Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Bakalářská práce

Bezpečnostní analýza školního informačního systému

Petr Firman

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Petr Firman

Zemědělské inženýrství
Informační a řídicí technika v agropotravinářském komplexu

Název práce

Bezpečnostní analýza školního informačního systému

Název anglicky

Security analysis of the school information system

Cíle práce

Primárním cílem práce je analyzovat vybraný informační systém konkrétní školy podle stávajících legislativních a normativních zásad. Na základě provedené analýzy a testů (včetně analýzy uživatelů) stanovit doporučení a návrhy na případná opatření.

Metodika

1. Úvod
2. Cíl práce a metodika
3. Výběr školy a informačního systému
4. Normy a legislativa spojená s analýzou IS
5. Návrh postupu řešení
6. Analýza a závěry
7. Doporučení a závěr
8. Finanční náročnost

Doporučený rozsah práce

30 až 40 stran textu včetně obrázků, grafů a tabulek

Klíčová slova

informační systém, bezpečnost, normy

Doporučené zdroje informací

BUCHALCEVOVÁ, A. *Metodiky vývoje a údržby informačních systémů : kategorizace, agilní metodiky, vzory pro návrh metodiky.* Praha: Grada, 2005. ISBN 80-247-1075-7.

SODOMKA, P. – KLČOVÁ, H. *Informační systémy v podnikové praxi.* Brno: Computer Press, 2010. ISBN 978-80-251-2878-7.

SVATÁ, V. *Audit informačního systému.* Praha: Professional Publishing, 2011. ISBN 978-80-7431-034-8.

ŠULC, V.: Kybernetická bezpečnost, Plzeň, 2018, ISBN 978-80-7380-737-5

VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE, – VOŘÍŠEK, J. – BASL, J. *Principy a modely řízení podnikové informatiky.* V Praze: Oeconomica, 2008. ISBN 978-80-245-1440-6.

Předběžný termín obhajoby

2019/2020 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 7. 1. 2019

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 15. 2. 2019

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 29. 03. 2020

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma Bezpečnostní analýza školního informačního systému vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí. Jsem si vědom že, na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

V Praze dne .....

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce Ing. Zdeňkovi Votrubovi, Ph.D. za konzultace, připomínky a cenné rady při vedení práce.

Bezpečnostní analýza školního informačního systému

Abstrakt:

Cílem práce je provedení analýzy školního informačního systému a návrh na modernizaci informačního systému ve vybrané škole. Návrh inovace vychází ze závěrů analýzy stávající školní sítě a vybraného informačního systému a reálných možností vybudování nové infrastruktury školní sítě.

Klíčová slova: bezpečnost, analýza, informační systém, síť, vyhláška, norma, škola,

Security analysis of the school information system

Abstract:

The aim of this work is to carry out an analysis of the school information system and a proposal for modernization of the information system in the selected school. The innovation proposal is based on the conclusions of the analysis of the existing school network and the selected information system and real possibilities of building a new school network infrastructure.

Keywords: security, analysis, information system, network, regulation, standard, school

Obsah

Seznam zkratek:

IS – informační systém

PC – počítač

SMS – služba krátkých textových zpráv

USB – univerzální sériová sběrnice (moderní způsob připojení periferií k počítači)

ICT – informační a komunikační technologie

GDPR – obecné nařízení o ochraně osobních údajů

EU – Evropská unie

ISMS – systém řízení bezpečnosti informaci

TPS - transakční systémy

MIS - informační systémy pro řízení

DSS - systémy pro podporu rozhodování

EIS - informační systémy pro vrcholové řízení

LAN – lokální síť

VLAN – virtuální LAN

DHCP – Dynamic Host Configuration Protocol (dynamické přidělování IP adres, masky sítě, implicitní brány a adresy DNS serveru)

DNS – Domain Name Systém

MAC – Media Access Control

SSID – Service Set Identiflier

WPA – Wi-Fi procted access, zabezpečení sítě Wi-Fi

MŠMT – Ministerstvo školství, mládeže a tělovýchovy

1 Úvod

Podle většiny lidí je 21. století významným obdobím lidstva. Vývoj informačních systémů a technologií téměř neustále roste. Počítače a digitální technologie nás obklopují všude kolem a ulehčují nám život. Dnes mají své nezastupitelné místo i ve školách, kde usnadňují učení dětem. Školy využívají různé softwarové vybavení, aby ulehčily práci sobě i samotným učitelům. Školy a celkově školský systém začíná být více závislý na informačních technologiích. Přínosem informačního systému je zefektivnit způsob učení a řízení škol. Učitelé více využívají mediální prostředky k výuce, k ověřování znalostí a komunikaci mezi sebou. Proto je kladen velký důraz na bezpečnost informačního systému.

Bakalářská práce je zaměřena na bezpečnostní analýzu školního informačního systému. V první teoretické části je charakterizován pojem informační systém. Další část je věnována problematice bezpečnosti informačního systému. Je uvedeno, co se skrývá pod pojmem bezpečnost informačního systému a jsou představeny pojmy s ním spojené, jako je autentizace, autorizace a ochrana dat.

V druhé praktické části je představena samotná škola a její informační systémy. Pomocí metody analýzy byly zjištěny přednosti a nedostatky stávajícího informačního systému. Pro prokázání nástrojů bezpečnosti informačního systému je do bakalářské práce zařazena i kapitola věnovaná právním normám a legislativě.

V závěru bakalářské práce je navrženo určité opatření ke zlepšení stávajícího informačního systému ve škole na základě provedené analýzy školního informačního systému a jeho složek. Hlavní přínos bakalářské práce spočívá v návrhu opatření ke zlepšení informačního systému a jeho bezpečnostním režimům. Zjištěné závěry budou předloženy managementu školy tak, aby jich bylo možno efektivně využít.

2 Cíl práce a metodika

Cílem mé práce bude bezpečnostní analýza školního informačního systému a zpracování návrhu efektivnější formy školního informačního systému včetně jeho bezpečnostních režimů.

V práci budou používány tyto metody:

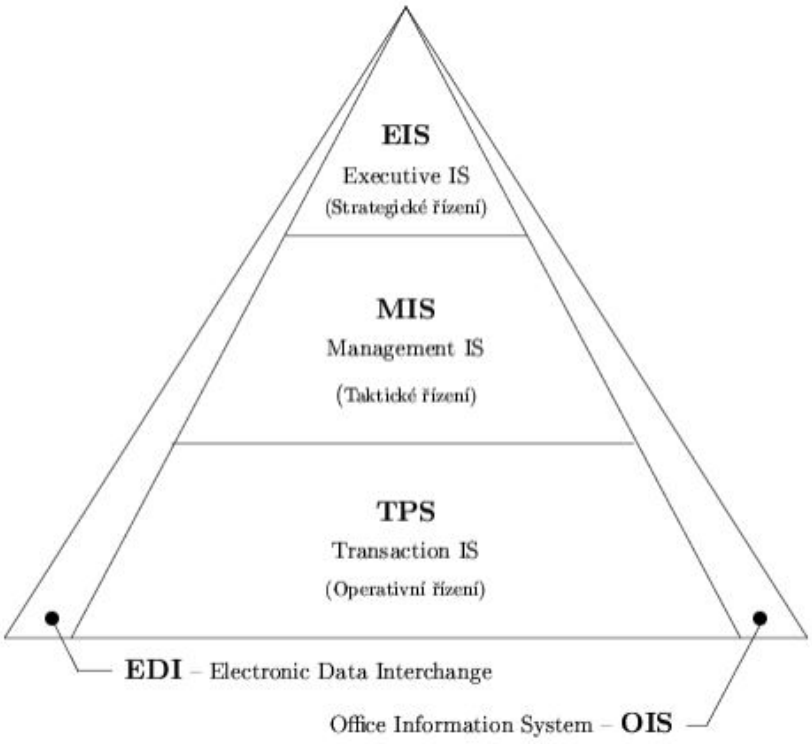
- analýza (zkoumání jednotlivých složek dané problematiky)
- kompilace (shromažďování souvisejících informací o dané problematice)
- komparace (srovnání)
- řízený rozhovor (tazatel pokládá otázky za účelem sběru dat).

3 Úvod do informačního systému

Pojem informační systém má mnoho definic. Dá se chápat jakou systém pracující s informacemi neboli s daty a s procesy. Je složený z hardwaru a softwaru, ke kterému patří i lidé. Využívá se k šíření informací sloužící k řízení, rozhodování a plánování. Charakteristickým rysem pro informační systém je sada programů daná do jednoho celku, který plní úkoly pro uživatele nebo organizace. Programy, které jsou v IS, běží na výkonném serveru a uživatelé k nim přistupují prostřednictvím počítače, notebooku, tabletu v režimu klient-server. Komunikace uživatele a serveru probíhá na dálku. [9], [10]

Aspektů, podle kterých můžeme rozdělit informační systém, je mnoho. Například od komplexnosti až po vztah k systému řízení uživatele nebo pak organizace. [9], [10]

Obr. 1 Pyramida rozdělení IS



Zdroj: https://docplayer.cz

Na nejvyšším stupni pyramidy jsou informační systémy, které řeší problémy organizace, u nichž je potřeba znalostí externích odborníků. Na nejnižším stupni pyramidy se nacházejí informační systémy, které zpracovávají konkrétní údaje organizace na úrovni úloh. [11], [13]

Informační pyramidu tvoří tyto informační systémy:

- Transakční systémy (TPS – Transaction Processing System) - TPS obsahují dávkové systémy, které zpracovávají úlohy, jako např. účetnictví, evidenci, skladové či rezervační systémy. Značná část informačních systémů, které jsou běžnými uživateli využívány v každodenním životě, jsou právě tohoto typu. [13]

- Informační systémy pro řízení (MIS – Management Information System) - jejich hlavní úkolem je zpřístupnit různé součtové sestavy nebo přehledy. [13]
- Systémy pro podporu rozhodování (DSS – Desicion IS) jsou nadstavbou pro MIS. Jejich cílem je zprostředkovat různé analýzy, aby řídící pracovníci mohli přijímat důležitá rozhodnutí. [13]
- Informační systémy pro vrcholové řízení (EIS – Executive IS) - jejich hlavním účelem je poskytnout důležité informace vedoucím pracovníkům, podle kterých by mohli učinit strategické rozhodnutí o budoucnosti organizace. Data, se kterými pracuje systém typu EIS, jsou většinou pořizována v systémech TPS a MIS. [13]
- Strategické informační systémy - tento typ systému se snaží o zvýšení konkurenceschopnosti podniku. Jsou spojeny přímo s výrobkem nebo výrobou. Příkladem je elektronická pošta. [13]
- Prognostické systémy - tyto systémy jsou tvořeny nástroji, které dovolují provádět analýzu typu „co když“ a tím vytvářet prognózy. Patří sem např. expertní systémy (ES), které jsou často považovány za zvláštní druh informačních systémů. [13]

3.1 **Informace**

Informace je aktivum, které vyžaduje určitou úroveň ochrany, protože jsou pro organizace důležité. Informace je možno uchovávat v několika formách, a to v digitální formě jako například datové soubory na elektronických nebo optických medií. Další forma je materiální, a to znamená informace napsaná na papíře. Poslední forma je jako nevyjádřená informace v podobě znalostí zaměstnance. Informace se dají přenášet, a to několika různými způsoby jako je například elektronickou nebo verbální komunikací nebo kurýrem. Informace mnoha organizací jsou závislé na informačních a komunikačních technologiích. Technologie jsou v organizaci podstatným prvkem a usnadňují vytváření, zpracování, ukládání, přenášení, ochranu a zničení informací. [11], [13]

Bezpečnost informací

Bezpečnost informace určují tři hlavní vlastnosti: dostupnost, důvěrnost a integrita informace. Aby byla dosažena úspěšná bezpečnost informace a minimalizované dopady incidentů, musí být použito vhodné opatření bezpečnosti informací zohledňující velký rozsah hrozeb. [5], [7], [8]

Bezpečnost IS

Dříve byla bezpečnost k složkám systému posunuta do pozadí, dnes se jedná o jednu z hlavních priorit informačních systémů. V současnosti se dynamicky vyvíjejí způsoby obrany a útoků, identifikují se původy hrozeb kyberteroristických útoků, analyzují se množství škodlivých kódů, rozlišují se způsoby na zajišťování webové bezpečnosti, shrnují se pozitiva i negativa a společnost se zaměřuje na problematiku ztráty elektronických dat více než kdykoliv předtím. [5], [7], [8]

Zde jsou uvedeny základní pojmy:

Bezpečný informační systém

- systém, kde je zajištěna důvěryhodnost a bezpečnost informací.

Autentizace

- je proces ověření identity subjektu.

Analýza rizik

- je rozbor současného stavu bezpečnosti informačního systému.

Aktivum

- je vše, co má pro subjekt hodnotu, která může být zmenšena působením hrozby.

Řízený přístup

- prostředky zajištující, aby přístup k aktivům byl autorizován a omezen na základě bezpečnostních požadavků.

Organizace

- osoba nebo skupina osob, které mají své vlastní funkce s odpovědností, pravomocemi a vztahy, pomocí nichž mohou dosáhnout svých cílů.

Školní informační systém

- je soubor lidí, metod a technických prostředků, zajišťujících sběr, uchování, analýzu a prezentaci dat vyhrazených pro poskytování informací v oblasti vzdělávání
- umožňuje zefektivnění fungování celé vzdělávací instituce
- jde převážně o izolované aplikace, ale současně o celkové komplexní systémy, které jsou navzájem kompatibilní
- může současně zahrnovat evidenci žáků a zaměstnanců, evidenci klasifikace, tisk vysvědčení a třídních výkazů, grafické zpracování prospěchu, přípravu úvazků, sestavení rozvrhu hodin, plánování akcí školy, suplování, inventarizaci majetku, rozpočet školy, evidenci knih v knihovně a jejich půjčování, tvorbu tematických plánů atd. [4]

Riziko

- jde o nebezpečí vzniku negativní odchylky od požadovaného cíle, dále se také může jednat o chybné rozhodnutí.

Kryptologie

- je nástroj ochrany dat, tzn. utajení dat, autentizaci, integritu informací.

Hrozba

- znamená možnost využití zranitelného místa informačního systému k útoku.

Bezpečnost informačních systému má dnes několik cílů:

- integrita informace (nesmí dojít ke změně obsahu dat)
- autentičnost informace (pravdivost dat)
- dostupnost informace (data jsou k dispozici oprávněné osobě)
- důvěrnost informace (obsah dat má k dispozici pouze oprávněný subjekt)
- nepopíratelnost (původ informace).

Ochrana přístupu k datům je založena na tom, aby do systému neměl přístup uživatel, který k tomu nemá dostatečná přístupová práva. Pro tento účel musíme tedy dostatečně ověřit identitu uživatele. Systém tedy potřebuje důkaz, že se jedná o tu osobu, která se za ni

prohlašuje. Před vlastní autentizací uživatele musí proběhnout identifikace, v níž uživatel potvrdí, že je skutečně tím, za koho se vydává. [5], [7], [8]

3.2 Bezpečnost a kvalita IS

Bezpečnost IS se stává jednou z klíčových vlastností informačních systémů. V současnosti se dynamicky vyvíjejí způsoby obrany, ale i možnosti útoků, jak proniknout do IS. Podoba dnešních počítačových útočníků je různá. Může to být bývalý nebo nespokojený zaměstnanec, konkurent, nudící se teenager nebo sofistikovaný hacker. Tyto typy útočníků používají různé metody a techniky k prosazení svých zájmů.

K hodnocení zabezpečení počítačových zařízení, systémů nebo aplikací se používají různá testování pomocí bezpečnostních testů.

Bezpečnostní testy reálně simulují pokus o kompromitaci IS s cílem zjistit, jaké škody by mohli nastat nebo jaké informace by mohli uniknout. Provádí se simulací možných útoků na IS jak zevnitř, tak zvenčí. Důležité je také, aby byl zvolen odpovídající rozsah testů. Sada bezpečnostních testů dokáže odpovědět na otázky, jak zranitelný daný informační systém skutečně je. Mezi obvyklé typy testů patří penetrační testy. [5]

Penetrační testy

Cílem penetračního testu není vyřešit bezpečnostní problémy, ale prověřit a zhodnotit úroveň zabezpečení. Tento proces zahrnuje podrobnou analýzu sytému se zaměřením na případné bezpečnostní nedostatky vycházející z chybného nastavení systému, známých či neznámých hardwarových a softwarových nedostatků nebo nedostatečných funkčních protiopatření. Využití penetračních testů je následující:

- určují zneužitelnost
- odhalují velké bezpečnostní nedostatky, které mohou vzniknout nahromaděním malých nedostatků
- odhalují nedostatky, které mohou být nezjistitelné automatickou detekcí
- testují schopnost odhalovat útoky a následně na to reagovat
- poskytují podklady pro zvýšení zabezpečení systému. [5]

Existuje několik základních kritérií, podle kterých se penetrační testy dělí, např.:

Komplexní nebo omezený - test zahrnuje část nebo celý IS.

Agresivní nebo opatrný - určuje, jaké techniky se použijí pro testování.

Skrytý nebo otevřený - podle rozsahu informací, které má tester o cílovém IS.

Black box nebo white box - množství informací, které má tester k dispozici.

Interní nebo externí - podle pozice útočníka/ testera vůči cílovému IS.

Další typy testů, které se používají:

Unit testy – jde o ověření kódu a jeho funkčnosti.

Integrační testy – testuje se, zda jednotlivé komponenty a moduly fungují dohromady.

Funkční testy – zkoumají, co systém opravdu dělá.

Objemové testy – ověřují schopnost systému zpracovat požadované množství dat v požadovaném čase.

Zátěžové testy – ověřují schopnost systému zvládnout velké množství současně pracujících uživatelů a spuštěných programů. [5]

Cílem bezpečnosti informačních systémů je dosáhnout přiměřené bezpečnosti. Důležité je slovo „přiměřená“ bezpečnost, neboť přehnané požadavky na kvalitu, zvyšují náklady na vývoj a na provoz aplikace. Nedostatečná kvalita aplikace může poškodit návrhy v ostatních dimenzích. Můžeme říci, že IS je kvalitní, pokud splňuje uživatelské požadavky a funguje bezpečně a spolehlivě. Tvůrce aplikace vydává opravy a bezpečnostní záplaty. V oblasti bezpečnosti se analyzují všechna bezpečnostní rizika, která mohou bezpečnost aplikace ovlivnit. [8], [9]

Nejčastější neoprávněné přístupy jsou:

- neoprávněný přístup k funkcím a datům
- odcizení dat
- zničení dat.

Nejznámější techniky a nástroje, které zabrání neoprávněnému uživateli využívat funkce a data IS je kontrola přístupových práv. Identity management je velice vhodným konceptem přístupových práv, využívá tzv. „single sign on“, který zajišťuje, že všichni uživatelé školního IS používají ke všem aplikacím IS pouze jednu autentizaci (obvykle uživatelské jméno nebo heslo). Uživatelské jméno a heslo není pro některé aplikace dostatečným prokázáním totožnosti uživatele. Pro zjištění totožnosti uživatele se používají další techniky a nástroje, jako je například SMS na uživatelův telefon s jednorázovým přístupovým kódem nebo čtečka otisku prstu či čtečka zornice oka.

Mezi techniky, které mají zabránit odcizení nebo zničení dat patří: ochranný prostor výpočetního střediska/datového centra před vstupem neoprávněné osoby, ochranný prostor datového centra proti požáru a povodni, ochrana proti výpadku elektrické energie (záložní baterie a generátory). [8], [9]

3.3 **Autentizace**

Autentizace ověřuje identitu člověka porovnáním jednoho nebo více faktorů s databází platných identit. Schopnost subjektu a systému zachovat mlčenlivost o ověřování faktoru pro identity přímo odráží úroveň bezpečnosti tohoto systému identifikace a autentizace. Oba pojmy jsou vždy společně jako jeden s dvěma kroky procesu. Poskytování identity je první krok a poskytování autentizačních faktorů vede ke kroku druhému. [6], [9], [10]

Rozlišujeme autentizaci:

- entity (osob, programů)
- dat.

Svoji identitu na úřadech jako je např. banka, pošta a další úřady již prokazujeme občanským průkazem. V elektronickém světě, kde je nejrozšířenější způsob jak prokázat identitu, je to jméno a heslo. Tento způsob však není bez rizik. Například uživatelská hesla mohou být narušena špionskými programy tzv. keyloggery, přihlašovacími okny na podvržených webových stránkách, phishingovými útoky, metodou sociálního inženýrství a dalšími

způsoby. Je tedy potřeba na všech internetových systémech zajistit bezpečnost ověřování identity především přístupných z veřejného internetu. Dnes se využívá informační systém datových schránek. Existuje několik způsobů jejich zabezpečení, jako je například osobní certifikát, jednorázový kód nebo SMS zpráva. Datová schránka umožňuje zprávy přijímat, ale také podávat zprávy vůči orgánům veřejné správy. V dnešní době spousta uživatelů bezpečnost datových schránek neřeší. To pak může vést k tomu, že se útočník zmocní přístupového hesla a může jednat za pravého uživatele, který tak snadno přijde o svá data. [6], [9], [10]

Pro autentizaci je třeba pravidelného zálohování dat. Jejich archivování je vhodné provádět na dvou fyzicky odlišných místech v případě požáru. Zároveň je doporučeno zvolit vysokou úroveň bezpečnosti ověřování identity. K tomu slouží tzv. dvou faktorová autentizace. K tomuto zabezpečení se používá USB tok nebo čipová karta s certifikátem. Uživatel vlastní tzv. token a současně zná jeho PIN kód. [6], [9], [10]

3.3.1 **Autentizace pomocí hesla**

Tato technika je nejvyužívanější a nejrozšířenější v dnešní době a její podstatou je zadávání přihlašovacího jména a hesla. Použití hesel funguje na principech kryptografie a jejich ukládání v šifrované podobě. Dále se musí nastavit určitá kvalita hesla. Kvalita se určuje podle počtu zvolených znaků a délky hesla. Uživatel předkládá systému heslo, které je řetězcem znaků společně se svou identifikací (loginem). Dnes je tato metoda zabezpečení viděna ve velkém množství aplikací. Doporučovaným způsobem pro zvyšování bezpečnosti hesla je kombinace všech znaků. Kombinují se malá a velká písmena společně s čísly a dalšími znaky jako je například pomlčka nebo podtržítko či tečka. [6], [9], [10]

Hesla se dělí na statická, jednorázová a dynamická. Jsou běžnými prostředky identifikace na základě znalostí osobních identifikačních čísel nebo kódů. Dynamická hesla zčásti odstraňují nedostatky statických hesel. Při každém přihlášení se heslo generuje dle stanoveného algoritmu a nemůže být znovu použito. Jednorázová hesla (one-time pasword - OTP) platí

pouze pro jeden login nebo jednu transakci. Výhoda jednorázových hesel spočívá v tom, že jsou odolná proti tzv. replay útokům. [6], [9], [10]

3.3.2 Autentizace pomocí tokenů

Autentizační token je zařízení, pomocí něhož se může uživatel přihlásit do systému. Pro přihlášení je podmínkou mít dané zařízení v době přihlašovaní u sebe. Token je zařízení, jehož podoba má několik druhů. Mezi nejběžnější druhy patří čipové a paměťové karty, USB tokeny a autentizační kalkulátory. Všechny tokeny mají funkci, která umožnuje uložení citlivých údajů na sofistikovaná zařízení. Tokeny nabízejí obecně bezpečnější a efektivnější metodu autentizace oproti heslům a společně s biometrikami jsou považovány za silné autentizační metody. [6], [9], [10]

Paměťové karty

Jedním z příkladů tokenů jsou paměťové tokeny, které uchovávají informace. Je to speciální čtecí a zapisovací zařízení, které kontroluje psaní a čtení dat z a do tokenu. Jedná se magnetickou kartu s tenkým proužkem magnetického materiálu umístěného na povrchu karty. [6], [9], [10]

Mobilní zařízení

Dalším běžným příkladem tokenů jsou mobilní zařízení. Jsou využívány jako ověřovací zařízení. Mají funkci vícefaktorového ověření a uživatel tudíž nepotřebuje vlastnit žádné další fyzické zařízení. Někteří prodejci nabízí toto řešení, které používá šifrovací klíč pro autentizaci. Ten poskytuje vysokou úroveň bezpečnostní ochrany. [6], [9], [10]

3.4 Autorizace

Je to proces, kde uživatel získává oprávnění k vykonání určitých funkcí IS v organizaci. Autorizace umožnuje strukturovat oprávnění jednotlivých uživatelů informačního systému. Například v systému Bakaláři, kde jsou odděleni uživatelé podle pravomocí a rolí. Do jeho

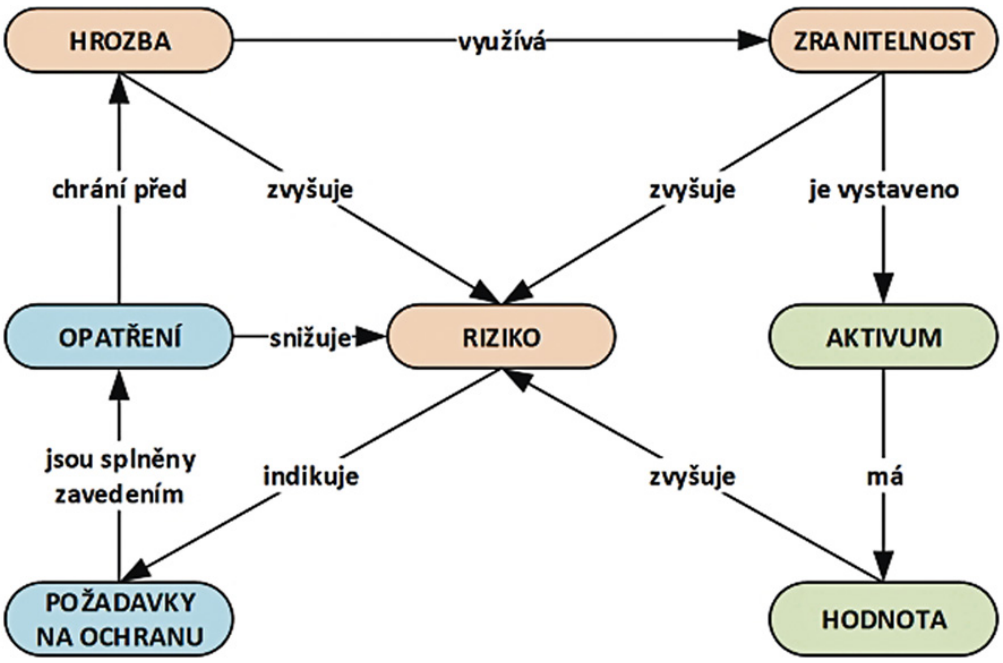
modulu elektronická žákovská knížka má přístup učitel i žák. Učitel zapisuje známky a žák na ně může pouze nahlížet.

Uživatelské účty v systémech spravovat je obtížná, ale důležitá věc. Jedná se tak o nástroj k řešení přístupu do systému. Další využití je k auditu i kontrole zdrojů. Ve správě účtů je dobře vidět, kdo co dělá v dané aplikaci, a k jakým informacím se může dostat. [6], [9], [10]

3.5 Ochrana dat

Bezpečnost dat je v každém ohledu specifická. Proces zabezpečování informačního systému ve školském zařízení nebude nikdy ukončen, protože je potřeba ho neustále zdokonalovat na nové zavedené technologie. [8], [9], [10]

Obr. 2 Přehled schémat rizik



Zdroj: https://m.systemonline.cz

3.5.1 **Zranitelná místa**

Zranitelnými místy nazýváme slabinu informačního systému, kde dochází ke vzniku škod nebo ztrátě dat. Tato místa vznikají důsledkem chyb, selhání v analýze nebo návrhu IS. Další příčiny mohou být způsobeny velkým množstvím uložených informací, složitostí software a skrytými kanály pro přenos dat. [8], [9], [10]

Zranitelná místa mohou být:

- fyzická místa, která jsou snadno dostupná k sabotáži
- přírodní faktory typu požár, záplava, zemětřesení a blesk
- lidský faktor, který představuje největší zranitelnost ze všech možných variant
- v návrhu IS
- specifické požadavky, které systém může splnit a může mít všechny bezpečnostní rysy dle určených požadavků, ale stále obsahuje zranitelná místa
- v konstrukci IS, kde do něj byla implementovaná zranitelná místa v důsledku špatných konstrukčních standardů nebo zvoleného návrhu
- v provozu, kde sice funguje správně, ale ve výsledku byl použitý neadekvátní provozní nástroj.

3.5.2 **Hrozba**

Pojem hrozba označuje okolnost, událost či osobu, která působí na zranitelné místo systému. Může způsobit různá poškození, zničení, ztrátu důvěry nebo potenciální škodu na aktivu. Škoda způsobená hrozbou se nazývá dopad hrozby.

Charakteristickými prvky hrozby jsou její vnitřní či vnější zdroj, motivace potenciálního útočníka, získání konkurenční převahy a frekvence uplatnění hrozby. [8], [9], [10]

Hrozby lze dělit na:

Subjektivní hrozby

- úmyslné, které představují vnější útočníci (špioni, teroristé, hackeři) a vnitřní útočníci (vlastní zaměstnanci).
- neúmyslné (nezaškolený uživatel či správce).

Objektivní hrozby

- fyzikální (elektromagnetické vyzařování)
- přírodní, fyzické (požár, povodeň, poruchy)
- logické nebo technické (špatné propojení komponentů, porucha paměti).

3.5.3 **Opatření**

Opatření je postup, který se vytvořil pouze za účelem zmírnění působení hrozby, snížení zranitelnosti nebo dopadu hrozby. Je to návrh kroků, kterými se má předcházet vzniku škody. Charakteristickými rysy je efektivita a náklady. Do nákladů na opatření se započítávají náklady na pořízení, zavedení a provozování opatření. Společně s efektivitou opatření jsou tyto náklady důležitými parametry při výběru opatření. [8], [9], [10]

3.5.4 **Riziko**

Pod pojmem riziko si představíme pravděpodobnost využití zranitelného místa. Charakteristickým rysem je pravděpodobnost výskytu bezpečnostního incidentu a potenciálně způsobená škoda. Jeden z nejdůležitějších aspektů v oblasti bezpečnosti IS je analýza rizik. Jejím cílem je identifikace a odstranění událostí, které ohrožují organizace. Dalším cílem je zjištění rizik a možných škod, které mohou nastat a zároveň odstranění škod a minimalizace nákladů na odstranění. [8], [9], [10]

Provedení analýzy rizik musí být důkladné. Když se provádí analýza, je dobré seskupit aktiva do skupin. Provede se jejich inventura a stanoví se reálná hodnota aktiv. Podle hodnoty aktiv a zhodnocení možných škod se stanoví úroveň hrozeb a zranitelností pro

všechna aktiva. Výsledkem analýzy je určení, kterým hrozbám informační systém čelí. [8], [9], [10]

Analýzu rizik rozdělujeme na:

- orientační analýza rizik – patří do celkového budování bezpečnostní politiky. Výsledkem je rozhodnutí, která z následujících čtyř analýz se použije.
- elementární analýza rizik - přebírá opatření z podobných systémů a norem. Tato analýza je specifická v tom, že věnuje minimální finanční a časové náklady na provedení analýzy. To může mít za následek zvolení příliš silného a drahého opatření nebo naopak.
- neformální analýza rizik – v této analýze se projevují znalosti odborníků na bezpečnost. Oproti předešlé analýze je zde vynaloženo málo finančních a časových nákladů na provedení analýzy rizik a případně jejich opatření.
- detailní analýza rizik – jejím charakteristickým rysem je malá pravděpodobnost přehlédnutí rizik. Analýza se provádí za použití normalizovaných metod.
- kombinovaná analýza rizik – tato analýza je kombinací uvedených předchozích analýz.

Obr. 3 Analýza rizik

Zdroj: https://www.cleverandsmart.cz

4 Škola a informační systém

Pro bakalářskou práci byla vybrána Základní škola J. A. Komenského v Mostě, protože jsem byl jejím žákem. Díky tomu znám její prostředí a bylo mi umožněno získat dané podklady ke zpracování analýzy jejího informačního systému.

4.1 Základní charakteristika školy

Základní škola J. A. Komenského v Mostě byla postavena a otevřena v roce 1985 na betonovém panelovém sídlišti o velikosti středně velkého města jako pavilonová škola, tvoří ji centrální pavilon, spojovací chodba, a čtyři další pavilony. Protože je budova umístěna uprostřed sídliště, je docházková vzdálenost žáků minimální. Navíc není v okolí školy dopravní síť, což zvyšuje bezpečné prostředí pro její žáky a zaměstnance. Pro velký počet žáků na sídlišti byla projektovaná kapacita školy (620 žáků) stále překračována. Až v roce 2004 poklesl počet žáků a tím i počet tříd. Poklesem počtu žáků došlo k optimálnímu naplnění školy.

Od roku 1992 zaujímá škola významné místo v celostátním projektu „Škola podporující zdraví“. Vedení školy s pedagogickými pracovníky zpracovali svůj vlastní program, který nastínil hlavní cestu v její transformaci. Pedagogičtí pracovníci začali spolupracovat s ostatními školami, které spojovaly hlavní myšlenkové linie: zpřístupnit školu dítěti, otevřít školu životu, vytvořit školu přirozenou, smysluplnou tak, aby vzniklo zdravé prostředí k plnohodnotnému životu a kvalitní práci. Škola podporující zdraví je založena na demokratických principech vedoucích k podpoře učení, osobnostního i sociálního rozvoje a zdraví. Program podpory zdraví je ve škole založen na třech pilířích – pohoda prostředí, zdravé učení, otevřené partnerství.

Škola je charakteristická svým bezpečným, klidným a příjemným prostředím. Pedagogičtí pracovníci při výuce používají efektivní metody a formy práce inspirované různými pedagogickými směry. Zvýšenou pozornost věnují práci s informacemi, zdravému životnímu stylu včetně vytváření podmínek pro větší možnost přirozeného pohybu žáků.

Vzdělávání žáků probíhá podle rámcového vzdělávacího programu určeného ministerstvem školství, mládeže a tělovýchovy pro základní školy. Vedení školy a pedagogičtí pracovníci ho rozpracovali do školního vzdělávacího programu pod názvem RADOST – ÚSPĚCH - ZDRAVÍ, podle kterého se ve škole vzdělává ve všech ročnících.

Pracovníci školy se zaměřují na to, aby škola byla školou bezpečnou a nabízela žákům a jejich rodičům takový program, ve kterém se mohou realizovat a být spokojeni, úspěšní a šťastní všichni žáci bez rozdílu. Reagují na současný vývoj ve společnosti.

Škola je přístupná všem dětem bez rozdílu. A tak se vedle sebe učí děti běžné populace, děti nadané i děti se speciálními vzdělávacími potřebami. Ve škole funguje školní poradenské pracoviště, žákům a jejich rodičům poskytuje služby speciální pedagog, výchovný poradce a metodik prevence.

Ve školním roce 2019/2020 školu navštěvuje 523 žáků, z toho 15 dětí je v přípravné třídě.

Na 1. stupni je 13 tříd a na 2. stupni 12 tříd. V pavilonech je 31 učeben. Žáci 1. – 5. ročníků mají své kmenové učebny. Učebny pro žáky 6. – 9. ročníků jsou zaměřeny a vybaveny dle předmětu, jehož výuka zde převládá. Odborných učeben je 8, z toho jsou dvě odborné učebny pro výuku ICT. Mezi další odborné učebny patří učebna fyziky, chemie, výtvarné výchovy, dílny, kuchyňka, keramická dílna. V pavilonu pro mimoškolní činnost jsou dvě tělocvičny, knihovna, přípravná třída, školní družina a školní klub. Všechny pavilony jsou zasíťovány. Síť je rozvedena do tříd, kabinetů a kanceláří, do školní jídelny, družiny i klubu pomocí kabelů. Pro výuku ICT a dalších předmětů škola využívá dvě počítačové učebny s počítači připojených do školní sítě. Jedna učebna disponuje 12 počítači značky Acer typu All in one. Ve druhé učebně je 15 počítačů značky HP typu stolní počítač. Pro přístup do těchto počítačů žáci využívají univerzální heslo. Učitelé mají pro svojí práci k dispozici školní notebook. Každý uživatel notebooku dostal přidělené heslo od správce počítačů. Notebooky jsou různých značek například HP, Asus, Acer. Dále při výuce využívají 18 interaktivních tabulí, 12 dataprojektorů a 15 tabletů. Mezi ostatní pracovníky, kteří používají notebook, patří ředitelka školy a dva zástupci ředitele. Stolní počítače mají v kanceláři zástupce ředitele pro ekonomiku, sekretářka, vedoucí školní jídelny, vedoucí školní družiny

a jeden je umístěn v odborné učebně – v hudebně. Ve školním klubu mají žáci k dispozici 4 stolní počítače a vychovatelka využívá svůj notebook. Veškeré vybavení výpočetní techniky má na starosti v dané škole správce, který je současně i ICT koordinátor. Vede evidenci počítačů a další ICT techniky, předává a eviduje přístupová hesla. Dále má odpovědnost za jejich bezpečnost a zabezpečení. Škola k tomu využívá antivirový program ESET Endpoint Antivirus.

Škola je bezdrátově připojena k internetu prostřednictvím Wifi. Tu nejvíce využívají žáci ve školním klubu a někteří učitelé podle jejího dosahu.

Celkovou síť ve škole spravuje externí firma HSC Computers s.r.o. Její službu pro školu zařizuje zřizovatel a také finančně přispívá na její činnost.

Jedním z dalších informačních systémů školy jsou webové stránky. Přes 20 let měla původní verzi webových stránek vytvořenou ve WINDOWS FrontPage. Tyto stránky celé sestavil a spravoval zástupce ředitele školy. V programu vytvořil základní schéma, graficky zpracoval vstupní plakát a nastavil odkazy např. prolink na Bakaláře, na rajce.net s fotkami, na participující organizace a další. Celý model byl postaven na indexu na HDD v PC. Prostřednictvím poskytovatele internetu byl vytvořen webový prostor, na nějž byla uploudovaná data prostřednictvím FTP protokolu.

V roce 2018 došlo k výměně managementu školy a byl zadán pokyn k jejich obnově. Od září 2019 má škola nové webové stránky, které jim sestavila podle jejich požadavků firma NEXU s.r.o. K administraci webu se používá intuitivní a rychlý redakční systém CMS. Jejich hlavním správcem je opět zástupce ředitele školy. Součástí webových stránek jsou povinné dokumenty. Mezi ně patří:

- koncepce rozvoje školy
- rozpočet školy
- střednědobý výhled
- výroční zpráva o činnosti školy
- výroční zpráva o poskytování informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím v platném znění
- školní řád

- klasifikační řád
- informační memorandum o nakládání s osobními údaji – GDPR.

K jednotlivým úsekům školy mají přístup další vedoucí pracovníci a to např. vedoucí školní družiny a klubu, vedoucí školní jídelny, za poradenské pracoviště – kariérní poradce, metodik prevence, speciální pedagog a další. Přístup k jednotlivým třídám pak mají třídní učitelé. Každý uživatel se přihlašuje pomocí uživatelského jména a hesla. Příslušné údaje generuje daná externí firma NEXU s.r.o. a předá je správci k užití.

Třídní blog a jednotlivé úseky školy se mohou spravovat jak ve škole, tak i z domova z jakého-li počítače přes webové rozhraní. Webové stránky se automaticky přizpůsobí chytrým telefonům a tabletům. Zálohu provádí firma, která je vytvořila. Také je možné je průběžně doplňovat novými prvky. O jejich vložení musí hlavní správce požádat tvůrce daných webových stránek.

4.2 Informační systémy ve škole

Škola nemá jednotný informační systém. Využívá několik různých systémů pro určitá odvětví ve škole:

- Bakaláři (https://www.bakalari.cz/)
- VeMa – systém na zpracování mezd a personalistiky (https://www.vema.cz/)
- MRP – systém, který škola používá na zpracování účetnictví (https://www.mrp.cz/)
- VIS – Veřejná informační služba - stravovací systém (https://web.visplzen.cz/produkty/stravovaci-systemy/)
- webové stránky (https://www.mostzs15.cz/
- mailové služby: Office365 (https://www.office.com/)

4.2.1 Charakteristika školní sítě

Stávající Wi-Fi infrastruktura nepokrývá celou školu dostatečně. Je postavena na UBNT technologii a řízena základním, jednoduchým controllerem. Uživatelům jsou přidělovány IP

adresy z DHCP hlavního routeru podle konkrétních pěti VLAN. Jako hlavní router školy je používán Mikrotik RB951G-2HnD. Na routeru bylo zřízeno pět VLAN pro jednotlivé segmenty sítě. Každá VLANa má svůj vlastní DHCP rozsah.

Rozdělení VLAN je uvedeno v příloze 1.

Kabelová síť pokrývá školu lépe, ale je odpovídající době vzniku a postupnému rozšiřování podle aktuální potřeby, viz schémata v příloze 2. Datové přepínače jsou většinou volně přístupné a jsou sériově zapojeny, což není vhodné. Jediná ochrana nastavení SWITCHů jsou již zmíněné VLANy. V této podobě nelze zabránit tomu, aby žák nebo učitel vypnuli SWITCH a tím způsobili řetězový výpadek datové sítě v návazně připojených SWITCHích. Datové přepínače jsou staré 5 až více let. Nedosahují odpovídajících přenosových rychlostí a neumožňují podrobný monitoring datové sítě.

Datová síť zahrnuje dva stávající datové rozvaděče. Hlavní rozvaděč je umístěn v počítačové učebně PC1, kde jsou uloženy i servery a hlavní přívod internetu. Servery jsou zabezpečené antivirovým programem ESET File Security. Starý datový rozvaděč se nachází v učebně PC2.

Kabeláž není vždy ukončena datovou zásuvkou. Také nejsou známé délky kabelů. V propojení pavilonů jsou délky vzhledem ke stáří kabeláže již nevhodné a to pro dosahování vyšších přenosových rychlostí.

Filtrování nežádoucího obsahu z Internetu je řešeno externí službou OpenDNS, ve které je možné třídit kategorie a URL adresy s nežádoucím obsahem.

Elektronické podpisové certifikáty jsou uloženy na zabezpečených médiích TokenMe. Mají je všechny odpovědné osoby v managementu školy, zástupce ředitele školy pro ekonomiku, vedoucí školní jídelny a sekretářka. Při aplikaci elektronického podpisu je nutné mít token v PC a znát příslušný PIN kód.

Pro mailové řešení využívá škola Microsoft Office 365 plán A1, který je pro školy zdarma. V rámci multilicence může škola využít i placené plány A3 for Faculty.

Bezpečnostní prvky systému a školní sítě:

Pro stávající informační systém a školní síť jsou stanovena následující pravidla:

- pravidelně jsou aktualizovány počítače a mobilní přístroje ve školní síti

- jsou nastaveny síťové bezpečnostní prvky - firewall, proxy apod., a jsou pravidelně aktualizovány
- do části školní sítě s instalací systému Bakaláři mají přístup pouze oprávnění zaměstnanci školy
- jsou nastavena práva přístupů do školní sítě až do úrovně adresářů
- veškerý potřebný software na školní počítače instaluje pouze IT specialista nebo pověřená osoba
- uživatelé mají zakázáno používání vlastních přenosných paměťových zařízení (Flash disky, CD…) nebo jsou poučeni o bezpečném zacházení, aby se eliminovala možnost zanesení virů do školní sítě
- každý uživatel pracuje na počítačích ze svého vlastního účtu, není využíván žádný společný účet
- nikdo nepoužívá k běžné práci systémový či administrátorský účet
- uživatelé jsou poučeni o opatrnosti při práci s maily - otvírání neznámých příloh, posílání osobních údajů atd.
- aktuální data jsou pravidelně zálohována pro omezení možnosti ztráty
- soubory a složky záloh jsou zabezpečeny proti neoprávněné manipulaci.

4.2.2 **Charakteristika informačního systému Bakaláři**

Bakaláři je informační systém, který obsahuje různé moduly pro správu školy. Program je určen jak pro management školy, tak pro jednotlivé pracovníky, rodiče i žáky. Umožňuje propojení s několika jinými programy pro převod dat z jiných systémů až po individuální úpravy dle požadavků.

Škola začala využívat informační systém Bakaláři od roku 1997, kdy ještě nebyl na trhu takový výběr informačních systémů, jako je v současné době. Do roku 2004 pomocí Bakaláře zavedla evidenci žáků i zaměstnanců školy a využívala modulu pro tisk vysvědčení. Od roku 2005, kdy začal ve školství probíhat tzv. sběr dat, rozšířila jeho nabídku

o školní matriku. Informační systém se vyvíjel, rozšiřoval a nabízel nové moduly pro potřeby školy. Velkým přínosem je modul pro tvorbu rozvrhu. Ve škole ho sice nepoužívají při jeho generování, ale po sestavení rozvrhu pak vloží data do Bakaláře a rozvrhy pro učitele, žáky a učebny se mohou vytisknout. Modul suplování a týdenní plán akcí používá zástupce ředitele školy. V dalších letech provedli rozšíření sítě z kabinetů i do učeben a tak zahájili nový modul třídní knihy a školní docházku v elektronické podobě.

Vzhledem k tomu, že se učitelé začali v tomto prostředí informačního systému dobře pohybovat, rozhodli se využít modulu elektronické žákovské knížky. Ta se využívá pouze však od 5. až do 9. ročníku. V souvislosti s využíváním Bakaláře pro klasifikaci se zpřístupnilo webové rozhraní pro rodiče. Rodič zde uvidí docházku a známky svého dítěte. Postupně začali učitelé používat i další moduly např. omluvenky, zadávání domácích úkolů, rychlou komunikaci s rodiči. Posledním modulem, který škola využívá je evidence školních úrazů.

Při rozhovoru s ředitelkou školy mi byla sdělena informace, že právě zakoupili nový modul informačního systému ZápisyOnline. Důvodem nákupu tohoto modulu byla situace, jenž nastala v naší republice. Všechny školy se uzavřely díky rozšíření nákazy koronaviru COVID – 19. Na základě nařízení MŠMT se bude konat zápis dětí do 1. tříd bez přítomnosti dětí.

Celý informační systém Bakaláři ve škole má na starosti jedna osoba a tou je učitel ICT, což je současně správce, koordinátor ICT a poradce informačního systému Bakaláři. Další oprávnění mají ředitelka školy a její zástupce. Pro přístup do Bakaláře všichni používají přihlašovací jméno a heslo, které generuje správce.

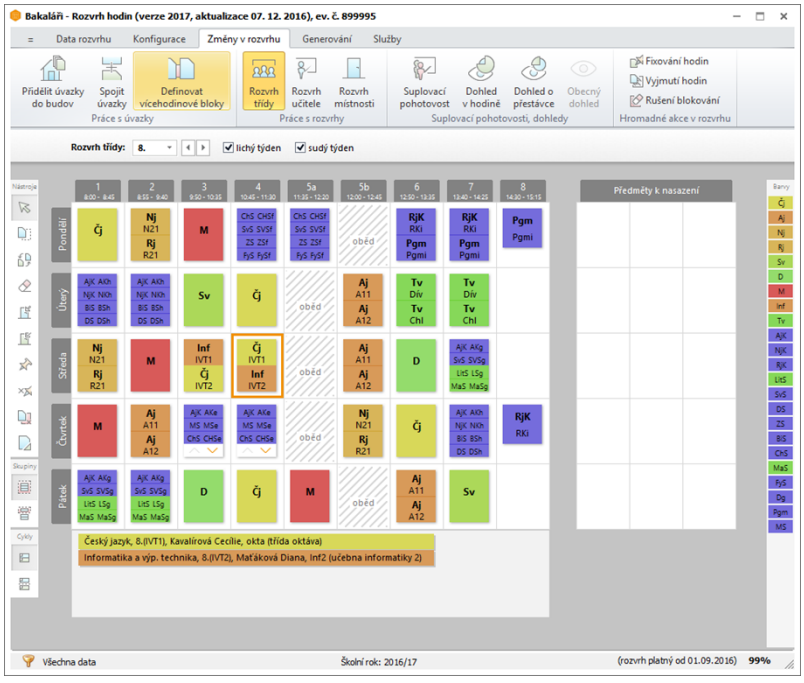
Bezpečnostní prvky softwaru Bakaláři:

- je nainstalována aktuální verze Bakalářů včetně nejnovějších průběžných aktualizací
- aktuální data jsou uložena na SQL serveru, kde ručí za bezpečnost poskytovatel serveru, firma HSC Computers s.r.o.
- webový přístup je provozován zabezpečeně přes https protokol

- od uživatelů je vyžadována vysoká složitost hesla (nejméně 8 znaků, nejlépe 12-14 znaků)
- uživatelé jsou poučeni o zacházení s hesly (nesdělovat, nepsat na pomocné papíry, pravidelně měnit)
- doporučuje používat dodatečné bezpečnostní prvky (např. počítače v zamčených kabinetech, pro přihlášení přístupové karty)
- je nastaven mechanismus na předávání hesla rodičům a žákům (a jeho změnu)
- jsou správně nastavena práva dle funkcí v systému Bakaláři včetně správného nastavení práva přístupu k jednotlivým položkám osobních údajů
- je nastaveno automatické odhlašování tam, kde je to možné (Portál, Třídní kniha)
- uživatelé jsou instruováni o nutnosti zamykání počítače vždy, pokud je bez dozoru
- pokud to není nutné, nikdo nepoužívá k běžné práci administrátorský účet Správce systému Bakaláři
- je pod kontrolou seznam všech uživatelů, kteří mohou do systému vstupovat, a je definován způsob, jak tento seznam udržovat.

Zde je ukázka z modulu Rozvrh informačního systému Bakaláři.

Obr. 4 Rozvrh



Zdroj: https://www.bakalari.cz

5 Normy a legislativy

5.1 GDPR

Je to právní rámec ochrany osobních údajů s cílem hájit práva občanů EU proti neoprávněnému zacházení s jejich osobními údaji. Týká se to jednotlivců, organizací, firem, online služeb jako jsou e-shop a všech institucí. GDPR je zkratka pro General Data Protection Regulation. Česky to přeložíme jako Obecné nařízení o ochraně osobních údajů. [18]

Důvod vzniku

V roce 1995 začala platit směrnice na ochranu osobních údajů, která se postupem doby stala zastaralou. V dané době ještě neexistovali sociální sítě, e-shop, cloudová uložiště a mnoho dalších technologií. Dalším důvodem bylo, že některé tajné služby států mimo Evropu shromažďovaly údaje o občanech EU v poměrně velkém měřítku. To mělo za následek, že v roce 2018 začalo platit nařízení GDPR. Dalším aspektem vzniku GDPR bylo obchodování s osobními údaji. Osobní údaje se získávají registrací na webu nebo při nákupu na internetu. Osobní údaje na facebooku jednoho člověka se ohodnocují průměrně na 1000 dolarů a jejich cena stále roste. Hodnota osobních údajů vytváří velkým korporacím zisk, protože pak odesílají jako zpětnou vazbu cílené reklamy nebo realizují telefonní hovory, kde různé společnosti nabízí své služby. Ke společnostem, které obchodují s osobními údaji, patří například UPC, T- Mobile, O2 či jiné velké společnosti, například distributoři energií.

Osobní údaje

V GDPR jsou definovány jako informace vztahující se k identifikované nebo identifikovatelné osobě. Obecné osobní údaje jsou jména, pohlaví, věk, osobní stav a datum narození, dále ještě IP adresa a fotografie. Protože se to vztahuje i na podnikatele, patří tam rovněž organizační údaje. Mezi ně se řadí e-mailová adresa, telefonní číslo nebo a údaje vydané státem. Speciální pozornost na zpracování osobních údajů upoutává kategorie s údaji o rasovém či etnickém původu, politických názorech, členech odborové organizace, o zdravotním stavu, náboženského nebo filozofického vyznání, sexuální orientaci a trestních

provinění nebo pravomocně odsouzených. Nese název citlivé údaje. Dále se sem řadí i genetické a biometrické údaje spolu s údaji o dětech. Pod názvem genetické údaje si můžeme představit znaky získané geneticky nebo zděděním určité fyzické osoby. Ty plynou z analýzy biologického vzorku dotyčné fyzické osoby. Biometrické údaje vychází přímo z konkrétního technického zpracování a týkají se fyzických znaků nebo znaků chování, které jsou použitelné k identifikaci určité osoby. [18]

5.2 Technická opatření školy pro dosažení souladu s nařízení GDPR

Opatření jsou navrhována na základě provedené analýzy rizik, kde byla shledána následující rizika:

- v případě využití emailu pro předávání osobních údajů musí být šifrována (nejméně metodou ZIP s heslem)
- nedoporučuje využití freemailových účtů a pokud, tak pouze s kompletně šifrovaným obsahem
- namísto elektronické pošty lze bezplatně využít informační systém datových schránek
- limitovat přístupy na webové stránky pro sdílení dat (uloz.to, uschovna.cz aj.)
- zajistit omezení připojení flash, vypalování CD/DVD z jednotlivých stanic na úrovni politiky, jejich zpřístupnění pouze na jednotlivé pracovníky, kteří nezbytně potřebují flash disky nebo externí disky využívat
- v případě využití flash disku nebo externího disku k uložení osobních údajů je nezbytné tato data šifrovat, pokud jsou datová média vynášena mimo prostory organizace
- zajistit opakované technické testování znalostí uživatelů v rámci sociálního inženýrství (testování podvrženým emailem aj.)
- notebooky, které obsahují osobní údaje a jsou vynášeny mimo prostory organizace, musí být šifrovány
- chytré telefony, které obsahují osobní údaje a jsou vynášeny mimo prostory organizace, musí být zabezpečeny přihlašovacím heslem a dále vzdáleně ovladatelné v nejlepším případě (výmaz).

5.3 Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor

Tato vyhláška stanovuje požadavky na informační systém nakládající s utajovanými informacemi. Informační systém nakládající s utajovanými informacemi má různé stupně utajení. Důvěrné nebo vyšší musí zajišťovat bezpečnostní funkce, k jejichž zajištění se v informačním systému realizují identifikovatelné programově technické mechanismy. Ty musí být v celém životním cyklu informačního systému chráněny před narušením nebo neautorizovanými změnami. [17]

Bezpečnost informačního systému

Bezpečnosti informačního systému se dosahuje uplatněním souboru opatření z oblasti:

- počítačové a komunikační bezpečnosti
- kryptografické ochrany
- ochrany proti úniku kompromitujícího vyzařování
- administrativní bezpečnosti a organizačních opatření
- personální bezpečnosti
- fyzické bezpečnosti informačního systému. [17]

Soubor opatření je specifikován v bezpečnostní dokumentaci informačního systému, kterou tvoří projektová a provozní bezpečnostní dokumentace informačního systému.

Pro každý informační systém musí být v počáteční fázi jeho vývoje zpracována bezpečnostní politika informačního systému. Bezpečnostní politiku informačního systému tvoří soubor norem, pravidel a postupů, který vymezuje způsob, jakým má být zajištěna důvěrnost, integrita a dostupnost utajované informace, dostupnost služeb informačního systému a odpovědnost uživatele, bezpečnostního správce a správce informačního systému za jeho činnost v informačním systému. [17]

Bezpečnostní politika informačního systému se formuluje na základě:

- minimálních bezpečnostních požadavků v oblasti počítačové bezpečnosti
- systémově závislých bezpečnostních požadavků, požadavků uživatele a výsledků analýzy rizik
- bezpečnostních požadavků bezpečnostní politiky nadřízeného orgánu, pokud byla zpracována. [17]

Bezpečnostní požadavky odvozené z analýzy rizik

Pro stanovení hrozeb, které ohrožují aktiva informačního systému, musí být provedena analýza rizik. V rámci analýzy se vymezují aktiva informačního systému a hrozby, které působí na jednotlivá aktiva informačního systému. Posuzují se zejména hrozby, které způsobují ztrátu funkčnosti nebo bezpečnosti informačního systému. Po stanovení hrozeb se vymezují zranitelná místa informačního systému tak, že ke každé hrozbě se najde zranitelné místo nebo místa, na která tato hrozba působí. Výsledkem provedené analýzy rizik je seznam hrozeb, které mohou ohrozit informační systém, s uvedením odpovídajícího rizika. Na základě provedené analýzy rizik se provádí výběr vhodných protiopatření a určují se zbytková rizika a jejich úroveň, přičemž se dbá na to, aby byly implementovány pouze funkce, zařízení a služby, které jsou nezbytné pro splnění účelu, pro který je informační systém zřizován. [17]

Bezpečnostní správa informačního systému

V informačním systému se zavádí vhodný systém bezpečnostní správy informačního systému, kde je důležitá role bezpečnostního správce informačního systému. V případě potřeby zajistit stanovený rozsah činnosti pro zajištění bezpečnosti informačního systému, se zavádějí další role v bezpečnostní správě informačního systému, zejména organizační struktura bezpečnostních správců, bezpečnostní správci jednotlivých lokalit, bezpečnostní správce pro oblast komunikační bezpečnosti nebo bezpečnostní správce bezpečnostního rozhraní informačních systémů. Role bezpečnostního správce informačního systému obsahuje výkon správy bezpečnosti informačního systému spočívající zejména v přidělování přístupových práv, správě autentizačních a autorizačních informací, správě konfigurace

informačního systému, správě a vyhodnocování auditních záznamů, aktualizaci bezpečnostních směrnic, řešení bezpečnostních incidentů a krizových situací a vypracování zpráv o nich, zajištění školení uživatelů v oblasti bezpečnosti informačního systému, kontroly dodržování bezpečnostních provozních směrnic, jakož i v dalších činnostech stanovených v bezpečnostní dokumentaci informačního systému. [17]

5.4 ISMS - Systémy řízení bezpečnosti informací

Systém řízení bezpečnosti informací se skládá z postupů, směrnic a příslušných zdrojů a činností, kterými se organizace řídí, aby zaručila ochranu informačních aktiv. Představuje systematický přístup k nařízení, implementaci a provozování, monitorování, přezkoumávání, udržování a zlepšování informací organizace tak, aby byly zajištěny její cíle. Princip ISMS je založen na posuzování rizik a úrovni přijetí rizik organizace, které byly navrženy pro minimalizaci rizik a jejich zvládnutí. K tomu, aby byl ISMS úspěšný, přispívá analýza požadavků na ochranu informačních aktiv a aplikace opatření s cílem zajistit ochranu aktiv v souladu s požadavky. Pro úspěšnou implementaci ISMS přispívají tyto základní principy: [16]

- povědomí o potřebné bezpečnosti informací
- určení odpovědnosti za bezpečnost informací
- začlenění závazku managementu a zájmů zúčastněných stran
- zvýšení společenských hodnot
- posouzení rizik, díky kterému se stanový patřičná opatření, aby byla splněna přijatelná úroveň rizika
- bezpečnost začleněná jako základní prvek do informačních sítí a systémů
- aktivní prevence a detekce incidentů bezpečnosti informací
- zajištění komplexního přístupu k řízení bezpečnosti informací
- neustálé posuzování bezpečnosti informací a provádění modifikací dle potřeby. [16]

Zavedení ISMS je pro organizaci velké rozhodnutí a musí se začlenit, odstupňovat a aktualizovat s potřebami organizace. Návrh a implementace jsou rovněž ovlivněny potřebami a cíli organizací. Dále se pak zohledňují požadavky na bezpečnosti a procesy organizace. ISMS je pro činnost organizace jak veřejného, tak privátního sektoru velmi důležitý. Zásluhou téhle normy je i to, že organizace mohou demonstrovat obchodním partnerům a dalším zainteresovaným stranám svojí schopnost používat konzistentní a vzájemné principy bezpečnosti informací. [16]

5.4.1 ČSN ISO/IEC 27000 Systémy řízení bezpečnosti informací - Přehled a slovník

Norma ČSN ISO/IEC 27000 udává přehled systému řízení bezpečnosti informací a termíny a definice obecně používané v několika normách ISMS. ISMS je zkratka pro Information Security Management Systém. Normu je možno použít pro veškeré typy organizací. Organizace tak díky normě ISMS může vytvořit a použít bezpečnostní řízení aktiv obsahující informace, které získaly nebo jim byly poskytnuty zákazníky či třetími stranami.

Dnešní zákony, které se týkají informační bezpečnosti, jsou vytvořené z norem ISO/IEC 27000. Normy ISO/IEC 27001 a ISO/IEC 27002 jsou základním podkladem pro vytvoření bezpečných informačních systémů. V nich jsou určeny zásadní postupy a hodnocení pro budování bezpečnosti IS. Umožnují snadné ověření stavu bezpečnosti, výměny informací, které spolupracují s institucemi nebo obchodními partnery. [16]

5.4.2 ČSN ISO/IEC 27001 Systémy řízení bezpečnosti informací – Požadavky

Zmíněná norma zavádí požadavky na ustanovení, implementování, udržování a zlepšování systému řízení bezpečnosti informací pro organizací. Norma se skládá z několika oblastí: [15]

- požadavky na ISMS
- odpovědnost vedení organizace
- vnitřní audit ISMS
- ISMS zkontroluje vedení organizace

- vylepšování ISMS .

Stanovení rozsahu systému řízení bezpečnosti informace

Aby organizace mohla určit rozsah, musí nejprve stanovit hranice a aplikovatelnost ISMS. Když se určuje rozsah, musí se zvážit externí a interní aspekty výstupu ISMS a stanovit zainteresované strany a jejich požadavky. Posledním kritériem je propojení a závislost mezi organizacemi a činnostmi mezi nimi. [15]

Opatření zaměřená na rizika

Při posuzování rizik si musí organizace definovat a aplikovat procesy, které určí kritéria rizik bezpečnosti informací. Ty zahrnují akceptace rizik a samotné provedení posouzení rizik. Dále musí zajistit jejich neustálé pozorování, které vyprodukuje kompaktní a porovnatelné výsledky. Podle toho se rizika identifikují a analyzují. Dle výsledků se hodnotí rizika a stanovují patřičná ošetření rizik. U ošetření rizik musí organizace rozhodnout o vhodné variantě použitelného ošetření s ohledem na předešlé výsledky. [15]

Vnitřní audit

Velký důraz je kladen na pravidelné provádění interních auditů k získání informace, zda systém řízení bezpečnosti vyhovuje požadavkům organizace a mezinárodních norem. Zjišťuje, jestli je efektivně implementován a udržován. Tato norma doporučuje organizacím používat vhodné auditní programy. U auditu se musí definovat kritéria a rozsah auditu, vybrat auditory, kteří provedou samotný audit objektivně a nestranně. Výsledky jsou pak předány vedoucím pracovníkům. Norma dále nařizuje uchovávat dokumentaci a výsledky auditů. [15]

Zlepšování

Při výskytu neshody organizace musí zajistit opatření k nápravě. Vyhodnotit potřeby k odstranění příčin neshody a vylepšit systém, aby se znovu nevyskytla. To zahrnuje přezkoumání a určení příčin neshody, implementaci opatření a vylepšení ISMS. [15]

6 Analýza informačního systému školy

Pro bakalářskou práci byla vybrána metoda SWOT analýza. Tato metoda umožňuje jednoduché a vhodné zpracování získaných informací. Byla provedena pouze jednou osobou se závěrem zmapovat školní informační systém.

SWOT analýza je nástroj ke zjištění jakékoliv situace v organizaci. Zkratka SWOT se skládá z prvních písmen čtyř anglických slov, kterými jsou Strenghts, Weaknesses, Opportunities a Threats. V překladu se SWOT analýza zabývá zkoumáním silných a slabých stránek, dále příležitostí a hrozeb. Tato analýza je využívána především v marketingu a je součástí dlouhodobého, tedy strategického plánování organizace. Z tohoto důvodu není SWOT analýza pouhým vyjádřením silných a slabých stránek, možností a hrozeb, ale také nalezení možných strategií při řešení problémů, které se v organizaci vyskytují.

Obr. 5 Analýza SWOT

	POMOCNÉ (k dosažení cíle)	**ŠKODLIVÉ** (k dosažení cíle)
VNITŘNÍ PROSTŘEDÍ	**STRENGHTS** (silné stránky)	**WEAKNESSES** (slabé stránky)
VNĚJŠÍ PROSTŘEDÍ	**OPPORTUNITIES** (příležitosti)	**THREATS** (hrozby)

Zdroj: https://www.fucik.cz

6.1 Analýza školní sítě

Na základě poskytnutých materiálů a rozhovorů se správcem školní sítě byla zpracována analýza celé školní sítě.

Silné stránky:

- ve všech učebnách a kabinetech je možný přístup do školní sítě a na internet
- nasazení dvou nových serverů (lepší výkonnost, větší úspora energie)
- umístění serverů do serverové skříně
- elektronické podpisové certifikáty používají všechny odpovědné osoby spojené s administrativou, jsou uloženy na zabezpečených médiích TokenMe.

Slabé stránky:

- Wi-Fi síť nepokrývá celou školu
- Wi-Fi je zřízena jednoduchým controllerem
- nevhodné umístění SWITCHů
- sériové zapojení SWITCHů
- stáří SWITCHů
- nevhodná použitá kategorie kabeláže datové sítě
- nedostatečné pokrytí sítě optickým kabelem
- nevhodné použití koncových přípojných bodů školní sítě v učebnách a kabinetech
- nedostatečná kapacita přístupových bodů Wi-Fi
- nedostatečné zabezpečení Wi-Fi sítě.

Příležitosti:

- získání finančních prostředků od zřizovatele školy na modernizaci celé školní sítě
- využití projektů EU na modernizaci školní sítě
- možnost zajištění potenciálních dárců pro modernizaci školní sítě
- zvýšení přenosové rychlosti a stability školní sítě
- posílení monitoringu datové sítě
- možnost rozšíření nástrojů Microsoft Office 365
- možnost zavedení moderního a funkčního přístupového systému (monitorování vstupů žáků, čipování zaměstnanců pro přehled pracovní doby, odesílání SMS rodičům a jiné)
- zvýšení bezpečnosti a možnost dohledávat bezpečnostní incidenty.

Hrozby:

- výpadek školní sítě

- fyzické poškození optického kabelu
- napadení vnitřním uživatelem sítě
- špatné technické zapojení komponentů
- odcizení technického vybavení
- morální zastarání systému školní sítě.

Shrnutím zjištěných informací se došlo k závěru, že je potřeba nahradit zastaralé datové rozvody a rozšířit optickou síť. Tato výměna by měla být provedena v prvním kroku. Z analýzy dále vyplynulo nevhodné umístění, stáří a způsob zapojení SWITCHů, které budou vyměněny v druhém kroku. Protože Wi-Fi síť nepokrývá celou školu, dalším krokem by mělo být její rozšíření do všech pavilonů budovy školy, přičemž k tomu bude zapotřebí nový výkonný controller. V původním zachování mohou zůstat servery, které jsou dostačující pro potřeby školy.

6.2 Analýza informačního systému Bakaláři

Na základě poskytnutých materiálů a rozhovorů se správcem Bakaláře a s managementem školy byla zpracována i jednoduchá analýza informačního systému Bakaláři.

Silné stránky:

- využití modulů informačního systému pro jednodušší administraci
- zajištění přístupu ve všech vhodných prostorách školy do informačního systému
- automatická aktualizace na nejnovější verzi
- automatické zálohování dat na SQL server
- umístění na jednoduchém serveru
- využití Bakaláře v různých typech zařízení (PC, tablet, chytrý telefon)
- možnost pracovat v režimu home office
- člen pedagogického sboru je poradce systému Bakaláři, spolupracuje s tvůrci systému a je držitelem licence k realizaci školení dalších uživatelů.

Slabé stránky:

- nevyužití všech zakoupených modulů informačního systému
- velmi jednoduché zabezpečení přístupu do informačního systému
- pro úpravu Bakaláře neustálá komunikace přes zprostředkovatele (externí firma)
- omezený časový režim správce školní sítě (externí firma).

Příležitosti:

- rozšíření dalších funkčních modulů informačního systému, které jsou na trhu.

Hrozby:

- výpadek serveru
- odcizení osobní údajů z informačního systému
- nedostatečné proškolení uživatelů Bakaláře
- progresivnější vývoj konkurenčních systémů na trhu
- nežádoucí rizikové chování uživatelů.

Informační systém Bakaláři se jeví jako velmi efektivně nastavený systém, který je klíčovým nástrojem pro zajištění plynulého procesu vzdělávání ve škole a v režimu home office se potvrdila jeho využitelnost. V budoucím období by byla potřeba zvolit vhodný systém zabezpečení, aby se snížilo riziko jeho zneužití a poškození.

Vzhledem k okolnostem koronavirové pandemie nebylo možno ve spolupráci s externím dodavatelem realizovat vhodný penetrační test pro analýzu úrovně zabezpečení zvoleného informačního systému ve škole.

7 Návrh na zlepšení IS ve vybrané škole

Z předchozí kapitoly, kde byla provedena analýza školní sítě školy, bylo zjištěno, že její stav je zastaralý a neodpovídající dnešním moderním standardům a požadavkům pro maximální využití ICT techniky ve škole. Pro modernizaci sítě bylo navrženo řešení ve dvou oblastech.

Modernizace a rozšíření kabelové infrastruktury

Zastaralé datové rozvody by měly být nahrazeny rozvody datové kategorie vyšší (UTP kategorie 6). Tyto kabely by se měly uložit do vhodných elektroinstalačních lišt, aby se zamezilo jejich poškození. Pro rychlejší datový přenos mezi rozvaděči a zlepšení propustnosti celé datové sítě by se měla vybudovat optická síť. Škola je pavilonová, proto je nutné optické kabely zavést do všech pavilonů. Současný počet rozvaděčů pro novou síť by byl nedostatečný, proto je potřeba do každého pavilonu umístit nový rozvaděč (celkem 5 rozvaděčů). Tím by se zároveň zvýšila bezpečnost a stabilita školní sítě. Totiž ve stávající infrastruktuře jsou například SWITCHe přidělané různě na zdech po škole a kdokoliv je může vypnout, nebo se do nich připojit, tím může dojít ke zneužití. Dále by měla být navržena realizace nových přístupových bodů ke školní síti LAN v učebnách, v kabinetech, u vstupů a v ostatních prostorách školy, kde je přítomnost datové sítě nezbytná pro výuku či provoz školy. Současné rozmístění koncových přípojných bodů je nedostačující a v některých prostorech chybí. Toto je v provedené analýze uvedeno jako slabá stránka.

Modernizaci Wi-Fi infrastruktury

Stávající Wi-Fi nepokrývá celou školu, proto je potřeba ji posílit tak, aby bylo možné využít Wi-Fi sítě pro výuku moderními mobilní prostředky. Byla navrhnuta instalace nových aktivních přístupových bodů Wi-Fi s dostatečnou kapacitou. Současná síť používá pouze jednoduchý controller, proto by bylo vhodné ho nahradit výkonným hardwarovým controllerem pro centralizované řešení Wi-Fi segmentu. Na základě jednoduchého zabezpečení stávající Wi-Fi sítě by bylo možno doporučit zvýšení úrovně zabezpečení pro novou síť. Zabezpečení by se mělo řídit minimálně těmito základními pravidly:

- nastavit vlastní SSID a následně jej skrýt
- nastavit filtrování MAC adres

- a zvolit šifrování sítě WAP2
- přihlašovací heslo bude tvořeno nejméně z 8 znaků složených z malých a velkých písmen, číslic a speciálních znaků.

Druhou provedenou analýzou byla analýza informačního systému Bakaláři. Tento informační systém je pro školu velice důležitý z hlediska vlastní organizace celého systému vzdělávání ve škole. V soudobých školách bez informačních systémů již nelze fungovat, protože jsou na ně kladeny požadavky ohledně centralizace určitých dat k příslušným orgánům a tyto systémy práci významně zefektivňují.

Současné nastavení informačního systému Bakaláři je na velmi dobré úrovni. Pro efektivnější práci s tímto informačním systémem bylo navrženo ještě využití dalších modulů, které jsou součástí základního balíčku informačního systému Bakaláři a škola je má k dispozici. Jedná se o následující moduly:

- modul knihovna
- modul pokladna
- modul anketa
- modul nástěnka.

Seřazení těchto modulů je dle priority zjištěné šetřením s managementem školy.

Pro eliminaci nežádoucího rizikového chování uživatelů a tím pro zvýšení úrovně zabezpečení vstupu do informačního systému Bakaláři bylo navrženo přihlašování pomocí autentizačního tokenu. Autentizační token může být mobilní zařízení, které poskytuje funkci dvoufázového ověřování prostřednictvím SMS zprávy. V první fázi se zadá přihlašovací jméno a heslo. Ve druhé fázi se zadá kód, který se získá pomocí SMS zprávy. Tímto by byla posílena ochrana osobních dat dle směrnice GDPR.

8 Závěr

Obsahem bakalářské práce bylo analyzovat vybraný informační systém a navrhnout efektivnější opatření pro zvolenou školu. To znamená najít ta konkrétní opatření, která by vybavila školu odpovídajícím technickým zázemím a vytvořila vhodné prostředí pro efektivní užívání informačních a komunikačních technologií ve vzdělávání.

Ze základní charakteristiky školy vyplynulo, že je to škola středně veliká, která nebyla dlouhou dobu modernizována, jak stavebně, tak technicky. Sice na základě požadavků doby se vždy technicky přizpůsobila potřebám ICT, ale současná situace využívání ICT, jenž je mnohem vyšší a náročnější, je na hranici odpovídající technickému provedení infrastruktury sítě školy. Škola využívá celou řadu informačních systémů, které potřebují odpovídající infrastrukturu. Nejdříve byla zmapována stávající školní síť včetně jejích bezpečnostních prvků a z informačních systémů byl zmapován nejdůležitější IS, a to systém Bakaláři. Na základě této analýzy byly formou SWOT analýzy nastíněny kladné a záporné stránky sítě a systému Bakaláři a navrženy příležitosti k zefektivnění jejich užívání, včetně uvedení rizik.

Výsledkem bakalářské práce je návrh pro modernizaci stávající sítě a tím i zvoleného informačního systému školy. Provedenou modernizací by měla být kompletní rekonstrukce kabelové infrastruktury včetně vybudování vhodného zázemí pro správu sítě, modernizace Wi-Fi infrastruktury a návrhy inovace IS Bakaláři včetně vyšší úrovně zabezpečení.

Velmi důležitým faktorem při rozboru a řešení problematiky bezpečnosti je komplexní pohled. Nevyváženost může být způsobena zaměřením se na oblast technického zabezpečení, která je zpravidla v popředí, ale neméně důležitá je i oblast „lidského“ zabezpečení. Celý systém řízení bezpečnosti IS ve škole by se měl zaměřit jak na povědomí všech pracovníků školy o bezpečnosti IS, tak na výběr a implementaci vhodných technických opatření.

Pro správnou funkci bezpečnostních opatření v dané škole platí a i nadále bude platit dodržování základních pravidel při práci s informačními systémy:

- navzájem nesdělovat přístupová jména, hesla a kódy
- nezapisovat hesla na volně přístupná místa
- obezřetně se pohybovat na internetu
- dodržovat nařízení týkající se zasílání a přijímání nepovolených typů příloh

- nestahovat neznámé aplikace
- nenavštěvovat nepovolené či rizikové stránky.

Výběrem a implementací vhodných technických opatření v rámci inovace IS budou například zavedení přístupových cest formou SMS zpráv, omezení práv přístupu uživatelů k datům podle jejich skutečných potřeb, nastavení práv uživatelů komunikujících prostřednictvím internetu, protivirová kontrola veškeré komunikace směřující dovnitř i ven z vnitřní sítě.

Výsledky analýzy a návrh opatření budou následně předloženy a projednány s managementem školy za účelem modernizace technického prostředí pro budoucí užívání informačních a digitálních technologií ve škole 21. století.

9 Seznam použitých zdrojů

[1] *Bakaláři* [online]. [cit. 2020-03-17]. Dostupné z: https://www.bakalari.cz/

[2] BUCHALCEVOVÁ, Alena. *Metodiky vývoje a údržby informačních systémů: kategorizace, agilní metodiky, vzory pro návrh metodiky*. Praha: Grada, 2005. Management v informační společnosti. ISBN isbn80-247-1075-7.

[3] ČERMÁK, Miroslav. *Analýza rizik: Jemný úvod do analýzy rizik* [online]. 2010, , 1 [cit. 2020-03-17]. Dostupné z: https://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/

[4] DOSTÁL, Jiří. *Školní informační systémy*. Olomouc: Univerzita Palackého v Olomouci, 2011. ISBN isbn978-80-244-2784-3.

[5] IT Systems: *IT Security - Penetrační testy v praxi* [online]. 2019, 19 [cit. 2020-04-06]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/it-security/penetracni-testy-v-praxi.htm

[6] KNOPOVÁ, Martina. Bezpečnost dat v informačních systémech. *Ikaros* [online]. 2011, 2011, 15(6), 1 [cit. 2020-02-19]. ISSN 1212-5075. Dostupné z: https://ikaros.cz/bezpecnost-dat-v-informacnich-systemech

[7] SODOMKA, Petr a Hana KLČOVÁ. *Informační systémy v podnikové praxi*. 2., aktualiz. a rozš. vyd. Brno: Computer Press, 2010. ISBN isbn978-80-251-2878-7.

[8] SOMSEDÍK, Jan. *Zabezpečení informačního systému v podniku* [online]. Praha, 2014 [cit. 2020-02-19]. Dostupné z: https://is.ambis.cz/th/y7tmx/JAN_SOMSEDIK_.pdf. Diplomová práce. Bankovní institut vysoká škola Praha.

[9] SVATÁ, Vlasta. *Audit informačního systému*. Praha: Professional Publishing, 2011. ISBN isbn978-80-7431-034-8.

[10] ŠULC, Vladimír. *Kybernetická bezpečnost*. 2018. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN isbn978-80-7380-737-5.

[11] POKORNÝ, Miroslav a Jan LAVRINČÍK. *Teorie systémů I*. Olomouc: Moravská vysoká škola Olomouc, 2009. ISBN 978-80-87240-09-0.

[12] ŘEPA, Václav. *Analýza a návrh informačních systémů*. Praha: Ekopress, 1999. ISBN isbn80-861-1913-0.

[13] VOŘÍŠEK, Jiří a Josef BASL. *Principy a modely řízení podnikové informatiky*. V Praze: Oeconomica, 2008. ISBN isbn978-80-245-1440-6.

[14] VOŘÍŠEK, Jiří. *Informační systémy a jejich řízení*. 3. vyd. Praha: Bankovní institut vysoká škola, 2007. ISBN 978-80-7265-100-9.

[15] *ČSN EN ISO/IEC 27001 (369797): Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. 2014. Brusel: CEN-CENELEC, 2006.

[16] *ČSN EN ISO/IEC 27000 (369790): Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. 2017. Brusel: CEN-CENELEC, 2017.

[17] Vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. In:. Praha: Národní bezpečnostní úřad, 2005, ročník 2, 523/2005 Sb.

[18] *Nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů*. In:. Praha: Evropský parlament, Evropská rad, 2018, ročník 1, 2016/679.

[19] *Z norem řízení bezpečnosti informací se postupně vytrácí řada užitečných věcí* [online]. 2019, 19(5) [cit. 2020-03-17]. ISSN 1802-615X. Dostupné z: Z norem řízení bezpečnosti informací se postupně vytrácí řada užitečných věcí

10 Seznam použitých obrázků

11 **Přílohy**

Příloha 1: Nastavení VLAN

Zabezpečení sítě a jejích segmentů pomocí VLAN:

Rozsahy DHCP serveru:

Název oboru	Počáteční IP	Koncová IP	Počet IP v rozsahu	Maska	Server DNS	Výchozí brána
SYS	192.168.1.10	192.168.1.200	91	255.255.255.0	192.168.1.3	192.168.1.1
Ped	192.168.2.10	192.168.2.200	91	255.255.255.0	192.168.1.3	192.168.2.1
ZAC	192.168.3.10	192.168.3.200	91	255.255.255.0	192.168.1.3	192.168.3.1
ADM	192.168.4.10	192.168.4.100	91	255.255.255.0	192.168.1.3	192.168.4.1
INF	192.168.5.10	192.168.5.200	91	255.255.255.0	192.168.1.3	192.168.5.1

Popis virtuálních podsítí:

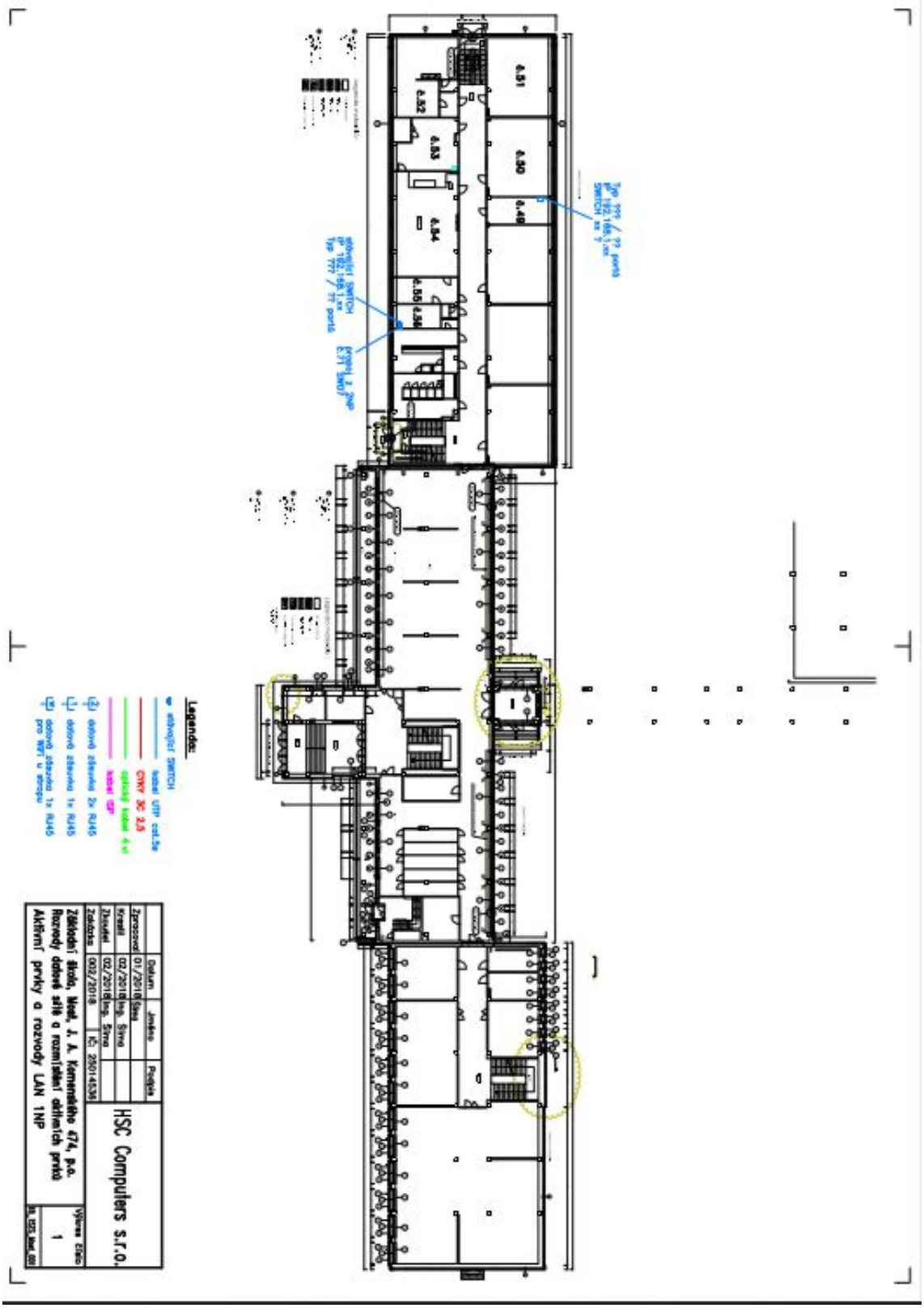
VLAN ID	Alias	Název	Podsíť / maska
1	SYS	Systém	192.168.1.0 / 24
2	PED	Pedagogové	192.168.2.0 / 24
3	ZAC	Žáci	192.168.3.0 / 24
4	ADM	Administrativa	192.168.4.0 / 24
5	INF	Infocentrum	192.168.5.0 / 24

Obecná matice řízení přístupu mezi jednotlivými podsítěmi:

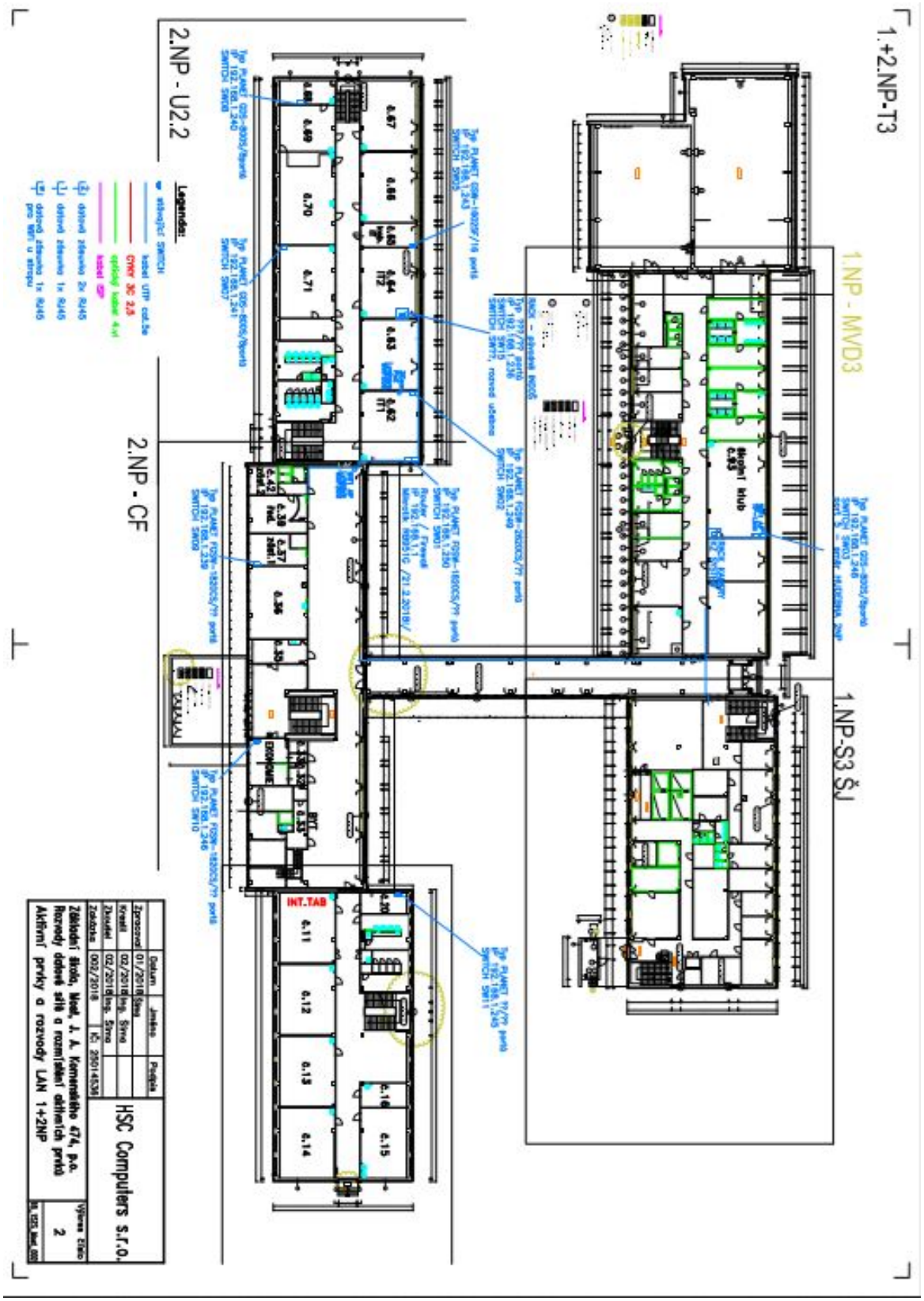
FROM / TO	**SYS**	**PED**	**ZAC**	**ADM**	**INF**
SYS	ANO	NE	NE	NE	NE
PED	ANO	ANO	NE	NE	NE
ZAC	ANO	ANO	ANO	NE	NE
ADM	ANO	NE	NE	ANO	NE
INF	ANO	NE	NE	NE	ANO

Příloha 2: Rozvody datové sítě a rozmístění aktivních prvků

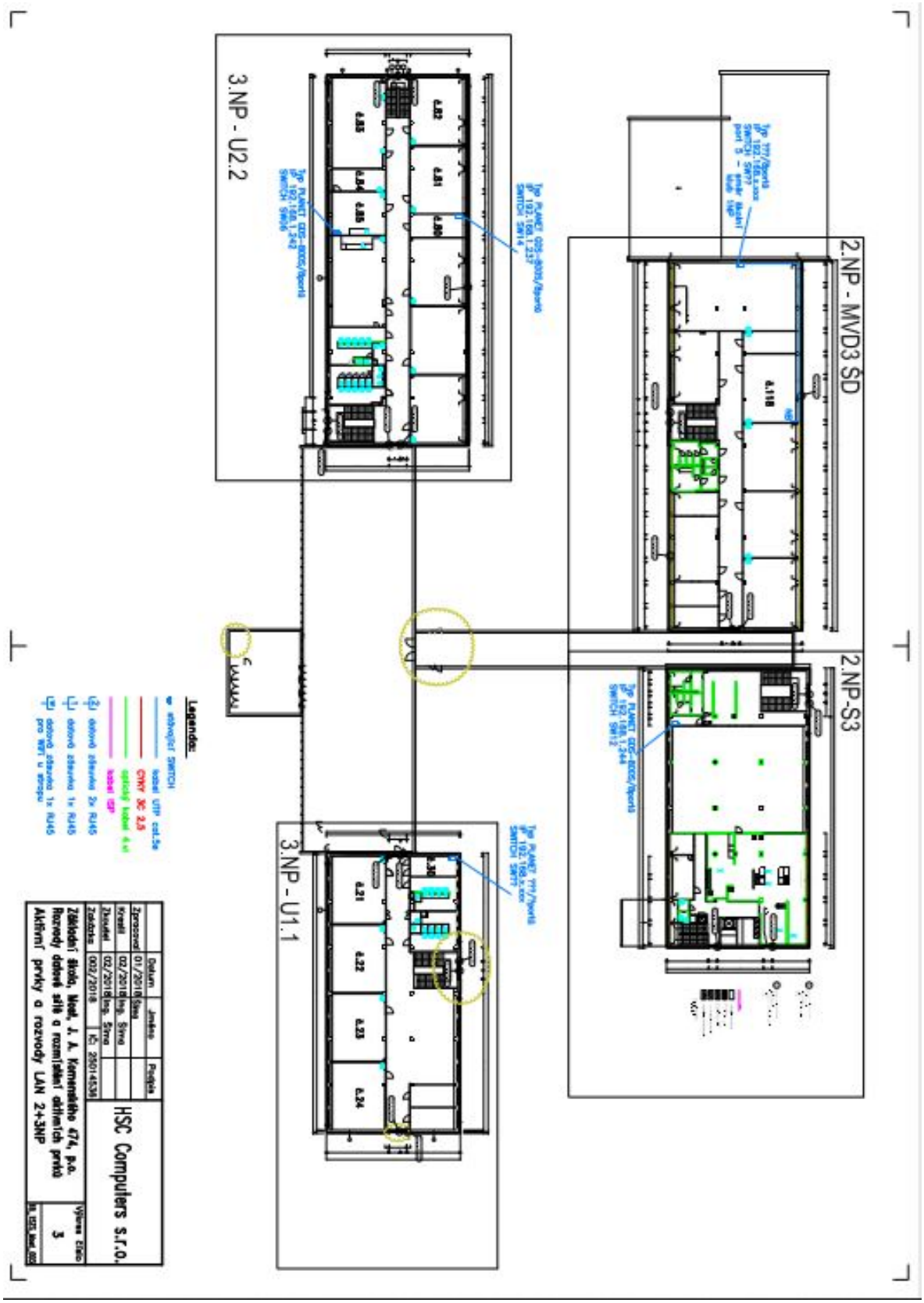
Schéma rozmístění rozvodů a aktivních prvků s popisem: 1NP



1 + 2NP


1.+2.NP-T3
1.NP - MVD3
1.NP-S3 ŠJ
2.NP - U2.2
2.NP - CF
Legenda:
INT.TAB
HSC Computers s.r.o.
Základní škola, Most, J. A. Komenského 474, p.o.
Rozvody datové sítě a rozmístění aktivních prvků
Aktivní prvky a rozvody LAN 1+2NP
2

2 + 3NP


2.NP - MVD3 SD
2.NP-S3
3.NP - U2.2
3.NP - U1.1
Legenda:
HSC Computers s.r.o.
Základní škola, Most, J. A. Komenského 474, p.o.
Rozvody datové sítě a rozmístění aktivních prvků
Aktivní prvky a rozvody LAN 2+3NP
3