Univerzita Karlova v Praze

Pedagogická fakulta

BAKALÁŘSKÁ PRÁCE

2014 **Petr Brejcha**

Univerzita Karlova v Praze

Pedagogická fakulta

Centrum školského managementu

Petr Brejcha

ICT a bezpečnost v základních uměleckých školách

ICT and security in elementary art schools

Bakalářská práce

Studijní program: Specializace v pedagogice (B7507)

Studijní obor: B SMG (6208R102)

Vedoucí závěrečné práce: PhDr. Jan Voda, Ph.D.

Rok 2014

Prohlašuji, že jsem závěrečnou práci vypracoval pod vedením vedoucího práce samostatně a citoval všechny použité prameny a literaturu. Dále prohlašuji, že práce nebyla využita k získání jiného nebo stejného titulu.

Souhlasím s trvalým uložením elektronické verze mé práce v databázi meziuniverzitního projektu Theses.cz za účelem soustavné kontroly podobnosti kvalifikačních prací.

V Praze 14.6.2014

.....

podpis

Poděkování

Děkuji PhDr. Janu Vodovi, Ph.D. za korektní a konkrétní připomínky, za pozitivní přístup a rychlou odezvu při vedení mé práce.

.....

podpis

ABSTRAKT:

Tato bakalářská práce určuje a popisuje bezpečnostní rizika v základních uměleckých školách v oblasti zajištění bezpečnosti majetku, osob a informací prostředky ICT. Popisuje procesy řízení bezpečnosti, managementu rizika, principy managementu bezpečnosti informací podle skupiny norem ISO/IEC 27000, některá technická řešení zabezpečovacích systémů a bezpečnost elektronických dat, tedy přínos a rizika spojená s používáním informačních systémů a datových sítí. Vysvětluje jednotlivé principy pro zpřístupnění orientace v problematice a usnadnění procesu rozhodování. Výzkumná část této práce zjišťuje, jaké zabezpečovací prostředky ZUŠ využívají a s jakými výsledky, které systémy považuje management škol za účelné v budoucnu nainstalovat. Dále je zkoumán stav zabezpečení počítačů a pevných počítačových sítí v ZUŠ, zejména v oblasti využívání silných hesel a politiky jejich tvorby, taktéž způsob ochrany bezdrátové počítačové sítě před jejím zneužitím, principy zálohování dat, nebo bezpečnost práce se vzdálenou plochou.

KLÍČOVÁ SLOVA:

Řízení bezpečnosti, management rizika, ISO/IEC 27000, ICT bezpečnost, ochrana osob a majetku

ABSTRACT:

This bachelor thesis identifies and defines the security threats for the personal, property, and information safety management by the means of ICT in primary art schools. The manuscript describes processes of security control and risk management, principles of information security guidance according to the ISO/IEC 27000 standard and some of the security system technical designs. The security of electronic data and benefits or drawbacks of information system and data network utilization are also discussed. For better orientation in the topic and to simplify the decission process, an explaination of particular technological principles is provided. The research part of this work is focused on the means of security currently used by primary art schools, the effectivenness of such tools, and the plans for future instalation of new technology. Further, the state of the computer and cable network security in primary art schools is studied with the emphasis on the strength of account password and the password making policy. Finally, the means of wireless network protection, principles of data back-up, and remote desktop work safety are investigated.

KEYWORDS:

Security control, risk management, ISO/IEC 27000 standard, ICT security, protection of person and property

Obsah

Úvod

Základní umělecké školy vzdělávají žáky od pěti do cca dvaceti let věku. To znamená, že se v ní sejdou děti z mateřských, základních i středních škol. Těmto všem žákům je základní umělecká škola povinna zajistit bezpečné prostředí pro jejich vzdělávání. A nejen jim, bezpečno musí být i pro pedagogy, ekonomický i technický personál. Některé bezpečnostní otázky jsou podobné jako v ostatních školách, jiné naopak rozdílné. Podobně se bude řešit zabezpečení ochrany majetku, požární ochrany, zabezpečení elektronických dat. Jinak se musí přistupovat k zabezpečení vstupu do budovy proti vniknutí nežádoucích osob. Vyplývá to z odlišného provozu školy. Ve všech těchto zmíněných, ale i dalších bezpečnostních otázkách se dnes s úspěchem využívá prostředků ICT – informačních a komunikačních technologií. V tomto případě slouží ke zvýšení bezpečnosti, k případnému snížení škod na zdraví a majetku, nebo ke snížení nákladů.

ICT prostředky však ve školách plní i mnohé jiné úlohy, než jen zajištění bezpečnosti. Jistě si dnes nikdo nedovede představit ekonomické oddělení, které by účtovalo ručně na papíře. Počítač se stal nedílnou součástí každodenního života. S úspěchem se dnes i v základních uměleckých školách využívá informačních systémů, které slouží k vedení elektronické matriky školy a dalších databázových systémů nutných ke správě školy a k dalším činnostem. V tomto informačním systému je uloženo mnoho osobních, citlivých a dalších údajů žáků i pracovníků školy. Vedení školy proto musí zajistit zavedení a používání bezpečnostních pravidel pro práci s těmito údaji, aby se zamezilo jejich ztrátě, nebo zneužití. To znamená, že s těmito daty mohou přijít do styku pouze oprávněné osoby, které jsou proškoleny a řídí se pravidly bezpečnostní politiky, které management školy stanovil. Pro bezpečnost dat už dnes nestačí pečlivě zamykat. Je nutno zabezpečovat počítačové sítě, po kterých by data mohla být odcizena, poškozena, zneužita útočníkem zvenčí, ale i zevnitř organizace. Tyto a další bezpečnostní otázky by mělo vedení základních uměleckých škol dnes a denně řešit, aby mohla škola plnit svoje poslání v bezpečném prostředí.

Tato bakalářská práce si klade za cíl určit a popsat bezpečnostní rizika v ZUŠ v oblasti zajištění bezpečnosti majetku, osob a informací. V teoretické části jsou popsány procesy řízení bezpečnosti, managementu rizika, principy managementu bezpečnosti informací podle skupiny norem ISO/IEC 27000, některá technická řešení zabezpečovacích systémů a bezpečnost elektronických dat, tedy přínos a rizika spojená s používáním informačních systémů a datových sítí. Jedná se o základní seznámení s jednotlivými principy pro

zpřístupnění orientace v problematice a usnadnění procesu rozhodování. Management školy musí znát rizika, která při provozu školy hrozí a předcházet jim.

Výzkumná část této práce pomocí dotazníkového šetření zjišťuje:

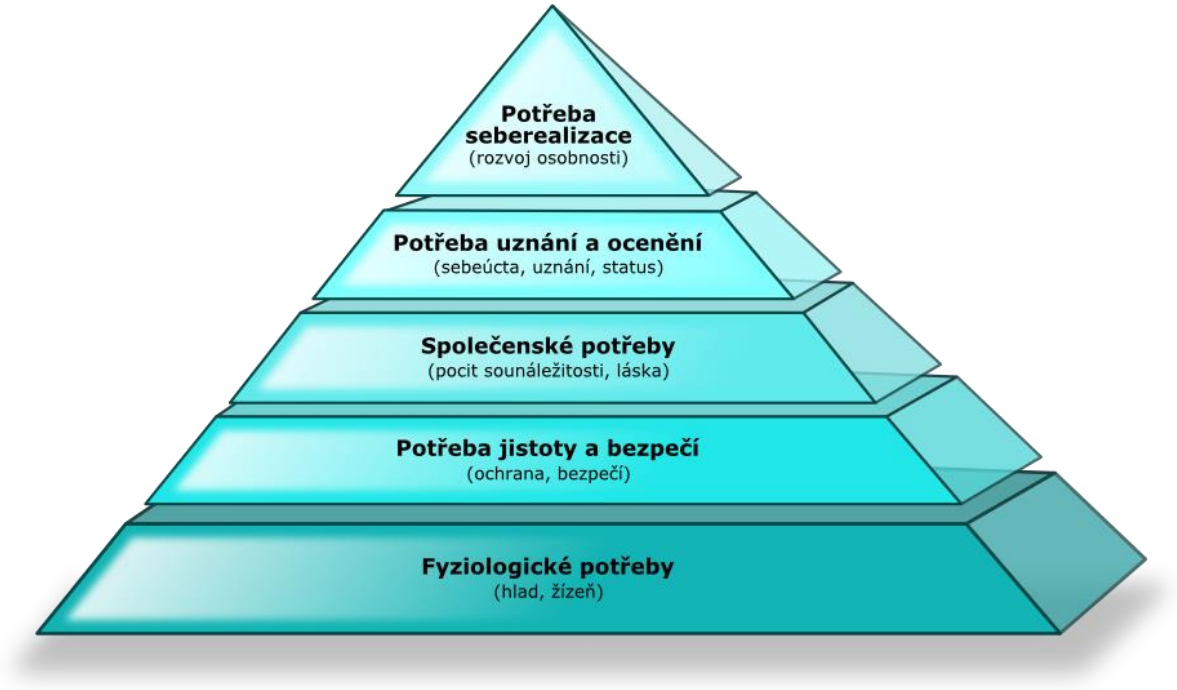
- zda a jaké ICT prostředky využívají školy při ochraně osob a majetku a s jakými výsledky
- zda a jak školy zabezpečují data před zneužitím

Dotazníkové šetření mezi řediteli ZUŠ mimo jiné zjišťuje, v jak lidnatém sídle škola působí, kolik má škola žáků, zda působí v budově (budovách) pouze jejich ZUŠ, nebo sdílejí budovu s jinou školou atd. Tyto proměnné totiž mohou mít vliv při rozhodování ředitele na způsob a rozsah zajišťování bezpečnosti v ZUŠ, nebo při výběru prostředků na zajištění bezpečnosti, na správu školy, na požadavky rodičů žáků, atd.

Dále je zkoumáno, zda vůbec konkrétní prostředek (myšleno typ) využívají, s jakými výsledky. Konkrétně například existenci elektronického zabezpečovacího systému, kamerového systému, zabezpečení proti vstupu nežádoucích osob do budovy, výsledky a zkušenosti při jejich využití. Dále je zjišťován stav zabezpečení počítačů a počítačových sítí v ZUŠ, zejména v oblasti využívání silných hesel a politiky jejich tvorby, taktéž způsob ochrany bezdrátové počítačové sítě, principy zálohování dat, nebo bezpečnost práce se vzdálenou plochou.

Teoretická část

Ředitelé základních uměleckých škol, tak jako jiní vrcholoví manažeři, čelí mnoha bezpečnostním rizikům, která jejich organizaci hrozí. Musí je včas správně identifikovat, vyhodnotit a konat kroky k jejich eliminaci, nebo ke snížení škod, které mohou vzniknout. Bezpečnost organizace je jedním ze základních pilířů jejího fungování a rozvoje. Potřeba bezpečí je podle Abrahama Maslowa druhou nejdůležitější základní lidskou potřebou.



Obrázek 1 - http://halek.info

Pojem „bezpečnost“ podle Jelšovské (1) představuje stav vědomí člověka, ve kterém se necítí být ohrožený, život bez ohrožení, stav bez strachu o sebe a druhé, jistotu do budoucnosti, absenci ohrožení zdraví, ztráty života či majetku, psychický stav umožňující realizaci životních cílů a záměrů.

1 Řízení bezpečnosti

Řízením bezpečnosti podle (2) rozumíme oblast řízení, kterou je zajišťována bezpečnost aktiv (zdrojů) v organizaci, myšleno jak bezpečnost fyzickou tak bezpečnost elektronického světa. Řízení bezpečnosti těsně souvisí s řízením rizik a směřuje k vytvoření či trvalému zajištění podmínek, které budou předcházet či snižovat možná rizika, či umožňovat

se vyhnout problémům a to zejména pomocí různých metod, procedur, směrnic, standardů a nástrojů.

Řízení bezpečnosti je soustavná, opakující se sada navzájem provázaných činností, jejichž cílem je zajistit bezpečný provoz a zamezit bezpečnostním rizikům a hrozbám, jako jsou ohrožení či poškození života a zdraví, hmotných a nehmotných aktiv organizace. (2)

Bezpečnost bývá obvykle zajišťována ve větších organizacích odbornými útvary a odborníky, primárně je součástí každodenní práce vedoucího zaměstnance a statutárního orgánu, který nese hlavní odpovědnost. Při řízení bezpečnosti management schvaluje, umožňuje a kontroluje přístup osob k financím, informacím, movitému i nemovitému majetku organizace. S řízením bezpečnosti těsně souvisí řízení kontinuity činností organizace.

Nejvyšší odpovědnost za bezpečnost má přirozeně statutární orgán a nejvyšší management (top management) organizace. Ve velkých a středních organizacích má odpovědnost za řízení bezpečnosti manažer bezpečnosti. Mnoho větších organizací zřizuje pozici manažera informační bezpečnosti, která je zaměřená výhradně na bezpečnost informací či ICT bezpečnost. Velké organizace nebo organizace, které působí v rizikovém prostředí (například banky, pojišťovny), mohou mít ještě další specialisty řízení bezpečnosti.

V malých organizacích, typicky ve školách, je odpovědnost za řízení bezpečnosti koncentrována na úrovni statutárního orgánu, protože není efektivní zaměstnávat specializovaného manažera bezpečnosti na plný úvazek.

V praxi bezpečnostní management řeší tyto otázky:

- co chránit – definuje druhy a hodnoty chráněných zájmů
- před kým a čím chránit – analyzovat bezpečnostní rizika a vypracovat analýzu
- jak chránit – pojmenovat koncepci a politiku bezpečnosti, navrhnout a uvést do praxe bezpečnostní systémy

1.1 Bezpečnostní audit

Jedná se o souhrn činností, při kterých je zjišťován současný stav bezpečnosti organizace. Je vhodné, aby byl vykonáván zaměstnanci různých profesí, každý z nich si všimne jiných nedostatků. Nejčastěji se jedná o formální, či neformální inspekční pochůzku, na které je

týmem konstatován stav bezpečnosti organizace podle níže uvedených okruhů. Výsledkem bezpečnostního auditu je zpráva s pojmenováním rizik a navrhnutím možných nápravných opatření. Pojem Bezpečnostní audit je dnes často zaměňován s pojmem Audit ICT. Oba tyto audity mají společné prvky, ale v zásadě se liší. Bezpečnostní audit organizace má za úkol prověřit tyto okruhy:

- Fyzická bezpečnost
- Bezpečnost majetku (včetně hotovosti a cenností), bezpečnost budov, ostraha
- Osobní bezpečnost, včetně řízení lidských zdrojů
- Informační bezpečnost - ve smyslu ochrany zákonem nebo smluvně chráněných či cenných informací
- ICT bezpečnost, ve smyslu použití a nastavení hardware a software, včetně speciálních prostředků
- Bezpečnost práce a ochrana zdraví, požární ochrana

Vidíme, že bezpečnostní audit obsahuje i oblast informační bezpečnosti a ICT bezpečnosti. Naproti tomu audit ICT dále obsahuje činnosti ke zjištění stavu ICT prostředků v organizaci vzhledem k dosahování vytyčených cílů organizace, což už nelze považovat za bezpečnostní audit.

Také v základních uměleckých školách je nutno periodicky provádět bezpečnostní audit. Pro jeho provádění je vhodné vydat směrnici, podle které se audit řídí, a která zaručí jasné a měřitelné výsledky a stanoví konkrétní a termínovaný způsob jejich zaznamenání, zpracování a řešení.

Hodnocení systému ochrany osob a majetku

Při hodnocení systému ochrany objektu zjišťujeme podle (1):

- stav klasické mechanické ochrany – systémy zábran, specifické nástroje a prostředky
- stav fyzické ochrany – bezpečnostní hlídání objektu fyzickými osobami, najatá bezpečnostní agentura, nebo ve školách dozory učitelů
- stav režimové ochrany – posouzení systému organizačně – administrativních opatření (pohyb osob v objektu, pracovní režim, evidence pracovníků, vozidel, návštěv)

- použití technických prostředků ochrany – elektronický zabezpečovací systém, elektronická požární signalizace, systém průmyslové televize (kamerový systém)

Výzkumná část této práce se snaží najít mimo jiné odpovědi na otázky týkající se aktuálního vybavení a využívání systémů ochrany osob a majetku v českých základních uměleckých školách.

Hodnocení systému informační a ICT bezpečnosti

V rámci bezpečnostního auditu sledujeme též informační bezpečnost. Jedná se o informace, které jsou zásadní pro chod organizace, např. Know How organizace, cenná nashromážděná data, výsledky činnosti organizace, nebo citlivé údaje. Dříve byly tyto informace uchovávány v listinné podobě, dnes však jde v drtivé většině o elektronická data uložená a zpracovávaná v informačních systémech. Jedná se o rizika ztráty dat, nebo úniku a zneužití dat. Tyto informace mohou být ohroženy útokem zevnitř, nebo z vnějšku organizace, fyzickým útočníkem, nebo jinými jevy.

Je potřeba vyhodnocovat bezpečnost uložení a správy dat ve smyslu elementárního zabezpečení přístupu k počítačům a serverům (zamykání místností, systém přidělování klíčů pouze povolaným osobám a jejich poučení o specifičnosti jejich přístupu), zabezpečení uživatelských účtů počítačů bezpečnými, průběžně měněnými hesly, kontrola nastavení vnitřní sítě a uživatelských přístupů, kontrola zálohování dat atp.

V ZUŠ se jedná především o bezpečnost citlivých údajů žáků a zaměstnanců, data elektronické matriky školy, data povinné školní dokumentace, ekonomická data a data správní a provozní.

Na některé otázky týkající se stavu elementárního zabezpečení ICT prostředků v základních uměleckých školách se opět snaží odpovědět výzkumná část této práce.

1.2 Bezpečnostní politika

Informační bezpečnost podle (3) při provozu, správě a rozvoji informačního systému i informační bezpečnost v dalších částech organizace (personální, organizační a procesní) je potřeba řešit komplexně a systematicky. Pouhé nasazování jednotlivých bezpečnostních technologií nezaručí kvalitní a komplexní řešení bezpečnosti aktiv organizace. Sporná také bývá efektivita takto vynaložených prostředků. Pro efektivní řízení informační bezpečnosti v

organizaci je nutno vytvořit, přijmout a prosazovat bezpečnostní opatření a nařízení - politiku bezpečnosti informací.

Politika bezpečnosti informací tvoří základní stavební kámen bezpečnosti informací každé společnosti. Politika bezpečnosti informací je strategický dokument, definující základní koncepci ochrany informačních aktiv organizace. (3)

Politika bezpečnosti informací si klade za cíl pomocí základních bezpečnostních opatření nastavit dostatečnou úroveň bezpečnosti informací v celé organizaci. K prosazování požadavků politiky bezpečnosti informací v praxi musí být zvolena vhodná struktura dokumentů politiky bezpečnosti informací a vhodná forma prezentace cílených bezpečnostních opatření. Do adekvátních materiálů, které upravují interní chod organizace, mohou být implementována bezpečnostní opatření chránící informace. Jedná se o např. interní směrnice, pracovní řád, pracovní postupy, provozní předpisy apod. Tato opatření mohou být členěna podle chráněných oblastí (práce v internetu, lokální síti, práce z domova), nebo podle řízení uživatelských přístupů (administrátoři, vývojáři, uživatelé na různých úrovních organizační struktury)

Návrh struktury dokumentů politiky bezpečnosti informací

Hlavní politika bezpečnosti informací organizace

- jedná se o strategický dokument k vedení organizace: definuje bezpečnostní cíle, strategická informační aktiva organizace a základní bezpečnostní opatření, strukturu bezpečnostního řízení, apod.

Systémová politika bezpečnosti informací

- konkrétně pojmenovává jednotlivá bezpečnostní opatření pro specifikované oblasti organizace

Detailní politika bezpečnosti informací

- detailně specifikuje postupy pro implementaci a realizaci jednotlivých bezpečnostních opatření.

Základní umělecké školy v České republice jsou různě velké organizace od několika set až po jednotky tisíc žáků, některé jsou samostatnými organizacemi, jiné jsou součástí základních škol, některé působí v jedné budově, jiné v několika budovách, které např. sdílejí

s jinou školou. Těmto faktorům musí vedení školy přizpůsobit strukturu a obsah bezpečnostní politiky. Pokud nestanoví bezpečnostní politiku organizace samostatnou směrnicí (vhodné u velkých škol s rozsáhlejší organizační strukturou) je možno tuto implementovat do Pracovního řádu organizace (stanovit jednotlivé kompetence, odpovědnosti, sankce, povolení přístupů aj.) a do Školního řádu (pravidla pro práci s počítači a sítí pro žáky a jejich zákonné zástupce a sankce za jejich porušení).

2 Management rizika

Práce s rizikem je podle (4) nedílnou součástí manažerských aktivit. Riziko je spojeno s nadějí na dosažení výrazně dobrých výsledků na jedné straně, ale na straně druhé i s nebezpečím neúspěchu, který může vést k výrazným ztrátám ohrožujícím existenci organizace. Kvalitní management rizika jako určitý podsystém řízení organizace výrazně působí na snížení negativních důsledků nepříznivého vývoje okolního prostředí pro organizaci a její budoucí výsledky a také zvyšuje její připravenost na využití příležitostí. Zvyšuje se tak odolnost organizace i pružnost její reakce na změny. Ačkoliv je riziko spojováno především s komerčními organizacemi, musí být respektováno i u neziskových organizací včetně škol. Ani zde se nelze vyhnout neočekávaným skutečnostem, které závažně ovlivňují chod instituce.

2.1 Pojetí rizika

Na riziko je možno nahlížet ze dvou úhlů pohledu. Užší pohled vnímá riziko především jako možnost vzniku ztráty, možnost výskytu událostí ohrožujících dosažení cílů organizace, či jako nebezpečí negativních odchylek od určených úrovní cílů organizace. U tzv. čistých rizik (mají pouze negativní stránku) je toto pojetí do značné míry oprávněné. Naopak u tzv. podnikatelských rizik (nebezpečí podnikatelského neúspěchu spojené s nadějí dosažení zvláště dobrých hospodářských výsledků) sledujeme variabilitu možných výsledků procesů a aktivit, možnosti a pravděpodobnosti odchylek (oběma směry) od očekávaných a plánovaných výsledků.

Rizika z hlediska managementu bezpečnosti základní umělecké školy jsou rizika čistá. Školy jako neziskové organizace neusilují o hospodářský růst, proto se podnikatelská rizika při jejich činnosti vyskytují velmi zřídka. Dále tedy vzhledem k předmětu této práce budou popisována pouze rizika čistá.

Čistá rizika se obvykle vztahují ke ztrátám a škodám na majetku organizací a jednotlivců, poškození zdraví, resp. ztrátám života jednotlivců a členů organizačních jednotek, vyvolaných přírodními jevy (např. povodně, požáry, zemětřesení aj.), technickými systémy a jejich selháním (např. havárie výrobních zařízení) a jednáním lidí (krádeže a zpronevěry, stávky apod.) (4)

2.2 Proces managementu rizika

Proces managementu rizika lze podle Vebera rozdělit do několika dílčích částí:

- vymezení kontextu managementu rizika, identifikace rizik (faktory rizika)
- stanovení významnosti rizika, jeho vyhodnocení a rozhodnutí, zda je či není potřeba na riziko reagovat
- přístupy a opatření ke snížení rizika
- monitorování a prověřování systému řízení rizika

Vymezení kontextu a cílů managementu rizika

Smyslem vymezení kontextu je určení vnějšího a vnitřního prostředí, ve kterém organizace existuje. Zároveň se stanovují cíle řízení rizika v souvislosti se strategickými cíli organizace.

Jednou z nejvýznamnějších fází managementu rizika je identifikace faktorů rizika. Řídit je totiž možno pouze rizika včas a správně identifikovaná, na která se organizace připravila vhodnými způsoby jejich řešení. V této fázi je potřeba určit všechny faktory, které by mohly ohrozit dosahování především strategických cílů organizace, ale i cílů podřízených jednotek organizace. Identifikace faktorů vnitřních rizik je založena na znalosti a intuici řídících pracovníků. Faktory vnějších rizik musí management organizace průběžně pečlivě sledovat.

Metody pro usnadnění určení faktorů rizika:

- rozčlenění činností organizace na jednotlivé procesy a následné stanovení oblastí zranitelnosti a potenciálních problémů ohrožujících realizaci těchto procesů. Je potřeba si klást otázky co, kdy a kde by mohlo ohrozit průběh a výsledky jednotlivých procesů; (např. Jaký je vývoj dětské populace v oblasti, kde škola působí? Jaká je zde zaměstnanost? Jaké procento žáků opouští školu před

absolvováním prvního a druhého stupně ZUŠ a proč? Jsou žáci a pedagogové s činností školy spokojeni? Jaký je věkové rozložení zaměstnanců? Nehrozí náhlý současný odchod více pedagogů stejné kvalifikace? Hospodaří škola s vyrovnaným rozpočtem? atd)

- zpochybňování významných faktorů ovlivňujících výsledky činnosti organizace, které byly doposud považovány za jisté na základě dosavadních zkušeností (Dlouhodobá nájemní smlouva v budově školy – skutečně nehrozí vypovězení či ukončení? Hrozí zásadní změna legislativy? Ačkoliv za dobu trvání školy nedošlo k požáru, jsou stále činěna všechna dostupná opatření k jeho zamezení?);
- nápovědní listy, tedy seznamy otázek průběžně sestavované na základě dosavadních zkušeností a průběhu činnosti organizace (viz výše);
- kontrolní seznamy (checklist), resp. registry rizik, poskytující úplný přehled možných rizikových faktorů;
- skupinové diskuse a rozhovory s odborníky. Ideální formou je schůzka všech pracovníků zainteresovaných na konkrétní činnosti organizace při účasti expertů a formou brainstormingu s moderátorem diskutovat nad problémem a dojít k jasným závěrům a výstupům;
- strategické analýzy vnějšího a vnitřního prostředí – analýzy SWOT, PEST aj.;
- myšlenkové (kognitivní) mapy, jedná se o grafický nástroj zobrazení jednotlivých faktorů příčin rizik a dopadů rizik, mezi nimiž vytváříme orientované spojnice od příčin k dopadům.

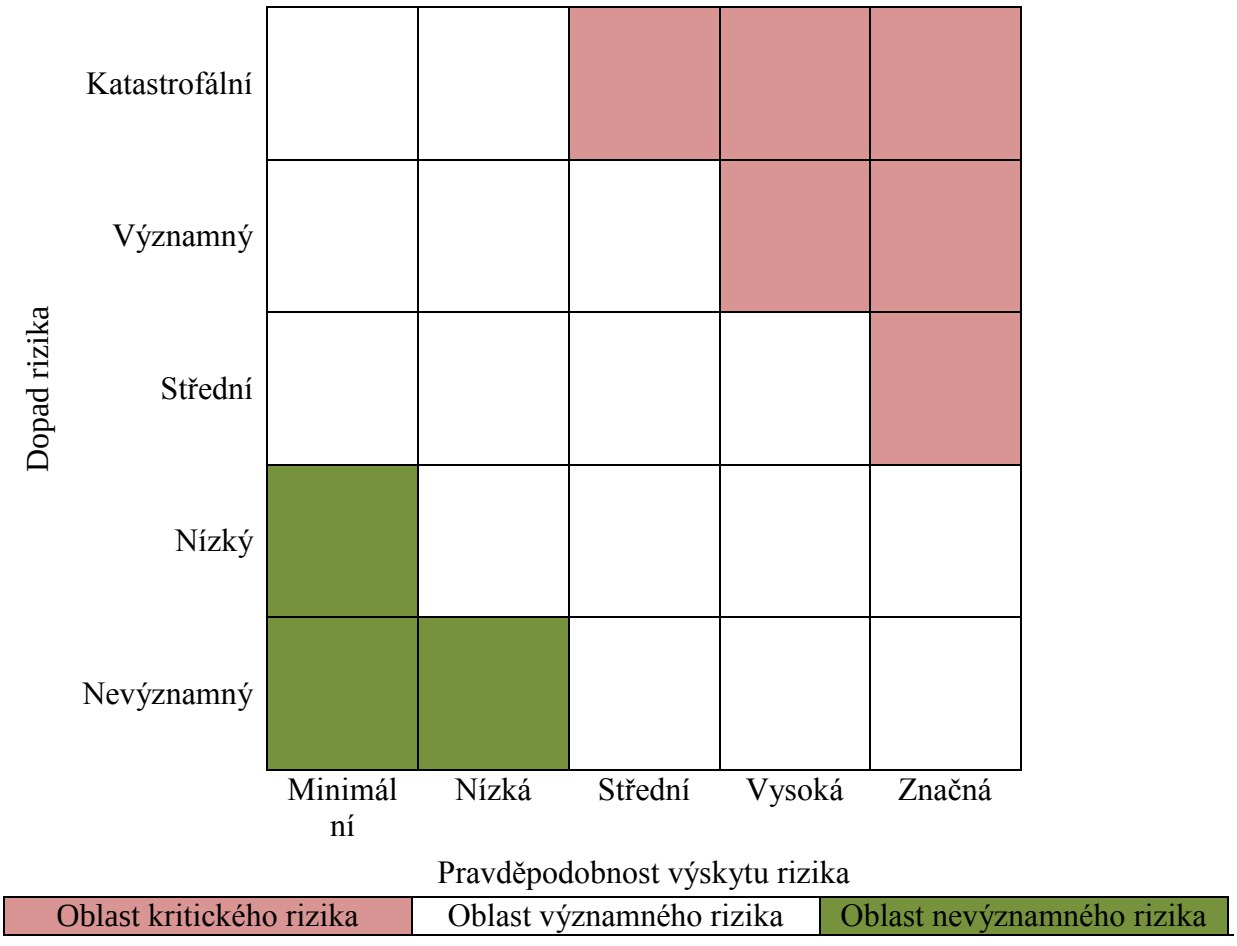
Výstupem fáze identifikace rizik je písemný seznam všech faktorů rizika, které mohou ohrozit činnost a existenci organizace. Nejedná se o činnost jednorázovou, ale o periodickou (čtvrtletně, ročně) či průběžnou činnost.

Stanovení významnosti rizika

Prostředí, ve kterém organizace působí, se dynamicky rozvíjí. S tímto rozvojem roste počet identifikovaných rizikových faktorů, kterých jsou řádově desítky až stovky. Omezené lidské a finanční zdroje (zvláště u neziskových organizací) a odlišný dopad různých rizik vedou k nutnosti diferencovat pozornost podle významu rizik. K tomu podle (4) slouží metody a nástroje stanovení významu rizik, zahrnující především analýzu citlivosti a matici hodnocení rizik.

Analýza citlivosti zjišťuje změnu hospodářských výsledků firmy v závislosti na změnách faktorů, které tyto ukazatele ovlivňují a jejichž budoucí hodnoty jsou nejisté. Jedná se tedy o sledování změny hospodářského výsledku v závislosti na změně např. velikosti prodejů, cen výrobků a služeb, nákupních cen vstupů, měnových kurzů aj. Analýza citlivosti se však obtížně provádí v neziskových organizacích, jejichž cílem není kladný hospodářský výsledek, ale jiné nehmatatelné hodnoty.

Matice hodnocení rizik je nástrojem expertního hodnocení organizace. Hodnocení konkrétních faktorů rizika provádí na základě svých zkušeností a znalostí pracovníci organizace, nebo externí odborníci. Významnost faktorů rizika se posuzuje ze dvou hledisek. Prvním je pravděpodobnost výskytu rizika, druhým intenzita negativního dopadu. Konkrétní faktor rizika je pak tím významnější, čím pravděpodobnější je jeho výskyt a čím intenzivnější je jeho negativní dopad. U obou hledisek obvykle používáme stupnici od jedné do pěti a konkrétní faktory zaznamenáváme do tabulky. Viz tab. 1



Tabulka č.1 - Matice hodnocení rizik (4)

Po zaznamenání všech faktorů rizika vyhodnocujeme jejich významnost a toto hodnocení je východiskem pro určení odpovědnosti za rizika pro konkrétní pracovníky a také pro volbu způsobu jejich řešení.

Měření rizika

Měření rizika se používá v ziskových organizacích pro vyjádření ovlivňování cílů organizace, např. výši zisku, likvidity, rentability atd.

Hodnocení rizika a rozhodování o něm

V této fázi managementu rizika posuzujeme přijatelnost rizika na základě vyhodnocení v matici hodnocení rizik, popřípadě měření rizika a rozhodujeme o jeho zvládání. Přijatelnost rizika posuzujeme vzhledem k rizikové toleranci, tj. výši rizika, kterou je organizace ochotna akceptovat. Pokud riziko nepřesahuje tuto toleranci, může je organizace přijmout, aniž by realizovala opatření na snížení rizika. Organizace je tedy připravena vypořádat se s případnými negativními dopady rizika. Je-li riziko posouzeno jako nepřijatelné, rozhoduje se organizace, zda se riziku vyhnout, či hledat strategie ke snížení rizika. Vyhnutí se riziku znamená upuštění od dané aktivity. Hlavní strategie ke snížení rizika jsou podle (4) tyto:

- eliminování či oslabení příčin vzniku rizika
- snižování negativních dopadů rizika
- transfer, čili přesun rizika na jiný subjekt (pojišťovnu, dodavatele, odběratele apod.)

Riziko snížené uvedenými strategiemi nazýváme zbytkové (reziduální) riziko.

<u>Přístupy ke snižování rizika</u>

<u>Opatření zaměřená na příčiny rizika</u>

Jedná se o prevenci rizika, neboť smyslem těchto opatření je eliminovat, nebo oslabit příčiny vzniku rizik, tedy předejít vzniku rizikových situací.

Ve školním prostředí se jedná např. o ochranu majetku a osob, zabezpečení informačních systémů, bezpečnostní politika, průběžné proškolování zaměstnanců, sledování vnějšího prostředí (např. vývoj populační křivky) a včasné přizpůsobení organizace novým vlivům aj.

Opatření orientovaná na oslabení negativních dopadů rizika

- Pokud nelze rizikům předcházet, je třeba snižovat nepříznivé důsledky rizik. Diverzifikace neboli rozložení rizika (v ZUŠ např.: nespecializovat se na jeden obor výuky, hrozí výpadek žáků, pokud nebude zájem o konkrétní obor; multifunkční učebny – v případě nenadálé události je možno výuku plnohodnotně přesunout do jiné učebny; zastupitelnost pedagogů, vedení školy; multioboroví pedagogové, zálohování dat atd.)
- Dělení (sdílení) rizika – dva i více účastníků se navzájem podílí na aktivitě či projektu, která může přinést negativní (obvykle finanční) dopad. (např. dvě ZUŠ se podílí na produkci náročného divadelního představení – próza, hudba, zpěv tanec, dekorace, propagace, pronájmy…)
- Zvyšování flexibility organizace – možnost rychle a bez velkých finančních nároků reagovat na změny v poptávce (multifunkční budova a třídy, multioboroví pedagogové)
- Kvalitní smluvní zajištění – smluvní vztahy obsahují časově, kvalitativně, cenově specifikované závazky a zároveň jednoznačné sankce za nesplnění závazků. (pronájem budov, dodavatelé energií, technologií, stavebních prací)
- Snižování fixních nákladů a vytváření rezerv – umožní snazší překonání období poklesu poptávky. (u neziskových organizací omezeno přesnými pravidly pro tvorbu rozpočtu)

Přenos rizika

Základním nástrojem pro přenos (transfer) rizika je pojištění. Právě oblast čistých rizik je oblastí pojistné ochrany. Pojišťovny zajišťují krytí nákladů vzniklých při nenadálých situacích (požár a další živelné škody, zranění pracovníka či klienta (žáka), pojištění za škody vzniklé třetím stranám, pojištění škod vzniklých při krádeži a vloupání.

Monitorování a prověřování systému managementu rizika

Cílem monitorování a prověřování managementu rizika je udržování, resp. zvyšování účinnosti tohoto systému v závislosti na měnících se podmínkách i případných změnách strategických cílů organizace, včetně cílů managementu rizika. (4)

Aktivní management rizika vede k průběžnému vytváření a aktualizování databáze rizik, která podporuje jejich účinné řízení.

Tato databáze by podle (4) měla především poskytovat

- popis jednotlivých faktorů rizik se zdůvodněním možnosti jejich výskytu
- rozdělení faktorů do kategorií
- odhad pravděpodobnosti výskytu a dopadu každého faktoru
- kvantitativní ohodnocení významu rizikových faktorů a jejich seřazení podle významnosti
- konkrétní přijatá opatření ke snížení rizik a termíny jejich realizace
- specifikování členů organizační struktury zodpovědných za sledování jednotlivých rizik a realizaci opatření
- přehled nejdůležitějších reziduálních (zbytkových, následných) rizik, která hrozí při realizaci opatření (pravděpodobnost výskytu a významnost dopadu)
- stupnice užité pro měření pravděpodobnosti výskytu a dopadů rizikových faktorů aj.

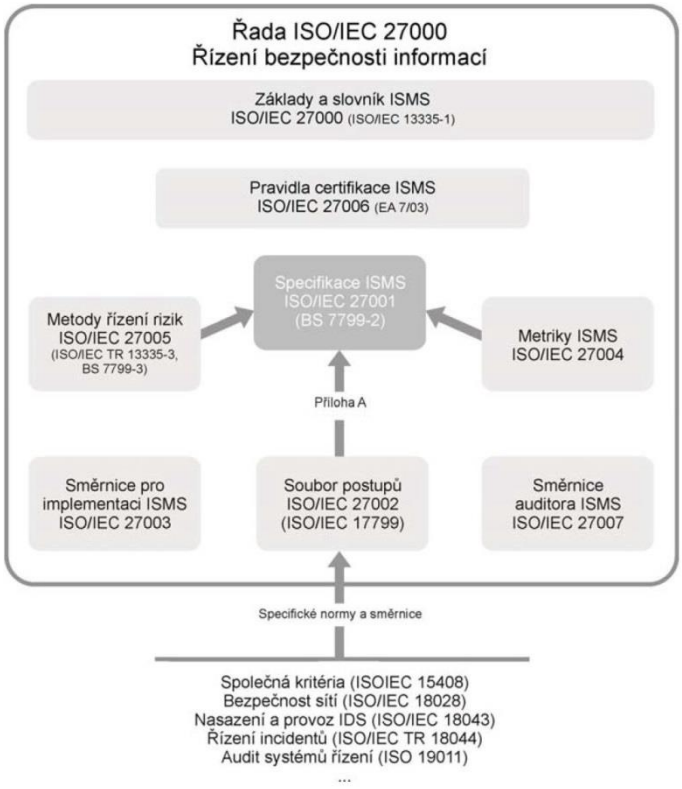
Management rizika je v neziskovém sektoru neprávem opomíjen. Právě základní umělecké školy bývají z hlediska bezpečnosti řízeny intuitivně bez profesionálního přístupu. Je vhodné implementovat moderní způsoby řízení používané v komerční sféře i v základním uměleckém školství. Mezi tyto způsoby řízení patří i management rizika. Ač se v případě škol jedná hlavně o tzv. rizika čistá, je na místě principy řízení rizika aplikovat i zde.

3 Management bezpečnosti informací podle ISO/IEC 27000

Cílem zavádění systémů managementu bezpečnosti informací je povýšit tuto oblast mezi jednotně řízené disciplíny v rámci funkčního integrovaného systému managementu. ISO/IEC 27000 je celosvětově uznávaná skupina norem, která určuje požadavky na systém managementu bezpečnosti informací, zásadně pak řízení bezpečnosti důvěry informací pro zaměstnance, procesy, ICT systémy a strategie organizací. Tyto standardy definuje Mezinárodní organizace pro normalizaci (ISO).

Řízení bezpečnosti informací procházelo v předcházejících dvaceti letech postupným vývojem a v posledních letech zaznamenalo významné změny. Potřeby řízení bezpečnosti informačních systémů vznikaly až s masovým rozšířením komunikační a výpočetní techniky

mezi běžné uživatele. Prvotní aktivity vycházely zejména z oblasti vojenství, kde také vznikaly první počítačové sítě. Jak se rozšiřovalo využití počítačů v komerční praxi, rostla i nutnost ochrany investic do IS/ICT před neoprávněnými přístupy a před zničením nebo výrazným omezením funkčnosti informačních systémů. Dalším prvkem, který výrazně posílil význam bezpečnosti informací, byla rostoucí globalizace ekonomiky a prohlubující se celosvětová dělba práce. (5)



Obrázek 2 - Koncept řady norem ISO/IEC 27000 (5)

Se zaváděním a certifikací systémů managementu bezpečnosti informací podle ISO/IEC 27000 se podle (6) začalo poměrně nedávno, přesto tato oblast zaznamenává od vydání normy v roce 2005 relativně rychlý vývoj. Zajímavý je hlavně pro organizace pracující s velkým množstvím dat, to však neznamená, že menší organizace typu škol nemohou principy popsané v této skupině norem využít při zabezpečování dat.

Cílem skupiny norem ISO/IEC 27000 je pomoci organizacím se zaváděním systémového přístupu při bezpečném zajišťování dat. Využívá se principu smyčky PDCA (z anglického plan-do-check-act), česky „plánuj, udělej, zkontroluj, jednej“ používaného při dosahování neustálého zdokonalování.

Při zajišťování bezpečnosti dat čelí manažeři stále novým rizikům, která ohrožují uložené informace. Proto je nutná neustálá snaha o zdokonalování systému bezpečnosti dat. Pod pojmem bezpečnost informací rozumíme jejich dostupnost, integritu (správnost a úplnost) a důvěrnost. Zásadní vliv na bezpečnost informací mívají ta rizika, která právě nejsou systematicky řízena. Např. výchova a loajalita pracovníků, smlouvy s dodavateli služeb v oblasti hardware a software, propojování informačních systémů aj. Proto je podstatné, aby o úrovni zabezpečení nerozhodoval útvar informačních technologií, ale vedoucí pracovníci sekcí, v nichž se s daty pracuje. To však na vedení sekcí (nebo přímo na vedení menších organizací typu škol) klade nárok na požadavek alespoň elementárních znalostí z oblasti ICT. Ne vždy je ale právě v základních uměleckých školách tomuto požadavku vyhověno. Chybí systematické proškolování (nejen vedoucích) pracovníků ZUŠ v oblasti ICT a to jak z uživatelského hlediska, ale i z hlediska základní stavby IS/ICT prostředků v organizaci.

Základem analýzy rizik, kterou plánování začíná, je důsledné sepsání všech informačních aktiv, posouzení jejich významu ohodnocení jejich zranitelnosti a jejich vyčíslení. Hodnota informačních aktiv organizace přímo souvisí s výší rizika, proto jsou tak významná pro analýzu rizik a tvoří její základní položku. Proto je počáteční a následně pravidelná inventura informačních aktiv (včetně určení jejich hodnot a držitelů) důležitým systémovým krokem.

Do seznamu aktiv by měla být zahrnuta všechna aktiva, která jsou pro organizaci z pohledu informací cenná, jako například informační systémy, databáze, hardware, software, ale také smlouvy, personální agenda, zaměstnanci, partneři, zákazníci dodavatelé atd., a díky své hodnotě si zaslouží přiměřený stupeň ochrany. (6)

Důležitost nebo cena konkrétních aktiv proto má být součástí seznamu aktiv. Skutečnou hodnotu aktiv je možno vyjádřit kvalitativně nebo kvantitativně, nebo například stupnicí. Podle (6) mnoho organizací, které certifikaci požadují, provádí chybně analýzu rizik až ke konci přípravy na certifikaci. Nejdříve intuitivně odhadují rizika a přijmou opatření k jejich snížení a teprve později (z důvodu požadavku v normě) formálně sestaví analýzu rizik. Může se tak stát, že některá rizika (např. technického rázu) budou eliminována velmi důkladně a za odpory nemalých finančních nákladů a na jiná (např. rizika personálního a organizačního charakteru) nebude pamatováno vůbec, nebo jen formálně, přitom jejich zajištění vyžaduje mnohonásobně nižší finanční podporu.

Analýzu rizik je nutno periodicky opakovat, neboť v dynamicky se rozvíjející organizaci přibývají stále nová aktiva a s nimi jejich nové možné zranitelnosti. Příčinou může být nejen rychlý rozvoj ICT, ale i měnící se legislativa aj.

3.1 Preventivní ochrana informací

Systematickým nástrojem k preventivní ochraně dat je plán zvládání rizik**.** Při jeho zpracovávání je nutno určit omezující faktory a závislosti, určit priority, schválit cíle a termíny, odhadnout požadavky na zdroje a určit zdroje, získat souhlas k využití zdrojů a identifikovat kritickou cestu.

Významná a pro firmu nepřijatelná rizika se zpravidla urychleně řeší přiměřených investičním nebo organizačním opatřením, které se zavádí formou projektového managementu. (6)

3.2 Provozování systému popsaného souborem pravidel

Pro zajištění sníženého dopadu rizik lze využít kombinace technických a organizačních opatření, z nichž velká část je předepsána normou. Ideálně popisuje opatření pro zajištění bezpečnosti organizační i technickou cestou norma ČSN ISO/IEC 27002, která dopodrobna vysvětluje opatření zmíněná v příloze A. Oba přístupy k přijímání opatření, organizačních i technických, musí být zajišťovány v harmonickém souladu (tab. 2).

Organizační opatření		**Technická opatření**	
Článek normy	Kritérium	Článek normy	Kritérium
Čl. 5	Formulace bezpečnostní politiky	Čl. 10	Řízení komunikace a řízení provozu
Čl. 6	Vnitřní organizace a externí partneři	Čl. 11	Řízení přístupu
Čl. 7	Řízení aktiv	Čl. 12	Akvizice, vývoj a údržba informačních systémů
Čl. 8	Bezpečnost lidských zdrojů	Čl. 14	Řízení kontinuity
Čl. 9	Fyzická bezpečnost a bezpečnost prostředí		
Čl. 13	Řízení incidentů, jejich správa a zlepšování		
Čl. 15	Soulad s právními požadavky	Čl. 15	Soulad s normami pro technickou shodu

Tab. č. 2 - Výčet organizačních a technických opatření (6)

Zatímco technická opatření jsou zpravidla zajišťována ve firmách na dobré úrovni, organizační opatření jsou spíše sporadická.

3.3 Monitorování chodu systému a odchylek

Systémový požadavek, který je pravděpodobně nejdůležitější a podle (6) v praxi nejvíce opomíjený, je pravidelné monitorování a přezkoumávání všech implementovaných nástrojů řízení a opatření ke snížení rizik.

O tomto monitorování a přezkoumávání musí být vedeny příslušné záznamy. Nestačí tedy obecně předepsat, že někdo má v pravidelných intervalech kontrolovat určité logy, protokoly ze zálohování, zprávy o reinstalaci antivirových databází apod., ale je bezpodmínečně nutné, aby o každém provedení těchto opatření zodpovědná osoba vedla i příslušné záznamy, a to nejen v případě, že dojde k bezpečnostnímu incidentu nebo bezpečnostní události, ale i tehdy, když je vše v pořádku. Forma těchto záznamů může být velmi jednoduchá a příslušného pracovníka nemusí prakticky vůbec zatěžovat. (6)

3.4 Management incidentů

Důležitou součástí managementu bezpečnosti informací je management incidentů. Tento druh řízení bývá obtížné zavést, ale je nepostradatelný. Kvalitní systém řízení bezpečnosti dat se bez sledování incidentů a výskytu anomálních událostí neobejde. Vedení organizace proto musí vynakládat velké úsilí při přesvědčování sebe i organizace o účelnosti shromažďování těchto údajů a jejich rozboru.

Nejčastější nedostatky managementu incidentů:

- bezpečnostní incidenty jsou zaznamenávány jen zřídka, nebo vůbec,
- není určeno, jak mají být bezpečnostní incidenty klasifikovány (např. riziko – nedostatek – incident), nebo není knihovna bezpečnostních incidentů kontrolována a řízena,
- není prováděn pravidelný rozbor bezpečnostních incidentů nebo nejsou přijímána odpovídající nápravná opatření,
- neprovádí se „učení se z bezpečnostních incidentů“.

3.5 Učení se z chyb

Aby měly předchozí kroky smysl, je nutno výsledky monitorování vyhodnocovat, identifikovat slabá místa a přijímat nová opatření pro zlepšení. Z důvodu neustálého technického pokroku a pozitivní i negativní vynalézavosti v oblasti ICT je třeba být neustále ve střehu a známá rizika přehodnocovat a nová identifikovat. Z negativních dopadů je nutno vyvozovat důsledky pro eliminování jejich příčin.

Podle (6) je pro efektivní zavedení systémového přístupu k managementu bezpečnosti informací zapotřebí:

- pochopit, co je to management rizik a jak se správně realizuje,
- naučit se zacházet s informacemi podle klasifikace jejich míry důvěrnosti,
- hodnotit efektivnost systému na základě sběru informací,
- naučit se využívat záznamů o incidentech k analýzám a dalšímu zlepšování systému.

3.6 Certifikování zavedených systémů

Certifikací systému managementu bezpečnosti informací zvýší organizace důvěryhodnost vůči svým partnerům. Při certifikačním auditu se podle (6) harmonicky posuzuje:

- systematický přístup založený na rozhodnutí vedení o míře přijatelnosti rizik a způsob nakládání organizace se svými riziky,
- stav povědomí pracovníků o jejich vlivu na bezpečnost informací vzhledem k pracovní pozici,
- objektová a technická bezpečnost,
- bezpečnost informačních a komunikačních technologií (bývá často protěžována na úkor předchozích tří oblastí) – vzhledem k rychlému rozvoji má ICT největší dynamiku rizik.

Řízení bezpečnosti informací podle řady norem ISO/IEC 27000 není pro základní umělecké (ani jiné) školy povinností. Může však být dobrým vodítkem pro vystavění funkčního a kvalitního systému bezpečnosti informací. Jen škola, která nepodceňuje možnost negativních dopadů překotného rozvoje prostředků ICT, se může s klidným svědomím věnovat svému poslání.

4 Ochrana osob a majetku

Následující stať zkráceně popisuje nejzákladnější elektronické prvky ochrany osob a majetku. Jejím cílem je letmé nahlédnutí do problematiky. Je určeno zájemcům z řad školského managementu pro primární seznámení s problematikou. Autor vychází ze svých znalostí nabytých předchozím vzděláváním a zároveň se snaží teorii propojit se zkušenostmi z praxe řídícího pracovníka v základní umělecké škole.

Bezpečnost subjektu je chápána jako stav, kde rizika plynoucí z hrozeb jsou eliminována na akceptovatelnou úroveň. Má-li se subjektu zajistit bezpečnost, musí být známy základní hrozby, které mu mohou způsobit újmu. Mezi základní hrozby v současnosti patří činnost kriminálních živlů či jiných osob, jejichž cílem je zcizení, neoprávněné nakládání, poškození nebo úplné zničení chráněných aktiv. (7)

Další základní hrozbou subjektů je riziko požáru a dalších přírodních živlů, popř. havárií, jejichž důsledkem je ohrožení života a zdraví lidí, či poškození nebo úplné zničení movitého i nemovitého majetku a ztráta dat.

4.1 Elektronické zabezpečovací systémy (EZS)

Předně je potřeba zmínit, že jakémukoliv elektronickému zabezpečení objektu musí předcházet adekvátní zabezpečení mechanické – mechanické zábranné systémy. Podle (8) je dělíme na tři kategorie. Prostředky obvodové ochrany (ploty, zdi, brány aj.), prostředky objektové ochrany (zabezpečení všech stavebních otvorů v objektu: dveří, oken, balkonových dveří, sklepních oken, vikýřů, zásobovacích a energetických šachet apod.) a prostředky individuální ochrany (mobilní a stabilní trezory, ohnivzdorné skříně, příruční pokladny apod.)

Vedení školy musí zhodnotit (např. v rámci bezpečnostního auditu viz výše) rizika překonání MZS a vniknutí neoprávněných osob do budovy školy, ať v době vyučování, nebo mimo ni a přiměřeně tomu zvolit adekvátní prostředky. Obecné povědomí o mechanických zábranných systémech pro školu vhodných je poměrně dobré i v prostředí školského managementu, proto by nebylo účelné zde tuto problematiku rozebírat do větší šíře.

Elektronické zabezpečovací systémy (někdy též elektronická zabezpečovací signalizace, nebo poplachové zabezpečovací a tísňové systémy - PZTS) mají za úkol odhalit narušení střeženého prostoru, nebo manipulaci se střeženým předmětem nepovolanou osobou a předat tuto informaci dál ať už prostřednictvím akustického a optického alarmu, GSM sítí, nebo na

pult centralizované ochrany. EZS tudíž sám nezabrání vstupu nepovolané osoby do střeženého prostoru, ale spolehlivě informuje o jeho narušení a tím snižuje možné škody. EZS se vždy skládá z několika součástí, které mají podle (9) tyto svou specifickou funkci:

- **ústředna** - srdce i mozek celého systému. Přebírá signály ze svých periferií, signály vyhodnocuje a následně informuje o stavu, v jakém se systém nachází, zajišťuje napájení čidel a prvků EZS elektrickou energií, pomocí ovládacích zařízení umožňuje nastavení a řízení systému (uvedení do stavu střežení a do stavu klidu), umožňuje diagnostiku EZS;
- **čidla** - zařízení, která monitorují narušení střeženého prostoru. Dělíme je na prvky ochrany plášťové (magnetické kontakty na dveře a okna, detektory tříštění skla), prostorové (infračervená, ultrazvuková, mikrovlnná čidla a jejich kombinace) a předmětové (otřesová a závěsná čidla);
- **ovládací a indikační zařízení** - slouží především k aktivaci a deaktivaci střežení objektu a k indikaci stavů zařízení EZS (typicky kódová klávesnice)
- **tísňové hlásiče** – slouží k vyhlášení tichého poplachu v případě ohrožení osoby;
- **prostředky poplachové signalizace** – akustické a optické hlásiče upozorňující na narušení objektu, nebo grafické tablo (zobrazení na PC) pomáhající u velkých objektů k rychlé identifikaci místa narušení;
- **přenosová zařízení** – součástí ústředny EZS, slouží k ovládání, nastavení a monitorování EZS pomocí telefonní linky, mobilního telefonu nebo internetu, nebo přeposílání informací na PCO (pult centralizované ochrany)

Ředitelé základních uměleckých (jakož i jiných) škol nesou odpovědnost za správu svěřených hodnot a bezpečnost prostředí pro žáky a zaměstnance školy. Je proto samozřejmé, že se musejí zajímat o adekvátní zabezpečení budovy jak mechanickými zábrannými systémy tak doplňkově i elektronickými zabezpečovacími systémy. MZS chrání školu v době vyučování i mimo ni proti vniknutí nepovolaných osob. V době mimo vyučování (a jiný provoz školy) je vhodné zvýšit zabezpečení budovy instalací EZS, která hlasitým nebo tichým poplachem upozorní na vniknutí nepovolané osoby do objektu školy a případně přivolá pomoc hlášením alarmu na pult centralizované ochrany, nebo pomocí GSM přenosu. Už sám fakt nainstalovaného EZS (nutno tento fakt vyvěsit na vnějším plášti objektu) narušitele obvykle odradí.

4.2 Systémy průmyslové televize (CCTV)

Zkratka CCTV vychází z anglického Close Circuit TeleVision v českém překladu uzavřený televizní okruh. Jedná se o systém, který za pomoci kamer, přenosových prvků, zobrazovacích a případně záznamových zařízení pomáhá střežit určený prostor. Dříve byl tento okruh skutečně uzavřeným, čili distribuovaným pouze ve sledovaném objektu, dnes je možno za pomoci třeba jen webového prohlížeče a příslušných kodeků záznam z kamer sledovat kdekoli. Uzavřenost systému je tedy dnes myšlena spíše zabezpečením (zaručí správce sítě) a omezeným přístupem.

Podle způsobu zpracování a přenosu signálu dělíme dnes CCTV systémy na:

- **Analogové** – nejstarší, avšak stále hojně využívaný systém. Kamery jsou dnes často digitální, což usnadňuje ovládání, umožňuje nadstavbové funkce, avšak přenos signálu je analogový.
- **Digitální** – HD-SDI (High Definion Serial Digital Interface) - technologie, která přišla z televizního vysílání. Jedná se o systém s vysokým rozlišením, signál se přenáší v nekomprimované podobě bez zpoždění a zkreslení po stejných přenosových cestách, jako analogový. Je tedy možné snadno systém upgradovat bez nutnosti budovat nové vedení.
- **IP kamery** - digitální kamey, které v sobě mají zabudovaný web server, takže je možné je připojit ke stávající ethernetové síti a jejím prostřednictvím kameru ovládat (pohyb, nastavení objektivu atd.), přenášet digitální signál a prostřednictvím technologie PoE (Power over Ethernet) kameru i napájet. Ceny IP kamer se dnes již přiblížily cenám standartních kamer, jedná se tedy o výhodnou alternativu při existenci ethernetové sítě, nebo o úsporu při budování pouze jedné sítě.

Kamerové systémy obsahují podle (10):

- **Kamery** – snímací zařízení:
    - objektiv - sledované parametry: ohnisková vzdálenost (čím menší ohnisková vzdálenost, tím širší úhel záběru), rozsah nastavení ohniskové vzdálenosti (transfokace) u objektivů ZOOM, rozsah clony (minimální

clona má vliv na světelnou citlivost, maximální má vliv na kvalitu obrazu za vysokého osvitu);

- snímací chip - sledované parametry: CCD vs. CMOS (11), rozlišení 1,3 – 11,4 Mpix, počet snímků za sekundu (FPS);
- elektronika;
- servomotor pro pohyb – pokud je požadováno (pozor na dostatečnou rychlost pohybu);
- vyhřívání při venkovním provedení;
- adekvátní kryt podle prostředí – do vlhka, prachu, antivandal apod.

- **Přenosové cesty** – koaxiální kabel, kroucený pár, optické kabely, radiový přenos, LAN přenos, GSM přenos, protokoly RS-232 a RS-485 (12) (13)
- **Ovládání kamer PTZ** – z anglického Pan Tilt Zoom. Povolaná osoba na sledovacím stanovišti (dohledové centrum, velín, vrátnice, ředitelna) ovládá přepínání a pohyb kamer podle aktuální potřeby, jinak je provoz automatizován;
- **Záznamová zařízení** - DVR (Digital Video Recorder), HD-SDI videorekordéry, Síťové videorekordéry NVR (Network Video Recorder), Videosystémy pro PC (13)
- **Zobrazovací zařízení** - koncové zařízení, které umožňuje sledovat obraz přímo z kamer, nebo záznam z videorekordéru. Nejdůležitějším parametrem pro výběr CCTV monitoru je poměr stran, neboť poměr 4:3 je vhodný pro analogové CCTV kamery a poměr 16:9 se používá pro HD-SDI kamery;

Nedílnou součástí provozování systému průmyslové televize je právní aspekt. Jedná se o problematiku zacházení s osobními údaji, kterou řeší zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů (dále jen zákon). Zkráceně lze říci, že pokud se jedná o kamerový systém se záznamem, jedná se o zpracování osobních údajů a je nutno postupovat podle zákona. Dále jsou uvedeny některé povinnosti související podle (14) s provozem kamerového systému se záznamem.

- nasazení kamerového systému ve škole je možné pouze v případě, že selhaly ostatní méně invazivní prostředky pro ochranu osob a majetku;

- doba uchování záznamů – za standartní se považuje doba maximálně tří dnů, což je doba nezbytná pro místní prošetření i v případě že se incident stal o víkendu. V období prázdnin je povolena doba přiměřeně delší;
- správce osobních údajů (škola) může zpracovávat osobní údaje pouze se souhlasem subjektu údajů (žáků, zaměstnanců, návštěvníků aj.). Možno využít výjimek podle § 5 odst. 2 písm. a) až g) zákona, avšak je nutno dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů;
- správce osobních údajů je povinen informovat subjekty údajů v jakém rozsahu a pro jaký účel budou osobní údaje zpracovávány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny. Dále jej musí informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21 zákona. Žáky a zaměstnance informuje ve vnitřním předpisu, ostatní osoby informuje informačními tabulkami u vstupu do sledovaných prostor;
- správce je povinen, a to ještě před zahájením zpracovávání dat prostřednictvím kamerového systému, oznámit zamýšlené zpracování osobních údajů Úřadu pro ochranu osobních údajů;
- shromážděné údaje je možno použít pouze v souladu s účelem, ke kterému byly shromážděny (jsou-li záznamy pořízené za účelem ochrany majetku, nelze je použít např. pro kontrolu docházky);
- správce je povinen přijmout a dokumentovat taková technicko-organizační opatření týkající se provozu kamerového systému, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k uchovávaným osobním údajům;

4.3 Přístupové systémy (ACS)

Elektronický přístupový systém (Access Control System) (15) umožňuje kontrolovat vstup osob do budovy, oddělení, místnosti. Dá se říci, že je to pohodlnější a bezpečnější varianta klasických klíčů. Využívá se čipových karet, nebo přívěšků, dále biometrických údajů, jako otisk prstu, nebo scan oční duhovky. Po např. přiložení čipu k terminálu u dveří, nebo turniketu systém identifikuje osobu a podle přidělených práv jej vpustí do dalšího prostoru, či nikoli. Je možné systém propojit s docházkovým systémem a kontrolovat tak

pracovní dobu zaměstnanců. Dále je možné zpětně vyhledat pohyb zaměstnanců a např. v případě krádeže tak případně identifikovat pachatele z „vlastních řad“, častěji však krádeži předejít. Čipy není možné kopírovat tak snadno, jako klíče, biometrické údaje není možno kopírovat vůbec, snižuje se tak riziko zneužití neoprávněnou osobou. V případě škol, tedy objektů, do kterých často oprávněně vstupují „nahodilé“ návštěvy, je vhodné systém doplnit vrátným, který posoudí oprávněnost návštěvy a osobu do budovy vpustí. Další možností je využití tzv. elektronického vrátného, tedy systému zvonků a domovního telefonu (videotelefonu). Oprávněnost návštěvy zde posoudí a případně povolí odpovědný pracovník.

4.4 Přepěťové ochrany

Přepěťové špičky jsou krátkodobé extrémní nárůsty elektrické energie v elektrickém obvodu. Tyto energetické špičky jsou sice krátkodobé, ale mohou vážně poškodit elektronická zařízení. Přestože netrvají déle než několik mikrosekund, mohou iniciovat následný destruktivní proces celých komplexních systémů. (16)

Dvěma nejběžnějšími druhy vzniku přepěťových špiček jsou **blesk** a **spínací přepětí**. Blesk může způsobit vznik přepětí při úderu do samotné budovy, nebo blízkých objektů, nebo při úderu do vnějšího přenosového elektrického vedení, v tom případě se přepětí může přenášet i na velké vzdálenosti. Spínací přepětí mohou způsobit vypadlé jističe, zkraty, odběrové změny. Například opětovné připojení elektrické rozvodny po větším výpadku elektrické rozvodné sítě může spínací přepětí způsobit. Je tedy nabíledni zajímat se o přepěťovou ochranu z důvodu ochrany nejen elektrických spotřebičů, ale hlavně výpočetní techniky a počítačových sítí. K jejich ochraně slouží přepěťové ochrany. Vyrábějí se pro různé kategorie ochrany, které jsou stanoveny v normě ČSN EN 60664-1. Je tak možno chránit nejen napájecí elektrická vedení, ale i datové sítě.

4.5 Elektronická požární signalizace (EPS)

Jak už je z názvu patrné, systém Elektronické požární signalizace je soubor zařízení, který má za úkol lokalizovat a hlásit požár, případně se pokusit o jeho uhašení. Hlášení probíhá akusticky (siréna) a opticky (maják, monitor počítače). U budov, které bývají v některých denních či nočních dobách bez pracovníků (typicky školní budovy) je vhodné

napojit elektronickou požární signalizaci na pult centralizované ochrany, jinak hrozí, že i funkční požární signalizace nepomůže ani snížit škody.

Druhy požárně bezpečnostních zařízení (17):

- **zařízení pro požární signalizaci** – manuální hlásiče (požární tlačítka), optické (kouřové) hlásiče, teplotní hlásiče, hlásiče vyzařování plamene, detekce pomocí CCTV
- **zařízení pro potlačení požáru** (samočinné hasicí systémy),
- **zařízení pro únik osob** (nouzové osvětlení, panikové kování dveří),
- **zařízení pro omezení šíření požáru** (např. požární klapka, požární dveře)

Další prvky elektronické požární signalizace:

- **požární ústředna** – zajišťuje napájení systému (ze sítě a záložní akumulátor), sbírá data z požárních čidel a hlásičů, vyhodnocuje je a v případě potřeby spustí alarm, hlásí požár na pult centralizované ochrany (pokud je funkce k dispozici), spouští automatický hasící systém, požární vzduchotechniku, požární rozhlas (pokud jsou instalovány) umožňuje spravovat, diagnostikovat a nastavovat systém, signalizuje provozní a poruchové stavy, předává obsluze informaci o lokalizaci požáru;
- **další zařízení systému EPS** - po vyhlášení poplachu ústřednou jsou aktivovány akustické a vizuální signalizační zařízení (sirény, majáky, hlášení požárního rozhlasu). Nadstavbou pro systém EPS a další systémy může být komplexní monitorovací systém, který na jednom místě (tzv. velíně) slučuje správu všech elektronických systémů. Velín bývá umístěn ve vrátnici, pokud budova disponuje fyzickou ostrahou.

4.6 Hrozby pro školu z hlediska využití elektronické ochrany a jejich možná prevence

Z hlediska provozu základních uměleckých škol je potřeba tuto kapitolu rozdělit na dva časové úseky. Na dobu mimo provoz školy (noc, víkend, prázdniny) a na dobu během vyučování.

4.6.1 V době mimo provoz školy

V době mimo provoz školy, tedy v noci, o víkendech a prázdninách hrozí škole vloupání a s ním spojené poškození majetku, odcizení majetku, ztráta elektronických i papírových dat, včetně citlivých údajů žáků a zaměstnanců a s tím spojené jejich zneužití. Toto riziko se dá účinně snižovat instalací kvalitního mechanického zabezpečení (dveře, zámky, mříže) a to v rámci obvodové ochrany i dalším mechanickým zabezpečením důležitých prostor uvnitř budovy (kancelář, ředitelna, prostory obsahující cenné vybavení, server apod.). Dále je vhodné instalovat též výše popsaný systém elektronického zabezpečení, napojený na pult centralizované ochrany a jako nadstavbu kamerový systém se záznamem.

Dále je možné účinně snížit dopady požáru (úmyslně založeného žhářem, nebo náhodně vzniklého např. zkratem v elektroinstalaci) instalací elektronické požární signalizace, která však musí být napojena na pult centralizované ochrany, aby byla zajištěna její funkce i v nepřítomnosti osob v budově školy.

4.6.2 V době provozu školy – nepovolané osoby, žáci, jejich doprovod

V době provozu základní umělecké školy (v dopoledních hodinách administrativní činnost, úklid, údržba, v odpoledních hodinách výuka) je potřeba kontrolovat pohyb osob v budově a zabránit vstupu nepovolaných osob. Hrozí totiž krádeže školního i soukromého majetku pracovníků a žáků školy na chodbách, v šatnách i ve třídách, kabinetech, kancelářích, skladech, dále poškozování majetku, žhářství nebo ublížení na zdraví patologickým jedincem. Třídy, kanceláře, sklady apod. je bezpodmínečně nutné zamykat v době, kdy se v nich nenalézá odpovědný pracovník. Vstup osob je možno monitorovat elektronickým přístupovým systémem, který však vyžaduje i přítomnost vrátného, neboť by se do budovy nedostali nahodilé návštěvy. Další možností je použití elektronického vrátného, tedy systému zvonků a domovního telefonu, kdy se každý příchozí (žák, jeho doprovod, návštěva) ohlásí příslušnému pracovníkovi školy, který jej pak podle uvážení do budovy vpustí. Pro snížení rizika vstupu nepovolané osoby např. se žákem je vhodné instalovat u vstupu do školy kameru, aby bylo možné v případě potřeby identifikovat možného pachatele. Zde je nutné připomenout, že kamerový systém nesmí být využit ke sledování pohybu osob oprávněných, znamenalo by to nepřiměřený zásah do jejich soukromí.

Neoprávněná osoba se rovněž po vstupu do budovy může ukrýt na skrytých místech (WC, půda, sklep, úklidová komora apod.). Je tedy vhodné před uzavřením budovy vždy při ukončení provozu taková místa kontrolovat.

5 Základní zabezpečení elektronických dat

Pokud bychom chtěli používat jednotlivé osobní počítače jen jako důmyslnější psací stroje, data bychom si nosili na přenosném médiu, tiskli pouze na místní tiskárně, případně bychom počítač měli pro krácení dlouhé chvíle, zřejmě bychom se bez počítačových sítí obešli. Avšak v dnešní době je tato myšlenka poněkud absurdní. Počítačové sítě a s nimi přicházející hrozby jsou všude kolem nás, aniž bychom si to uvědomovali.

5.1 Počítačové sítě

Dnešní doba je typická využíváním počítačových sítí, ať už z pohledu získávání informací, publikování vlastních myšlenek, nebo zábavou, komunikací, studiem i prací přes internet, nákupem a prodejem zboží, pomocí webových stránek atd…

Díky počítačovým sítím a zejména internetu se v současnosti děje mnoho věcí snáze a rychleji. Získávání a předávání informací je díky vyhledávačům a elektronické poště rovněž snadné a rychlé. A to je jen střípek z celkového množství výhod a služeb, které lze dnes pomocí počítačových sítí využívat. (18)

5.1.1 Typy sítí

LAN (Local Area Network) – lokální síť, která umožňuje lokální komunikaci, sdílení dokumentů a tiskáren. Její součástí jsou koncová zařízení (např. počítače se síťovou kartou, tiskárny, scannery), přenosová média (metalické kabely, optické kabely, vzduch) a další síťová zařízení, která propojují koncová zařízení. Nejběžnějším technologií umožňující přenos dat po síti LAN je Ethernet.

Se sítí typu LAN s technologií Ethernet se nejčastěji setkáme ve školním prostředí.

WAN (Wide Area Network) – rozlehlá síť, která spojuje jednotlivé lokální sítě, často na velké vzdálenosti. Umožňuje přenášet v reálném čase soubory, komunikovat, využívat přístup k webovým stránkám. Dnes nejběžnější technologie, které umožňují přenos dat v rozlehlých sítích, jsou ISDN a DSL (v různých variantách).

Typickým představitelem sítě WAN je Internet.

Intranet *– termínem Intranet můžeme označit webové služby dostupné oprávněným uživatelům v rámci LAN pouze z počítačů v této síti.*

Extranet – *termínem Extranet můžeme označit webové služby podniku, které jsou dostupné i vnějším uživatelům, například obchodním partnerům. Uživatelé musí mt uživatelská jména a přístupová hesla.* (18)

5.1.2 Bezpečnost sítí

Abychom mohli vnitřní počítačovou síť zabezpečit, musíme napřed vědět, před kým a proč ji máme chránit. Útočníky můžeme rozdělit na dva druhy – na průzkumníky a crackery.

Průzkumník - hacker je člověk, který v důsledku nechce škodit, ale jde mu jen o proniknutí do systému za účelem jeho dobrého pocitu, že to dokázal, něco obešel, prokázal své schopnosti. Je mu v podstatě jedno, kam se dostává a nejde mu o zisk.

Cracker si konkrétní systém vybírá cíleně za účelem finančního, či jiného zisku. Může být úkolován konkurencí pro krádež dat, pro paralyzaci systému, může napadený systém zneužít pro ukládání nelegálních dat, nebo využít jeho výpočetní potenciál.

Proč útočník systém napadá? Může hledat zajímavý obsah. Chce nainstalovat software, který mu umožní další nelegální činnost. Snaží se obejít Firewall, aby se dostal do vnitřní sítě. Chce využít diskovou, nebo výpočetní kapacitu napadené sítě. Chce na napadeném webserveru zveřejnit své informace.

5.1.3 Přehled nejčastějších síťových útoků

V následující pasáži budou pouze okrajově zmíněny některé druhy síťových útoků, hlubší rozbor by nutně vedl k příliš odbornému textu z oblasti informatiky, což není cílem této práce. Pro základní informaci vedoucím pracovníkům škol stačí stručný souhrn.

Odposlouchávání komunikace – hrozí v nešifrovaném kanálu na internetu. Komunikace probíhá mezi dvěma privátními sítěmi, nebo počítači. Řešení – zásadně používat šifrovanou komunikaci, např. SSL, SSH, GnuPG, PGP.

DoS útok (Denial Of Service) – při tomto útoku je server útočníkem zahlcen mnohonásobně vyšším množstvím dat, než je normální stav. Útok může být veden i z více strojů najednou. Server se proti tomuto útoku může bránit kontrolou počtu spojení z jedné IP adresy. Po překročení limitu odepře další spojení.

Podvržení IP adresy – tento útok hrozí, pokud se stroje, nebo Firewall spoléhají na autentizaci pouze podle IP adresy. Řešení – autentizace nesmí být založena pouze na kontrole IP adresy – nastavení Firewallu.

Man In the Middle (muž uprostřed) - při tomto útoku je přímá komunikace mezi dvěma stroji přesměrována přes útočníkův stroj. Ten se vydává za cílový server a odposlechne, popřípadě změní data, která proudí od klienta k serveru. Typicky je tento útok využíván při krádeži přihlašovacích údajů k internetovému bankovnictví. Řešení – používat pouze komunikaci s ověřenými klíči od certifikační autority. (19)

5.1.4 Základní zásady zabezpečení

Zabezpečení sítě je hlavně prací správce sítě, ředitel školy tedy musí pověřit touto činností odpovědného pracovníka. Ideálním případem je zaměstnat člověka přímo na pozici správce sítě, avšak to může být rentabilní pouze u velkých škol, potažmo větší sítě. Druhou možností je najmout externí firmu, která však není ve škole k dispozici ihned, když se vyskytne problém. Třetí možností je pověřit funkcí správce sítě učitele, který je v oblasti IT dostatečně zdatný (nezaměňovat funkci správce sítě a ICT koordinátora-metodika) (20). Zde by však ředitel měl být velmi obezřetný, neboť se dá předpokládat, že tento pedagog nebude znát všechna úskalí problematiky. V tom případě je možná kombinace předchozích variant, najatá externí firma síť instaluje a zajišťuje její bezpečnost a pověřený pedagog řeší každodenní drobné problémy, na které stačí.

Ředitel by se měl zajímat, jak je počítačová síť koncipována a zda je adekvátně zabezpečena. V prvé řadě zda je oddělena od vnější sítě (Internetu) Firewallem, který je aktivní. Zda jsou důležité síťové prvky v místnostech, kde je minimální riziko zneužití. V případě používání WiFi je potřeba určit okruh osob, které budou mít právo přístupu do sítě přes WiFi a podle tohoto okruhu stanovit její zabezpečení a oddělení od vnitřní sítě. Pokud je používána vzdálená plocha, zda jde o bezpečný software a zda se zaměstnanec chová z hlediska bezpečnosti dat správně. Zda a jakým způsobem se pracuje s hesly. Zda se data pravidelně a dostatečně zálohují. Zda počítače, na kterých pracují žáci, mají filtrovány nevhodné webové stránky.

Je vhodné též poučit pracovníky, kteří na počítačích pracují, jak se bezpečně chovat. Zejména při práci s emailem, při sdílení souborů, při vytváření hesel, při přihlašování k uživatelským účtům, zda a za jakých podmínek mohou použít síť WiFi. Pracovníci musejí též správci sítě, nebo vedení školy hlásit všechny podezřelé skutečnosti, které v souvislosti s provozem systému zjistí, aby bylo možno včas adekvátně zasáhnout. Dále je nutné zaměstnance upozornit na možnost postihu v případě nelegálního využívání sítě a počítačů.

Výzkumná část

6 Úvod

Cílem tohoto výzkumu bylo ověřit skutečný stav bezpečnosti českých Základních uměleckých škol z hlediska využití informačních a komunikačních technologií.

Pomocí dotazníkového šetření bylo zjišťováno:

- zda a jaké ICT prostředky využívají školy při ochraně osob a majetku a s jakými výsledky
- zda a jak školy zabezpečují data před zneužitím

6.1 Metodologie výzkumu

Peter Gavora (21) tvrdí, že si výzkumník *„musí vybrat vhodnou výzkumnou metodu (metody) a v rámci ní výzkumný nástroj“*. Uvádí jako výzkumný nástroj *„konkrétní pozorovací schéma nebo hotový dotazník“*. Pro splnění cíle tohoto výzkumu byl sestaven *„vlastní výzkumný nástroj“* ve formě dotazníku (je přiložen v příloze). Jedná se o kvantitativní (*„kvantitativní výzkum pracuje s číselnými údaji“)*, reprezentativní výzkum (*„každý respondent základního souboru měl stejnou pravděpodobnost dostat se do výběrového souboru“*) se stratifikovaným výběrem (*„základní soubor se rozloží dle podstatného znaku“* (21)).

Základní soubor je *„soubor všech osob nebo jevů, kterých se výzkumný problém týká“* (21). V tomto výzkumu se skládá ze všech Základních uměleckých škol ve 14 krajích celé ČR. Tento základní soubor byl rozdělen na čtyři podsoubory podle velikosti sídel, ze kterých byly náhodně vybírány ZUŠ, které tak tvoří výběrový soubor.

6.2 Výzkumné otázky

Tento výzkum se zabývá bezpečností Základních uměleckých škol v ČR z hlediska využívání ICT. Výzkum byl rozdělen na dvě části - Ochrana osob a majetku a Základní zabezpečení elektronických dat.

Výzkumné otázky:

- Řeší základní umělecké školy ochranu osob a majetku?
- Jakými prostředky a s jakými výsledky?
- Chrání základní umělecké školy elektronická data?

6.3 Předvýzkum

„Cílem předvýzkumu je zjistit, zda výzkumný nástroj funguje a jak funguje“ (21) Na základě stanovených výzkumných otázek byl sestaven uživatelsky přívětivý dotazník, který byl ověřen pomocí interview s osobami jak z prostředí školského managementu, tak osobami mimo obor. Na základě jejich připomínek k nejasnosti některých otázek byl dotazník upraven. Vyplněné dotazníky od těchto osob byly vyhodnoceny a výsledek prokázal dostatečnou validitu a reliabilitu dotazníku. Podle Gavory (21) byla úspěšnost/neúspěšnost předvýzkumu vyhodnocena takto:

- Respondenti se ochotně zapojovali do výzkumu.
- Sesbírané údaje se daly správně vyhodnotit.
- Respondenti neměli větší problémy s porozuměním položeným otázkám.

6.4 Výsledky výzkumu

Pro potřeby výzkumu byl emailem rozeslán dotazník (příloha č.1) sedmdesáti dvěma ředitelům - ředitelkám základních uměleckých škol v České republice. Průměrně do pěti škol z každého kraje. Do obcí nad 100.000 obyvatel (Praha, Brno, Ostrava, Plzeň, Olomouc) šlo šest dotazníků, do každého města jeden, v Praze dva. Odpověděli tři ředitelé. Do obcí s počtem obyvatel mezi dvaceti a sto tisíci putovaly dvacet dva dotazníky, vrátilo se sedm dotazníků. Do obcí s počtem obyvatel mezi pěti a dvaceti tisíci byly zaslány třicet dva dotazníky a vrátilo se osm odpovědí. A konečně do obcí s počtem obyvatel do pěti tisíc bylo odesláno dvanáct dotazníků a přišly čtyři odpovědi. Souhrn je v následující tabulce.

Počet obyvatel obce, města	Do 5.000	5.000-20.000	20.000-100.000	nad 100.000	Celkem
Počet rozeslaných dotazníků	12	32	22	6	72
Počet obdržených odpovědí	4	8	7	3	22

Tab. č. 3

Návratnost dotazníků je tedy zhruba třicetiprocentní. Tuto nižší návratnost si autor vysvětluje tím, že některé otázky v dotazníku byly technického typu. Mohly respondenty

odradit od dokončení a odeslání formuláře. Avšak bez nich by výzkum bezpečnosti škol z hlediska ICT postrádal smysl.

V dotazníku se autor ředitelů ZUŠ mimo jiné ptal, v jak lidnatém sídle škola působí, kolik má škola žáků, zda působí v budově (budovách) pouze jejich ZUŠ, nebo sdílejí budovu s jinou školou atd. Tyto proměnné totiž mohou mít vliv při rozhodování ředitele na způsob a rozsah zajišťování bezpečnosti v ZUŠ, nebo při výběru prostředků na zajištění bezpečnosti, na správu školy, na požadavky rodičů žáků, atd.

Dotazníkové šetření bylo anonymní, z otázek a odpovědí nelze zpětně určit respondenta. Pro účely rozboru jsou respondenti označeni čísly od jedné do dvaceti dvou.

6.5 Základní údaje

V otázce č. 1 bylo zjišťováno, kolik obyvatel má sídlo, ve kterém je daná škola zřízena. V otázce č. 2 bylo zjišťováno kolik žáků dotazovaná škola má. Předpokládaným zjištěním je, že počet obyvatel sídla souvisí s velikostí školy, tedy s počtem žáků. Čím větší obec, tím větší škola. V následující tabulce je porovnání. Pro názornost jsou respondenti označeni barevně.

Počet obyvatel sídla	Do 5.000	5.000-20.000	20.000-100.000	nad 100.000
Číslo respondenta	**1,2,3,4,**	**5,6,7,8,9,10,11,12**	**13,14,15,16,17,18,19**	**20,21,22**
Počet žáků	Do 300	300 - 600	600 - 1.000	Nad 1.000
Číslo respondenta	**2,3,4,**	**6,9,12,**	**1,5,7,8,10,11,15,19,21**	**13,14,16,17,18,20,22**

Tab. č. 4

Otázka č. 3 zjišťovala, zda dotazovaná škola působí v jedné, či ve více budovách. Otázka č. 4 zkoumala, zda daná ZUŠ sdílí budovu (budovy) s jiným subjektem. A v odpovědích na otázku č. 5 se autor dozvěděl, jaké obory se v dané škole vyučují. Pro úplnost uvádíme, že v základních uměleckých školách je možno se vzdělávat ve čtyřech oborech, hudebním, literárně dramatickém, tanečním a výtvarném oboru. Ne každá škola má všechny obory. Pokud by například odpověděly i jednooborové školy (existují např. ZUŠ pouze s výtvarným oborem, provoz v takové ZUŠ může být odlišný od ostatních), bylo by zajímavé sledovat, zda se liší jejich pohled na zajišťování bezpečnosti od ostatních škol, či nikoliv. Bohužel všechny školy, které odpověděly, jsou víceoborové. Odpovědi na tyto tři otázky, potažmo prvních pět otázek vytváří obraz o konkrétní škole (aniž by byla prolomena anonymita šetření).

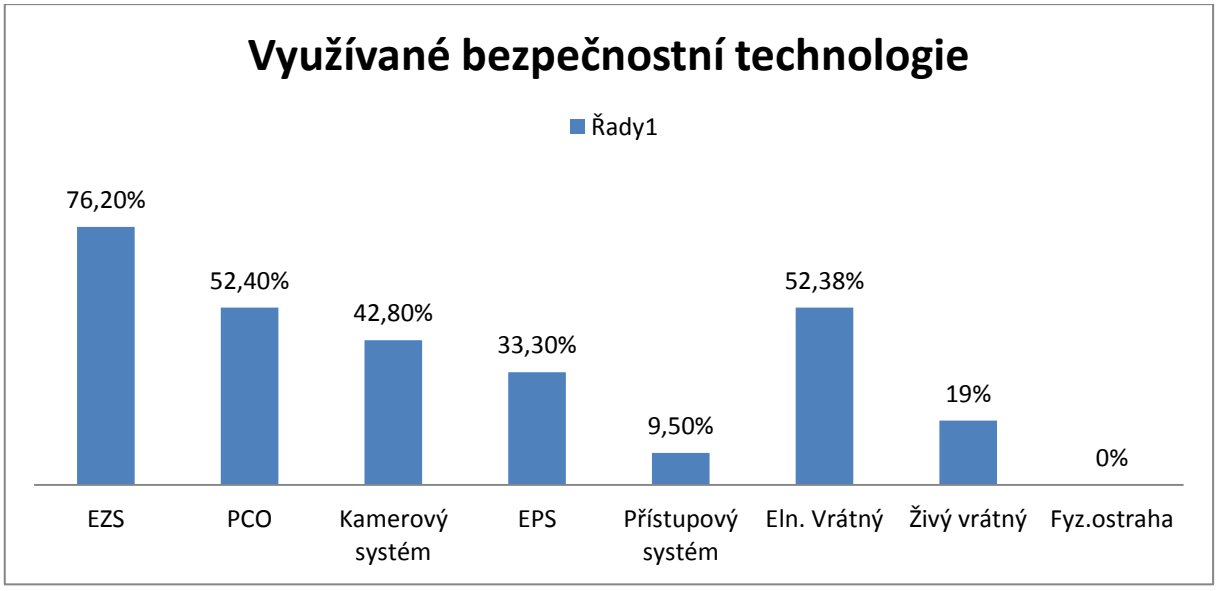
7 Ochrana osob a majetku

7.1 Bezpečnostní technologie

Otázka č. 6 zkoumá, jaké bezpečnostní technologie jsou v základních uměleckých školách využívány. Bylo možno vybrat jednu i více z těchto možností:

- Elektronický zabezpečovací systém (čidla, ústředna, siréna aj.)
- Napojení el. zabezp. systému na pult centralizované ochrany
- Kamerový systém (se záznamem i bez)
- Elektronická požární signalizace
- Přístupový systém (vstupní čipové karty atp.)
- Elektronický vrátný (zvonky s telefonem a bzučákem)
- Živý vrátný
- Fyzická ostraha
- Jiné:

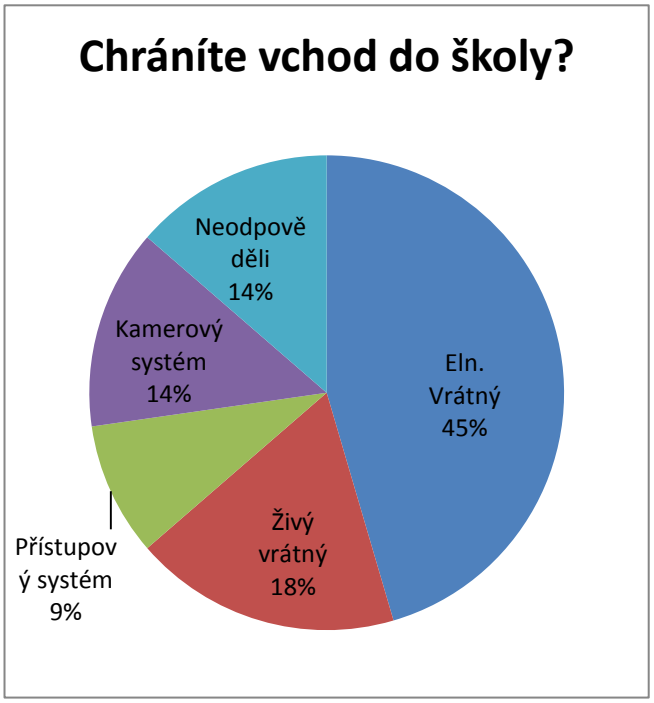
Následující tabulka obsahuje souhrn odpovědí na otázku č. 6.



Z odpovědí respondentů bylo zjištěno, že 76% z nich má instalován Elektronický zabezpečovací systém, který v době mimo provoz školy informuje o vniknutí neoprávněných osob do budovy. 52% dotazovaných škol má EZS napojen na pult centralizované ochrany, v případě narušení objektu je informována policie, nebo bezpečnostní agentura, která přijede

objekt zkontrolovat a případného pachatele zajistit. 43% škol má instalován kamerový systém, jehož pomocí lze identifikovat pachatele nezákonného jednání, ať už v době provozu školy, nebo mimo ni. Pouze třetina respondentů uvedla, že mají instalovánu Elektronickou požární signalizaci, tedy systém, který kdykoliv upozorní na vznikající požár a umožní jeho včasné hašení, evakuaci osob, přivolání hasičů atd.

K otázce zabezpečení vchodu do budovy školy proti vstupu nežádoucích osob směřovala další část této otázky. Dva respondenti uvedli, že mají ve škole instalován přístupový systém, tedy systém, který např. pomocí bezkontaktních karet umožní vstup oprávněným osobám a monitoruje jejich přítomnost (docházkový systém). V základních uměleckých školách je to zatím málo rozšířený nástroj. Vedle toho 52% dotázaných škol používá tzv. Elektronického vrátného, tedy systém zvonků a domovního telefonu. Tímto systémem je možno ověřit oprávněnost vstupu osob. V základních uměleckých školách je to rozšířený systém, neboť mají poměrně hodně žáků (typicky více než např. základní školy ve stejné oblasti), kteří přicházejí a odcházejí v průběhu celé provozní doby školy. Investice a správa elektronického přístupového systému (pokud by všichni žáci měli mít přístupové čipy, karty) bývá v takovém případě nerentabilní. 19% respondentů zaměstnává „živého“ vrátného, dnes moderně nazývaného recepčního, který osobně kontroluje osoby vstupující do budovy. Jeho přítomnost je také preventivním opatřením.

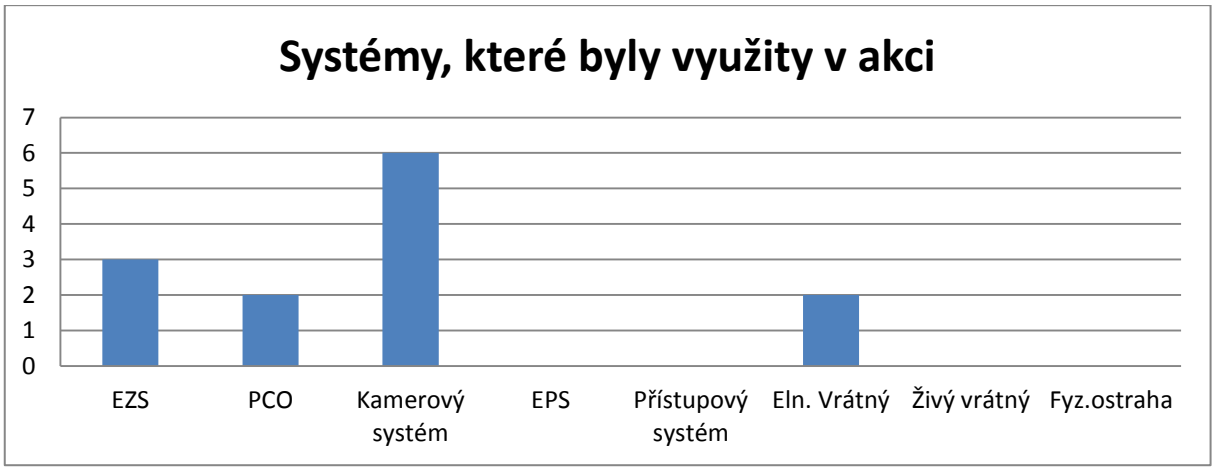


Autora zajímala otázka, zda každá základní umělecká škola uvedla alespoň jeden způsob ochrany vchodu (elektronický vrátný, živý vrátný, přístupový systém, kamerový systém) Devatenáct škol z dvaadvaceti vchod nějakým systémem chrání. Tři školy žádný z těchto systémů nevybraly, což ale neznamená automaticky negativní odpověď. Můžeme tedy konstatovat, že základní umělecké školy přístup do budovy chrání a snaží se eliminovat vstup nežádoucích osob.

Fyzickou ostrahu budov, tedy kontrolu budov v době mimo provoz školy, nevyužívá nikdo z dotazovaných. Příčinou je pravděpodobně cena za tuto službu neúměrná střeženému majetku. Následující tabulka obsahuje souhrn odpovědí na otázku č. 6.

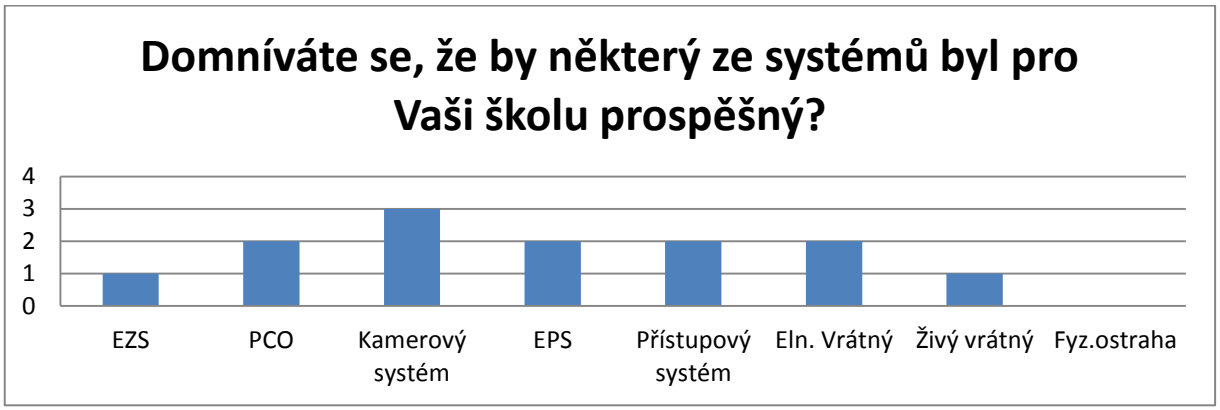
V otázce č. 7 jsem zjišťoval, který z výše uvedených systémů, který mají školy instalovány, pomohl v posledních deseti letech ke snížení škod na zdraví a majetku. Následně v otázce č. 8 bylo žádáno o stručný popis situace.

Nejvíce respondentů (šest) označilo jako prospěšný kamerový systém. Situace, při kterých se osvědčil, uvedli tyto: Pokus o vloupání, odhalení pachatele drobných krádeží z řad žáků, dokumentace pracovního úrazu, eliminace vandalismu. Tři respondenti uvedli jako prospěšný systém Elektronickou zabezpečovací signalizaci. Osvědčila se při vloupání a je chápána také preventivně. Ve spojitosti s Elektronickým zabezpečovacím systémem uvedli dva respondenti jako prospěšné jeho napojení na pult centralizované ochrany. Z jejich zkušenosti vyplývá, že městská Policie vyjíždí při vyhlášení poplachu, zloděj byl vyrušen už alarmem a nezpůsobil vysoké škody. Podle dvou respondentů je též účinným systémem elektronický vrátný, avšak konkrétní případ užití elektronického vrátného při snížení škod na zdraví nebo majetku nebyl uveden. Lze tedy odvodit, že jde o funkci preventivní, do budovy nejsou vpouštěny nežádoucí osoby. Ostatní bezpečnostní technologie (Elektronickou požární signalizaci, přístupový systém, živého vrátného a fyzickou ostrahu) nikdo neuvedl. Souhrn otázky č. 7 je v následující tabulce.



V otázce č. 9 se autor respondentů ptal, zda by byl některý ze systémů, uvedených v otázce č. 6, pro jejich školu prospěšný. Na tuto otázku odpovědělo pouze 9 dotazovaných. Třetina z nich by ve škole uvítala instalaci kamerového systému. Dva respondenti uvedli, že by rádi napojili školu na pult centralizované ochrany, v jednom případě už na stávající systém

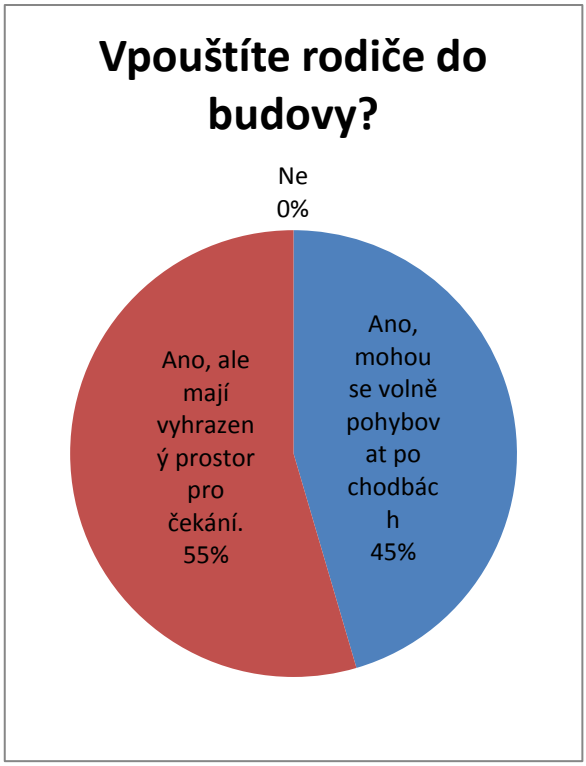
Elektronické zabezpečovací signalizace, ve druhém případě by EZS rádi instalovali. Potřebu instalace Elektronické požární signalizace vnímají dva ředitelé ZUŠ. A rovněž dva dotazovaní by chtěli využívat elektronického vrátného. Jeden dotazovaný by naopak preferoval zaměstnat „živého“ vrátného. O fyzickou ostrahu nikdo z ředitelů neprojevil zájem.

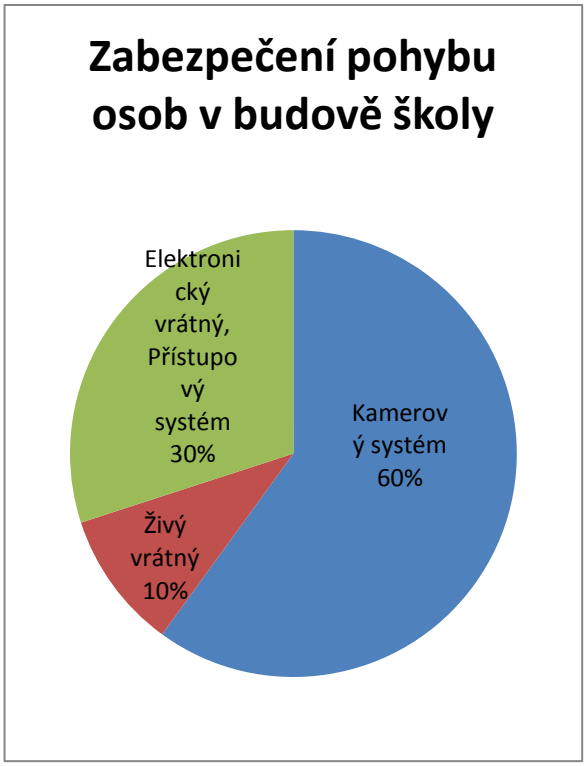


7.2 Pohyb osob v budově

V desáté otázce bylo u oslovených ředitelů základních uměleckých škol zjišťováno, zda vpouštějí rodiče, nebo jiný doprovod žáků v provozní době do budovy školy a zda se mohou volně pohybovat v budově, nebo mají vyhrazené místo pro čekání. Respondenti též dostali možnost krátce svou odpověď popsat.

Pokud je rodičům umožněn pohyb po celé budově, zvyšuje se riziko nepozorovaného pohybu nežádoucích osob, které nebudou od běžného doprovodu rozeznány. Ty se pak mohou buďto přímo dopouštět nežádoucího jednání, nebo si mohou najít úkryt a loupit, nebo jinak škodit mimo provozní dobu, kdy je budova prázdná. Toto riziko se dá snížit instalací kamerového systému alespoň u vchodů do budovy, nebo přítomností „živého“ vrátného. Nejprve tedy zhodnotíme, jak na otázku respondenti odpověděli, pak popíšeme, zda mají školy, které umožňují pohyb rodičů po budově, zajištěnu bezpečnost jinak.





Předně je potřeba říci, že podle odpovědí všechny školy vpouští rodiče, nebo jiný doprovod žáků do budovy. Je to pochopitelné, žáci v ZUŠ tráví relativně krátkou dobu, obvykle 1 – 3 vyučovací hodiny, rodiče je často doprovázejí a čekají na ně. Jelikož se školy k žákům a jejich rodičům chtějí chovat jako ke klientům, není vhodné je nechat v jakémkoliv počasí čekat venku. Zajímavé je, že téměř polovina dotazovaných škol (10 respondentů) nechává rodiče volně se pohybovat po budově, ostatní školy mají pro čekání rodičů vyhrazené prostory. Podle popisu se jedná obvykle o foyer školy, čekárny u vchodu, vstupní haly, chodby. Viz graf „Vpouštíte rodiče do budovy?“

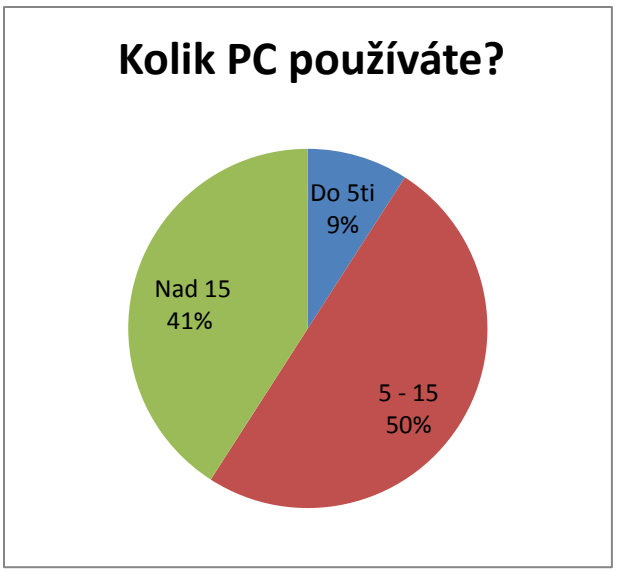
Zaměřili jsme se tedy na skutečnost, zda školy, které nechávají doprovod žáků volně se pohybovat po budově, mají bezpečnost osob a majetku zajištěnu jinak. V úvahu přichází především kamerový systém a přítomnost vrátného. V grafu „Zabezpečení pohybu osob v budově školy“ je znázorněno, jakým způsobem školy tento problém řeší. Šest škol z deseti má instalován kamerový systém, jedna zaměstnává „živého“ vrátného a tři školy mají instalován buď Přístupový systém, nebo Elektronického vrátného. U tohoto způsobu však můžeme pochybovat o jeho bezpečnosti, neboť může do budovy proklouznout s dítětem i nezvaný host. A právě v kombinaci s možností pohybu osob po budově školy vzniká vyšší riziko nežádoucího jednání nepovolaných osob.

Nyní opusťme problematiku zabezpečení osob a majetku a přejděme k zabezpečení počítačů, dat a počítačových sítí.

8 Základní zabezpečení elektronických dat

8.1 Počítače a počítačové sítě

V otázce č. 11 bylo zjišťováno, kolik počítačů v základních uměleckých školách respondenti, resp. jejich zaměstnanci a žáci, používají. Můžeme konstatovat, že většina dotazovaných základních uměleckých škol jde s dobou, počítače nakupují a používají nejen ke kancelářským činnostem (viz dále). Devět respondentů (41%) ve škole používá nad patnáct stanic, což už je na ZUŠ poměrně vysoké číslo. Polovina respondentů uvedla 5 – 15 strojů a pouze dva dotazovaní mají ve škole méně než šest počítačů.



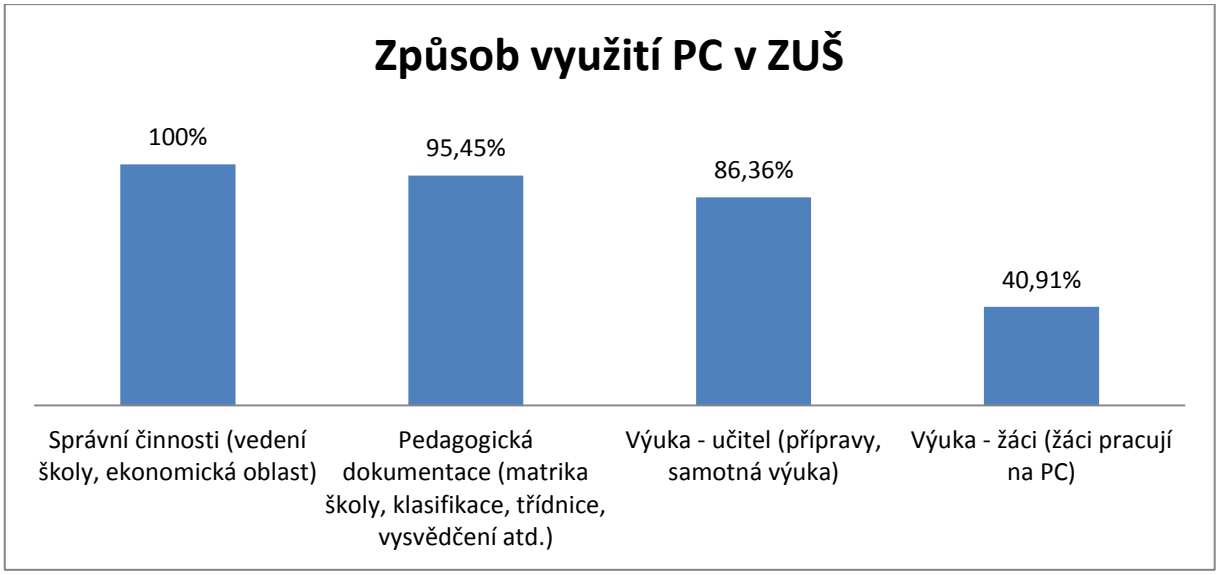
Přirozeně souvisí počet PC ve škole s její velikostí, tedy počtem žáků, ale ne vždy. V průzkumu odpověděla jedna škola, že při počtu žáků 600 – 1000 používají do 5 PC. V tomto ohledu velmi záleží na přístupnosti vedení školy novým trendům. Blíže následující tabulka.

Počet PC	Do 5ti PC	5 – 15 PC	Nad 15 PC
Číslo respondenta	2,11,	3,4,5,6,7,8,9,10,17,18,19	1,12,13,14,15,16,20,21,22
Počet žáků školy	Do 300, 300 - 600, 600 - 1.000, Nad 1.000		

Tab. č. 5

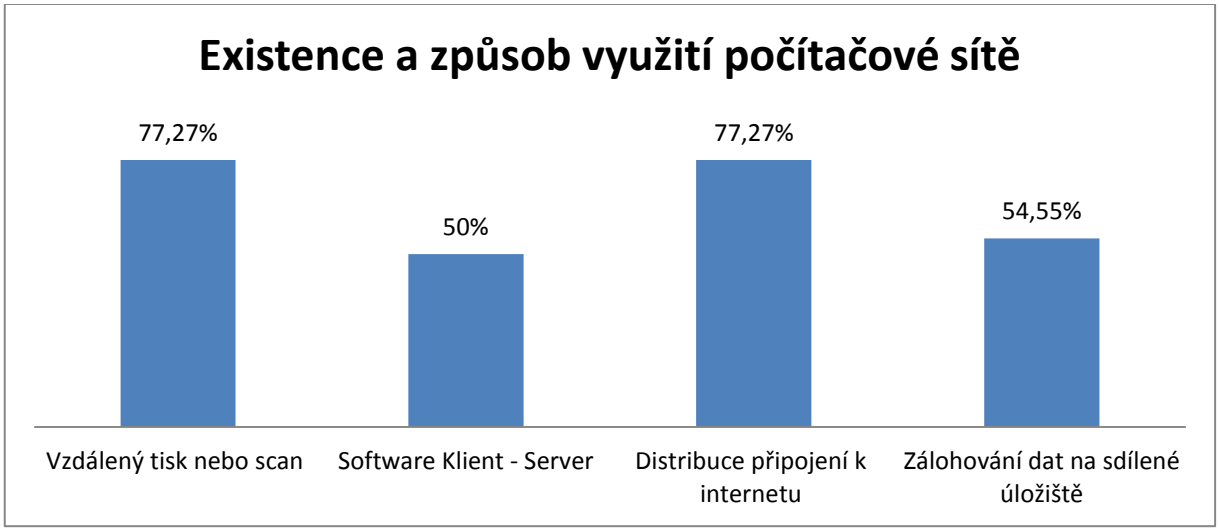
Otázka č. 12 zjišťovala, k jakým účelům jsou počítače využívány. Správa školy se dnes již bez počítače neobejde, proto by bylo zarážející, pokud by někdo z respondentů odpověděl, že počítač v této oblasti nepoužívá. Co se týče pedagogické dokumentace a využití počítačů odpověděla negativně pouze jedna škola. Jedná se však o malou školu - do 300 žáků. Dnes je

možné i na půdě základních uměleckých škol díky speciálním informačním softwarům vést kompletní elektronickou matriku školy, kompletní pedagogickou dokumentaci včetně online žákovských knížek a v neposlední řadě tisk vysvědčení. Právě tato možnost v mnoha školách iniciovala zavedení elektronické matriky, neboť například ve výtvarném oboru při plném učebním úvazku má učitel ve třídě kolem sta žáků a ruční psaní vysvědčení pro všechny žáky dvakrát ročně pedagogy zbytečně zatěžovalo. 86% dotazovaných odpovědělo, že počítačů využívá buď přímo k výuce, nebo k její přípravě. Zatím existuje na našem trhu málo elektronických knih a učebních pomůcek využitelných na půdě základních uměleckých škol, dá se však předpokládat, že ruku v ruce s pronikáním počítačů do ZUŠ poroste hlad po těchto prostředcích a trh se tomu přizpůsobí. Zatím jsou počítače využívány při výuce víceméně spontánně a velmi záleží na osobnosti učitele a přístupnosti vedení školy. S tím souvisí i poslední část této otázky, využití počítačů při výuce, kdy na nich pracují přímo žáci. Tuto alternativu uvedlo 41% respondentů. Nejčastěji se jedná o práci na interaktivních tabulích, ale nejsou výjimkou ani vzdělávací programy přímo vyžadující práci na PC, např. multimediální tvorba, zpracování zvuku, hudební skladba apod. Odpovědi na otázku č. 12 jsou přehledně znázorněny v následujícím grafu.



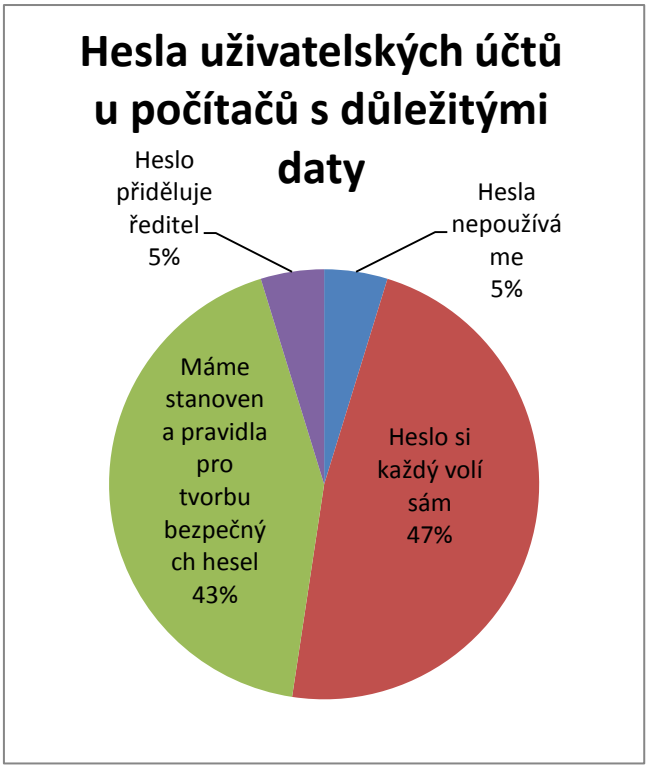
V otázce č. 13 bylo zkoumána existence a způsob využití vnitřní počítačové sítě. Konkrétně na tuto otázku odpovědělo 20 respondentů, avšak dva zbývající ředitelé škol v jiných otázkách uvedli, že mají 5 – 15 PC a také provozují síť WiFi, kterou zpřístupňují zaměstnancům. Zřejmě tedy tímto způsobem alespoň distribuují připojení k internetu, což si pravděpodobně neuvědomili a neuvedli to v otázce č. 13. Pokud tedy tyto dva případy

pomineme, uvedlo shodně sedmnáct respondentů (77%), že vnitřní síť využívají k vzdálenému tisku anebo skenování, respektive k distribuci připojení k internetu. 54%, tedy 12 dotazovaných zálohuje data přes interní síť na sdílené úložiště. A konečně jedenáct škol (polovina) odpovědělo, že provozuje po síti software Klient – Server, který se s úspěchem aplikuje třeba při týmové práci na udržování aktuálnosti elektronické matriky školy, ale i v jiných aplikacích.



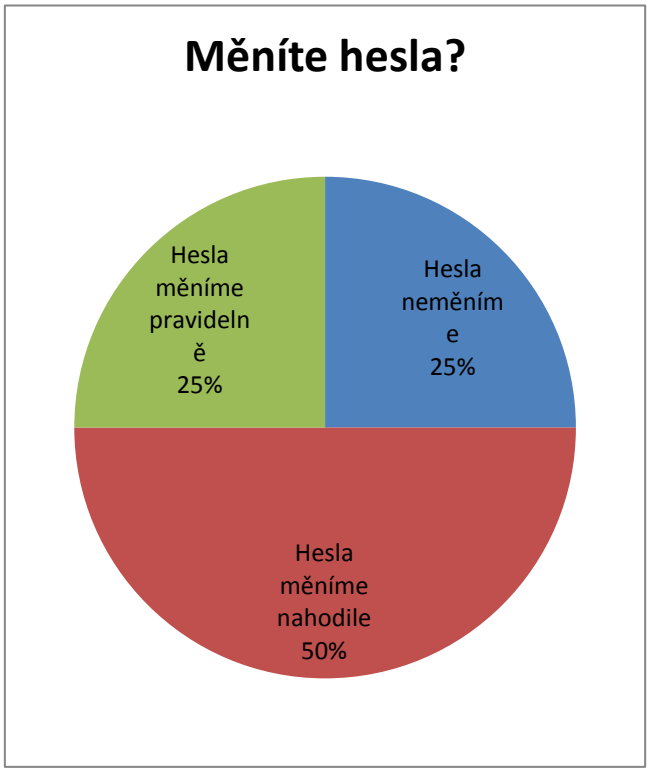
8.2 Zabezpečení počítačů a počítačových sítí

Otázka č. 14 přímo souvisí s bezpečností elektronických dat v základních uměleckých školách. Zjišťovala, jak respondenti pracují s hesly uživatelských účtů u počítačů s důležitými daty. Tím jsou myšleny citlivé údaje žáků i zaměstnanců, ekonomická data, data ke správním řízením, korespondence a další. Na tuto otázku odpovědělo 21 respondentů. Deset z nich uvedlo, že si heslo volí každý sám, což lze považovat za bezpečné z toho pohledu, že heslo zná pouze uživatel. Otázkou je, jak bezpečné heslo si zvolí,



má-li vůbec povědomí o způsobu tvoření bezpečného hesla. Devět respondentů přímo uvedlo, že instruuje zaměstnance o pravidlech pro tvorbu bezpečného hesla. Jeden dotazovaný naproti tomu odpověděl, že hesla nepoužívají, což je třeba považovat za krajně nebezpečné. Rovněž jeden tázaný odpověděl, že hesla přiděluje ředitel, což taktéž není šťastné řešení, uvědomíme-li si, že v takovém případě zřejmě existuje seznam všech hesel a je otázkou, jak ten je chráněn. Za uspokojivé je však třeba považovat, že naprostá většina počítačů ve školách, které na průzkum reagovaly, jsou uživatelské účty heslem chráněny.

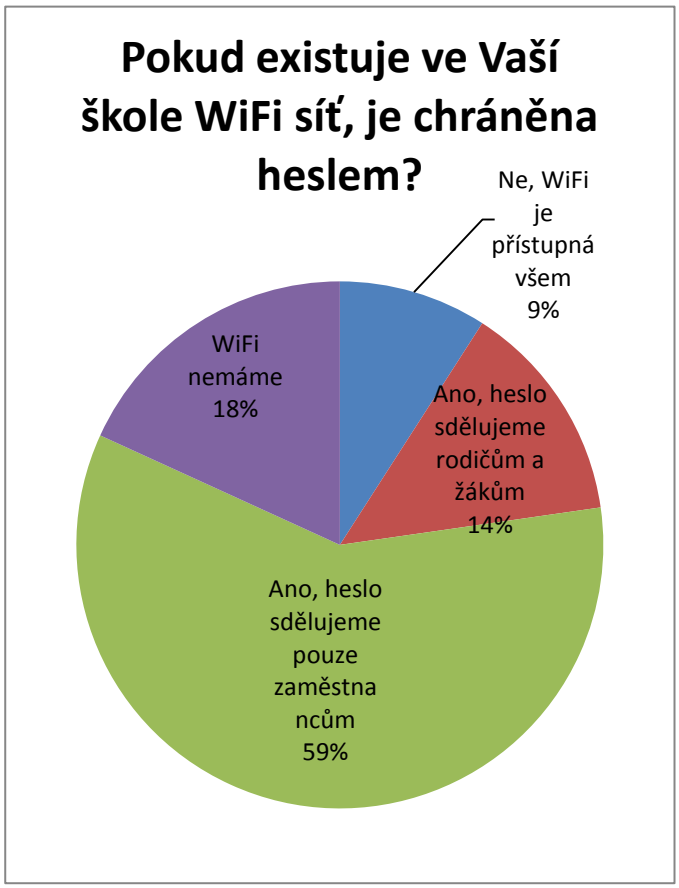
V otázce č. 15 byla položena otázka, zda jsou na počítačích s důležitými data hesla měněna. Na otázku odpovědělo 20 dotázaných, z nichž 5 hesla nemění, 10 hesla mění nahodile a 5 hesla mění pravidelně. Výsledek hodnotíme jako uspokojivý z hlediska bezpečnosti, když tři čtvrtiny respondentů hesla alespoň občas změní. Je třeba si uvědomovat, že riziko pokusu odcizení důležitých dat, případně napadení systému hackerem je právě v základní umělecké škole nižší, než například v komerční firmě.



Otázka č. 16 měla znění: Pokud existuje ve Vaší škole WiFi síť, je chráněna heslem? Možnosti odpovědí byly tyto:

- Ne, WiFi je přístupná všem
- Ano, heslo sdělujeme rodičům a žákům
- Ano, heslo sdělujeme pouze zaměstnancům
- Jiné:

Na tuto otázku odpovědělo osmnáct respondentů, že síť WiFi používají, dva odpověděli, že WiFi nemají a dva neodpověděli, zřejmě tedy také tuto síť nepoužívají. 82% respondentů tedy síť WiFi používá. Z nich třináct má síť chráněnou heslem a sděluje jej pouze zaměstnancům. Další tři ředitelé heslo sdělují též rodičům a žákům. Jiné dvě školy WiFi zaheslovánu nemají, je tedy přístupná všem.



Se sítí WiFi přicházejí do školy různá rizika, která je potřeba znát, vyhodnotit a zaujmout k nim náležitý postoj. Pokud je WiFi chráněna šifrováním a náležitě silným heslem a to je sdělováno pouze zaměstnancům, kteří jej nesmí šířit dál, jedná se o relativně bezpečnou cestu k rozšíření sítě a distribuci internetu v budově. Pokud je však heslo sdělováno veřejnosti, nebo heslo neexistuje, hrozí několik rizik a pokud je síť dosažitelná i vně budovy (skoro vždy), jsou tato rizika ještě vyšší. Jedno z nich je stahování vysokých objemů dat a tím zpomalení připojení pro celou školu, případně, pokud by je jednalo o stahování nelegálního obsahu, hrozí škole i právní postih. Dalším rizikem je nabourání hackera do vnitřní sítě školy, ať už za účelem poškození systému, krádeže dat, nebo parazitování na úložném prostoru a páchání útoků do internetu ze školní sítě, tedy pod cizí identitou.

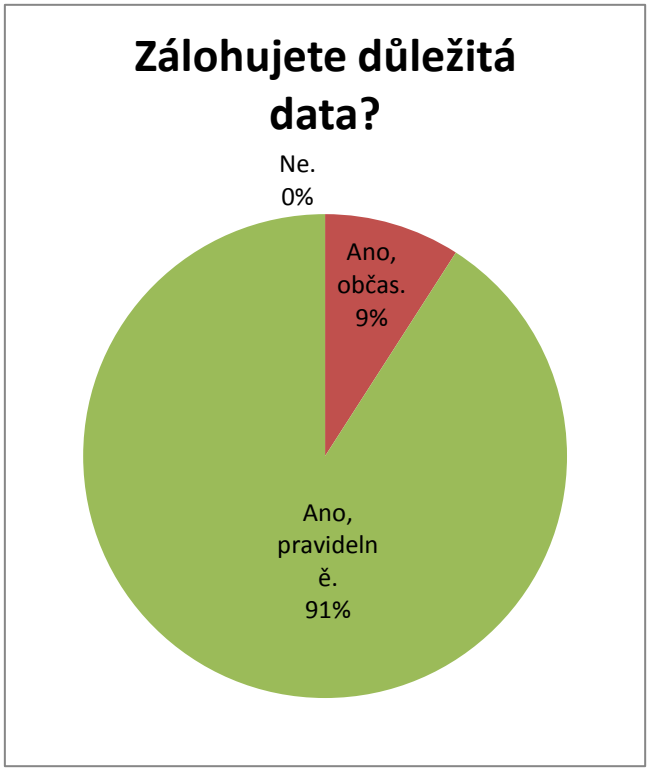
Pro rodiče čekající v základní umělecké škole na žáky je jistě WiFi připojení k internetu vítáno, mohou tak pracovat, nebo si krátit dlouhou chvíli. Proto je pochopitelné, že téměř čtvrtina škol WiFi připojení k internetu návštěvníkům školy umožňuje, je však třeba se soustředit alespoň na oddělení vnitřní počítačové sítě školy od této veřejné WiFi právě z důvodu možnosti nabourání se do systémů školy.

S tím souvisí otázka č. 17 - V případě, že WiFi síť využívají rodiče a žáci, je oddělená od vnitřní sítě školy? Na tomto místě je třeba konstatovat, že několik respondentů nerespektovalo podmínku „v případě, že WiFi síť využívají rodiče a žáci“ a odpovědělo i v jiných případech.

Byli jsme tedy nuceni tuto otázku rozdělit na dvě podotázky:

A) WiFi využívají pracovníci. Je oddělená od vnitřní sítě školy?
   Odpovědělo pět dotázaných, tři sítě oddělili, dva nikoliv.
B) WiFi využívají rodiče a žáci. Je oddělená od vnitřní sítě školy?
   Odpovědělo pět dotázaných, čtyři sítě oddělili, jeden nikoliv.

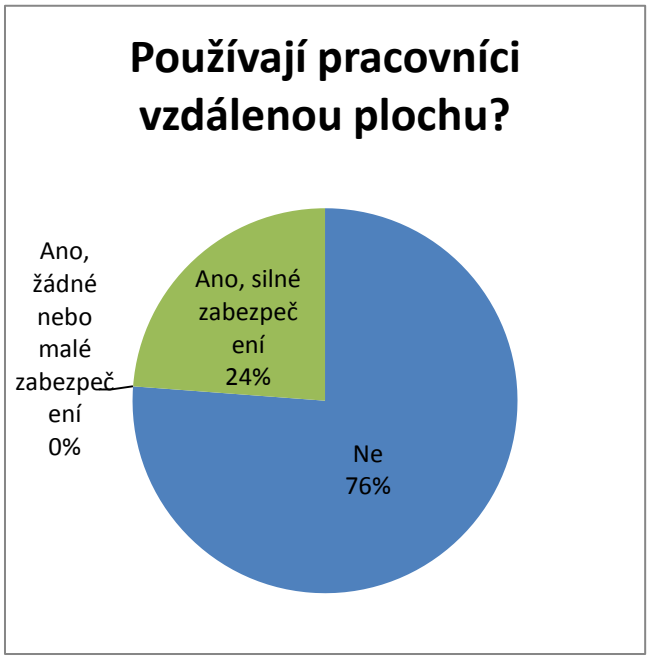
Dá se konstatovat, že z hlediska možnosti nabourání do vnitřní sítě školy osobou nepovolanou je bezpečnost dobrá, pouze v jednom případě není v tomto ohledu síť zabezpečena. Po dalším zkoumání dotyčné školy je nutno podotknout, že se jedná o školu s malým počtem žáků (do 300) a z malého sídla (do 5000 obyvatel). V tomto prostředí je přeci jen riziko útoku menší, než ve velké škole v anonymním prostředí velkoměsta.



Otázka č. 18 - Zálohujete důležitá data? Zálohování elektronických dat je beze sporu důležitou činností. Tak jako každý stroj se časem opotřebí i počítač není strojem bez možnosti poruchy. Také lidé se často dopouští nevratných chyb. Proto je třeba mít aktuální důležitá data

vždy zálohována alespoň na jednom dalším úložišti. Pokud možno vně počítače, lepší je i v jiné místnosti, či budově. Dnes je možno zálohovat na tzv. Cloudy, tedy vzdálená úložiště „kdesi na internetu“. Pokud by totiž došlo na nejhorší a škola kompletně vyhořela, nepomůže ani zálohování v rámci budovy.

Na tuto otázku odpovědělo všech 22 respondentů a nikdo z nich nevybral možnost „Ne“, tedy – nezálohujeme. Občas zálohují pouze dva respondenti, ostatní zálohují pravidelně. Z pohledu zálohování je tedy bezpečnost důležitých dat v zúčastněných základních uměleckých školách zajištěna.



V otázce č. 19 se autor ředitelů ptal, zda někteří jejich zaměstnanci (či oni sami) používají vzdálenou plochu, tedy nástroj pro ovládání např. počítače ve škole počítačem z domova. Je to dobrý sluha, ale zlý pán. Pokud například dojde k odcizení notebooku s povoleným přístupem, nebo k vyzrazení přístupových hesel, nepovolaná osoba tak dostane přístup k důležitým datům, k poškození systému atd., aniž by vstoupila do budovy školy. V případě používání vzdálené plochy je tedy nutností zároveň na obou počítačích používat bezpečná hesla.

Pět respondentů z 21, kteří odpověděli, vzdálenou plochu používá ve spojitosti se silným zabezpečením. Zbytek vzdálenou plochu nepoužívá. Nikdo z dotázaných vzdálenou plochu nepoužívá s žádným, nebo malým zabezpečením. Opět tedy můžeme konstatovat, že je datová bezpečnost dostatečně zajištěna.

8.3 Ochrana osobních údajů při zveřejňování

Poslední otázka č. 20 zkoumala, zda a jak řeší základní umělecké školy schvalování zákonnými zástupci zveřejňování uměleckých děl, výkonů, fotografií a jmen žáků. Základní

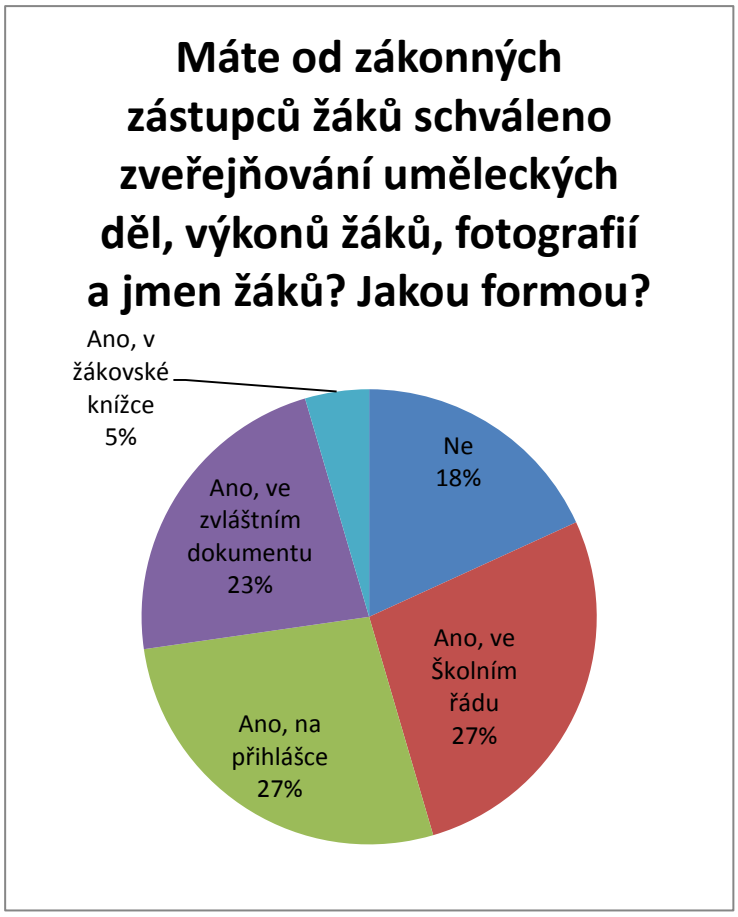
umělecké školy ze své podstaty vyprodukují mnoho uměleckých děl a výkonů, které je pak možno elektronicky zaznamenat, zpracovat a zveřejnit. Pochopitelně každá škola se chce pochlubit svými úspěšnými žáky, dnes nejčastěji na webových stránkách školy. Umělecká díla a jména žáků jsou považována za osobní údaje, fotografie a videozáznamy žáků jsou považovány za citlivé údaje podle Zákona č. 101/2000 Sb., o ochraně osobních údajů (22). Podle toho je třeba s nimi nakládat a nelze je zveřejňovat bez předchozího souhlasu zákonných zástupců žáka.

Znění otázky: Máte od zákonných zástupců žáků schváleno zveřejňování uměleckých děl, výkonů žáků, fotografií a jmen žáků? Jakou formou?

Byly nabídnuty tyto možnosti:

- Ne
- Ano, ve Školním řádu
- Ano, na přihlášce
- Ano, ve zvláštním dokumentu
- Jiné:

Do možnosti „Jiné“ připsal jeden dotazovaný „Ano, v žákovské knížce“, proto byla tato odpověď při vyhodnocení průzkumu zařazena jako další možnost. Podle odpovědí respondentů 82% (18) různou formou souhlas zákonných zástupců získává, 5% odpovědělo (4 dotazovaní), že souhlas od zákonných zástupců nezískávají. To lze bohužel označit jako porušení zákona o ochraně osobních údajů.



Závěr

Ve výzkumu záměrně nebyly zkoumány technické detaily problematiky ICT a bezpečnosti. Výzkumným vzorkem byli ředitelé ZUŠ, ne správci sítě. Výzkum se soustředil na zjišťování bezpečnosti základních uměleckých škol v možnostech povědomí ředitelů. Aby ředitel byl schopen posoudit rizika, která škole reálně hrozí, musí být s problematikou alespoň rámcově seznámen.

Výzkumná část této práce si kladla za cíl pomocí dotazníkového šetření objasnit:

1) zda a jaké ICT prostředky využívají školy při ochraně osob a majetku a s jakými výsledky
2) zda a jak školy zabezpečují data před zneužitím

AD 1) Můžeme konstatovat, že školy na elektronické zabezpečení majetku dbají. Tři čtvrtiny škol (které v průzkumu odpověděly) mají budovy zabezpečeny elektronickým zabezpečovacím systémem, často napojeným na pult centralizované ochrany. Dále tyto i jiné školy používají kamerový systém, ač je to byrokraticky i finančně náročná záležitost. Zároveň si školy tyto systémy pochvalují, neboť byly prakticky využity, když ochránily majetek, či zamezili vandalismu apod.

Horší bezpečnostní situace byla zjištěna v oblasti nasazení elektronické požární signalizace. Tu má instalovánu pouze třetina škol. Přitom riziko požáru je v přítomnosti dětí vždy větší. Navíc tento systém nechrání jen majetek, ale hlavně zdraví lidí. Díky včasné signalizaci může být škola dříve evakuována, sníží se riziko paniky. Proto se domníváme, že by základní umělecké školy, potažmo management škol měl investovat hlavně v tomto směru.

Velmi zajímavá byla otázka vpouštění žáků, rodičů a dalších osob do budovy školy a jejich následný pohyb po budově. Naprostá většina respondentů různými způsoby chrání vstup do budovy proti vniknutí nepovolaných osob. Zde je tedy bezpečnost zajištěna. Co se týče pohybu osob po budově školy během výuky, jsou školy rozděleny na dvě víceméně rovnocenné skupiny. Jedna určuje rodičům a jiným doprovodům žáků, kde mají na žáky čekat a druhá je nechává volně se pohybovat po chodbách školy. Tím vzniká větší riziko nepozorovaného pohybu nežádoucích osob po budově školy (splynou s davem). V těchto případech bylo zkoumáno, jak mají ZUŠ vchod zabezpečen. Dvě třetiny ze škol, které neomezují pohyb osob po chodbách, mají instalován kamerový systém, nebo zaměstnávají vrátného. Třetina má vchod zabezpečen elektronickým vrátným, nebo přístupovým systémem.

V tomto případě je vyšší riziko proniknutí nepovolané osoby do budovy. Avšak jedná se pouze o tři školy z dvaadvaceti, celkově tedy lze vchody a budovy základních uměleckých škol z hlediska pohybu nežádoucích osob považovat za bezpečné.

AD 2) V další části výzkumu jsme se zaměřili na datovou bezpečnost v počítačích a počítačových sítích instalovaných v základních uměleckých školách. Výzkum neukázal nějaký zásadní bezpečnostní problém. Počítače s důležitými daty jsou v naprosté většině chráněny heslem, které je v různých intervalech měněno. Velká část škol provozuje bezdrátovou síť WiFi, která je většinou chráněná heslem a pokud je přístupná i návštěvníkům školy (s heslem i bez) je oddělena od vnitřní sítě školy. Nehrozí tedy nabourání do počítačů s cennými daty. Kladně hodnotíme zjištění, že všichni respondenti zálohují důležitá data a naprostá většina z nich pravidelně. Pokud některý ze zaměstnanců škol pracuje někdy z domova a používá nástroj vzdálená plocha, používá též silná hesla. Můžeme tedy konstatovat, že základní zabezpečení elektronických dat je v základních uměleckých školách na dobré úrovni, nehrozí akutní nebezpečí ztráty, nebo zneužití dat.

Cílem této bakalářské práce bylo zjistit stav bezpečnosti v základních uměleckých školách z hlediska využívání ICT. Tohoto cíle bylo dosaženo pomocí dotazníkového šetření, které bylo následně vyhodnoceno. Stav bezpečnosti v českých základních uměleckých školách z hlediska využívání ICT je celkově dobrý, nebylo objeveno žádné mimořádně závažné riziko.

Použitá literatura

1. **Jelšovská, Katarína.** *Slezská univerzita v Opavě, Matematický ústav v Opavě, knihovna.* [Online] http://www.slu.cz/math/cz/knihovna/ucebni-texty.

2. *Management Mania.* [Online] [Citace: 15. březen 2014.] https://managementmania.com/cs/rizeni-bezpecnosti.

3. *Vítkovice IT Solutions.* [Online] http://itsolutions.vitkovice.cz/37/cs/node/2248.

4. **Veber, Jaromír a kolektiv.** *Management, .* Praha : Management Press, 2011. ISBN 978-80-7261-200-0.

5. **Doucek, Petr, a další, a další.** *Řízení bezpečnosti informací.* Praha : Professional Publishing, 2011. ISBN 978-80-7431-050-8.

6. **Šebestová, Marie.** Management bezpečnosti informací podle ISO/IEC 27001. *System On Line.* [Online] http://www.systemonline.cz/it-security/management-bezpecnosti-informaci-podle-iso-iec-27001.htm.

7. **Lukáš, Luděk a kolektiv.** *Bezpečnostní technologie, systémy a management I.* Zlín : VeRBuM, 2011. ISBN 978-80-87500-05-7.

8. **Křeček, Stanislav a kolektiv.** *Příručka zabezpečovací techniky.* Blatná : Cricetus, 2003.

9. **Chmiel, Pavel.** [Online] [Citace: 2. Leden 2014.] http://www.outech-havirov.cz/skola/files/knihovna_eltech/ete/ezs.pdf.

10. **Reindl, Filip.** *Využití technických a informačních prostředků k ochraně majetku a osob ve školách.* [Bakalářská práce] Praha : PedF UK, 2011.

11. CCD vs. CMOS. [Online] Teledyne Dalsa, 2013. [Citace: 2. 1. 2014.] http://www.teledynedalsa.com/imaging/knowledge-center/appnotes/ccd-vs-cmos/.

12. Viakom, dovozce a velkoobchod kamerových systémů. [Online] Viakom CZ s.r.o., 2013. [Citace: 5. Leden 2014.] http://www.viakom.cz/.

13. ESCAD, Váš patner v průmyslové televizi. [Online] ESCAD Trade s.r.o., 2014. [Citace: 5. Leden 2014.] http://www.escadtrade.cz/.

14. Praktické otázky provozování kamerových systémů ve školách a školských zařízeních. *Učitelské noviny.* 2007, Sv. 22.

15. Přístupový systém Alveno . *Alveno, moderní biometrické, docházkové a přístupové systémy.* [Online] Alveno, 2014. [Citace: 13. Únor 2014.] http://www.alveno.cz/cz/135/pristupove-systemy/.

16. Moxa - zpravodaj Červenec 2010. *Moxa - kompletní řešení průmyslové komunikace.* [Online] Moxa, 2010. [Citace: 13. Únor 2014.] http://www.moxa.cz/zpravodaj/2010/07/Plna-prepetova-ochrana-pro-prevenci-poruch-komunikacniho-spojeni.htm.

17. ČSN ISO 8421 1 - 8 (tř. zn. 38 9000). *Požární ochrana - Slovník. Část 3: Elektrická požární signalizace.*

18. **Spurná, Ivona.** *Počítačové sítě.* Prostějov : Computer Media s.r.o., 2010. 978-80-7402-036-0.

19. **Svoboda, Vladimír.** *Zabezpečení školní počítačové sítě na bázi operačního systému Linux.* [Diplomová práce] Praha : PedF UK, 2009.

20. **Roman, Úlovec.** ICT metodik, ICT koordinátor. *RVP, Metodický portál.* [Online] 10. Březen 2010. [Citace: 27. Únor 2014.] http://clanky.rvp.cz/clanek/o/z/8013/ICT-METODIK-ICT-KOORDINATOR.html/.

21. **Gavora, Peter.** *Úvod do pedagogického výzkumu.* Brno : Paido, 2000. 80-85931-79-6.

22. *Zákon č.101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.*

Přílohy

Příloha č. 1

Informační a komunikační technologie a bezpečnost ZUŠ

Dotazník pro účely výzkumu v rámci bakalářské práce "ICT a bezpečnost v základních uměleckých školách".
Autor: Petr Brejcha, zástupce ředitele
ZUŠ, Praha 9, U Prosecké školy 92
Student Školského managementu, Pedagogická fakulta, Univerzita Karlova, Praha

1) Kolik obyvatel má sídlo, ve kterém je Vaše škola zřízena?

- Do 5.000
- 5.000 - 20.000
- 20.000 - 100.000
- Nad 100.000

2) Jaký je počet žáků Vaší ZUŠ?

- Do 300
- 300 – 600
- 600 - 1.000
- Nad 1.000

3) Počet budov školy?

- Jedna budova
- Více budov

4) Sdílíte budovu s jiným subjektem?

- Ne, v budově(ách) je pouze naše ZUŠ.
- Ano, sdílíme budovu(y) s jiným subjektem.
- Máme více budov a platí obě předchozí možnosti.

5) Obory ve Vaší ZUŠ

- Hudební
- Literárně dramatický
- Taneční
- Výtvarný

6) Bezpečnostní technologie, které využíváte ve Vaší ZUŠ.

- Elektronický zabezpečovací systém (čidla, ústředna, siréna aj.)
- Napojení el. zabezp. systému na pult centralizované ochrany
- Kamerový systém (se záznamem i bez)
- Elektronická požární signalizace
- Přístupový systém (vstupní čipové karty atp.)
- Elektronický vrátný (zvonky s telefonem a bzučákem)
- Živý vrátný
- Fyzická ostraha
- Jiné:

7) Byl ve Vaší škole některý z uvedených systémů účinný při snížení škod na zdraví a majetku během posledních 10 let?

(prosím, vybírejte pouze z možností, které jste vybrali v předchozí otázce)

- Elektronický zabezpečovací systém
- Napojení EZS na pult centralizované ochrany
- Kamerový systém
- Elektronická požární signalizace
- Přístupový systém
- Elektronický vrátný
- Živý vrátný
- Fyzická ostraha
- Jiné:

8) Pokud jste v předchozí otázce některou možnost vybrali, stručně situaci, prosím, popište.

9) Domníváte se, že některý ze systémů by byl pro Vaši školu prospěšný?

(prosím, vyberte pouze možnosti, které jste NEzaškrtli v předchozích dvou otázkách)

- Elektronický zabezpečovací systém
- Napojení EZS na pult centralizované ochrany
- Kamerový systém
- Elektronická požární signalizace
- Přístupový systém
- Elektronický vrátný
- Živý vrátný
- Fyzická ostraha
- Jiné:

10) Vpouštíte rodiče a další osoby (kromě žáků) do budovy během provozu školy?

- Ano, mohou se volně pohybovat po chodbách.
- Ano, ale mají vyhrazený prostor pro čekání.
- Ne

11) Kolik osobních počítačů využíváte ve Vaší ZUŠ?

Do 5ti

- 5 - 15
- Nad 15
- 12) Způsob využití počítačů
- Správní činnosti (vedení školy, ekonomická oblast)
- Pedagogická dokumentace (matrika školy, klasifikace, třídnice, vysvědčení atd.)
- Výuka - učitel (přípravy, samotná výuka)
- Výuka - žáci (žáci pracují na PC)
- Jiné:

13) Existence a způsob využití vnitřní počítačové sítě ve Vaší škole.

Pokud je ve Vaší škole instalována vnitřní síť, vyberte způsoby jejího využití.

- Vzdálený tisk nebo scan (tisk nebo skenování po síti)
- Software Klient - Server (např. učitel na PC ve sborovně zapisuje známky, ty jsou pak v jiném PC využity při vypracování vysvědčení)
- Distribuce připojení k internetu
- Zálohování dat na sdílené úložiště
- Jiné:

14) Jak pracujete s hesly uživatelských účtů u počítačů s důležitými daty?

- Hesla nepoužíváme
- Heslo si každý volí sám
- Máme stanovena pravidla pro tvorbu bezpečných hesel
- Jiné:

15) Měníte hesla uživatelských účtů na počítačích s důležitými daty?

- Hesla neměníme
- Hesla měníme nahodile
- Hesla měníme pravidelně
- Jiné:

16) Pokud existuje ve Vaší škole WiFi síť, je chráněna heslem?

- Ne, WiFi je přístupná všem
- Ano, heslo sdělujeme rodičům a žákům
- Ano, heslo sdělujeme pouze zaměstnancům
- Jiné:

17) V případě, že WiFi síť využívají rodiče a žáci, je oddělená od vnitřní sítě školy?

(Tzn. z WiFi sítě není mozné přihlásit se do vnitřních systémů, např. ekonomických, matriky školy, ani na sdílená úložiště na žádném z vnitřních počítačů)

- Ano, WiFi je oddělená
- Ne, WiFi není oddělená

18) Zálohujete důležitá data?

- Ne.
- Ano, občas.
- Ano, pravidelně.

19) Používají pracovníci vzdálenou plochu?

(práce z domova i odjinud, při odcizení vzdáleného počítače hrozí únik citlivých údajů, ztráta dat)

- Ne
- Ano, žádné nebo malé zabezpečení
- Ano, silné zabezpečení (např. různá hesla na obou PC složená z písmen, znaků, číslic)

20) Máte od zákonných zástupců žáků schváleno zveřejňování uměleckých děl, výkonů žáků, fotografií a jmen žáků? Jakou formou?

- Ne
- Ano, ve Školním řádu
- Ano, na přihlášce
- Ano, ve zvláštním dokumentu
- Jiné: