kterou zprostředkovává aplikace Novel. O eDirectory se stará vyučující výpočetní techniky, který na začátku každého školního roku databázi eDirectory updatuje. Uživatelé, kteří na tuto školu nepatří, jsou smazáni a naopak noví jsou přidáni.

1.6.1 Přihlášení na pracovní stanice

Uživatelé se do systému přihlašují pomocí aplikace Novel klient, která se po zapnutí počítače objeví místo typické Windows přihlašovací obrazovky. Po přihlášení nejsou přihlášeni jako Administrátoři, ale jako obyčejní uživatelé, což znamená, že mají právo instalovat některé aplikace, ale nemají možnost upravovat jakoukoliv systémovou strukturu nebo nahlížet do profilových složek. Přihlášení do tohoto systému zaručuje uživateli připojení do školní sítě, zpřístupní se mu jeho síťový disk a některá rozšiřující nastavení, která plynou z použití eDirectory. Po přihlášení mají uživatelé možnost využít 100 MB volného místa na svém síťovém disku. Software je aktualizován nepravidelně přes server.

Přístupové údaje pro přihlášení na pracovní stanici jsou nastavovány zaměstnancem školy, který vyučuje informační technologie. Heslo vytváří přímo uživatel, nebo jej pracovník náhodně vytvoří a poté jej s konkrétním uživatelem změní. Hesla nejsou nastavována podle pravidel, což znamená, že zde lze použít libovolné heslo. Důvodem je chybějící dokumentace.

1.6.2 Přihlášení do aplikací

Jelikož uživatel byl již jednou vytvořen u aplikace Novel, vznikla databáze, podle které se uživatelé ověřují i v aplikacích Moodle a ve školním e-mailu. Je-li zapotřebí vytvořit uživatelský účet do aplikace Bakaláři, je potřeba kontaktovat zaměstnance školy, který vytvářel uživatelská jména a hesla do databáze Novelu. Tento zaměstnanec umožní zadání uživatelského jména a hesla do databáze aplikace Bakaláři. Jiné systémy, ve kterých by se uživatelé museli autorizovat, se na škole nevyskytují.

1.7 Monitoring

V tuto chvíli síť není nijak monitorována. Správce sítě a routeru uvádí jako důvod, preferování rychlosti před kontrolou síťového provozu. Síťový model je v tuto chvíli schopen zajistit rychlost přenosu dat až 5 Gb, ovšem podle slov správce by se mohla rychlost monitoringem razantně snížit.

1.8 Zálohování

Jediné co se zde zálohuje v pravidelném intervalu, je databáze programu Bakaláři, ve které jsou uloženy informace nezbytné pro běh školy. Zálohování probíhá pomocí programu Robocopy, který každý večer v pracovním týdnu vytvoří zálohu databáze do PC vyučujícího informatiky. Ostatní data jsou zálohována v nepravidelném intervalu, přibližně jednou za rok. Zálohy jsou uchovávány na DVD. Neexistují zde žádné dokumenty, které dokládají jak, kdy a co zálohovat, popřípadě jak by to mělo být obnoveno.

1.9 Management bezpečnosti ICT

Ze získaných poznatků vyplývá, že zde není možnost zastoupení členů starajících se o školní infrastrukturu ICT. Jediný člen, který má zástupce schopného teoreticky i prakticky okamžitě nastoupit, je ředitel. Jeho zástupkyně je s ním denně v kontaktu, konzultují spolu většinu rozhodnutí a sdílí mnohé informace.

Neexistují však žádní zástupci externích pracovníků. A především neexistuje zástupce pracovníka, který zde vyučuje výpočetní techniku a stará se o celou IT strukturu školy.

1.9.1 Principy bezpečnosti

Principy bezpečnosti ICT zde nejsou jasně a striktně definovány. I přesto je zde však možné nalézt správné návyky, mezi které bezesporu patří:

- Zamykání kabinetů v době nepřítomnosti vyučujícího,
- Zamykání tříd po ukončení vyučování,
- Uzamykání hlavního vchodu,
- Evidence příchozích a odchozích studentů mimo oficiální časy příchodu.

1.9.2 Dokumentace managementu ICT

Jediný dokument, který mi byl předložen, je provozní řád učeben výpočetní techniky, dokládající delegování povinností na konkrétního pracovníka. Tento dokument lze najít v příloze této práce.

1.9.3 Politika vzdělávání uživatelů

Vzdělávání žáků

Ohledně informačních technologií jsou žáci každoročně proškolováni v první hodině, která probíhá v počítačových učebnách. Dostávají zde poučení o chování v učebnách informatiky. Poučení v písemné podobě je vyvěšeno v učebnách a je kdykoliv k nahlédnutí. Proškolení je stvrzeno podpisem žáka do třídní knihy. Aktuální řád učeben informatiky lze najít v příloze této práce. Žáci jsou na začátku každého školního roku proškoleni také svým třídním učitelem, který jim předčítá školní řád. Žáci opět stvrzují podpisem, že řádu rozumí a budou jej dodržovat.

Vzdělávání zaměstnanců

Zaměstnanci žádné specializované školení pravidelně nepodstupují. Podle získaných informací, byli pracovníci učitelského sboru individuálně proškoleni v průběhu předešlých 10 let. Bohužel nejsou o tomto vedeny žádné veřejné záznamy, nelze tedy doložit míru ani kvalitu jejich znalostí.

1.10 Shrnutí analýzy

Poznatky získané z analýzy aktiv školy ukazují, že na této škole je problémem především vedení dokumentace týkající se managementu bezpečnosti ICT. Je zde problém také s nastavením politiky hesel, jejím dodržováním. Dále s dokumentací fyzické politiky a bezpečnosti ve vztahu k ICT. Chybí zde i pravidelné proškolování uživatelů, kategorizace dat podle důležitosti a s ním spjatá pravidla zálohování a obnovy.

V tuto chvíli zde nejsou nijak písemně podloženy směrnice, dokládající vedení managementu bezpečnosti. Za vše je zde zodpovědný ředitel školy a zastupitelnost pracovníků zabezpečujících management ICT je na velice nízké, prakticky nulové úrovni.

2 TEORETICKÁ VYCHODISKA ŘEŠENÍ

2.1 Management bezpečnosti ICT

Management - vycházející z anglického slova „to manage“ což znamená řídit, je často popisován jako proces tvorby a udržování prostředí, ve kterém jednotlivci pracují společně ve skupinách a účinně dosahují vybraných cílů (1, str. 7).

Zabezpečení, neboli bezpečnost je aktuální stav zajištění stability, funkčnosti a existence bezpečnostních aktiv v podmínkách potenciálního či reálného narušení bezpečnostními hrozbami (2, str. 32).

ICT je zkratka pocházející z anglického „Information and Communication Technologies“. Označuje pojem informační a komunikační technologie (3).

Management bezpečnosti ICT tedy můžeme přeložit jako řízení rizik, nebo řízení hrozeb v informačních technologiích.

2.1.1 Úskalí zavádění managementu bezpečnosti

Při testování bezpečnosti je zapotřebí mít na zřeteli šest hlavních oblastí. V prvé řadě je to **utajení.** Jde o soubor bezpečnostních opatření, chránících před vyzrazením informací neoprávněným subjektům. Jedná se jak o cílené vyzrazení, tak o vyzrazení nedopatřením. Jde tedy nejen o technické, ale také (často především) organizační prvky. Drtivá většina kompromitací z pohledu utajení je totiž způsobena selháním lidského faktoru, nejasnými pravomocemi a špatnou konfigurací zařízení – nikoliv tedy vnějšími útočníky (4).

Dále řešíme **integritu,** tedy vlastnost zaručující, že informace je přesná. Tedy úplnost a neporušenost dat, a tím pádem jistotu, že nepracujeme s daty poškozenými nebo podvrženými. Integritu je zapotřebí řešit a zajistit nejen během přenosu či zpracovávání dat, ale také v průběhu ukládání dat. Jen tak je možnost zajistit, že data nebudou poškozena nebo že je někdo nemodifikuje (4).

Další oblast je **autentizace.** Jde o potvrzení identity osoby nebo jiné entity, sledování původu artefaktu, důvěryhodnost aplikace apod. Naproti tomu **autorizace** řeší otázku, zdali je žadatel oprávněný získat přístup nebo poskytnutí služby (4).

Dostupnost se na informační bezpečnost dívá z pohledu dostupnosti informací nebo služeb tehdy, jsou-li potřeba. Dostupnost je přitom mnohem širší pojem, než si mnohdy uvědomujeme. Netýká se totiž jen vlastních dat, ale třeba také komunikačních kanálů nebo odpovídajícího hardware. K čemu jsou dostupná data uložená např. na paměťové kartě, nebo magnetickém pásku, když po ruce není zařízení, které by je mohlo přečíst? Nebo když nemůžeme využít službu pro nedostatečné pásmo připojení či jeho kolísavou kvalitu (4).

Poslední oblastí je **nepopiratelnost.** Tedy skutečnost, že nelze popřít provedení nějakého úkonu (odeslání zprávy, provedení změn, smazání dat…). Bez zajištění nepopiratelnosti nelze provádět většinu úkonů v kybernetickém prostoru, ovšem stejně tak nelze provádět monitorování a dohled (4).

2.1.2 Zavádění managementu bezpečnosti

Management bezpečnosti by měl být zaveden z důvodu předcházení bezpečnostním hrozbám. Bezpečnostní hrozby jsou konkrétní jevy či procesy, které negativním způsobem narušují či dokonce ohrožují stabilitu, funkčnost, dokonce i existenci daného prostředí, jeho prvků či vztahů mezi těmito prvky. Působením bezpečnostní hrozby vždy dojde k narušení prostředí a ke způsobení nějaké škody rámci prostředí (2, str. 19).

Pro realizaci bezpečnostní politiky se vytváří bezpečnostní systém organizace. Bezpečnosti systém organizace v sobě zahrnuje:

- Konkrétní činnosti realizované pro zajištění bezpečnosti organizace.
- Materiální infrastrukturu nezbytnou pro zajištění bezpečnosti organizace.
- Osoby vykonávající potřebné role (a nesoucí tudíž odpovědnost) při realizaci zajišťování bezpečnosti organizace (2, str 130).

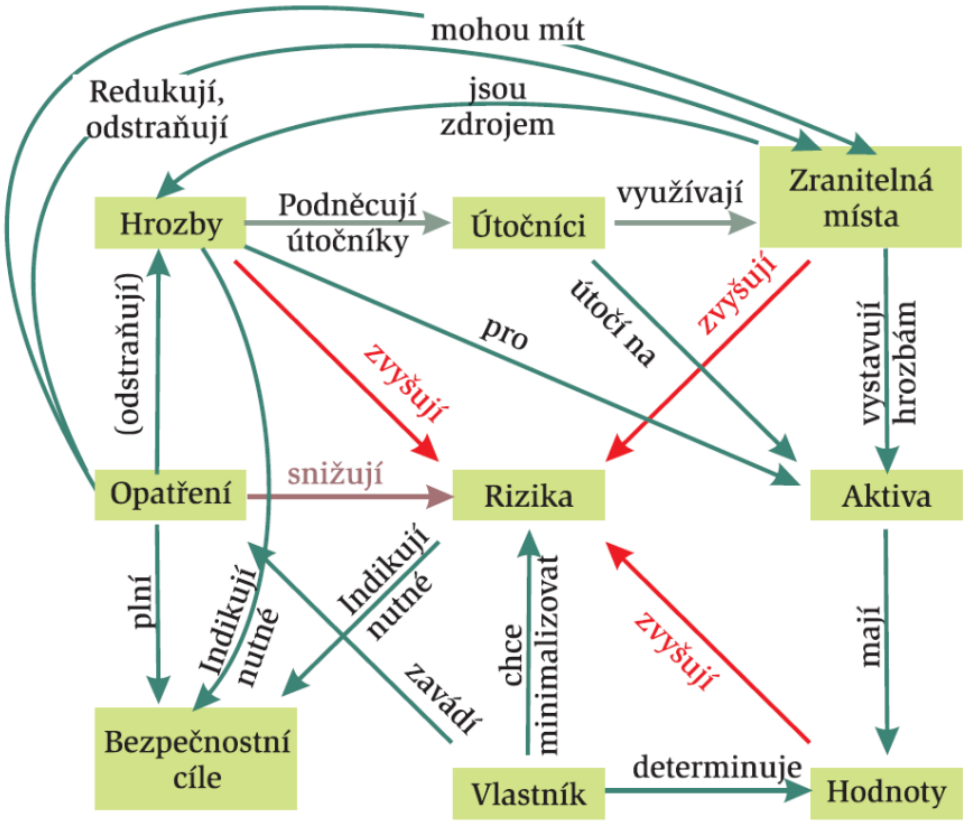
Díky realizace této politiky, by měli být na funkce, které jsou v dokumentech popsány delegováni lidé, kteří dané problematice alespoň částečně rozumí, či mají předpoklady rychle se v ní vzdělat. Zavedením bezpečnostní politiky se můžeme, vyhnou problémům, jako jsou:

- Nevědomost uživatelů o chodu systému.
- Nevědomost uživatelů systému v případě krizové situace.
- Nesprávné, nebo neoprávněné používání daných aktiv uživatelem.

- Vynesení citlivých dat.

2.1.3 Obecný model bezpečnosti

Řešení managementu bezpečnosti ICT je dlouhodobý proces, jehož cílem je neustále se zlepšovat a pružně reagovat na nově vznikající rizika. Následující obrázek zachycuje obecný model bezpečnosti. V tomto modelu jsou zachyceny hlavní požadavky na řešení bezpečnosti, přičemž jsou zde zachyceny vazby mezi komponentami bezpečnosti IS (5).

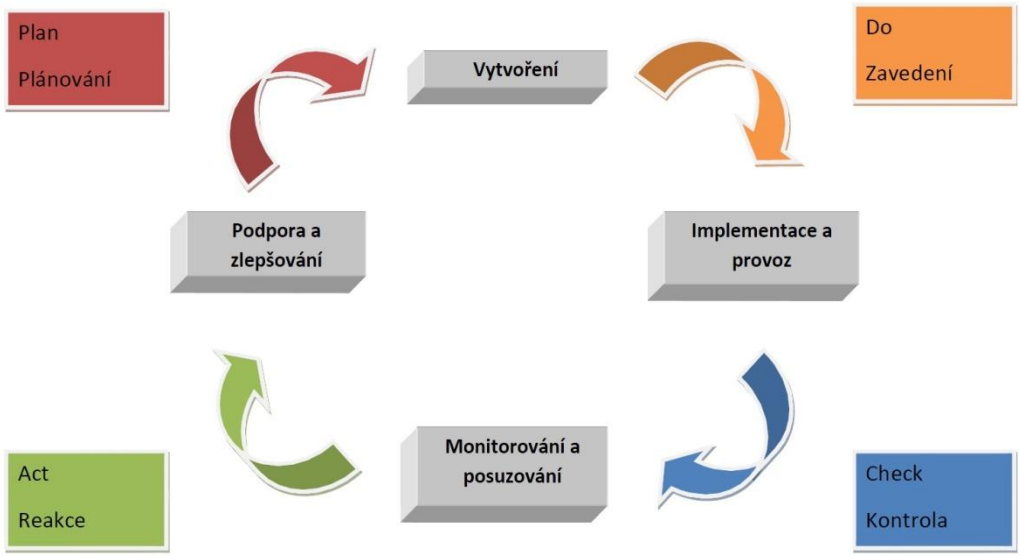


Obr. 4: Obecný model bezpečnosti informačních technologií (5, str. 16)

2.1.4 Demingův cyklus

V realizační části zavádění managementu ICT je často používaná metoda Demingova cyklu. Jedná se o jednoduchou metodu zlepšování. Používá se zde také zkratka PDCA. Písmeno P zde znamená – fázi plánování, D – fázi realizace, C – fázi přezkoumávání, A – fázi reakce na dané změny. Tuto frázi lze přeložit, jako *plánuj-*

udělej-zkontroluj-uskutečni. Obrázek níže znázorňuje grafickou podobu tohoto cyklu (6, str. 8).



Obr. 5: Demingův cyklus (Zdroj: Vlastní zpracování podle (7, str. 6))

2.1.5 Hodnocení bezpečnostní povědomosti v organizacích

V různých organizacích je obvykle velmi různé bezpečnostní povědomí. V zásadě se můžeme setkat se třemi úrovněmi.

Vysoká úroveň je obvykle reprezentována velmi dobrou informovaností pracovníků organizací o základních aspektech bezpečnosti informačního systému. Bývají to organizace typu nadnárodních společností, bankovních a finančních institucí a speciálních státních úřadů, jako je například Ministerstvo obrany, Ministerstvo vnitra, Národní bezpečnostní úřad apod. (8, str. 78).

Střední úroveň je reprezentována převážně privátním sektorem firem. V nich jsou znalosti některých pracovníků o bezpečnosti informačních technologií velmi dobré, znalosti jiných jsou naopak menší a někteří z nich nejsou tímto problémem poznamenáni vůbec (8, str. 78).

Nejnižší úroveň představují malé a střední firmy a některé organizace centrální a regionální státní a veřejné správy. Celkové bezpečnostní povědomí u většiny pracovníků je nízké (8, str. 78).

2.2 Zákony v legislativě ČR

Zákon č. 101/2000 Sb. o ochraně osobních údajů. *„Tento zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby a řeší problematiku zpracování osobních údajů.“* (9)

Zákon č. 227/2000 Sb. o elektronickém podpisu. *„Tento zákon upravuje používání elektronického podpisu, poskytování souvisejících služeb, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.“* (10)

Zákon č. 480/2004 Sb. o některých službách informační společnosti. *„Tento zákon zdůrazňuje povinnost členských států EU zajistit důvěrný charakter sdělení přenášených pomocí veřejné komunikační sítě a veřejně dostupných elektronických služeb.“* (11)

Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností *„Tento zákon vymezuje skutečnosti, které je nutno v zájmu České republiky utajovat způsob jejich ochrany, působnost a pravomoc orgánů státu při výkonu státní správy v oblasti ochrany utajovaných skutečností, povinnosti orgánů státu, práva a povinnosti fyzických a právnických osob a odpovědnost za porušení povinností stanovených tímto zákonem a upravuje postavení Národního bezpečnostního úřadu.“* (12)

2.3 Norma

Norma neboli také standard je požadavek na chování nebo vlastnosti věci, člověka, situace apod., který buď předepisuje a vyžaduje, nebo popisuje, co je normální (přijatelné nebo obvyklé). Normy jsou psané i nepsané a liší se různou mírou závaznosti a různým rozsahem platnosti (13, str. 9).

Registrací norem se zabývají různé organizace. Mezi nejvýznamnější mezinárodní organizace, které se zabývají standardizační činnosti, ale také standardizací bezpečnosti IT, patří:

- International Organization for Standardization (ISO),
- International Electrotechnical Comission (IEC),
- International Telecommunications Union (ITU) (14).

2.3.1 Normy zabývající se ICT

Účelem norem zabývající se managementem a správou ICT, je poskytnout uživateli podrobnou metodiku zabezpečení, správy a užívání informačních a komunikačních technologií. Pracovníci zodpovědní za informační bezpečnost a zejména za bezpečnost sítě by v normách tohoto typu měli nalézt všechny důležité podklady pro tvorbu specifických předpisů a pravidel.

Primárně je nutné zabývat se řadou norem ISO/IEC 27000, která se postupně vyvíjí a přebírá náležitosti norem, jako jsou ISO/IEC 18028, ISO/IEC 17799. Předpokládá se, že normy, z kterých řada norem ISO/IEC 27000 vychází, časem zaniknou.

2.3.2 Řada norem ISO/IEC 27000

Tato norma nám poskytuje metodiku popisující zavedení bezpečnostních opatření s možností výběru dle činností a rizik organizace. Zahrnuje plánování, provoz, monitorování, udržování a zlepšování ISMS. Vybraná opatření jsou přiměřená požadavkům konkrétního subjektu a poskytují odpovídající jistotu. Opatření jsou vždy zaváděna podle priorit a ekonomických zdůvodnění. Tato norma také může sloužit k posouzení zainteresovanými stranami, například při certifikaci. Mohou ji používat všechny typy organizací (15).

2.3.3 Výhody certifikace ISO/IEC 27000

Certifikát, který daná organizace obdrží, pokud splní daná kritéria, jí umožňuje prokázat ochranu dat (osobních a utajovaných) a tím dodržet zákon o ochraně osobních údajů. Dále firma prokazuje, že má nastavena opatření proti ztrátě, záměně, zneužití, poškození informací a dalším rizikům. Tato norma funguje na principu hodnocení rizik se snahou o minimalizaci rizik z pohledu bezpečnosti informací.

2.3.4 Nástroje k zavedení norem

Pro zavedení norem je potřeba mít zdokumentovány konkrétní procesy, směrnice a mít zavedený systém interní dokumentace bezpečnostní politiky.

Zavedením libovolné bezpečnostní politiky však není garantována absolutní bezpečnost provozovaného informačního systému. Přestože součástí zajištění bezpečnosti je implementace různých bezpečnostních funkcí a protiopatření, zůstávají v informačním systému zranitelná místa a ta představují rizika (16).

2.4 Směrnice, Procesy

Sestavení vnitropodnikových směrnic přináší poměrně rozsáhlou a časově náročnou práci. Ideální je, pokud při tvorbě směrnic spolupracuje konkrétní člověk s dalšími osobami, například auditorem, daňovým poradcem, ekonomem, majitelem či jednatelem firmy. Dále jsou uvedeny údaje, které by směrnice, popřípadě proces měly obsahovat.

Základní údaje, které by měly být obsahem hlavičky:

1. **Název a sídlo** subjektu.
2. **Název písemnosti** a její jednoznačné číselné označení.
3. **Název vlastní směrnice.** Jde o identifikaci a rozlišení vlastního obsahu. Nedoporučuje se používat krkolomné názvy, jednoduchost naopak usnadňuje orientaci v dokumentech.
4. **Schválení.** Na každé vydané vnitropodnikové směrnici musí být uveden podpis osoby schvalující danou směrnici. Touto osobou bývá zpravidla jednatel, generální ředitel, vedoucí, hlavní účetní atd., tedy osoba s přidělenou pravomocí přikázat a rozhodnout o dané problematice (17).

Další informace, které se doporučuje v záhlaví jednotlivých předpisů uvádět:

1. **Revize**. Každá směrnice během času zastará a je třeba ji aktualizovat či zcela přepracovat. Je dobré uvádět, o kolikáté novelizované vydání se jedná. Bylo by nepraktické a hlavně nepřehledné vydávat každou novelu pod zcela novým číslem.
2. **Účinnost.** Účinnost je velice důležitý údaj, podle kterého se řídí většina kontrolorů, ať už jde o finanční úřad, či auditora. Účetní jednotka musí dohlídnout, aby změny vyvolané novelami zákonů byly v souladu s účinností vnitropodnikových směrnic.
3. **Rozdělovník**. Rozdělovník informuje o tom, kdo danou směrnici obdrží, kolik exemplářů se vydává. Ve větších společnostech jsou tyto rozdělovníky pevně stanoveny.
4. **Vydal.** Jde o označení osoby, na kterou se ostatní zaměstnanci budou obracet v případě nejasností. Uvedený pracovník by měl mít na starosti tuto normu po celou dobu její platnosti Také by měl sledovat legislativní i vnitropodnikové změny a iniciovat aktualizace a revize. Ve velkých organizacích je rovněž

vhodné připojit i údaje o osobě, která danou směrnici kontrolovala a případně o útvaru, který ji vydal.

5. **Přílohy**. Jestliže je nutné ke směrnici přiložit určitý dokument, který se jí týká, musí tak být učiněno jasně a srozumitelně. Tak, aby byl každý pracovník, který s ní bude pracovat, ihned schopen určit o jakou přílohu se jedná, jaký je její název a kolik má stran (17).

2.5 Důležité momenty analýzy bezpečnostní politiky

Revizí a analýzou firemních bezpečnostních politik lze identifikovat konkrétní zranitelná místa, která se nachází u analyzovaného subjektu. Všeobecně jsou definovány do čtyř sektorů.

- Fyzická bezpečnost organizace.
- Personální bezpečnost organizace.
- Informační bezpečnost organizace.
- Provozní bezpečnost organizace (2, str. 129).

Mezi konkrétní body, kterým by se měla věnovat pozornost, patří například:

- Politika hesel – zaměření na požadovanou délku, frekvenci obměny, požadovanou strukturu.
- Odstraňování účtů bývalých zaměstnanců a jiných osob, kteří měli do sítě přiřazen účet, a již jej není zapotřebí.
- Doménovou politiku – v případě existence domény umožňuje vzdálenou skupinovou aplikaci a správu bezpečnostních nastavení klientských zařízení a uživatelských účtů ve firemní síti.
- Interní směrnice týkající se například instalace aplikací třetích stran. Toto opatření by mělo být zabezpečeno omezením instalovat aplikace na koncové stanice uživatelů bez povolení administrátora (18, str. 113-114).

2.5.1 Fyzická bezpečnost

Při zajišťování fyzické bezpečnosti organizace je hlavním cílem zabránit, nebo účinně bránit neoprávněnému vniknutí do objektů, poškození, zničení nebo neoprávněné manipulaci s majetkem (aktivy) dané organizace. Fyzická bezpečnost musí odpovídat výsledkům analýzy možných fyzických útoků na majetek a jiná

aktiva organizace. Fyzická bezpečnost se realizuje především formou kontroly konkrétního prostoru organizace (2, str. 130).

2.5.2 Personální bezpečnost

Při zajišťování personální bezpečnosti organizace je hlavním cílem eliminovat, nebo omezit rizika generovaná negativním působením lidského faktoru v rámci činnosti organizace. Tj. vznikem hrozeb podvodu, krádeže, sabotáže, neúmyslné či úmyslné chyby, nebo neodborného užití či manipulace s negativními dopady důsledky na aktiva organizace, jejichž nositelem je buď přímo zaměstnanec organizace, nebo osoba působící v rámci organizace na základě jiného než pracovněprávního vztahu. Personální bezpečnost je realizována především formou výběrového a kontrolovaného přístupu osob k různým aktivům organizace (2, str. 131).

2.5.3 Provozní bezpečnost

Při zajišťování provozní bezpečnosti organizace je hlavním cílem eliminovat nebo omezit rizika generovaná negativním působením přírodních či technických faktorů na jednotlivé zejména provozní činnosti či aktiva organizace. Provozní bezpečnost se realizuje především uplatněním různých opatření z oblasti protipožární ochrany, bezpečnosti a ochrany zdraví při práci, ochrany životního prostředí atd. (2, str. 132).

2.5.4 Bezpečnost informací

Při zajišťování informační bezpečnosti organizace je hlavním cílem eliminovat, nebo omezit rizika generovaná negativním působením lidského či jiného (např. technického) faktoru v rámci činnosti organizace využívající pro svou činnost informační a telekomunikační systémy. Dále zajistit, aby nedošlo k narušení důvěrnosti, dostupnosti a integrity informací, dat a nedošlo k přerušení hlavních procesů činnosti organizace v důsledku omezení funkčnosti či existence jí využívaných informačních a telekomunikačních systémů. Bezpečnost informací se realizuje především formou sběrového a kontrolovaného přístupu k informační a komunikační infrastruktuře organizace (2, str. 132).

2.5.4.1 Autentizace

Je důležitým pojmem v oblasti managementu bezpečnosti. Znamená ověření identity subjektu (osoby, systému) s požadovanou zárukou. Tedy ověření, zda je daný subjekt ten, za který se vydává. Autentizace může být jednosměrná, obousměrná, nebo průběžná. Autentizace může probíhat na základě:

- Toho **co subjekt má** (například identifikační karta, identifikační dokument, platební karta, klíč).
- Toho **co subjekt zná** (například PIN, heslo, přístupová fráze).
- Toho **čím subjekt je** (například různé biometrické údaje, jako otisk prstu) (13, str. 83).

2.5.4.2 Síla hesla a tvorba hesla

Tvorba kvalitního hesla je všeobecně velmi podceňována. A to i přesto, že jde o velice účinnou obranu. Při správném nastavení hesla, zařízení a aplikace by nemělo být metodou hrubé síly v reálném čase prolomeno. (18, str. 202).

Obecně není přesně vymezeno, kdy se již jedná o heslo silné a kdy ne. Obvykle si instituce volí pravidla pro tvorbu hesel interně. Většina zdrojů se však shoduje, že relativně bezpečné heslo pro běžné použití (e-mail, doménové heslo…) by mělo mít následující vlastnosti (18, str. 200).

- Nemělo by obsahovat jméno, příjmení, login či název firmy.
- Nemělo by být slovníkovým výrazem.
- Mělo by obsahovat minimálně 8 znaků (ideální počet je okolo 14 znaků).
- Mělo by obsahovat znaky ze všech 4 skupin (velké písmeno, malé písmeno, číslici, ostatní speciální znaky).
- Nemělo by obsahovat stejné znaky ze stejné skupiny (dvakrát použito „a“).
- Ideální doba pro použití hesla je 1 měsíc, poté je vhodné jej změnit.
- Jedno heslo by se nemělo používat pro více systémů (18, str. 200).

Existuje mnoho dalších parametrů, které by hesla měla splňovat. Zde jsou uvedeny ty nejdůležitější.

2.6 Dopady narušení bezpečnosti

Narušení bezpečnosti je pro daný subjekt vždy velice nemilá a mnohdy katastrofická situace. Dochází tak totiž nejen ke ztrátě důležitých dat, ale často i ke ztrátě dobré reputace a důvěryhodnosti pro klienty. Dále jsou uvedeny příklady narušení bezpečnosti a jejich dopady (19).

- Prozrazení osobních údajů – pokuty, odnětí svobody.
- Prozrazení obchodního tajemství – ztráta konkurenční výhody.
- Nežádoucí konání jménem určitého subjektu – poškození dobrého jména, nebo značky.
- Možnost využití vašeho IS jako východiska k útoku (19).

3 NÁVRH ŘEŠENÍ

Díky nedostatkům, které se na této střední škole nachází, není možno zavádět management bezpečnosti podle řady norem ISO 27000. Tyto normy mohou v tuto chvíli posloužit pouze jako vodítko při vytváření prvotních zárodků managementu bezpečnosti ICT. Mezi velice důležité dokumenty, které v následujících kapitolách obecně nadefinuji, patří dokument týkající se vzdělávání zaměstnanců a žáků, dokument týkající se zavedení procesů zabývajících se zodpovědností, proškolováním a dalšími okruhy bezpečnosti ICT. Tyto dokumenty by podle mého názoru měly být začleněny ředitelem a správcem sítě do chodu školy ve smyslu zavedení do pracovních smluv a do školního řádu.

3.1 Organizační struktura

Organizační struktura má z mého pohledu ve škole správnou hierarchii. Vyskytuje se zde však obrovský problém týkající se zastupitelnosti jednotlivých pracovníků starajících se o infrastrukturu ICT. Stejně tak jako je důležité, aby měl zástupce ředitel, je důležité, aby existoval plnohodnotný zástupce i pro správce ICT infrastruktury.

Doporučuji, aby byly pracovní funkce rozlišovány. Funkci technického administrátora a učitele informačních technologií není vhodné automaticky spojovat. Zastávat ve škole obě tyto funkce najednou v plném rozsahu je náročné. Z tohoto důvodu doporučuji, aby byl zaškolen další pracovník na pozici technického administrátora, který bude schopen síť spravovat v případě nedostupnosti nynějšího správce sítě.

3.2 Obecná bezpečnostní politika

Jak vyplývá z analýzy, bezpečnostní opatření nejsou v tomto prostředí definována. Navrhuji vytvořit jeden hlavní ucelený dokument zabývající se obecnou bezpečnostní politikou. Tento dokument by pak odkazoval na konkrétní směrnice školy. Nejen u tohoto dokumentu, ale i u ostatních směrnic a procesů, důrazně doporučuji, aby byly dodrženy všechny náležitosti související s tímto typem dokumentů.

Při vytváření bezpečnostní politiky doporučuji spolupráci s vedením školy, s technickou podporou, učitelským sborem a nejlépe i s žáky. Vytvořená dokumentace by měla být všem dostupná a všichni by s ní měli být seznámeni. Tímto by mělo být docíleno určitého logického rámce, který by měl být funkční.

Doporučuji, aby se vedení školy při vytváření struktury vyhnulo lidem neznalým, kteří by nebyli schopni zabezpečit procesy či funkce díky jejich neznalosti tématu. Prozatím je zde totiž vše řízeno na „dobré slovo“ a mnozí vyučující nebo žáci nemají ponětí, že se dopouštějí chyb, které znamenají pro tuto organizaci bezpečnostní riziko.

3.3 Politika bezpečnosti sítě

Jak vyplývá z analýzy, politika bezpečnosti sítě zde není téměř nijak definována. Proto bych doporučil vycházet alespoň z toho mála, co škola má a na co je zvyklá. Jedná se dokument Osnova poučení žáků SŠ v učebně informatiky. Je však zapotřebí tento dokument aktualizovat a rozšířit do podoby, která by byla vhodná pro celou školu, nejen pro učebny výpočetní techniky. To znamená, že by měl kromě žáků platit i pro zaměstnance. Doporučuji, aby byl dokument být rozšířen či aktualizován například o body uvedené níže.

- Uživatel smí využívat školní síťovou infrastrukturu pouze ke studiu nebo k plnění pracovních povinností.
- Zákaz připojení se do sítě bez patřičných proškolení.
- Zákaz připojování jakéhokoliv hardwaru ke školním stanicím bez schválení správcem.
- Zákaz jakkoliv ovlivňovat běh primárního operačního systému (bootovat jiný systém).
- Striktní zákaz provádět jakékoliv penetrační testy bez předchozí domluvy s vedením školy.
- Striktní zákaz provádět jakékoliv monitorování síťových aktivit bez předchozí domluvy s vedením školy.
- Zákaz připojování neschválených zařízení do školní síťové infrastruktury bez povolení vedení školy nebo zmocněného zaměstnance.

- Zákaz používat jakákoliv média či jiná zařízení a kopírovat na ně data či programy z počítače, nejsme-li jejich výhradními vlastníky.
- Zákaz používat jakákoliv média či jiná zařízení a spouštět z nich software, který by mohl jakkoliv negativně ovlivnit chod sítě.
- Zjednodušený popis politiky hesel.

Mým dalším doporučením je, aby byly rozděleny jednotlivé části školy do různých VLAN. To znamená, že místnost se servery a síťové uzly s aktivními prvky, které se ve škole vyskytují, by spadaly do VLAN1. Do této VLAN bych také začlenil počítač vyučujícího výpočetní techniky, který se stará o aktivní prvky a servery a který by měl možnost se k nim připojovat. Učebnám výpočetní techniky bych doporučil přiřazení VLAN2 a učebně B 215 přiřazení VLAN3. Do VLAN4 by spadal zbytek bloku B a blok C. Bloku A by byla přidělena VLAN5. VLAN6 a VLAN7 by byly vyčleněny pro zařízení Wi-Fi. Takovéto rozdělení z mého pohledu umožňuje mnohem lepší práci a kontrolu nad jednotlivými částmi školní sítě.

3.3.1 Uživatelská zařízení

Doporučuji vypracovat bezpečnostní pravidla, která musí splňovat jednotlivá zařízení připojená do sítě a následně jimi doplnit dokument obsahující poučení o chování v učebnách informatiky. Tento dokument by se měl vztahovat nejen na počítače používané v učebnách výpočetní techniky, ale na celou školu a na všechny zařízení, které se připojují ke školní počítačové síti. To znamená i na všechny soukromé zařízení, kterými disponují zaměstnanci či žáci (tablety, PDA, chytré mobilní telefony a laptopy).

Dokument by měl u zařízení definovat minimálně:

- Jaký typ zařízení se může / nemůže do sítě připojit.
- Jak by dané zařízení mělo / nemělo být konfigurováno.
- Jaké by mělo / nemělo obsahovat aplikace.
- Jak by se dané zařízení v síti mělo / nemělo chovat.

3.3.2 Aktivní prvky

3.3.2.1 Switche

Doporučuji zavést technickou dokumentaci týkající se správy a nastavení switchů. Doporučuji na rozvaděčích zavést a dodržovat politiku hesel. K tomuto účelu bych doporučil pořídit aplikaci typu Manage Engine Password Manager, která by pomáhala se správou hesel.

3.3.2.2 Wi-Fi přístupové body

Doporučuji zde zavést dokumentaci, která bude jasně definovat jak má být Wi-Fi zařízení nastaveno a spravováno.

Mezi rizika, která se zde vyskytují, jednoznačně patří riziko spojené se zasahováním signálu do přilehlých obydlí. U zařízení, které takto do přilehlých obydlí zasahují, doporučuji snížit výkon.

Další riziko a zároveň problém vidím v zařízeních zakoupených studenty. Tyto zařízení doporučuji ze sítě úplně vyloučit a to z několika důvodů. Prvním důvodem je jejich dosažitelnost a možnost žáků k takovému zařízení cokoliv připojit, popřípadě je rekonfigurovat. Zařízení je totiž stále majetkem studentů a ne školy. Dalším důvodem je zde funkce WPS, která u tohoto zařízení tvoří velkou bezpečnostní mezeru. Jako poslední chybu zde shledávám špatný firmware zařízení, který je sám o sobě lehce prolomitelný.

Z analýzy vyplývá, že ve školním prostředí jsou 3 SSID, na které je možno se připojit. Je zapotřebí definovat pro každé SSID pravidla, která budou následně zdokumentována. Tyto pravidla nemusí být u všech tří SSID nastavena identicky. Důvod je jednoduchý, jedná se totiž o tři úplně odlišně sítě se specifickým využitím. Doporučuji k těmto připojením vést dokumentaci, která splňuje strukturu náležící tomuto typu dokumentu. Jednotlivé problémy konkrétních SSID jsou zmíněny níže.

PUBLIC

V případě této sítě by měly být požadavky a pravidla definovány jasně a striktně, jelikož v této síti probíhá většina Wi-Fi síťového provozu. Doporučuji, aby se řídila pravidly dokumentu Osnova poučení žáků SŠ v učebně informatiky, jehož modifikaci jsem navrhl výše. Heslo by určitě nemělo být vyvěšeno na nástěnce, jak

je tomu doteď. Řešením tohoto problému by bylo zavedení RADIUS serveru, které jednoznačně doporučuji.

EMAN

Jelikož jsou v této síti připojeny pouze školní zařízení, která jsou používána výhradně pro účely vzdělávání a jsou přednastavena, není zde úplně nezbytné zavádět autentizaci jednotlivých uživatelů. Doporučuji však, aby se síťový provoz řídil pravidly dokumentu Osnova poučení žáků SŠ v učebně informatiky, jehož modifikaci jsem navrhl výše.

SECURITY

Pokud škola opravdu potřebuje tuto síť, doporučuji, aby pravidla a požadavky pro tuto síť byly definovány co možná nejpřísněji. Z mého pohledu je zde tato síť zbytečná a tvoří pro školu pouze hrozbu. Po připojení do této sítě se totiž uživatel dostane do stejné VLAN1, ve které jsou všechny počítače v učebnách a všechny aktivní prvky. Poté není problém použít například útok „ARP SPOOF“ a znepřístupnit celou školní infrastrukturu díky znemožnění správného překladu adres. Popřípadě zaútočit jako „man in middle“ a získat údaje o žácích či zaměstnancích.

3.3.3 Servery

Doporučuji zavést technickou dokumentaci specifikující nastavení a správu jednotlivých serverů. Tím je myšleno jak softwarové tak hardwarové nastavení, včetně popisu všech účtů na nich vytvořených a služeb které obstarávají. Také by zde měly být sepsány úlohy konkrétních zaměstnanců starající se o síťovou infrastrukturu. Dále doporučuji omezit počet uživatelských účtů na serverech na potřebné minimum.

Doporučuji na serverech zavést a dodržovat politiku hesel. K tomuto účelu bych doporučil pořídit aplikaci typu Manage Engine Password Manager, která by pomáhala se správou hesel.

3.4 Politika autentizace

3.4.1 Bezpečnostní politika hesel

Ve škole neexistuje žádná směrnice ani návod definující jak pracovat s hesly. Proto doporučuji tento dokument sepsat a uvést v platnost. Dokument by měl mít všechny náležitosti, které jsou u dokumentu tohoto typu nezbytné. Měl by zahrnovat poučení nejenom pro zaměstnance školy, ale také pro studenty.

Doporučuji, aby dokument obsahoval informace jak má heslo vypadat a jaké by mělo mít vlastnosti. Také by neměla být opomenuta neméně důležitá pravidla, týkající se starosti o hesla. Některá z nich jsou uvedena níže.

- Uživatel nesmí sdílet heslo s jiným uživatelem.
- Uživatel zodpovídá za to, že heslo není použito ve více systémech v jeden okamžik.
- Uživatel nesmí uchovávat heslo v podobě nešifrovaného textu a to jak v počítači, tak v tištěné či psané formě.
- Uživatel musí dle požadavků systému heslo pravidelně měnit v určený okamžik, nebo pokud to systém nevyžaduje, měnit heslo minimálně jednou za půl roku.

Doporučuji, aby pravidla hesel, která to umožňují, byla nastavena přímo v dané aplikaci. Nyní mluvím o aplikacích Novel a Bakaláři, kde lze nastavit jak sílu hesla, tak jeho exspiraci. Doporučil bych následující nastavení:

- Délka hesla minimálně 7 znaků.
- Heslo nesmí obsahovat login jméno a ani příjmení.
- Heslo musí obsahovat znaky ze všech 4 skupin.
- Heslo nesmí obsahovat více než 2 stejné znaky ze stejné skupiny.
- Heslo se nesmí být slovníkové.
- Heslo musí exspirovat jednou ročně.

3.5 Bezpečnost dat

Doporučuji zde provést kategorizaci dat, na základě které budou data rozdělena podle toho, jak moc jsou pro školu důležitá a kritická. Doporučuji použít metodiku,

kterou popisuje norma ČSN ISO/IEC 27005:2006. Pomocí této metodiky se dají posuzovat rizika i v jiných oblastech, než je bezpečnosti dat. Zvolenou metodiku doporučuji zdokumentovat. Níže uvádím příklad návrhu tabulek, dle kterých by škola měla rizika hodnotit. Tabulka 1 všeobecně popisuje hodnotu rizika. Tabulka 2 popisuje pravděpodobnost výskytu hrozby včetně příkladů a tabulka č. 3 nám ukazuje celkovou rizikovost po dosazení hodnot z tabulek 1 a 2.

Tab. 1: Hodnota aktiv a dopadu na ně (Zdroj: Vlastní zpracování)

Hodnota aktiva	**Hodnota dopadu na dané aktivum**
1 – Zanedbatelná	Dopad na aktiva školy je **zanedbatelný**. • Případné následky se neprojeví na chodu školy. • Odstranění následků proběhne bez jakéhokoliv problému v krátkém časovém horizontu, bez finanční nákladnosti • Nedošlo k porušení právních norem.
2 – Malá	Dopad na aktiva školy je **malý.** • Má negativní vliv na organizační celky působící ve škole, ale navenek se neprojeví. • Odstranění následků proběhne s malými problémy stále však v reálném časovém horizontu. A bez finanční nákladnosti. • Nedošlo k zásadnímu porušení právních norem.
3 – Významná	Dopad na aktiva školy je **vážný.** • Má negativní dopad nejenom na jednotlivé organizační celky, ale také se projeví navenek. • Újma způsobená jedné či více osobám mimo ohrožení zdraví či života. • Odstranění následků proběhne s velkým úsilím v neurčitém čase a značnou finanční nákladností. • Mohlo zde dojít k zásadnímu porušení právních norem.
4 – Velmi cenná	Dopad na aktiva školy je **velmi vážný.** • Veřejná negativní publicita. • Ztráta důvěryhodnosti. • Potencionální možnost zániku školy. • Citelná finanční ztráta. • Ohrožení života či vážné zranění. • Odstranění následků proběhne, pokud je možné je odstranit proběhne s velkým úsilím, v dlouhém časovém horizontu.

Tab. 2: Hodnocení úrovně hrozby (Zdroj: Vlastní zpracování)

Úroveň hrozby	**Hodnocení úrovně hrozby**
VN – Velmi nízká	Riziko je možné akceptovat. • Je zde velice nízká pravděpodobnost, že dojde k hrozbě. Zde můžeme řadit hrozby typu, jako jsou živelné pohromy a teroristické útoky.
N – Nízká	Riziko je možné akceptovat • Je zde malá pravděpodobnost, že dojde k hrozbě a vyskytne se dopad na činnost subjektu nebo jeho části. Zde můžeme řadit hrozby typu útoky hackerů.
S – Střední	Riziko by mělo být řešeno. • Je pravděpodobné, že dojde k hrozbě a vyskytne se dopad na činnost subjektu nebo jeho části. Zde můžeme řadit hrozby jako výpadek elektrického proudu, poškození dat, zneužívání Wi-Fi sítě, nebo napadení sítě viry.
V – Vysoká	Riziko musí být řešeno. • Je velmi pravděpodobné, že dojde k hrozbě a vyskytne se zde dopad na činnost subjektu nebo jeho části. Zde můžeme zařadit hrozbu jako zneužití přihlašovacích údajů.
VV – Velmi vysoká	Riziko musí být řešeno s nejvyšší prioritou. • Téměř s jistotou dojde k **velmi závažnému** dopadu na činnost subjektu nebo jeho části. V tuto chvíli se zde žádné takovéto riziko nevyskytuje.

Tab. 3: Vyhodnocení Hodnota rizika vůči hrozbě (Zdroj: Vlastní zpracování)

		Úroveň hrozby				
		VN	N	S	V	VV
Hodnota rizika	1	N (1)	N (2)	S (3)	S (4)	S (5)
	2	N (2)	S (3)	S (4)	S (5)	V (6)
	3	S (3)	S (4)	S (5)	V (6)	V(7)
	4	S (4)	S (5)	V (6)	V(7)	V (8)

3.5.1 Politika zálohování a obnovy dat

Doporučuji nastavit politiku zálohování a obnovy dat jasně a striktně. Záloha by měla být adekvátní důležitosti zálohovaných dat a jejich aplikaci. Doporučil bych zde vytvořit pravidla a následně je zdokumentovat.

V dokumentu politiky zálohování by měly být striktně nadefinovány tyto body.

- Úroveň zálohování závislá na druhu aplikace.
- Frekvence s jakou bude zálohování probíhat.
- Médium, na které bude zálohováno a jeho označení.
- Kdo zodpovídá za konkrétní zálohy.
- Jaký typ záloh a jak často se musí provádět (plná či rozdílová záloha).

Doporučuji, aby byla pro aplikace Novel tvořena plná záloha jednou za rok a rozdílová jednou za dva až tři měsíce. Plná záloha by měla být tvořena v okamžiku, kdy jsou nová data již zadána a stará smazána. Tato data doporučuji zálohovat na jeden ze serverů a uložit je i na nějaké jiné médium, které bude následně uloženo na konkrétní místo a správně popsáno. Tímto médiem může být například DVD, nebo přenosný disk. Doporučuji, aby byl vytvořen přesný manuál jak obnovovat a zálohovat data v aplikaci Novel.

U aplikace Bakaláři doporučuji vytvoření plné zálohy každý pracovní den večer. Doporučuji ukládání plné zálohy na serveru a zároveň na médiu vhodném k tomuto účelu (DVD, přenosný disk). Doporučuji, soubory záloh ponechávat minimálně čtrnáct dní. Dále také, aby byl vytvořen přesný manuál jak obnovovat a zálohovat data v aplikaci Novel.

Politika zálohování a obnovy by měla být minimálně jednou ročně testována a na základě testů by měla být doplněna daná dokumentace.

3.6 Politika vzdělávání uživatelů

Školení týkající se managementu by mělo probíhat v rámci každé organizace, mělo by tedy probíhat i zde. Doposud byli v intervalu jednoho roku proškoleni pouze žáci, nikoli však členové učitelského sboru. Proškolování zaměstnanců by mělo být řádně kontrolováno. Navrhuji pořádání pravidelného školení zaměstnanců, na kterém by se dozvěděli konkrétní informace o:

- Nebezpečí, která na ně internetu číhají.
- Jak se chránit před virtuálními útoky.
- Jak si vytvořit silné heslo a jak se o něj starat.
- Jak pracovat se softwarem a základní informace o licenčních právech.
- Jak bezpečně pracovat ve školní síti.
- Kde hledat informace o managementu zabezpečení v dané organizaci.

Školení by měl vést člověk v této problematice zběhlý, nejlépe certifikovaný. Výstupem by měl být dokument, obsahující probíraná témata shrnutá v bodech. Tento dokument by měli všichni zúčastnění podepsat a tím stvrdit svou účast. Takto lze zdokumentovat, zda a kdy daný zaměstnanec školením prošel.

Doporučuji proškolit pracovníky starající se o servery, školní stanice, nebo aktivní prvky v problematice jim blízké a umožnit jim certifikovat své znalosti. Toto může do školy přinést motivaci pro vzdělávání a také zvýšit kvalitu managementu bezpečnosti.

3.7 Monitoring

Doporučuji zavést nástroje pro monitoring celé sítě. Chápu, že rychlost sítě je pro školu důležitá a z důvodu realizace postupného upgradu celé sítě není možné jednorázově vyměnit všechna pomalejší zařízení najednou. Avšak z mého pohledu by měla být bezpečnost na prvním místě. Dle předloženého modelu by ztráta rychlosti v praxi neměla být nijak razantní.

Zavedení doporučuji z důvodu možného napadení popřípadě připojení cizího subjektu do sítě školy a následného zneužití některých pro školu klíčových informací. Díky monitorování by bylo možno zjistit, jak se útočník dostal do školní sítě popřípadě určit viníka. Další výhodou je bezesporu sledování přenosů na daných

stanicích. Při zvýšeném vytížení sítě pak lze zjistit zdroj potíží, mezi které můžou patřit uživatelé stahující množství nelegálních dat.

V této práci není místo pro konkrétní specifikaci softwaru, který tuto činnost obstarával, doporučil bych se tomuto věnovat v další práci, která by se zaměřila na monitoring ve škole.

3.8 Přínosy managementu bezpečnosti

U organizace, která je nezisková, nelze přesně vyčíslit, kdy by se daná investice do managementu zabezpečení ICT vrátila. Tato investice je dlouhodobého rázu a dá se předpokládat, že při správném zavedení a užití by škole mohla přispět k její dobré pověsti a zlepšení informovanosti uživatelů. Časem by zde byla také možnost přechodu k plné certifikaci podle normy ISO 27000.

V následující tabulce jsem shrnul výhody a nevýhody, které pro školu plynou ze zavedení managementu bezpečnosti ICT.

Tab. 4: Zhodnocení zavedení managementu bezpečnosti (Zdroj: Vlastní zpracování)

VÝHODY	NEVÝHODY
Ujasnění procesů a funkcí	Zvýšené náklady na vzdělání zaměstnanců a žáků
Bezpečnější fungování školy	
Větší znalosti týkající se bezpečnosti	
Bezpečnější uchovávání dat	Povinnost vytvoření nezbytné dokumentace a uvedení v platnost
Možnost certifikace	
Zvýšení konkurenceschopnosti	

ZHODNOCENÍ A ZÁVĚR

Reálným výstupem mé bakalářské práce jsou návrhy různých bezpečnostních prvků managementu bezpečnosti ICT, které by měly sloužit vedení školy jako důvod k zamyšlení a hlavně důvod k implementaci konkrétních opatření. Pokud budou mé návrhy realizovány, věřím, že mohou přispět k lepšímu vedení a fungování školy. Doufám, že tyto návrhy pomohou celkově pozvednout povědomí o bezpečnosti, která je na této škole v podstatě na nejnižší možné úrovni.

První část práce se zabývala analýzou prostředí školy. Mezi největší úskalí této části práce patřilo formálního seskupení dokumentu. Analýza samotného objektu, jeho vybavenosti a fungování byla díky vstřícnosti správce a vedení provedena bez větších problémů. V druhé části mé práce jsem se zabýval teoretickými východisky, termíny a znalostmi z pohledu managementu bezpečnosti ICT, které by samy o sobě bezesporu vydaly na mnoho publikací. V poslední části mé práce jsem se věnoval problémům, které se objevily v průběhu analýzy prostředí školy, navrhl jsem možná řešení. Tato řešení doporučuji zavést.

Hlavní, problémem, na který jsem narazil při vypracovávání této práce, byl nedostatek relevantních zdrojů. Neexistuje totiž žádný ucelený dokument, nebo publikace, který by tuto tématiku jednoduše a výstižně popisoval. Informace týkající se managementu bezpečnosti ICT jsou totiž pečlivě střeženy firmami, které provádějí auditorské činnosti. Tyto informace jsou totiž jejich nejcennějším majetkem.

V průběhu všech fází tvorby mé bakalářské práce jsem konzultoval mé nápady a poznatky jak s vedoucím mé bakalářské práce, tak se správcem školní sítě. Věřím tedy, že návrhy obsažené v mé práci škola zváží, a budou použity v praxi.

V této práci jsem se nezabýval bezpečností z pohledu HW, fyzické, či personální bezpečnosti. Důvodem byla rozsáhlost těchto témat.

SEZNAM POUŽITÉ LITERATURY

(1) OBST, O., M. HRABOVSKÝ, K. IVANOVÁ et al. *Základy obecného managementu*. 1. vyd. Olomouc: Univerzita Palackého v Olomouci, 2006. ISBN 80-244-1365-5.

(2) ŠTALMACH, P. a J. ŠEDIVÝ. *MANAGEMENT BEZPEČNOSTI*. 1. vyd. Praha: CEVRO Institut, 2012. ISBN 978-80-87125-19-9.

(3) RILEY, J. Tutor2u. *ICT - What is it?* [online]. 2012 [cit. 2013-03-15]. Dostupné z: http://www.tutor2u.net/business/ict/intro_what_is_ict.htm

(4) PŘIBYL, T. Testování bezpečnosti: na co nezapomenout. *Nezávislý odborný on-line magazín ICT security* [online]. 2012 [cit. 2013-04-12]. Dostupné z: http://www.ictsecurity.cz/odborne-lanky/testovani-bezpenosti-na-co-nezapomenout.html

(5) STAUDEK, J. *Úvod do problematiky bezpečnosti IT 3.[online]*. Brno: FI MU, verze podzim 2007. [cit. 2012-10-16]. Dostupné z: http://www.fi.muni.cz/usr/staudek/vyuka/

(6) ISO/IEC. *ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Switzerland: ISO/IEC, 2009. 26 p.

(7) ISO/IEC. *ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.* Switzerland: ISO/IEC, 2005. 42 p.

(8) DOUCEK, P. Bezpečnostní incidenty IS/ICT a jejich řešení. *Systémová integrace* [online]. 2005, vol. 3, 9 s.[cit. 2013-05-15]. Dostupné z: www.cssi.cz/cssi/system/files/all/doucek.pdf

(9) Zákon č. 101/2000 Sb., o ochraně osobních údajů ze dne 4. dubna 2000

(10) Zákon č. 227/2000 Sb. o elektronickém podpisu ze dne 29.6.200

(11) Zákon č. 480/2004 Sb. o některých službách informační společnosti ze dne 29. července 2004

(12) Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností ze dne 11. června 1998

(13) ISO/IEC. *ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management*. Switzerland: ISO/IEC, 2005. 128p.

(14) STAUDEK, J. a H. VYSTAVĚLOVÁ. Standardizace bezpečnosti informačních technologií. *Procesy a organizace standardizace bezpečnosti IT* [online]. 2013 [cit. 2013-05-16]. Dostupné z: http://www.fi.muni.cz/usr/staudek/vystavelova/index.html

(15) INTERNATIONAL ORGANIZATION FOR STANDARTIZATION. ISO/IEC 27000 [online]. 2013 [cit. 2012-11-19]. Dostupné z: http://www.iso27000.cz/

(16) Doucek, P. Bezpečnost IS/ICT a proces globální integrace – Proč bezpečnost?, In: AT&P Journal. *AT&P Journal*. 01/2005, ISSN 1335-2237.

(17) OTRUSINOVÁ, M. a K. ŠTEKER. *Vnitropodnikové účetní směrnice* [online]. 2007[cit. 2013-05-16]. Dostupné z: http://www.danarionline.cz/archiv/dokument/doc-d2607v3373-vnitropodnikove-ucetni-smernice/

(18) SELECKÝ, M. *Penetrační testy a exploitace*. 1. vydání. Brno: Computer Press, 2012. ISBN978-80-251-3752-9.

(19) DOUCEK. P., L. NOVÁK a V. SVATÁ. *Řízení bezpečnosti informací*. 1. vydání. Praha: Professional Publishing, 2008. ISBN 978-80-86946-88-7.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHY

Příloha 1: Osnova poučení žáků (Zdroj: Školní dokumentace)

Osnova poučení žáků SŠ v učebně informatiky (v počítačové učebně)

1) Do učebny informatiky vstupují žáci pouze v doprovodu vyučujícího.
2) V době mimo výuku a o přestávkách je povolen vstup žákům do učeben výpočetní techniky po nahlášení v kabinetu VT.
3) Bez souhlasu vyučujícího žáci z učebny nesmí odcházet.
4) Počítače žáci smějí zapínat a vypínat pouze síťovým vypínačem a se souhlasem vyučujícího.
5) Před zahájením práce na počítači žáci zkontrolují své pracoviště a případné závady a poškození ihned ohlásí vyučujícímu.
6) Žáci pracují na počítači pouze pod dohledem vyučujícího a respektují jeho pokyny a příkazy.
7) Žáci se chovají tak, aby neohrožovali zdraví a bezpečnost svoji a ostatních žáků, s vybavením učebny zacházejí šetrně.
8) Při pohybu v učebně žáci dbají zvýšené opatrnosti a omezují pohyb na co nejmenší míru.
9) Žákům je přísně zakázáno (bez souhlasu vyučujícího):
    a) Prohledávat disky počítače, provádět jakékoli změny v nastavení počítače a v jeho adresářích.
    b) Odpojovat a jinak přepojovat kabely a zařízení učebny, zasahovat do elektrické instalace, otevírat počítače a zasahovat do jejich vnitřního zařízení.
    c) Instalovat jakýkoliv software do počítačů.
    d) Používat vlastní diskety, CD a jiná přídavná zařízení, kopírovat na ně programy z počítače nebo spouštět jejich obsah.
    e) Zneužívat počítačovou síť k šíření informací, které jsou v rozporu se zákonem.
    f) Odesílat poštu, která by svým obsahem obtěžovala či urážela ostatní uživatele.
    g) Na internetu otevírat stránky propagující násilí, rasismus, drogy, sex apod.
    h) Konzumovat v učebně potraviny a nápoje a používat žvýkačky.
    i) Používat a dobíjet v učebně mobilní telefony.
10) Jakékoli nestandardní chování počítače hlásí žák vyučujícímu.
11) Při ukončení práce provede každý žák stanovené kroky v souladu s programem počítače, ve kterém pracoval, a zajistí úklid svého pracoviště.
12) Škodu na vybavení učebny, kterou žák způsobil úmyslně, je povinen uhradit.

Ve [redacted] dne 1. 9. 2010

[redacted]
předseda PK IVT

Příloha 2: Provozní řád učebny výpočetní techniky (Zdroj: Školní dokumentace)

Gymnázium a Střední odborná škola, [redacted]

PROVOZNÍ ŘÁD

Učebny výpočetní techniky vybavené počítači

1. Všeobecná ustanovení

1.1 Učebna výpočetní techniky (dále UVT) vybavena počítači je určena

- především pro potřeby výuky žáků GYMNÁZIA a SOŠ
- pro zpracování dat a údajů pracovníků škol
- v době mimo vyučování pak slouží rozvoji zájmu o VT žáků a vzdělávání dospělých ve spolupráci s organizací KVIC

1.2 Provozní řád UVT obsahuje

- vymezení odpovědnosti za provoz učebny
- zajištění bezpečnosti a hygieny provozu v učebně
- zásady manipulace s prostředky tvořícími vybavení učebny
- závěrečné ustanovení

2. Vymezení odpovědností za provoz učebny

2.1 Řízením UVT byl vedením školy pověřen [redacted], který odpovídá za celkový provoz. Stanoví zejména:

- rozvrh provozu UVT v době vyučování a v době mimo vyučování
- kontroluje provoz a dodržování Provozního řádu
- zajišťuje údržbu a opravy zařízení učebny

2.2 Vstup do UVT mají povolen:

- určení vyučující dle rozvrhu výuky
- žáci v doprovodu odpovědných pracovníků
- ředitel školy
- účastníci kurzu VT
- školník, údržbář a uklízečka
- další osoby se souhlasem a v doprovodu pracovníka pověřeného vedením UVT

2.3 Klíče od UVT má vedoucí pracoviště, učitelé VT, ředitel školy, uklízečka a sekretariát

2.4 Každý pracovník přebírá vstupem do učebny plnou zodpovědnost za vybavení, provoz a dodržování bezpečnosti provozu a ochranu zdraví.

Odpovědný pracovník po skončení práce je povinen:

- vypnout po skončení práce všechna elektrická zařízení
- dbát pořádku a čistoty na všech pracovištích i v celé učebně
- ohlásit vedoucímu UVT všechny případné poruchy
- v učebně musí být při odchodu uzavřena okna, zhasnuta světla. Učebna musí být vždy řádně uzamčena

3. Pravidla vlastního provozu

3.1 Za dodržování všech pravidel odpovídá učitel, který žáky vyučuje nebo má UVT dozor.

3.2. V učebně platí řád školy. Mimo to je UVT zakázáno jíst, pít, kouřit a manipulovat s otevřeným ohněm.

3.3 Jsou zakázány jakékoliv zásahy do sestavy počítačů a el. sítě učebny.

3.4 Povinnosti všech je udržovat v UVT čistotu a pořádek.

3.5 S počítači mohou manipulovat pouze osoby poučené a obsluhy znalé. Při obsluze musí být dodrženy předepsané postupy.

3.6 Všechny poruchy je třeba ihned hlásit správci učebny. Ten zajišťuje odbornou opravu.

3.7. Seznámení všech uživatelů UVT s tímto „Provozním řádem" bude pořádáno 1x ročně.

3.8. Nedbalost nebo opakované porušování „Provozního řádu" bude vedením školy trestáno ve smyslu zákonných ustanovení.

4. Závěrečná ustanovení

Tento provozní řád nabývá platnosti dne 1. 9. 2010

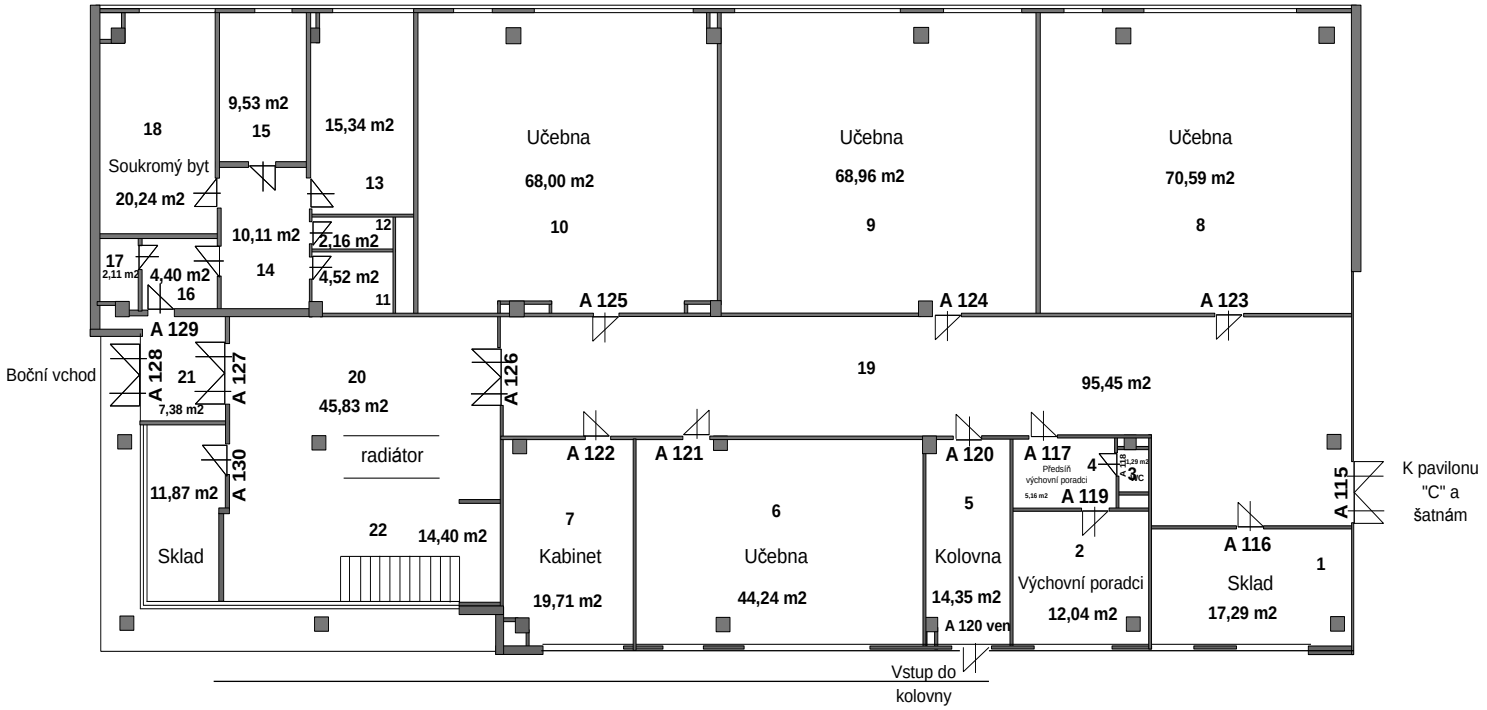
…….. ……..

podpis ředitele školy podpis správce učebny

Příloha 3: Pasportizace školní budovy (Zdroj: Školní dokumentace)

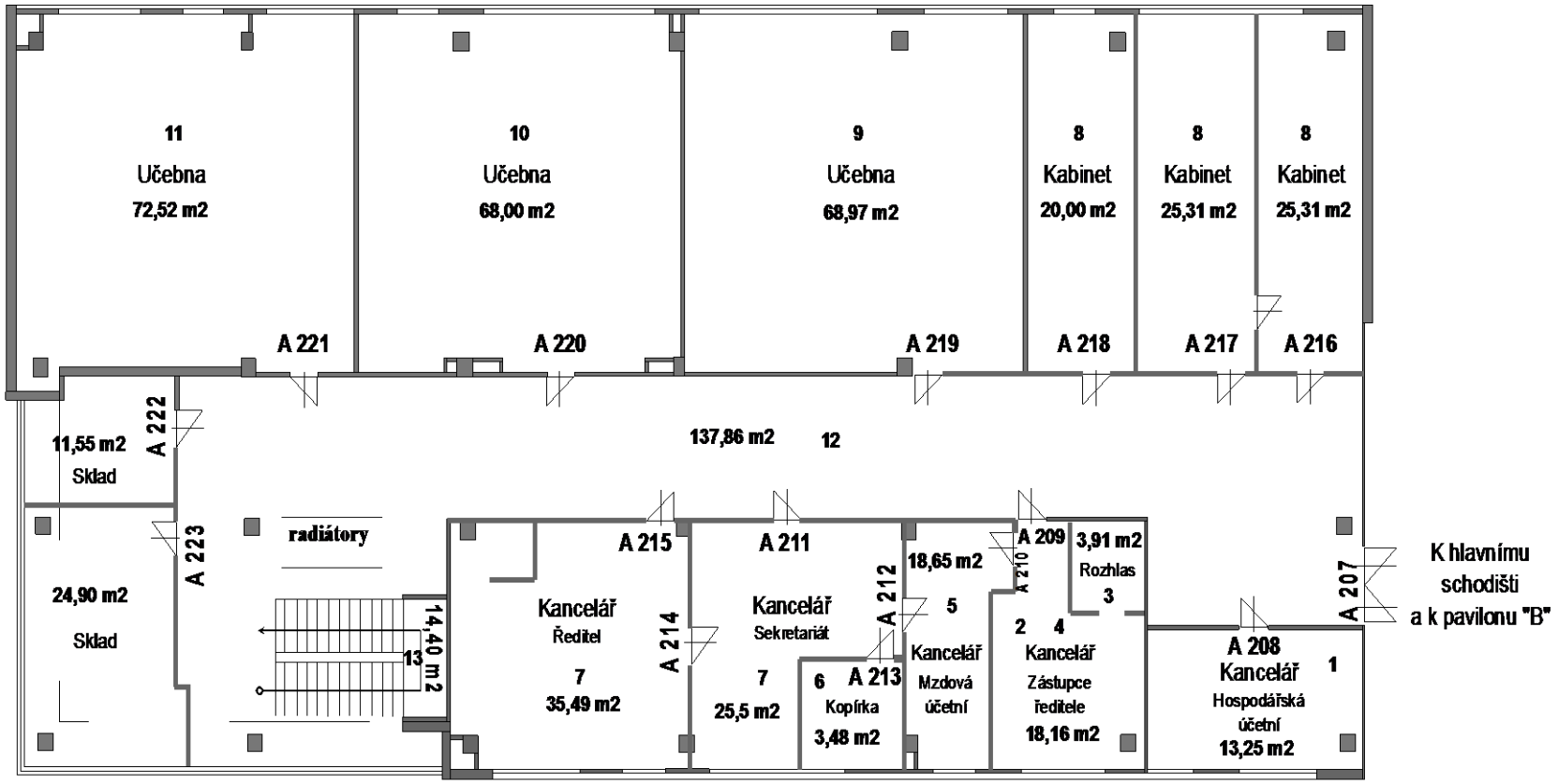
A 1NP

UV 13Z-0

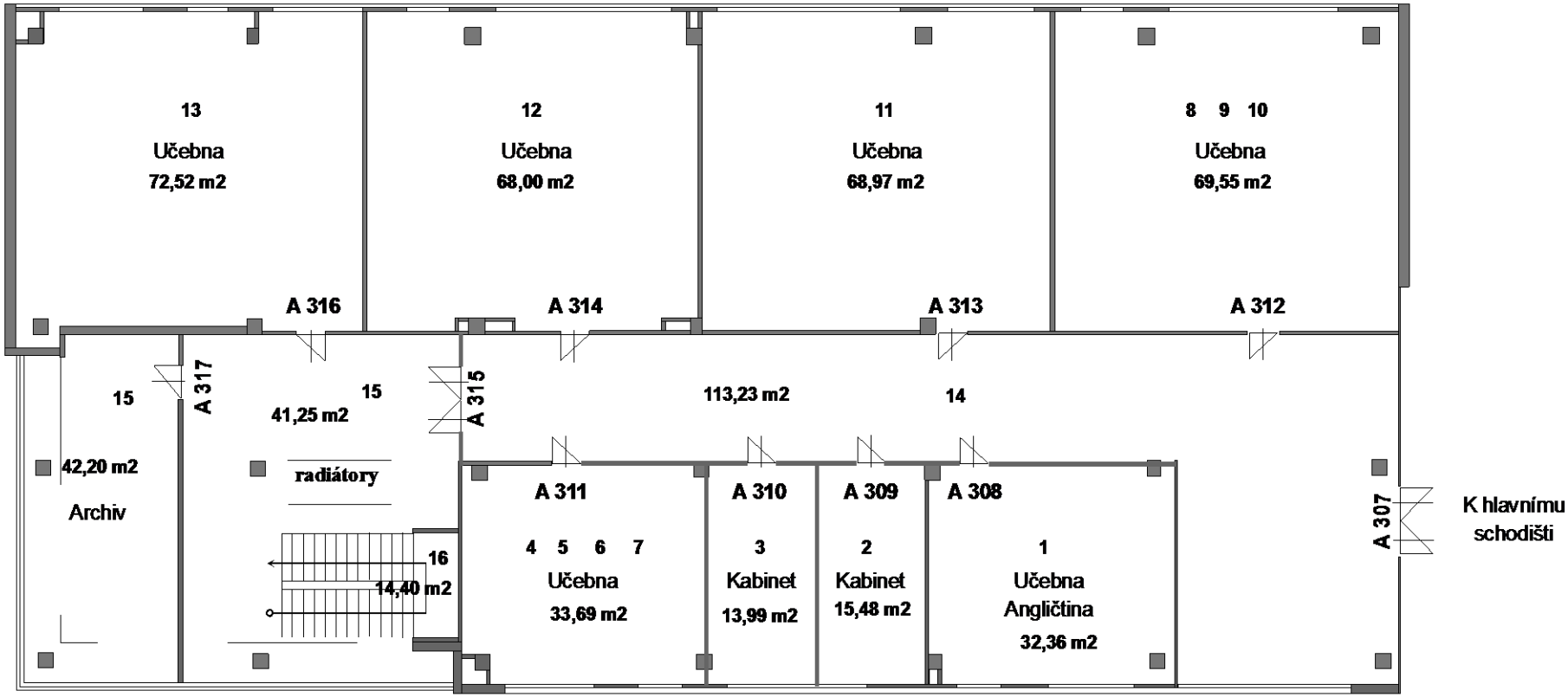


A 2NP

UV 13Z-0

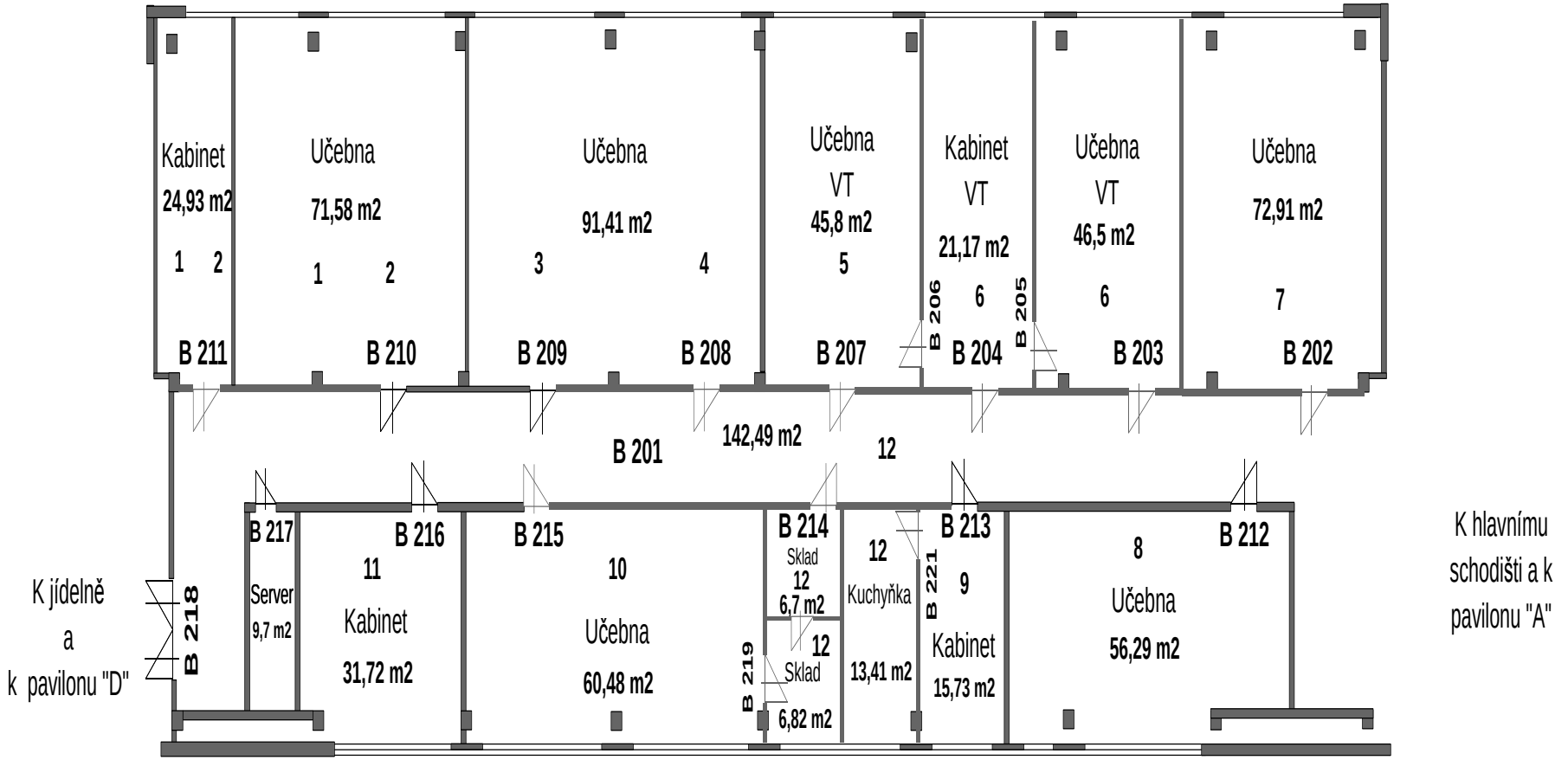

11
Učebna
72,52 m2
10
Učebna
68,00 m2
9
Učebna
68,97 m2
8
Kabinet
20,00 m2
8
Kabinet
25,31 m2
8
Kabinet
25,31 m2
A 221
A 220
A 219
A 218
A 217
A 216
A 222
11,55 m2
Sklad
137,86 m2
12
A 223
radiátory
24,90 m2
Sklad
14,40 m2
13
A 215
A 211
A 212
18,65 m2
A 209
3,91 m2
Rozhlas
3
A 210
A 207
K hlavnímu
schodišti
a k pavilonu "B"
Kancelář
Ředitel
7
35,49 m2
A 214
Kancelář
Sekretariát
7
25,5 m2
6
A 213
Kopírka
3,48 m2
5
Kancelář
Mzdová
účetní
2
4
Kancelář
Zástupce
ředitele
18,16 m2
A 208
Kancelář
Hospodářská
účetní
13,25 m2
1

A 3NP
UV 13Z-0


13
Učebna
72,52 m2
12
Učebna
68,00 m2
11
Učebna
68,97 m2
8 9 10
Učebna
69,55 m2
A 316
A 314
A 313
A 312
15
42,20 m2
Archiv
A 317
15
41,25 m2
radiátory
A 315
113,23 m2
14
A 311
4 5 6 7
Učebna
33,69 m2
A 310
3
Kabinet
13,99 m2
A 309
2
Kabinet
15,48 m2
A 308
1
Učebna
Angličtina
32,36 m2
16
14,40 m2
A 307
K hlavnímu
schodišti

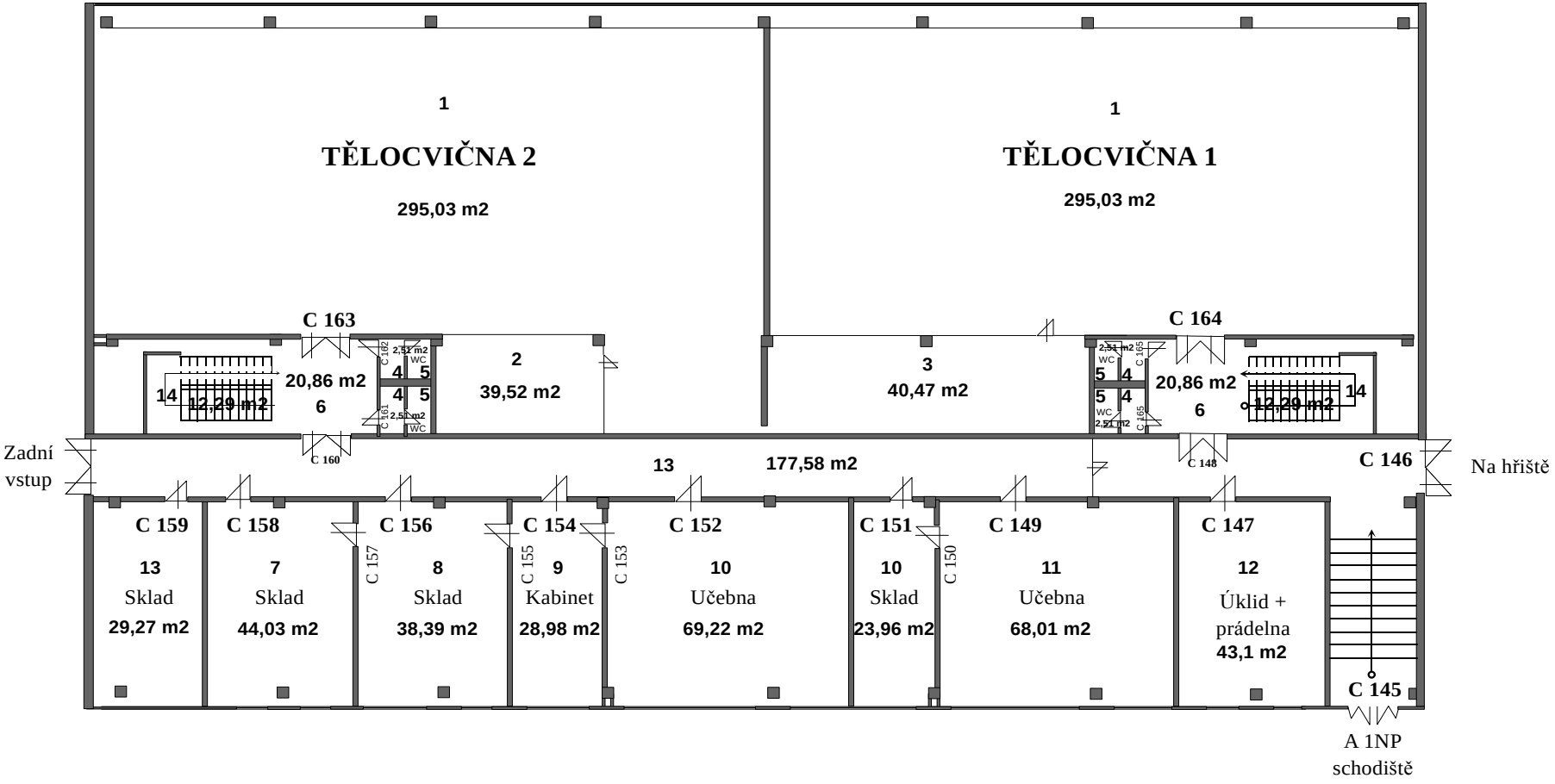
B 2NP

ŠM 4


Kabinet
24,93 m2
1
2
B 211
Učebna
71,58 m2
1
2
B 210
Učebna
91,41 m2
3
4
B 209
B 208
Učebna
VT
45,8 m2
5
B 207
Kabinet
VT
21,17 m2
6
B 206
B 204
B 205
Učebna
VT
46,5 m2
6
B 203
Učebna
72,91 m2
7
B 202
B 201
142,49 m2
12
K jídelně
a
k pavilonu "D"
B 218
B 217
Server
9,7 m2
B 216
11
Kabinet
31,72 m2
B 215
10
Učebna
60,48 m2
B 214
Sklad
12
6,7 m2
12
Sklad
6,82 m2
B 219
12
Kuchyňka
13,41 m2
B 221
B 213
9
Kabinet
15,73 m2
8
Učebna
56,29 m2
B 212
K hlavnímu
schodišti a k
pavilonu "A"

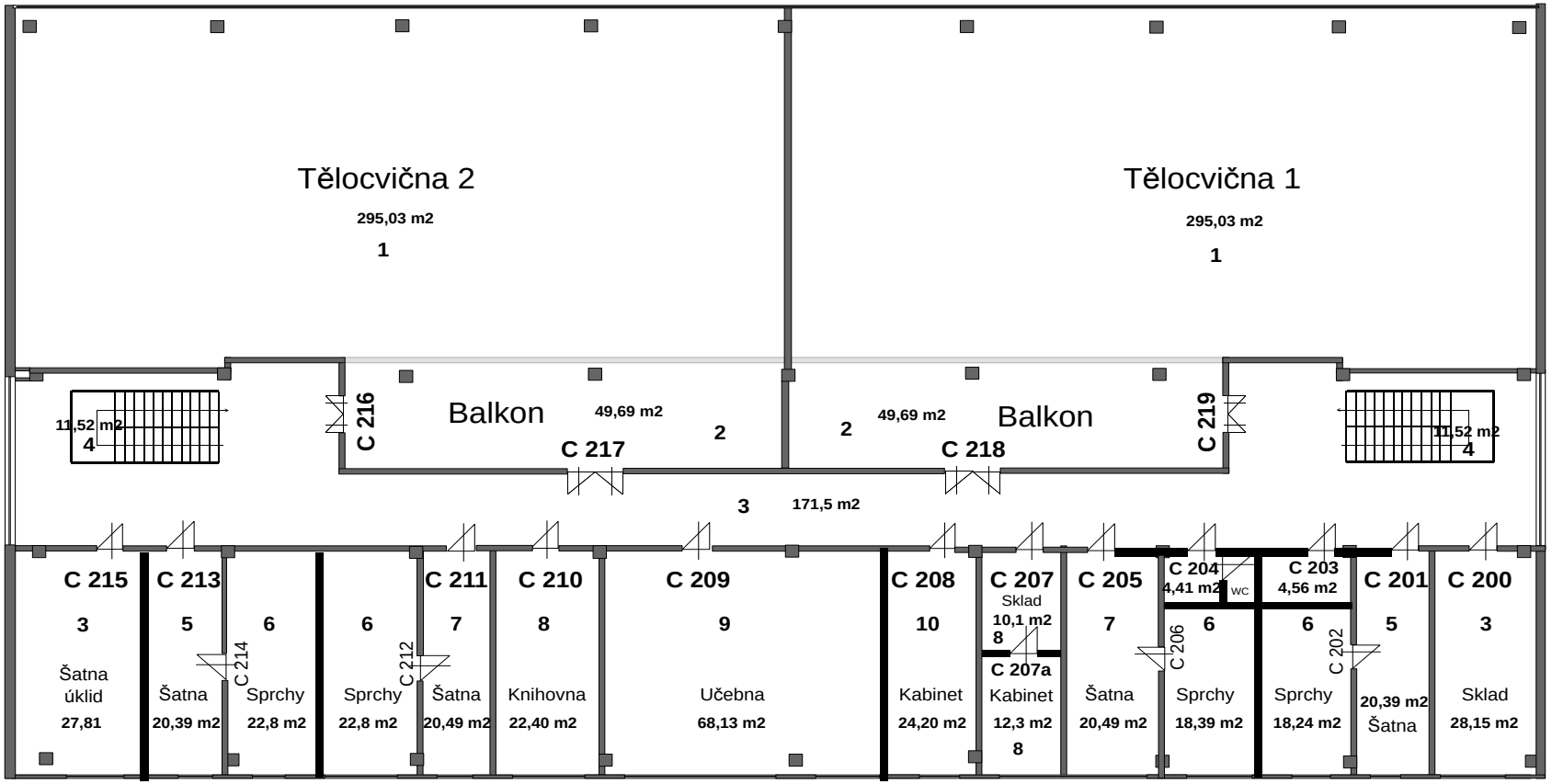
C 1NP

TD 3


1
TĚLOCVIČNA 2
295,03 m2
1
TĚLOCVIČNA 1
295,03 m2
C 163
20,86 m2
6
14
12,29 m2
C 162
2,51 m2
WC
4
5
4
5
C 161
2,51 m2
WC
2
39,52 m2
3
40,47 m2
C 164
C 165
2,51 m2
WC
5
4
5
4
C 165
2,51 m2
WC
20,86 m2
6
12,29 m2
14
Zadní
vstup
C 160
13
177,58 m2
C 148
C 146
Na hřiště
C 159
13
Sklad
29,27 m2
C 158
7
Sklad
44,03 m2
C 157
C 156
8
Sklad
38,39 m2
C 155
C 154
9
Kabinet
28,98 m2
C 153
C 152
10
Učebna
69,22 m2
C 151
10
Sklad
23,96 m2
C 150
C 149
11
Učebna
68,01 m2
C 147
12
Úklid +
prádelna
43,1 m2
C 145
A 1NP
schodiště

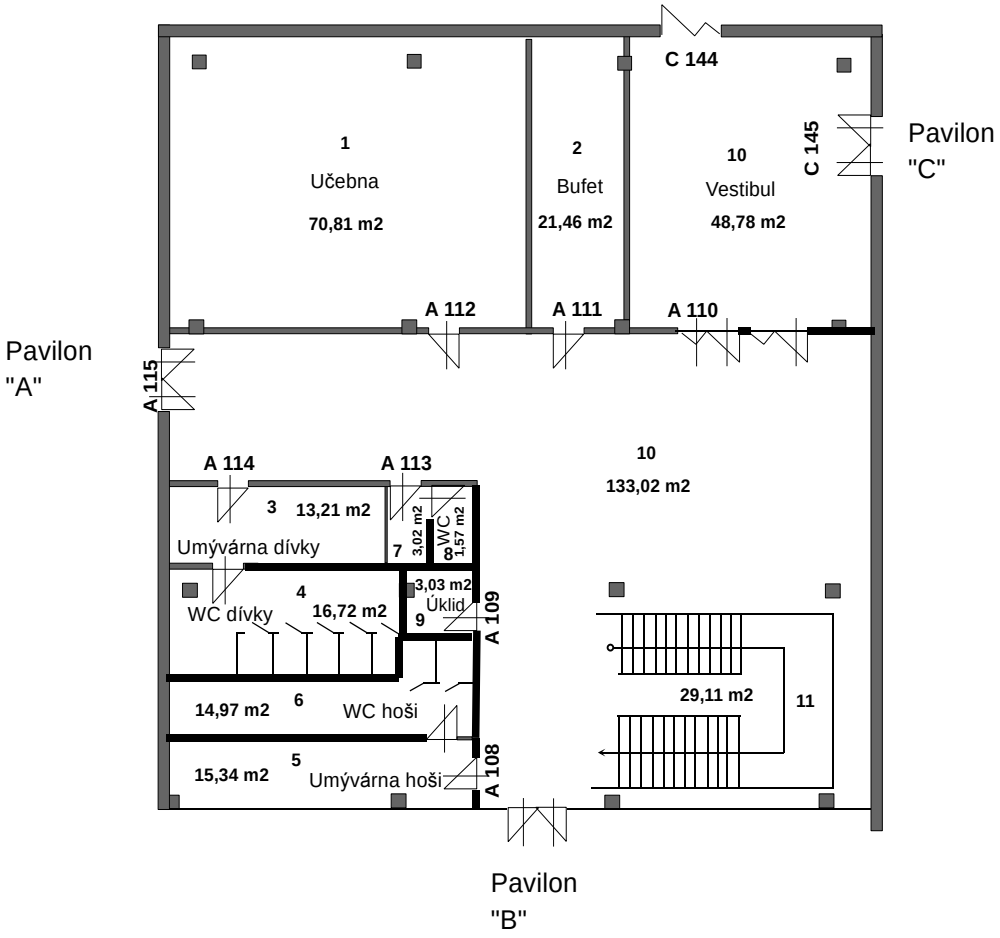
C 2NP

TD 3


Tělocvična 2
295,03 m2
1
Tělocvična 1
295,03 m2
1
11,52 m2
4
C 216
Balkon
49,69 m2
C 217
2
3
171,5 m2
2
49,69 m2
Balkon
C 218
C 219
11,52 m2
4
C 215
3
Šatna úklid
27,81
C 213
5
Šatna
20,39 m2
C 214
6
Sprchy
22,8 m2
6
Sprchy
22,8 m2
C 212
C 211
7
Šatna
20,49 m2
C 210
8
Knihovna
22,40 m2
C 209
9
Učebna
68,13 m2
C 208
10
Kabinet
24,20 m2
C 207
Sklad
10,1 m2
8
C 207a
Kabinet
12,3 m2
8
C 205
7
Šatna
20,49 m2
C 204
4,41 m2
WC
C 206
6
Sprchy
18,39 m2
C 203
4,56 m2
6
Sprchy
18,24 m2
C 202
C 201
5
20,39 m2
Šatna
C 200
3
Sklad
28,15 m2

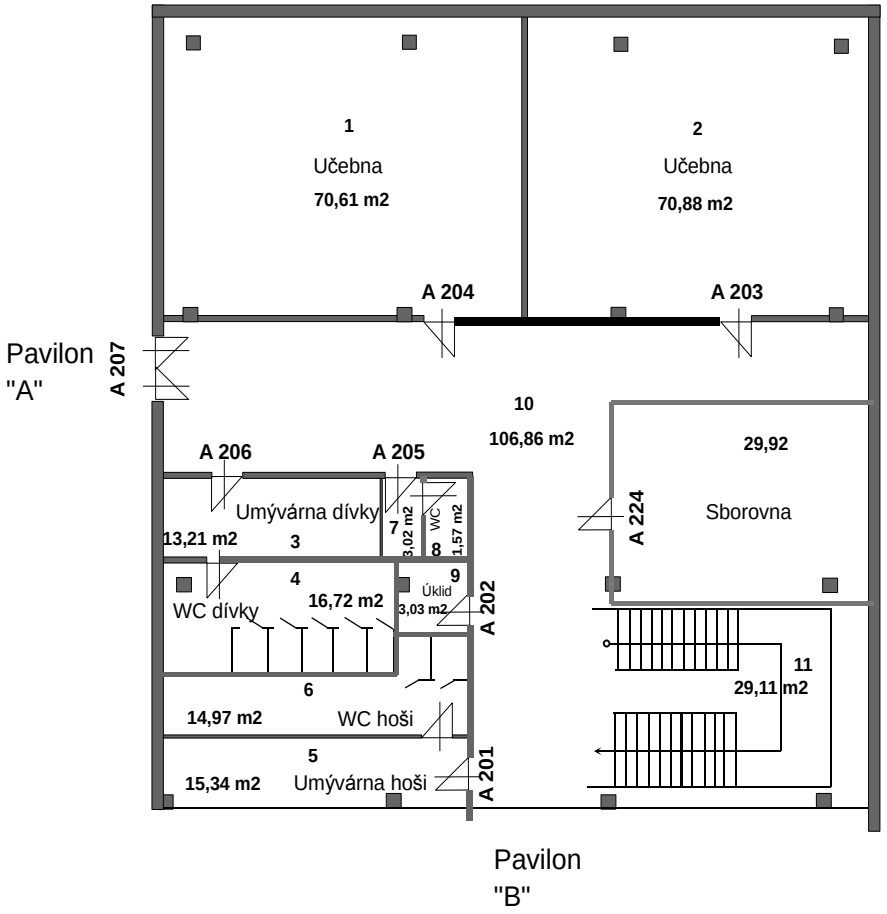
Schodiště A 1NP

UKV 14-0



Schodiště A 2NP

UKV 14-0



Schodiště A 3NP

UKV 14-0