VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

BUDOVÁNÍ BEZPEČNOSTNÍHO POVĚDOMÍ NA STŘEDNÍ A VYŠŠÍ ODBORNÉ ŠKOLE

INCREASE SECURITY AWARENESS AT THE SECONDARY AND HIGHER VOCATIONAL SCHOOLS

AUTOR PRÁCE — Bc. Aleš Kornelly

AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák

SUPERVISOR

BRNO 2016

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Kornelly Aleš, Bc.

Informační management (6209T015)

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

Budování bezpečnostního povědomí na střední a vyšší odborné škole

v anglickém jazyce:

Increase Security Awareness at the Secondary and Higher Vocational Schools

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současná situace
Vlastní návrh řešení, přínos práce
Závěr
Seznam použité literatury

Seznam odborné literatury:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.
ČSN ISO/IEC 27002, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.
DOUCEK P., L. NOVÁK, L. NEDOMOVÁ a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Vedoucí diplomové práce: Ing. Petr Sedlák

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/2016.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 29.2.2016

ABSTRAKT

Tato diplomová práce se zabývá návrhem a zavedením ISMS na konkrétní střední škole. Cílem práce je poskytnutí vlastních doporučení a návrhů na zlepšení současné situace. Úvodní část vysvětluje základní jednotlivé pojmy týkající se bezpečnosti ICT, další část popisuje vybavení školy a současný stav na škole. V praktické části jsou pak diskutována jednotlivá navrhovaná bezpečnostní opatření.

ABSTRACT

This thesis describes the design and implementation of ISMS to a particular high school. The aim is to provide my own recommendations and suggestions to improve the current situation. Introductory section explains the various basic concepts related to ICT security, the next section describes the facilities of the school and the current state of the school. In the practical part are individually discussed the proposed security measures.

KLÍČOVÁ SLOVA

IT bezpečnost, informace, data, ISMS, ISO/IEC 27001

KEYWORDS

IT Security, information, data, ISMS, ISO/IEC 27001

Bibliografická citace

KORNELLY, A. *Budování bezpečnostního povědomí na střední a vyšší odborné škole.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 88 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

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

V Brně dne 27. května 2016 …….

Podpis

Poděkování
Děkuji vedoucímu této práce Ing. Petru Sedlákovi za odborné vedení a ochotný přístup a také rodině, která mě během tvorby práce podporovala.

OBSAH

ÚVOD

Význam informační techniky roste nezadržitelným tempem a s ním se zvyšují také možnosti využívání komunikačních technologií ve všech aspektech života dnešní společnosti. S tím souvisí digitalizace lidské činnosti a všech součástí života jež je realitou, která přináší nové výzvy. Rostoucí objem dat vyprodukovaných člověkem se stal obchodním artiklem současnosti. S rostoucím objemem vyprodukovaných dat roste ovšem i počet útoků na tato data.

Jako reakce na vzrůstající počet útoků nabírá informační bezpečnost na důležitosti, jelikož si lidé a organizace začali uvědomovat, jakou cenu pro ně data a informace, respektive know-how, představují. Uvědomělá bezpečnost informací s pevně nastavenými pravidly již není výsadou pouze velkých korporátních společností, které ji využívají k ochraně obchodních tajemství, ale postupně se rozšířila díky rozmachu moderních technologií do všech aspektů běžného firemního provozu.

Ve světě se postupně rozšířilo mnoho různých bezpečnostních standardů zabývajících se informační bezpečností. V rámci Evropy je pak nejznámější řada norem ISO/IEC 27000. V současné době je informační bezpečnost začleňována i v legislativním prostředí EU, prostřednictvím direktivy NIS („the network and information security“). Momentálně v procesu překladu a přizpůsobování jednotlivým státním prostředí, České republiky nevyjímaje. V České republice už legislativa tuto problematiku postihující existuje. Jmenovitě zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a souvisejícími vyhláškami. Cílem je zvýšit bezpečnost v kyberprostoru a chránit kritickou infrastrukturu v rámci ČR. Tato legislativa postihuje pouze ty organizace, které splní stanovená kritéria a není tedy plošná pro všechny.

Zavedení sytému řízení bezpečnosti informací je pro společnost nebo organizaci zárukou přiměřené ochrany jejich informačních aktiv po celou dobu jejich životního cyklu. To nejen vede k internímu zvýšení informační bezpečnosti, ale také dává okolí, například obchodním partnerům, jasnou zprávu, že jde o důvěryhodného partnera.

CÍLE A METODIKA PRÁCE

V této diplomové práci se zabývám problematikou bezpečnosti informací na Střední zdravotnické škole a Vyšší odborné škole zdravotnické Znojmo, příspěvkové organizaci (dále „škola“). Za cíl si kladu především navrhnout taková bezpečnostní opatření, která povedou ke zvýšení informační bezpečnosti a z toho vyplývajících zlepšení zabezpečení aktiv v organizaci.

V první části práce popíši nezbytné teoretické minimum, ze kterého hodlám při tvorbě této práce vycházet. Dále následuje analytická část, ve které nastíním kontext zkoumané organizace

Poslední a stěžejní část práce tvoří moje vyjádření a doporučení k oblastem, které byly analyzovány v předcházející kapitole.

Jak analytická část, tak praktická část budou zpracovávány v souladu s normami z řady ISO/IEC 27000, které informační bezpečnost řeší, jsou mezinárodně uznávaným standardem a budou použity jako vodítko pro vypracování celé práce.

Výstup mé práce by měl posloužit zainteresovaným osobám lépe pochopit a zlepšit systém řízení bezpečnosti informací v organizaci a nastavit tak základní podmínky pro případnou certifikaci, zvýšit všeobecné bezpečnostní povědomí na škole a s jeho pomocí by mohlo vedení školy implementovat navrhovaná opatření do běžného provozu, což by zvýšilo i samotnou bezpečnost informací.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V této části se budu zabývat teoretickými východisky, která použiji v následujících částech diplomové práce.

1.1 Vymezení základních pojmů

Tato část má za úkol vymezit některé základní pojmy zmiňované v dalších teoretických východiscích práce.

Důvěrnost

Vlastnost, že informace není dostupná nebo prozrazená neautorizovaným osobám, entitám nebo procesům [1].

Integrita

Vlastnost chránící přesnost a úplnost aktiv [1].

Dostupnost

Vlastnost být dostupný a použitelný na základě požadavku entity, která je pro tento požadavek autorizována [1].

Aktivum

Cokoliv, co má pro organizace nějakou hodnotu [1].

Hrozba

Potenciální příčina nechtěného incidentu, která může vést k poškození systému nebo organizace [2].

Zranitelnost

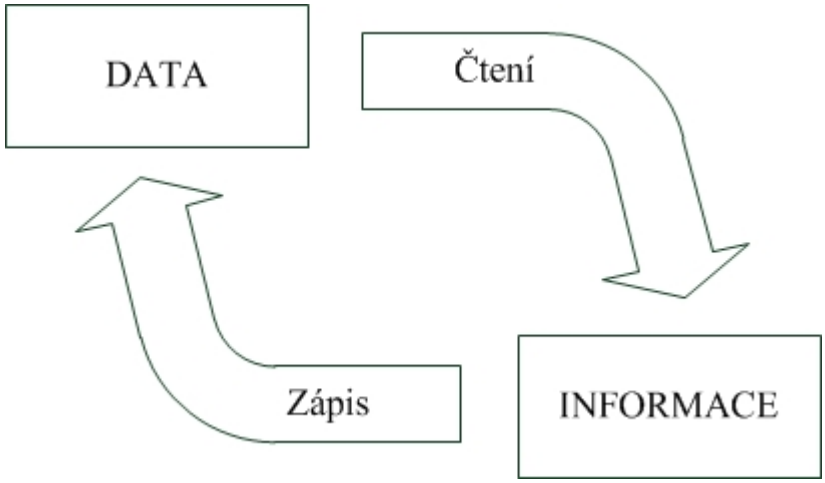
Slabé místo aktiva nebo skupiny aktiv, které může být zneužito jednou nebo více hrozbami [2].

Dopad

Nepříznivá změna ovlivňující stupeň dosažených cílů v rámci organizace [2].

1.2 Data

V praxi můžeme datům přisoudit význam zpráv. Jestliže jsou data použita k rozhodování, stávají se pro člověka informací, neboť ten datům přiřazuje význam a smysl. Proto je někdy datům přiřazován nejen význam zpráv, ale také informace. Data jsou z hlediska rozhodování tedy chápána jako potencionální informace [3].



Obr. 1: Transformace dat na informace [Upraveno dle 10]

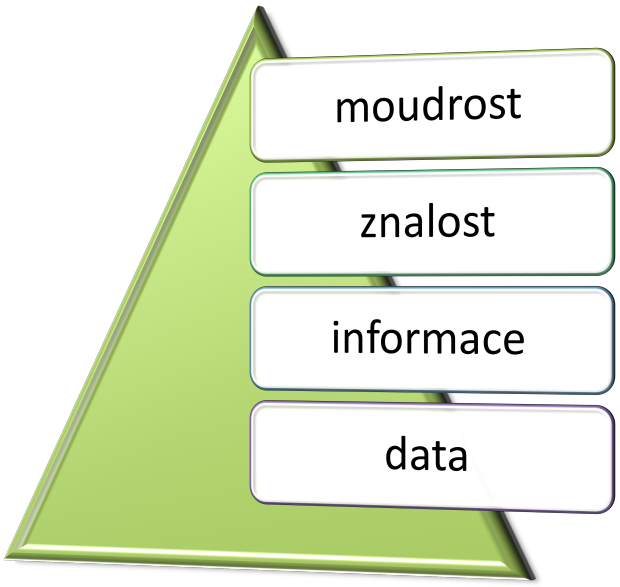
Lidé jsou neustále vystaveni působení zpráv. Některé zachytí a porozumí jim. To je pro subjekt to, co nazýváme data. Data může člověk uložit pro pozdější zpracování, transformovat je do jiné podoby, například zaznamenat na papír nebo převést prostřednictvím počítače do elektronické podoby [3].

1.3 Informace

V nejobecnějším smyslu se informace chápe jako údaj o reálném prostředí, o jeho stavu a o procesech v něm probíhajících. Informace snižuje nebo dokonce odstraňuje neurčitost systému, její kvantita je pak dána rozdílem mezi stavem „před“ a „po“ jejím přijetí. V tomto smyslu může být informace považována jak za vlastnost organizované hmoty vyjadřující její hloubkovou strukturu, tak za produkt poznání fixovaný ve znakové podobě v informačních nosičích. V informační vědě a knihovnictví se informací rozumí především sdělení, komunikovatelný poznatek, který má význam pro příjemce nebo údaj usnadňující volbu mezi alternativními rozhodovacími možnostmi.

V oblasti výpočetní techniky se za informaci považuje kvantitativní vyjádření obsahu zprávy. Za jednotku informace se ve výpočetní technice považuje rozhodnutí mezi dvěma alternativami (0, 1) a vyjadřuje se jednotkou nazvanou bit [3].

Informace můžeme členit podle různých hledisek; mezi základní členění informací můžeme řadit operativní, strategické a taktické, podle stupně řízení, krátkodobé a dlouhodobé, historické, aktuální a prognostické a existuje i mnoho dalších členění [3].



Obr. 2: Data, informace, znalosti, moudrost [Upraveno dle 10]

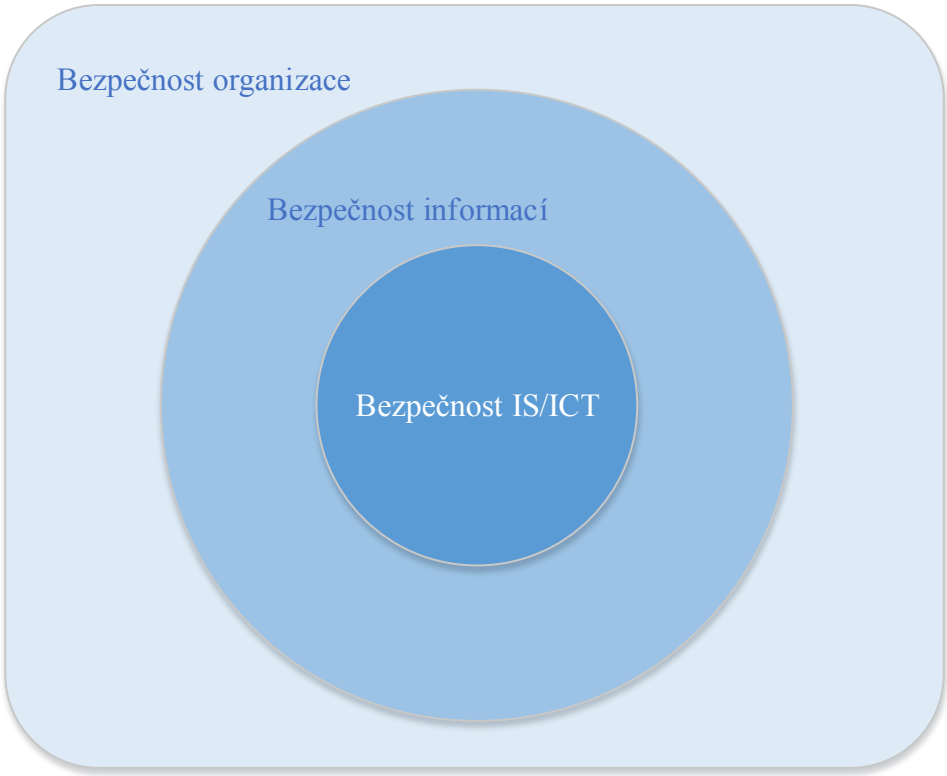
Rozdělení se zdá být poměrně jednoduché. Data jsou vše, co je kolem nás - článek v časopise, novinka na oblíbeném webu atp. Informace však vyžaduje jisté pochopení a je chápána jako komunikační hodnota. Znalost je pak chápána jako osvojení informací spolu s jejich užíváním. Pokud znalosti spojíme s intuicí a zkušenostmi, dosáhneme moudrosti [3].

1.4 Informační bezpečnost

Odvětví výpočetní techniky známé také pod názvem informační bezpečnost, uplatňované jak u počítačů, tak i u sítí. Jejím cílem je ochrana informací a majetku před krádeží, korupcí nebo přírodní katastrofou, přičemž informace a majetek musí zůstat přístupné a produktivní jeho oprávněným uživatelům. Právo vnímá kybernetickou

bezpečnost jako ochranu kyberprostoru před nebezpečnými hrozbami. Každý bezpečnostní incident samozřejmě může dosáhnout takové intenzity, že se negativně projeví v národním měřítku, například pokud dojde k výpadku páteřní sítě. Většina běžně se vyskytujících incidentů však nedosahuje takovéto závažnosti, aby musely být řešeny na úrovni národní kybernetické bezpečnosti. S běžnými incidenty se pak právo vypořádává podle trestního, správního a civilního práva. Typickým příkladem takového incidentu je unik osobních údajů nebo průnik do informačního systému [4].

Bezpečnost informací řeší ochranu informací a dostupnost informací. Je ve vzájemném vztahu s bezpečností organizace a bezpečností IS/ICT. Nejvýše je postavena bezpečnost samotné organizace s úkolem zajištění majetku organizace. Automaticky zahrnuje zajištění bezpečnosti IS/ICT a bezpečnosti informací. Bezpečnost informací zajišťuje kromě bezpečnosti IS/ICT i bezpečnost informací v nedigitální formě. Bezpečnost IS/ICT chrání informační systémy a komunikační technologie a informace, které jsou v nich uchovávány, zpracovávány a přenášeny [5].



Obr. 3: Vzájemné vztahy bezpečností v organizaci [Upraveno dle 5]

1.5 ISMS

Information Security Management System, v češtině Systém řízení bezpečnosti informací, se jak již název napovídá, zabývá řízením bezpečnosti informací se všemi atributy, které to obnáší. ISMS je částí celkového systému řízení organizace, je založen na využití modelu PDCA, z důvodu neustálého zlepšování, a jednotlivé fáze pro řízení bezpečnosti informací jsou tyto: ustanovení ISMS, zavedení a provoz ISMS, monitorování a přezkoumávání ISMS, údržba a zlepšování [5].

1.5.1 Zavádění ISMS

V první části je potřeba získat souhlas a podporu vedení, což nám umožňuje začít s implementací ISMS. Běžně je tento souhlas vyžadován i z praktického hlediska, jelikož je jedná o strategii zavádění svrchu dolů. Pro potřeby certifikace je souhlas vedení klíčový dokument, bez kterého nelze ISMS uskutečnit.

Následně je provedena identifikace aktiv, jejich ocenění a vypracovaní analýzy rizik. Po identifikaci aktiv je provedeno jejich hodnocení na základě integrity, dostupnosti a důvěrnosti jednotlivých aktiv, z čehož dostaneme hodnotu jejich jednotlivou hodnotu. Následně je provedena analýza rizik.

Na analýzu rizik navazuje dokument s návrhem opatření, který na základě nalezených kritických míst, bezpečnostních potřeb a určení priorit vybere vhodné bezpečnostní opatření, které umožní zjištěná rizika efektivně eliminovat, či pokud je riziko velmi malé a opatření extrémně drahé, riziko akceptovat.

V poslední části probíhá certifikace, která není pro funkčnost celého ISMS povinná, protože celý systém může fungovat i bez certifikace. Certifikace se skládá ze dvou částí, v první je certifikována povinná dokumentace a v té druhé je kontrolováno praktické zavádění ISMS [5].

1.5.2 Důvody pro zavedení ISMS

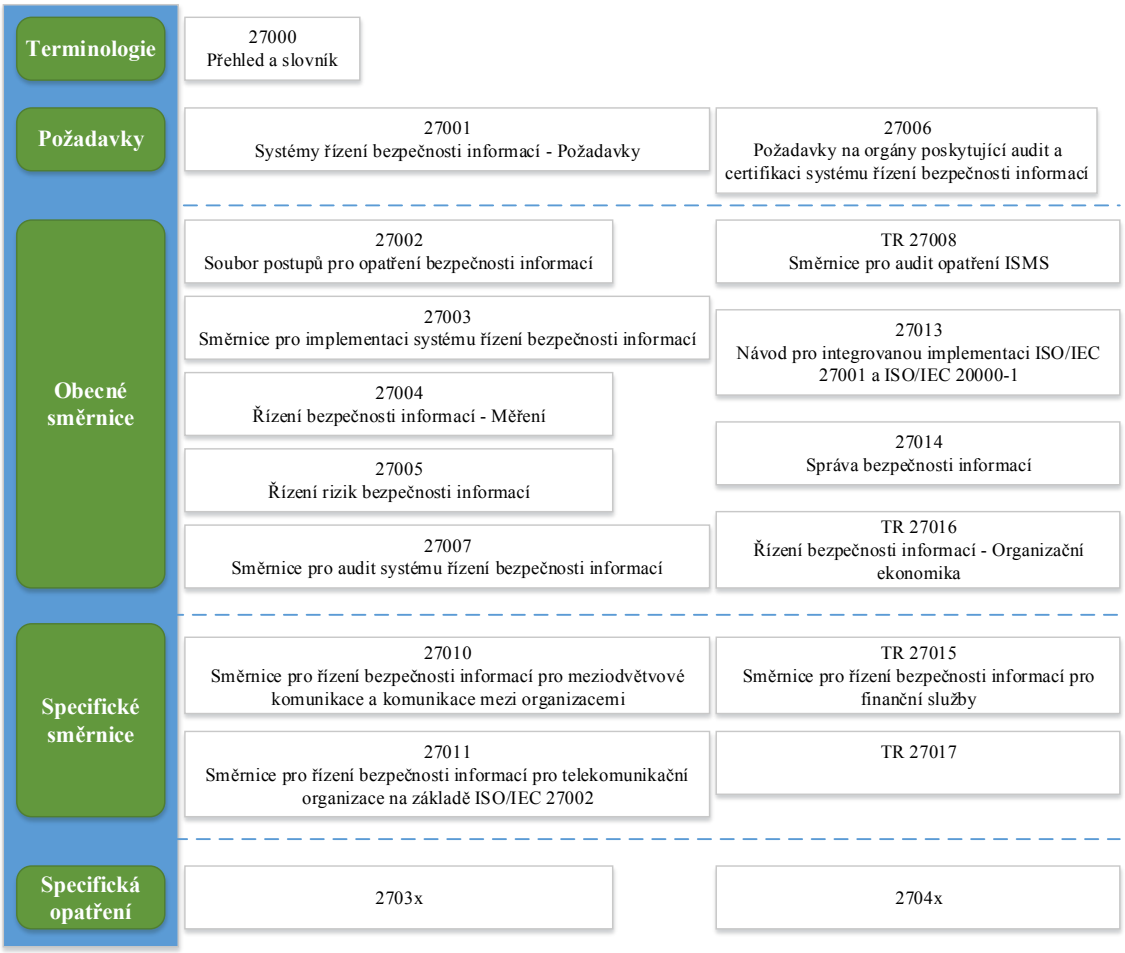
Výhod pro zavedení ISMS je mnoho, mezi ty nejdůležitější patří ochrana informací pro správné fungování podnikových procesů, ujištění stakeholderů o odpovídající ochraně informací a plnění požadavků legislativy ČR a EU. Zavedení ISMS navíc přináší systematické řízení rizik spojených s vnějšími i vnitřními hrozbami, inteligentní rozpočtování nákladů do rozvoje bezpečnosti [6].

1.6 Normy řady 27000

ISO normy z oblasti informační bezpečnosti poskytují rámec, kterým pomohou organizaci implementovat a řídit bezpečnost informací.

1.6.1 ČSN ISO/IEC 27000

Tato norma poskytuje přehled systémů řízení bezpečnosti informací (ISMS), termíny a definice obecně používané v řadě norem ISMS. Tato mezinárodní norma je použitelná pro všechny typy a velikosti organizací, její nedílnou součástí jsou definice a slovník [1].



Obr. 4: Vztahy mezi normami ISMS [Upraveno dle 1]

1.6.2 ČSN ISO/IEC 27001:2013

Tato norma nahrazuje ČSN ISO/IEC 27001 z října 2006. Oproti této předcházející normě je hlavní změna v užitých termínech a definicích [7].

Tato norma by měla poskytnout požadavky na ustanovení, implementování, udržování a neustálé zlepšování systému řízení informací v kontextu celé organizace. Je důležité, že ISMS je součástí procesů a struktury řízení organizace. Dále je důležité zvažovat bezpečnost informací už při samotném návrhu procesů, informačních systémů a opatření. Požadavky této normy jsou obecně použitelné a jsou aplikovatelné v různých organizacích bez ohledu na jejich velikost, typ či povahu činnosti. Navíc může být použita interními i externími stranami k posouzení schopnosti, jak organizace plní vlastní požadavky na bezpečnost informací [7].

Kontext organizace

Definování interního a externího aspektu organizace musí být v souladu se záměry a se zamýšleným výstupem ISMS. Organizace musí určit zainteresované strany, které mají vztah k ISMS, dále musí určit požadavky těchto stran, které jsou relevantní k bezpečnosti informací. Stanovení rozsahu ISMS musí určit hranice a aplikovatelnost. Při tomto stanovení je nutné zvážit externí a interní aspekty, požadavky a propojení a závislosti mezi činnostmi prováděnými organizací a činnostmi, které provádí jiné organizace. Organizace musí ustavit, implementovat, udržovat a neustále zdokonalovat systém řízení informací v souladu s touto normou [7].

Vůdčí role

Vrcholové vedení organizace musí s ohledem na ISMS demonstrovat vůdčí roli a závazek stanovení cílů bezpečnosti informací. Dále musí vedení schválit politiku bezpečnosti informací, která je přiměřená zájmům organizace a je slučitelná se strategickým směřováním organizace, a zajistit, aby odpovědnosti, pravomoci a role relevantní bezpečnosti informací byly přiřazeny a komunikovány [7].

Plánování

Organizace musí plánovat opatření zaměřená na rizika a příležitosti. Organizace musí stanovit cíle bezpečnosti informací, přičemž tyto cíle musí být konzistentní, měřitelné, brát v úvahu výsledky z posouzení rizik a ošetření rizik současně, dále musí být dle potřeb aktualizovány a komunikovány. Dokumentované informace o stanovených cílech musí organizace náležitě uchovávat. Při plánování cílů bezpečnosti informací musí být určeno, co bude vykonáno, jaké zdroje budou

vyžadovány, určení odpovědnosti, termín dokončení a jak budou výsledky vyhodnoceny [7].

Podpora

Organizace musí zajistit zdroje potřebné pro ustavení, implementování, udržování a neustálý rozvoj ISMS. Stanovit kompetence, včetně zajištění prokázání kompetencí. Zajistit uvědomění všech osob pracující pro organizaci jednak o politice bezpečnosti informací, ale i svého přínosu k efektivnosti systému a důsledkům nepřizpůsobení se požadavkům na ISMS. Určit potřeby komunikace (kdy, s kým, kdo, o čem a jaké procesy mají být komunikovány). Dokumentaci informací požadovaných touto mezinárodní normou a dokumentované informace určené za nezbytné pro efektivnost systému řízení informací [7].

Provozování

Organizace musí plánovat, implementovat, řídit procesy a implementovat opatření a plány, dokumentovat informace v nezbytném rozsahu, aby měla jistotu správného provedení procesů. Organizace musí posuzovat rizika bezpečnosti informací a tato rizika ošetřit implementováním plánu ošetření rizik bezpečnosti informací. Výsledky ošetřených rizik je třeba dokumentovat a uchovávat [7].

Hodnocení výkonnosti

Organizace musí vyhodnocovat výkonnost bezpečnosti informací a efektivnost ISMS, k tomu je potřeba nejprve určit co je třeba monitorovat a měřit, použitelné metody monitorování a měření, kdy a kdo bude monitorování a měření vykonávat a jakým způsobem budou výsledky vyhodnoceny. Úkolem interního auditu je získávat informace, zda nedochází k chybám vzhledem k požadavkům organizace a této normy a zjistit, zda je systém řízení bezpečnosti informací efektivní. Vrcholové vedení pak musí v plánovaných intervalech přezkoumávat systém řízení bezpečnosti informací pro zajištění jeho neustálé vhodnosti, přiměřenosti a efektivnosti [7].

Zlepšování

Při výskytu neshody musí organizace reagovat a přijmout opatření k nápravě neshody, pokud to situace dovoluje, případně se zabývat následky. Dále musí vyhodnotit potřebu pro opatření k odstranění příčin neshody, implementovat opatření,

přezkoumat efektivnost každého přijatého opatření, a pokud je to nezbytné, provést změnu v systému řízení bezpečnosti informací. Tyto dokumentované informace musí být uchovávány. Organizace musí systém řízení bezpečnosti informací neustále zlepšovat a zvyšovat jeho efektivitu a přiměřenost [7].

1.6.3 ČSN ISO/IEC 27002:2014

Tato norma poskytuje směrnice pro organizační normy bezpečnosti informací a postupy pro řízení bezpečnosti informací včetně výběru, implementace a řízení opatření. Norma je vhodná pro organizace, které chtějí zavést obecně uznávaná opatření bezpečnosti informací, vypracovat vlastní směrnice k řízení bezpečnosti informací, nebo chtějí vybrat opatření v rámci procesu zavádění ISMS založeném na normě ISO/IEC 27001 [8].

1.6.4 ČSN ISO/IEC 27005:2013

Tato norma poskytuje pokyny pro řízení rizik bezpečnosti informací v rámci organizace, zejména s ohledem na doporučení s ohledem na požadavky managementu bezpečnosti informací podle ISO/IEC 27001 [2].

Tab. 1: Propojení ISMS a procesu řízení rizik bezpečnosti informací [Upraveno dle 2]

Proces ISMS	Proces řízení rizik bezpečnosti informací
Plánuj	Stanovení kontextu Posouzení rizik Příprava plánu ošetření rizik Akceptace rizik
Dělej	Implementace plánu ošetření rizik
Kontroluj	Kontinuální monitorování a přezkoumávání rizik
Jednej	Udržování a zlepšování procesu řízení rizik bezpečnosti informací

Stanovení kontextu

V této části by měl být stanoven kontext pro řízení rizik bezpečnosti informací. Nejdůležitější je určit, za jakým účelem bude řízení rizik probíhat, protože toto ovlivňuje celý proces, tímto účelem může být:

- Podpora ISMS [2].
- Právní shoda a důkaz povinné péče [2].
- Příprava plánu kontinuity činnosti organizace [2].
- Příprava plánu reakce na incidenty [2].
- Popis požadavků na bezpečnost informací u produktu, služby nebo mechanismu [2].

Měl by být vybrán a vhodně přizpůsoben přístup k řízení rizik, který řeší základní kritéria: kritéria hodnocení rizik, kritéria hodnocení dopadu, kritéria akceptace rizik. Měla by být vytvořena kritéria hodnocení rizik bezpečnosti informací a následně pak vytvořena kritéria dopadu, která by měla být specifikována na základě stupně škod nebo ztrát organizace způsobených bezpečnostní událostí. Rozsah procesu řízení rizik musí být definován, aby bylo zajištěno, že jsou brána v úvahu všechna příslušná aktiva. V organizaci by měli být shromážděny informace, aby bylo možno určit prostředí a jeho důležitost pro proces řízení rizik bezpečnosti informací [2].

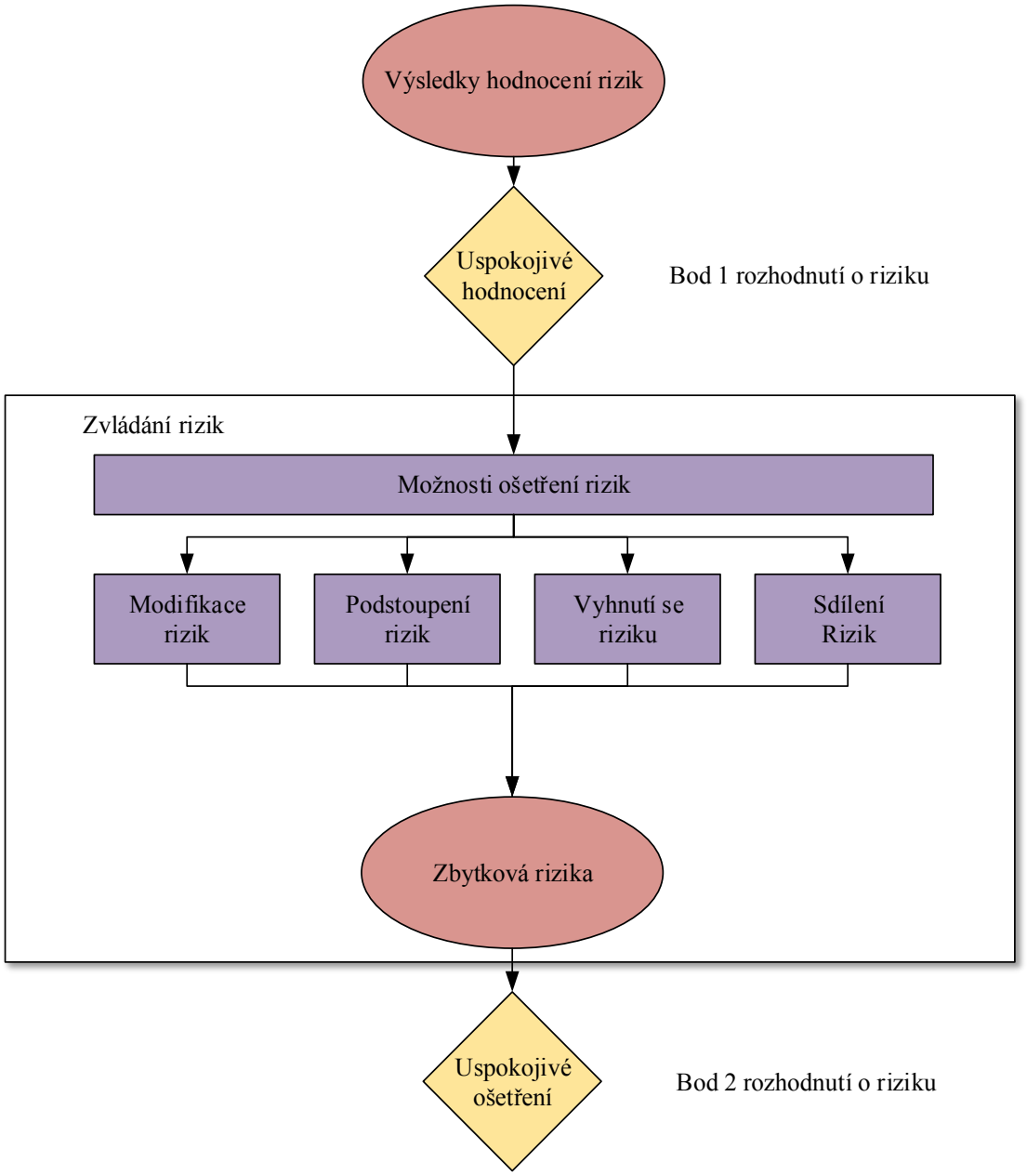
Posouzení rizik

Posouzení rizik určuje hodnotu informačních aktiv, identifikuje možné hrozby a zranitelnosti, které existují, identifikuje stávající opatření a jejich účinek na identifikované riziko, určuje potenciální dopady a nakonec stanoví, jakou prioritu kritériím hodnocení rizik určeným rizikům přiřadit ve stanovení kontextu [2].

Posouzení rizik se často provádí ve dvou nebo i více opakováních. Jako první se provádí přehledové posouzení, aby byla identifikována potenciálně vysoká rizika, která zasluhují další posouzení. Následující opakování může zahrnovat další důkladné zvážení potenciálně vysokých rizik, která byla identifikována v prvním kole posouzení. Tam, kde tyto kroky neposkytnou dostatečné informace pro posouzení rizika, se provedou další podrobné analýzy, pravděpodobně v částech celkového rozsahu a možná za použití jiných metod [2].

Ošetření rizik

V této části probíhá výběr opatření k jednotlivým rizikům uvedeným v seznamu rizik na základě jejich priority. K dispozici jsou čtyři volby pro pro ošetření rizik – redukce, modifikace, podstoupení rizika a vyhnutí se riziku [2].



Obr. 5: Ošetření rizik [Upraveno dle 2]

Akceptace rizik

Plány ošetření rizik by měly popisovat, jak se mají hodnocená rizika ošetřit, aby vyhovovala kritériím pro akceptaci rizik. Tyto kritéria mohou být komplexnější a nemusí tedy rozhodovat pouze fakt, zda zbytkové riziko spadá nebo nespadá nad nebo pod určitou úroveň. O akceptaci těchto rizik rozhodují vedoucí pracovníci organizace [2].

Komunikace rizik

Všechny zainteresované strany by si měli informace o rizicích vyměňovat nebo je sdílet. Tyto informace obsahují mimo jiné existenci, charakter, formu, pravděpodobnost, závažnost, ošetření a přijatelnost rizik. Komunikace těchto informací je důležitá, protože může mít vliv na rozhodnutí, které je potřeba učinit. Komunikace zajistí, že ti, co jsou odpovědni za uplatňování řízení rizik, rozumějí podkladům, na jejichž základě jsou činěna rozhodnutí, a také tomu, proč jsou nutné konkrétní akce. Další výhodou komunikace rizik je potlačení subjektivního vnímání daného rizika [2].

Monitorování a přezkoumávání rizik.

Rizika nejsou stálá, jelikož hrozby, pravidelnosti, zranitelnosti nebo následky se mohou náhle změnit. Proto je detekování těchto změn neustálé monitorováno. Mezi hlavní oblasti monitorování patří nová aktiva, nutné změny hodnot aktiv, nové hrozby, incidenty bezpečnosti informací [2].

Organizace by měla zajistit, aby proces řízení rizik bezpečnosti informací a relevantní činnosti zůstaly přiměřené současným okolnostem a byly dále naplňovány. Kromě toho by organizace měla pravidelně prověřovat, zda používaná kritéria jsou stále platná a jsou v souladu s obchodními cíli, strategií a politikou organizace a zda změny kontextu činností jsou během procesu řízení rizik adekvátně brány v úvahu [2].

1.7 Demingův cyklus

Demingův cyklus je metoda neustálého zlepšování s univerzálním použitím pro všechny typy organizací. Cyklus má čtyři fáze, které se do češtiny překládají jako: plánuj (plan), dělej (do), kontroluj (check) a jednej (act). Cyklus PDCA můžeme chápat jako nedílnou součást každého procesu, který se plánuje, realizuje a kontroluje. V praxi

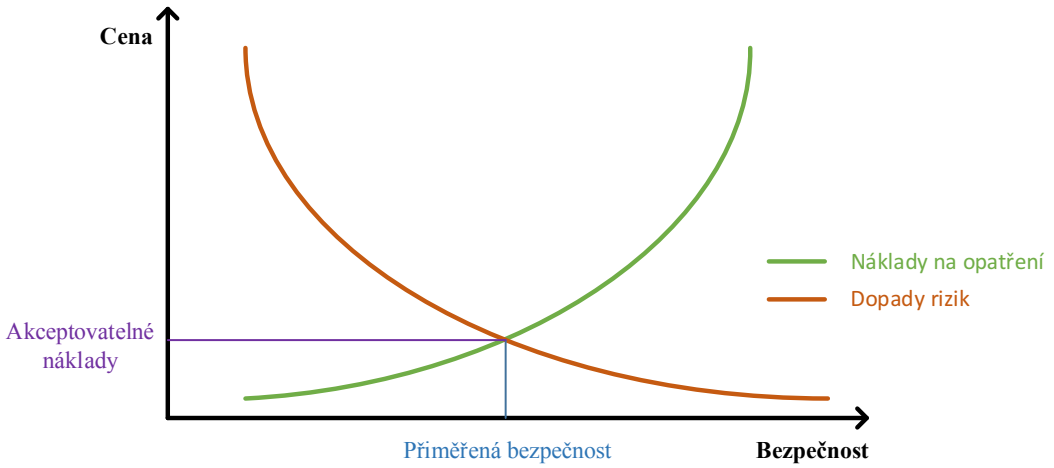
se tento cyklus využívá v řadě organizací k zavedení různých změn, je základním zobrazením procesu neustálého zlepšování [9].

- Plánuj – naplánování zamýšleného zlepšení, sestavení plánu,
- Dělej – realizace plánovaného,
- Kontroluj – ověření výsledku realizace, oproti plánovanému záměru,
- Jednej – úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe, jaké opatření musíme zavést ke zlepšení či opakovanému dosažení výsledku [9].

Obr. 6: Demingův cyklus [10]

1.8 Přiměřená bezpečnost

Při snaze efektivně zabezpečit informační systém by měla velikost investic do bezpečnosti odpovídat hodnotě aktiv a míře možných rizik. Je dobré si uvědomit, že absolutní bezpečnost je nedosažitelná, není ani stálá, a z toho vyplývá, že bezpečnost jako taková je trvalý proces. Přiměřená bezpečnost závisí na bezpečnostní politice organizace. Platí zde jednoduché pravidlo, jež je možné vyčíst i z následujícího grafu, čím větší náklady na opatření firma vynaloží, tím nižší bude dopad rizik na organizaci. Přiměřenou bezpečnost organizace stanovuje podnik dle svých akceptovatelných nákladů na bezpečnost [5].



Obr. 7: Přiměřená bezpečnost za akceptovatelné náklady [Upraveno dle 6]

1.9 ITIL

Jedná se o sbírku knižních publikací obsahující nejlepší zkušenosti z oboru řízení IT služeb. Současná verze (V3) obsahuje pět hlavních knih:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Těchto pět ITIL svazků zachycuje celý životní cyklus služby počínaje identifikací potřeb zákazníka a zdroji IT požadavků přes návrh a implementaci služby a konečně monitorování a fázi zlepšování služeb. Dále ITIL obsahuje ještě knihu The Introduction to the ITIL Service Lifecycle, která shrnuje principy vysvětlené v těchto pěti knihách a současně popisuje jednotlivé fáze životního cyklu [11].

Obr. 8: ITIL [11]

1.10 Management bezpečnosti pasivní vrstvy

1.10.1 Stupeň 0 – Identifikátory

Tento stupeň má za úkol usnadnit správu systému a naviguje správce sítě na správný způsob zapojení pomocí barevných rozlišení prvků. Lze využít širokou škálu barev barev jak u metalických, tak i optických konektorů, propojovacích kabelů, popisovacích štítků a značkovacích kroužků.

V praxi se hojně využívají štítkovače, různé barvy propojovacích kabelů či pouze různé barvy koncových krytek [5].

Obr. 9: Různé barvy koncových krytek pro konektor RJ45 [12]

1.10.2 Stupeň 1 – Blokátory

Tento stupeň zajišťuje základní fyzickou ochranu formou blokování portů a blokování přístupu fyzicky do sítě.

Blokování představuje více druhů, mezi ty základní paří blokování datového metalického, optického a USB portu. Toto blokování může být pouze dočasné (dá se odblokovat příslušným klíčem) anebo permanentní (nedá se odblokovat). Blokování kabeláže, jež má za účel zabránit neautorizovanému přístupu ke kabelovým svazkům, bývá nejčastěji prováděno formou zamykatelných žlabů. Blokování datového boxu proti neoprávněnému přístupu má za úkol ochránit aktivní prvek před přístupem neoprávněné osoby, nejčastěji bývá řešeno pomocí uzavíratelné skříňky [5].

Obr. 10: Blokátor konektoru RJ45 od firmy Panduit [13]

1.10.3 Stupeň 2 – Klíčování

Tento stupeň začleňuje prostředky, které znemožňují připojení do nepovolených portů. V praxi to znamená, že pokud je kabel vypojen, může být zapojen pouze zpátky do místa svého původního zapojení. Tento mechanismus funguje na základních bodech:

- neklíčovaný konektor nelze zasunout do žádné klíčované zdířky,
- klíčovaný konektor nelze zasunout do neklíčované zdířky a ani do zdířky s jiným klíčem [5].

Obr. 11: Klíčovaný plug pro RJ45 kategorie 6 [13]

1.11 Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti je jedním ze základních dokumentů nutných k certifikaci. Obsahuje dokumentované prohlášení o implementovaných opatřeních normy, případně dalších opatření navržených na pokrytí rizik. Hlavním cílem je dokumentovat rozhodnutí, proč dané opatření bylo či nebylo vybráno k zavedení. Zdůvodnění pro vyřazení cílů a jednotlivých opatření poskytuje zpětnou kontrolu, zda nebyly vyřazeny omylem. Pokud společnost do budoucna certifikaci neplánuje, není nutné toto samotný dokument vytvářet. Pro malou a střední firmu je plně dostačující, pokud se vhodným způsobem zaznamená výběr opatření tak, aby i za několik měsíců bylo stále jasné, proč není nutné určité opatření implementovat [14].

2 ANALÝZA SOUČASNÉHO STAVU

V této části se zaměřím na popis současného stavu uvnitř organizace s ohledem na bezpečnost informací. Jako kritéria analýzy posloužila norma ČSN ISO/IEC 27001, kterou používají také auditoři pro certifikaci ISMS.

2.1 Kontext organizace

Určit externí a interní aspekt organizace a definovat její hranice je důležité pro záměry organizace a ovlivňuje schopnost výstupu systému řízení bezpečnosti informací.

2.1.1 Všeobecný popis organizace

Střední zdravotnická škola a Vyšší odborná škola zdravotnická Znojmo je příspěvkovou organizaci, jejímž zřizovatelem je Jihomoravský kraj. Za 60 let své existence vychovala tři generace zdravotnického personálu, jež působí v nemocnicích nejen na jižní Moravě, ale po celé republice a v zahraničí (např. Německo, Rakousko, Velká Británie, ale i v takových zemích jako je Saudská Arábie či Austrálie). Škola spolupracuje s řadou nemocničních zařízení u nás i v Evropě, s charitativními organizacemi a sdruženími.

Absolventi středoškolského maturitního oboru Zdravotnický asistent a vyššího odborného oboru Diplomovaná všeobecná sestra nacházejí široké uplatnění ve zdravotnických zařízeních a jejich zaměstnanost dosahuje 100%. [15].

2.1.2 Organizační struktura

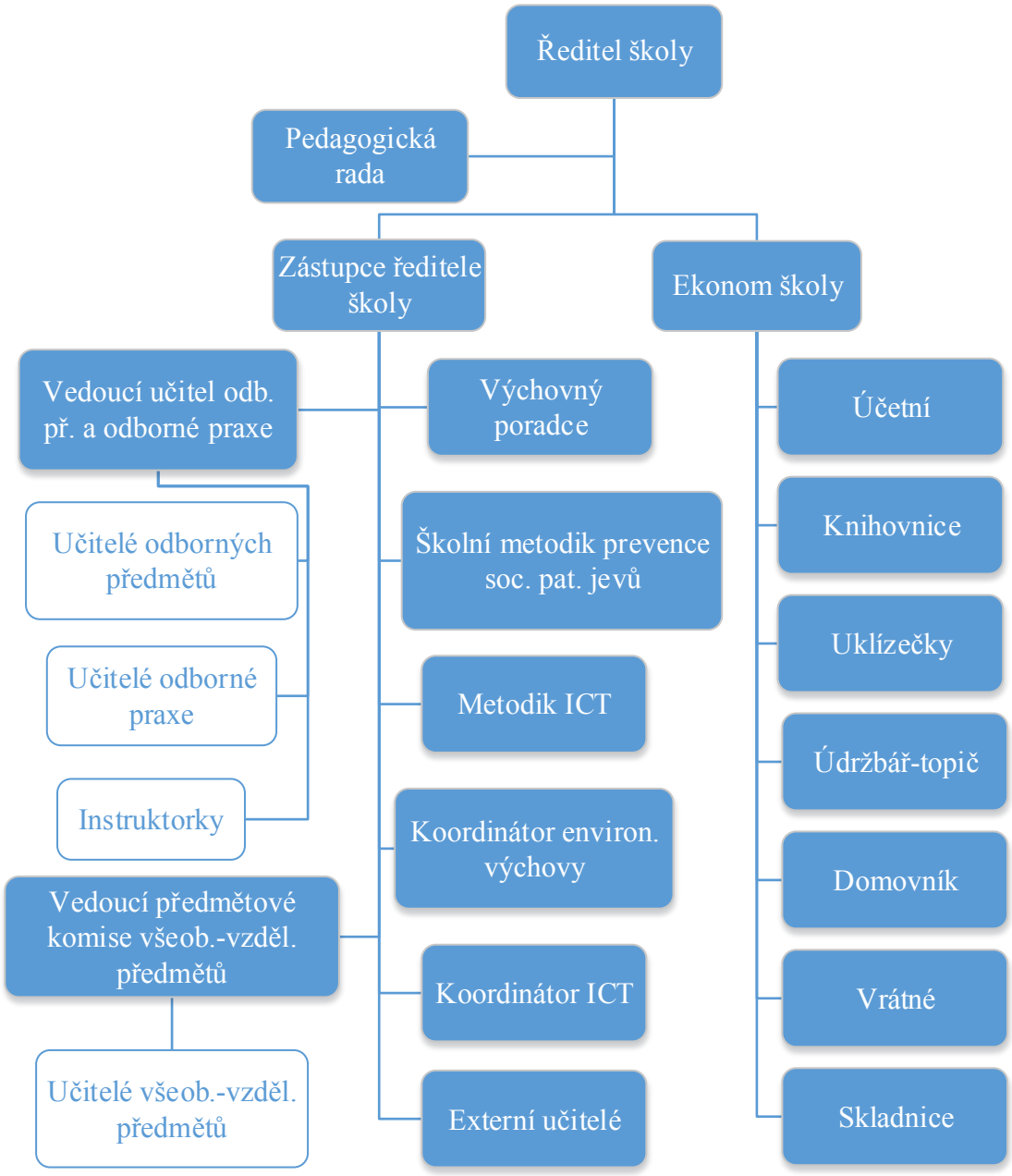
Za chod organizace odpovídá ředitel školy coby statutární orgán, který se zodpovídá Jihomoravskému kraji jako zřizovateli školy. V organizaci samotné se pak nacházení tyto řídící stupně:

1. Ředitel školy,
2. zástupce ředitele školy, ekonom školy,
3. vedoucí učitel odborných předmětů a odborné praxe.

Ředitel školy je přímo nadřízený zástupci ředitele školy a ekonomovi školy. Zástupce ředitele školy řídí vedoucího učitele odborných předmětů a odborné praxe, vedoucí předmětových komisí, učitele všeobecně vzdělávacích předmětů, externí

učitele, výchovné poradce, školního metodika prevence sociálně patologických jevů, metodika informačních a komunikačních technologií, koordinátora školního vzdělávacího programu a koordinátora environmentální výchovy. Ekonom školy řídí účetní, knihovnici, uklízečky, údržbáře-topiče, domovníka, vrátné a skladnici. Vedoucí učitel odborných předmětů a odborné praxe řídí učitele odborných předmětů a odborné praxe a instruktorky [16].

Vzdělávání a provoz školy zajišťuje více než 40 interních zaměstnanců a dalších více než 40 externích pracovníků (vrchní a staniční sestry). Všichni vyučující odborných předmětů jsou registrovanými zdravotnickými pracovníky na pozicích minimálně zdravotních sester. V aktuálním školním roce 2015/2016 je počet žáku na střední škole 227, studentů na vyšší odborné škole pak 91 [15].



Obr. 12: Organizační schéma školy [16]

2.2 Vůdčí role

Vedení organizace se musí ztotožnit s plánem zavést systém řízení bezpečnosti informací tak, že mu vyjádří svou plnou podporu, zajistí potřebné zdroje a integraci požadavků systému řízení bezpečnosti informací do procesů organizace, což v současné době není zavedeno.

Politika

Stanovením bezpečnostní politiky vedení organizace stvrdí své závazky. Organizace aktuálně stanovenou bezpečnostní politiku nemá, proto ji doporučuji ustanovit. Politika bezpečnosti informací musí být dokumentovaná a dostupná viz Příloha I.

2.3 Plánování

Při plánování ISMS musí organizace pochopit svůj kontext a požadavky zainteresovaných stran, na jejichž základě bude stanovovat rizika a příležitosti. Rizika a příležitosti jsou potřeba k určení, že ISMS může dosáhnout požadovaných výstupů, předcházení a snížení nežádoucích následků, neustálého zlepšování.

V organizaci dosud není stanoven proces, který by posuzoval rizika bezpečnosti informací, stanovoval kritéria akceptace, posuzoval, že opakovaná hodnocení rizik bezpečnosti informací jsou konzistentní, opodstatněná a porovnatelná, identifikoval rizika bezpečnosti informací a jejich vlastníky, analyzoval a hodnotil.

Další z procesů, který zatím v organizace není definován, je proces ošetření rizik bezpečnosti informací pro vhodný výběr ošetření rizika, určení všech opatření nutných k ošetření rizika, vytvoření SoA, formulaci plánu k ošetření rizik bezpečnosti informací a získání souhlasu od vlastníků rizik ohledně plánu ošetření a přijetí zbytkových rizik bezpečnosti informací.

2.4 Podpora

Organizace v současnosti nemá zdroje pro ustanovení, implementování, udržování a neustálé zlepšování ISMS. Napravit by to mohl závazek vedení o podpoře ISMS. Jako takový závazek můžeme chápat ustanovení bezpečnostní politiky, kterou musí schválit vedení organizace, důležité je také určit odpovědnostní role a do plánu školení zahrnout i školení ISMS, aby bylo neustále zvyšováno bezpečnostní povědomí.

2.5 Provozování

Provozování a řízení naplánovaných procesů ISMS v organizaci zatím neprobíhá, jelikož tyto procesy nebyly v rámci organizace dosud ustanoveny.

2.6 Hodnocení výkonosti

Aktuálně není výkonosti ISMS v organizaci vyhodnocována. K jejímu vyhodnocování do budoucna je potřeba stanovit metriky, na jejichž základě se bude hodnotit výkonost procesů ISMS. Dále je potřeba zajistit, že budou prováděny interní audity a k těmto auditům budou uvnitř organizace odborně způsobilé osoby. Je potřeba rozhodnout komu budou zprávy z auditů předávány a jak bude s těmito zprávami dále nakládáno a podobně.

2.7 Zlepšování

V návaznosti na hodnocení výkonosti musí organizace reagovat nevyhovující stavy definované metrikami. Je potřeba přijmout opatření k ošetření těchto neshod. Hlavním účelem zlepšování je odstranění chyb, které byly zjištěny při hodnocení výkonosti ISMS.

2.8 Aktiva

Aktiva, která se ve škole z hlediska bezpečnosti informací nacházejí, můžeme rozčlenit do pěti základních skupina a to jsou: hardware, software, sítě, lidé a lokality.

2.8.1 Hardware

Veškeré fyzicky existující technické vybavení školy.

Koncové stanice

Na škole se nachází 66 koncových uzlů, ty lze rozdělit do následujících kategorií:

2 stanice typu server

26 notebooků pro učitele

3 notebooky pro vedení školy

8 stolní PC pro agendu školy

17 stolních PC sloužících k výuce informatiky

4 stolní PC v knihovně školy

5 volně přístupných stolních PC ve vestibulu školy

1 počítač od společnosti CERMAT

Stanice typu server

Server 1

Operační systém: Microsoft Windows Server 2003 Standart Edition Service Pack 2

Procesor: Intel Xeon 3.00 GHz, 1M Cache, 667 MHz FSB, RAM: 2.00 GB

Tento server je ve škole již delší dobu, slouží především pro správu účtů prostřednictvím Active Directory a aplikaci Bakaláři, kde jsou vedeny elektronické třídní knihy a žákovské knížky.

Obr. 13: Server 1 [Zdroj: Vlastní zpracování]

Server 2

Operační systém: Microsoft Windows Server 2008 R2 Standart

Procesor: Intel® Xeon® Processor E5506 2.13 GHz, 4M Cache RAM: 6.00 GB DDR3 800 MHz

Tento server byl pořízen v rámci projektu Rozšiřování kompetencí ve využívání prostředků informačních a komunikačních technologií realizovaném v období let 2010 až 2012. Jeho hlavním využitím bylo hostování systému NIS (Nemocniční informační systém) od společnosti Stapro s.r.o., ten se využíval ve znojemské nemocnici, žáci s ním

tak byly seznámeni už v průběhu výuky. Od minulého roku však přešla Nemocnice Znojmo na jiný informační systém a tak tento server nemá nyní praktické využití.

Obr. 14: Server 2 [Zdroj: Vlastní zpracování]

Notebooky pro vedení školy

Tyto notebooky mají přiděleny pouze tři osoby z vedení školy za účelem zvýšení pracovního nasazení. Po pracovní době si tyto notebooky mohou odnést domu a pokračovat v rozdělané práci nebo je využívat ke svým soukromým účelům. Na těchto noteboocích je nainstalován operační systém MS Windows 7 Professional a kancelářský

balíček MS Office 2013. Zodpovědné osoby mají k notebooku administrátorská práva a mohou tak instalovat další aplikace.

Notebooky pro učitele

Slouží k ovládání interaktivních tabulí ve specializovaných učebnách. Pomáhají učitelům v naplňování jejich pracovních povinností. Tyto notebooky mají nainstalován operační systém MS Windows 7 Professional s kancelářským balíčkem MS Office 2013. Uživatelé těchto notebooku nemají administrátorská práva a nemohou tak instalovat další aplikace. Administrátorská práva pro instalaci aplikací má z interních zaměstnanců organizace pouze metodik a koordinátor ICT (jedna a tatáž osoba) a vedle něj i externí správce sítě. Ti společně zodpovídají za dodatečně doinstalovaný software.

PC pro výuku informatiky

Jedná se o 17 shodných PC skříní DELL Vostro sloužících pro výuku informatiky a dalších předmětů ve specializované učebně. Na těchto PC je nainstalován operační systém MS Windows 7 Professional s kancelářským balíčkem MS Office 2010.

PC pro agendu školy

Tyto počítače jsou umístěny v prostorách s omezeným přístupem, jedná se většinou o kabinety učitelů či prostory jako sekretariát školy a sborovna. Na těchto počítačích je nainstalován operační systém MS Windows 8.1 Professional s kancelářským balíčkem MS Office 2013.

PC v knihovně

Počítače v knihovně slouží především žákům o přestávkách k libovolným činnostem, vzhledem k jejich umístění se počítá se studijními účely například při psaní seminárních prací. Jedná se o počítače Lenovo s operačním systémem MS Windows 8.1 Professional s kancelářským balíčkem MS Office 2013.

PC ve vestibulu školy

Tyto počítače nejsou připojeny do vnitřní sítě školy, mají však přístup na internet, žáci se na nich nepřihlašují pod svými přihlašujícími údaji. Na těchto PC je zastaralý operační systém MS Windows XP ver. 2002 s kancelářským balíčkem MS Office 2003.

PC od CERMATU

Tento počítač se nachází v kanceláři ředitele školy, slouží pouze pro účely státních maturit a je proto v provozu pouze dva týdny v roce a nespadá ani do majetku školy.

Tiskárny

Ve škole se nachází 16 převážně inkoustových tiskáren. Hlavní tiskárna se nachází ve vestibulu školy a slouží k veřejnému tisku. U tiskárny je umístěn mincovník, kam musí žák ještě před provedením tisku vložit patřičnou sumu. Další velká tiskárna se nachází ve sborovně školy a slouží učitelům pro tisk výukových materiálů a jako kopírka. Tyto dvě tiskárny má škola v pronájmu. Společnost, která tiskárny škole pronajímá se stará o údržbu a doplňování tonerů. Zbylé tiskárny jsou rozmístěny různě po učebnách a po kabinetech.

Interaktivní tabule

Škola má v současnosti k dispozici 4 interaktivní tabule, ale vzhledem k tomu, že přibývá aktivních uživatelů na straně pedagogů, budou další pravděpodobně přibývat. Momentálně jsou rozmístěny ve specializovaných učebnách (učebna biologie, somatologie, cizích jazyků aj.).

Projektory

Škola má k dispozici také 16 projektorů, 4 jsou přidruženy k interaktivním tabulím, další jsou rozmístěny ve třídách.

2.8.2 Software

Počítačové programy k nichž má škola zakoupené licence a využívá je ke své činnosti.

Operační systém

Jak již bylo zmíněno při analýze hardware, na školních počítačích převládá operační systém MS Windows 7 a MS Windows 8.1. Mezi další operační systémy, co zde můžeme nalézt, lze řadit operační systém MS Windows XP, který je nainstalován pouze na pěti uživatelských stanicích a dále od budoucna se s ním nepočítá, aktuálně se ale jedná o hrozbu, jelikož společnost Microsoft přestala pro tento operační systém

vydávat aktualizace a ukončila jeho podporu. To znamená, že tento systém se stává zranitelnějším vůči virům a bezpečnostním hrozbám.

Aplikace Bakaláři

Tento software řeší školní administrativu, škola jej využívá hlavně pro rozvrhy a zápis známek do elektronických žákovských knížek, v českém školství je tento software hojně využíván. Z hlediska bezpečnosti jsou od roku 2014 veškerá uživatelská hesla uložena v hašované formě, což znemožňuje zjištění aktuálního hesla. Zobrazit heslo je tak možné pouze v okamžiku jeho vkládání do systému. Heslo si uživatel může v systému sám změnit pomocí funkce **zapomenuté heslo** [17].

Vema

Díky navázání spolupráce mezi BAKALÁŘI software s.r.o. a Vema, a. s., nabízí dnes společnost propojení těchto systému v oblasti personalistiky, softwaru pro zpracování mezd a řízení ekonomiky školy, čímž na trhu vzniklo komplexní řešení pro řízení školy. Propojení těchto systému má tyto výhody:

- jediné místo pro správu osobních údajů zaměstnanců [17]
- automatizované podklady pro výpočet mezd ze softwaru Bakaláři [17]
- mzdové přehledy dostupné přímo v softwaru Bakaláři [17]
- úspory v nákladech za pořízení obou systémů [17]

To, že se toto řešení jeví jako výhodné, jen podtrhuje fakt, že v České

a Slovenské republice možnost používat tyto systémy dohromady využívá více než 4200 školských zařízení [17].

Nemocniční systém

Nemocniční informační systém pořízen v rámci projektu Rozšiřování kompetencí ve využívání prostředků informačních a komunikačních technologií slouží k výuce žáků pro práci s nemocničními informačními systémy. Tento systém od společnosti Stapro s.r.o. s označením FONS je využíván převážně pro vedení zdravotnické dokumentace, zefektivnění administračních a organizačních procesů a zvýšení produktivity práce a kvality péče [18].

2.8.3 Síťová infrastruktura

Školní síť je ve velmi špatném stavu. Pro síťovou infrastrukturu, která se postupně budovala od roku 1999 a na jejíž instalaci se podílelo nekoordinovaně více firem, chybí mapa sítě a veškerá dokumentace. S postupným rozšiřováním počítačového vybavení (počítače, tiskárny, interaktivní tabule atd.) síť mohutněla, což vedlo k zmatečnosti a nepřehlednosti celé sítě. V případě potřeby připojení zařízení do sítě bylo často použito provizorní řešení, které však v mnohých případech přetrvává dosud. Aktivní síťové prvky typů switch jsou umístěny na nevyhovujících místech, například ve školní knihovně je switch umístěn na spodní straně desky stolu, viz obr. 16. Z tohoto a mnoha dalších důvodů (zastaralá infrastruktura, nedostatečně chráněné kabelové trasy, aj.) bych aktuální stav označil jako nevyhovující.

Obr. 15: Switch umístěný pod stolem [Zdroj: Vlastní zpracování]

Data pro interní potřebu školy

1. Doklady o přijímání uchazečů ke vzdělávání, o průběhu a ukončování vzdělávání,
2. výroční zprávy o činnosti školy, zprávy o vlastním hodnocení,
3. třídní knihy,
4. záznamy z pedagogických rad,
5. protokoly a záznamy o provedených kontrolách,
6. knihu úrazů a záznamy o úrazech žáků, popř. lékařské posudky [19].

2.8.4 Lidé

Z hlediska řízení bezpečnosti informací můžeme uživatele rozdělit do následujících uživatelských tříd:

Správci

V této třídě uživatelů se nachází ti uživatelé, kteří mají dostatečné informační podvědomí a určitým způsobem se podílí na chodu ICT školy. Budou sem patřit správci sítě, učitelé informatiky atd. Tito uživatelé zajišťují chod síťové infrastruktury a koncových zařízení. V případě technických problémů mohou kontaktovat firmu, se kterou má škola smlouvu o a provozu a podpoře ICT.

Učitelé

V případě učitelů na škole dochází poměrně často ke kontaktu s ICT, ať už přímo při vyučování, kde používají tyto technologie při výuce, tak i například při čtení elektronické pošty či zápisu známek do elektronické žákovské knížky či procházení webových stránek pro přípravu výuky.

Ostatní personál

Do této kategorie spadá především provozní personál školy, který se během své pracovní činnosti do kontaktu s ICT běžně nedostává. Do této třídy patří například pracovník ostrahy, který se přímo podílí na fyzické bezpečnosti školy.

Žáci

Poslední specifickou skupinou jsou žáci školy, tato skupina je z hlediska počtu uživatelů nejpočetnější. Do kontaktu s ICT školy se dostávají při hodinách informatiky, kde pro ně platí řád a režim odborné učebny informatiky anebo v rámci svého volného času, kdy mohou použít zpřístupněné počítače ve vestibulu školy či knihovně. V obou případech jsou pak žáci povinni řídit se školním řádem, který ovšem nezmiňuje informační bezpečnost a dbá spíše na správné chování žáků z morálního hlediska.

Citlivé údaje

Aktivem jsou také citlivé údaje o žácích a zaměstnancích uchovávané ve školní matrice a systémech školy.

Údaje o žácích

Osobní údaje uchovávané ve školní matrice:

1. identifikační údaje (jméno, příjmení, rodné číslo, popř. datum narození, nebylo-li rodné číslo přiděleno, státní občanství, místo narození, místo trvalého pobytu, u cizinců místo pobytu v ČR nebo v zahraničí),
2. údaje o předchozím vzdělávání, včetně dosaženého stupně vzdělání,
3. údaje o vzdělávání ve škole (obor, forma, délka vzdělávání, datum zahájení vzdělávání, údaje o průběhu a výsledcích vzdělávání, vyučovací jazyk, datum ukončení vzdělávání, údaje o zkoušce, kterou bylo ukončeno),
4. specifické údaje (zdravotní způsobilost ke vzdělávání a zdravotní obtíže s možným vlivem na vzdělávání, zdravotní postižení žáka včetně druhu postižení či zdravotního znevýhodnění, sociální znevýhodnění, je-li škole sděleno),
5. kontakt na zákonného zástupce nezletilého žáka (jméno, příjmení, místo trvalého pobytu nebo bydliště, pokud nemá v ČR trvalý pobyt, adresu pro doručování písemností a telefonické spojení) [19].

Údaje o zaměstnancích

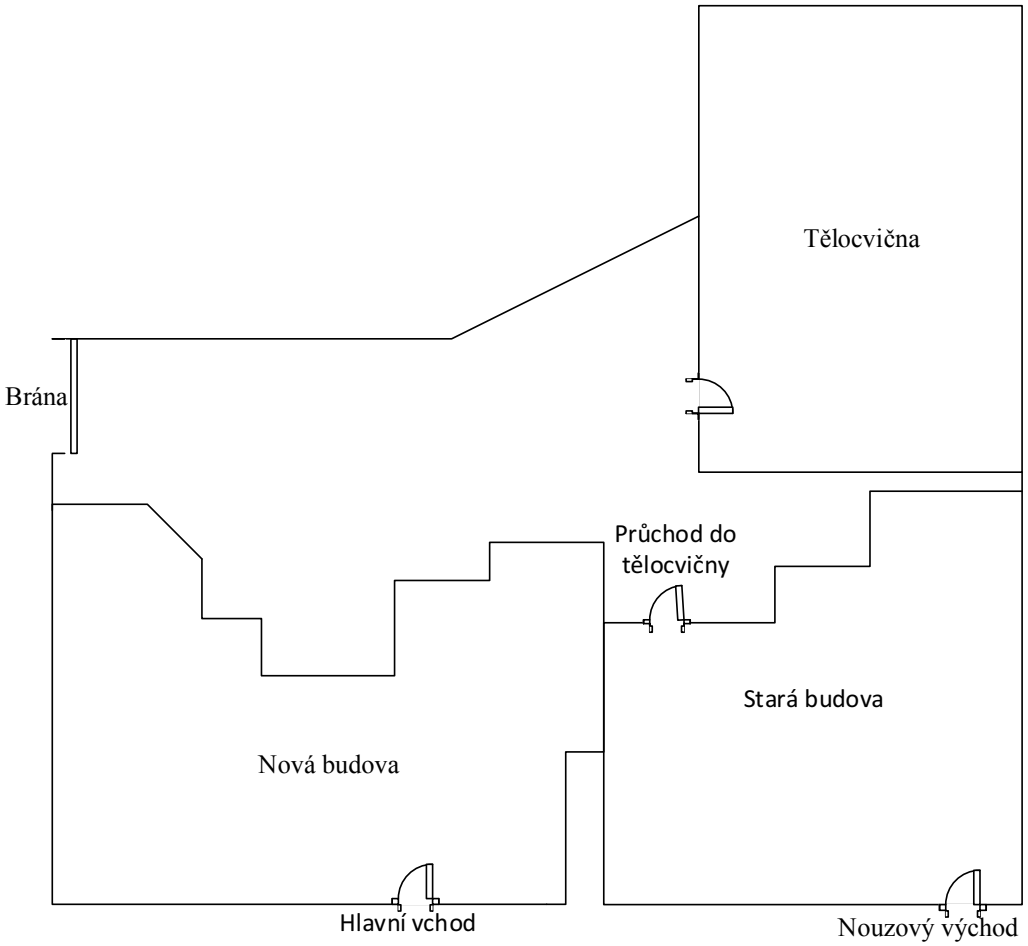
Zaměstnavatel má právo uchovávat pouze takové osobní údaje, které jsou nezbytné pro plnění povinností zaměstnavatele. Zaměstnavatel má právo uchovávat tyto údaje:

1. Identifikační údaje (jméno, příjmení, rodné číslo, popř. datum narození, nebylo-li rodné číslo přiděleno, státní občanství, místo narození, místo trvalého pobytu, u cizinců místo pobytu v ČR nebo v zahraničí),
2. údaje pro správný výpočet mzdy (vzdělání, předchozí praxe),
3. pro správný výpočet měsíčních záloh na daně (podle zákona o správě daní a poplatků, druh pobíraného důchodu),
4. prohlášení poplatníka daně z příjmu (podle zákona o správě daní a poplatků),
5. státní občanství (za účelem hlášení zaměstnávání cizinců),

6. zdravotní znevýhodnění (pro potřeby plnění povinného podílu osob se zdravotním postižením na celkovém počtu zaměstnanců podle § 83 zákona o zaměstnanosti),
7. informace o dětech (v případě ženy počet dětí pro zjištění nároku na odchod do starobního důchodu, jméno, příjmení a rodné číslo dítěte v případě, že zaměstnanec uplatňuje daňové zvýhodnění na vyživované dítě),
8. informace o manželovi/manželce (příjmení a jméno manžela/ky, název a adresa zaměstnavatele, v případě, že zaměstnanec uplatňuje daňové zvýhodnění a manžel/ka je zaměstnán/a),
9. zdravotní pojišťovnu zaměstnance (pro placení zdravotního pojištění, podle § 10 zákona o veřejném zdravotním pojištění) [20].

2.8.5 Lokality

Analyzována škola stojí uprostřed města a skládá se ze dvou vnitřně propojených budov a tělocvičny. Nová budova školy má čtyři patra, stará budova má pater pět. Na plánu školy můžeme vidět školní dvůr zabezpečený bránou, ta je přes den otevřená. U prostor hlavního vchodu v nové budově je vrátnice, která brání vstupu nepovolaných osob do objektu. Ve staré budově se nacházejí dva východy z budovy. Přední východ slouží jako nouzový a je zabezpečen čidlem, které v případě otevření dveří odesílá zprávu (SMS) školníkovi a řediteli školy. Zadní východ na dvůr lze otevřít pouze zevnitř školy a žáci jej používají pro přesun do tělocvičny pod dohledem vyučujícího.



Obr. 16: Plán budovy školy [Zdroj: Vlastní zpracování]

2.9 Analýza opatření

Níže se zaměřím na srovnání aktuálně zavedených opatření, která nabízí příloha A normy ISO/IEC 27001. Tato analýza lze využít i jako prohlášení o aplikovatelnosti, jelikož prohlášení o aplikovatelnosti nemá pevně danou formu, musí se pouze držet normy ISO/IEC 27001 a obsahovat cíle a důvody opatření, již existující opatření a vyloučená bezpečnostní opatření a důvod jejich vyloučení. Pro tuto analýzu jsem zvolil následující formát:

Opatření: číslo a název opatřeni dle přílohy A normy ISO/IEC 27001
Vyloučeno : opatření je vyloučeno nebo není
Aplikováno: jíž je v organizaci aplikováno nebo není aplikováno
Dokumenty: kterých dokumentů se toto opatření týká
Komentář: rozšiřující komentář, pro bližší specifikaci opatření

2.9.1 Politika bezpečnosti informací (A.5)

Směrování bezpečnosti informací vedením organizace

Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky organizace, příslušnými zákony a regulatorními požadavky.

Opatření: 5.1.1 Politiky pro bezpečnost informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Politika bezpečnosti informací
Komentář: Neexistuje politika bezpečnosti informací, proto ji doporučuji zavést.

Opatření: 5.1.2 Přezkoumání politik pro bezpečnost informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Zápis z přezkoumání dokumentace
Komentář: Doporučuji pravidelně přezkoumávat bezpečnostní politiky minimálně jednou za rok a při významných změnách.

2.9.2 Organizace bezpečnosti informací (A.6)

Interní organizace

Cíl: Ustavit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci.

Opatření: 6.1.1 Role a odpovědnosti bezpečnosti informací
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Organizační řád školy
Komentář: Doporučuji detailněji popsat přidělené kompetence v rámci ISMS.

Opatření: 6.1.2 Princip oddělení povinností
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Organizační řád školy
Komentář: V praxi oddělení povinností funguje, ovšem není podloženo patřičnou dokumentací.

Opatření: 6.1.3 Princip oddělení povinností
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Komunikační matice
Komentář: Doporučuji rozšířit komunikační matici pro případ kybernetického incidentu.

Opatření: 6.1.4 Kontakt se zájmovými skupinami
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty:
Komentář: Stanovit dle potřeb certifikace ISMS.

Opatření: 6.1.5 Bezpečnost informací v řízení projektů
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty:
Komentář: Postupovat dle bezpečnostních politik v rámci řízení projektu.

Mobilní zařízení a práce na dálku

Cíl: Zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku.

Opatření: 6.2.1 Politika mobilních zařízení
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Politika mobilních zařízení
Komentář: Doporučují vypracovat dokument politiky mobilních zařízení.

Opatření: 6.2.2 Politika mobilních zařízení
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: V dané organizaci se nevyužívá.

2.9.3 Bezpečnost lidských zdrojů (A.7)

Před vznikem pracovního vztahu

Cíl: Zajistit, aby zaměstnanci, smluvní strany byli srozuměni se svými povinnostmi a aby pro jednotlivé role byli vybráni vhodní kandidáti.

Opatření: 7.1.1 Prověřování
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Organizační řád školy, Pracovní řád
Komentář: Ověření deklarovaného vzdělání, totožnosti, způsobilosti vykonávat příslušnou roli, zajišťuje kancelář školy.

Opatření: 7.1.2 Podmínky pracovního poměru
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Organizační řád školy, Pracovní řád, Pracovní smlouva
Komentář: Odpovědnost za smlouvy se zaměstnanci připadá na kancelář školy.

Během pracovního vztahu

Cíl: Zajistit, aby si zaměstnanci a smluvní strany byli vědomi a plnili si svoje povinnosti v oblasti bezpečnosti informací.

Opatření: 7.2.1 Odpovědnosti vedení organizace
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Organizační řád školy, Pracovní řád, Bezpečnostní politika
Komentář: V praxi se využívá, ovšem chybí příslušná dokumentace.

Opatření: 7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Roční plán vzdělávání
Komentář: Do plánu školení doporučují zavést pravidelné školení ISMS.

Opatření: 7.2.3 Disciplinární řízení
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Pracovní řád
Komentář: Odpovědnost za provinění a zahájení disciplinárního řízení musí být vždy podloženo fakty a důkazy a musí probíhat dle platné legislativy.

Ukončení a změna pracovního vztahu

Cíl: Chránit zájmy organizace v rámci změny nebo ukončení pracovního vztahu.

Opatření: 7.3.1 Odpovědnosti při ukončení nebo změně pracovního vztahu
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Pracovní řád
Komentář: Odpovědnost dle platné legislativy, je nutné si uvědomit, že některé odpovědnosti (např. dohoda o mlčenlivosti) nezanikají s ukončením pracovního vztahu.

2.9.4 Řízení aktiv (A.8)

Odpovědnost za aktiva

Cíl: Identifikovat aktiva a definovat odpovědnosti k jejich přiměřené ochraně

Opatření: 8.1.1 Seznam aktiv
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Seznam aktiv
Komentář: Do seznamu aktiv doplnit kromě hardware i software a dataware.

Opatření: 8.1.2 Vlastnictví aktiv
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Seznam aktiv
Komentář: Všechna aktiva v seznamu musí mít přiděleného vlastníka.

Opatření: 8.1.3 Přípustné použití aktiv
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Seznam aktiv
Komentář: Aktiva je potřeba ohodnotit, k čemu můžeme použít normu ISO/IEC 27005.

Opatření: 8.1.4 Navrácení aktiv
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Doporučuji zavést výstupní list při ukončení pracovního poměru, kde bude shrnutí a potvrzení, že všechny závazky mezi zaměstnancem a zaměstnavatelem jsou vyrovnány a na jeho základě jsou po té zrušený všechny přístupy do systémů dan organizace.

Klasifikace informací

Cíl: zajištění odpovídající úrovně ochrany informací v souladu s jejich důležitostí pro organizaci

Opatření: 8.2.1 Klasifikace informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Rozdělení informací do příslušných tříd. Nejčastěji bývá použito tří tříd a to: veřejné, interní a chráněné.

Opatření: 8.2.2 Označování informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Veškeré dokumenty pro interní potřeby by měly být viditelně označeny.

Opatření: 8.2.3 Manipulace s aktivy
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Zacházeni s aktivy dle jejich klasifikace.

Manipulace s médii

Cíl: Předcházet neoprávněnému vyzrazení, modifikaci, odstranění nebo zničení dat uložených na médiích.

Opatření: 8.3.1 Správa výměnných médií
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Zacházeni s aktivy dle jejich klasifikace.

Opatření: 8.3.2 Likvidace medií
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Pokud nejsou média zapotřebí, je potřeba je zlikvidovat dle formálních postupů.

Opatření: 8.3.3 Přeprava fyzických medií
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: I při přepravě je potřeba media chránit před neoprávněným přístupem, před zničením či poškozením.

2.9.5 Řízení přístupu (A.9)

Požadavky organizace na řízení přístupu

Cíl: Omezit přístup k informacím a vybavení pro zpracování informací.

Opatření: 9.1.1 Politika řízení přístupu
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Probíhá prostřednictvím Active Directory.

Opatření: 9.1.2 Přístup k sítím a síťovým službám
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Probíhá prostřednictvím Active Directory. Pokud uživatel nemá mít právo přístupu k síťovým službám, může mu ho správce v AD zakázat.

Řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup k informacím a předcházet neoprávněnému přístupu k systémům a službám.

Opatření: 9.2.1 Registrace a zrušení registrace uživatele
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Stejně jako vytváření jednotného uživatele tak i rušení uživatele provádí ručně koordinátor ICT nebo jiný uživatel třídy správce dle potřeby.

Opatření: 9.2.2 Zřízení přístupu uživatele
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Zřízení uživatele probíhá buď jednotlivě (na školu přijde nový žák) anebo hromadně (začátek školního roku), všechny tyto účty jsou vytvářeny ručně.

Opatření: 9.2.3 Správa privilegovaných přístupových práv
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Aktuálně podle práv Active Directory, doporučuji lépe zdokumentovat kdo tyto práva má.

Opatření: 9.2.4 Správa tajných autentizačních informací uživatelů
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS
Komentář: Aktuálně probíhá distribuce hesel bezpečným způsobem, avšak uživatelé nejsou nuceni si dočasné heslo měnit, což považuji za problém a při prvním přihlášení do systému bych doporučil vygenerované heslo změnit.

Opatření: 9.2.5 Přezkoumání uživatelských přístupových práv uživatelů
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Doporučuji přezkoumávat, zda si uživatel změnil přidělené dočasné heslo.

Opatření: 9.2.6 Odebrání nebo úprava přístupových práv
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Doporučuji zadokumentovat jak postupovat při odebírání uživatele ve všech systémech, aktuálně probíhá rušení uživatele ručně, může se tak stát, že uživatelův účet zůstane aktivní i několik dnů po tom co by měl být zrušen.

Odpovědnosti uživatelů

Cíl: Zajistit ochranu autentizačních uživatelských informací pomocí odpovědnosti.

Opatření: 9.3.1 Používání tajných autentizačních informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS, e-learning
Komentář: Při změně hesla poučit uživatele o bezpečnostním povědomí z hlediska hesel. Doporučují každého nového uživatele pomocí e-learningu proškolit o bezpečném používání hesel.

Řízení přístupu k systémům a aplikacím

Cíl: Předcházet neautorizovanému přístupu k systémům a aplikacím.

Opatření: 9.4.1 Omezení přístupu k informacím
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS
Komentář: Každý uživatel má přístup jen ke svým souborům, to je řešeno pomocí správy uživatelských účtu v Active Directory.

Opatření: 9.4.2 Bezpečné postupy přihlášení
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS
Komentář: Je řešeno prostřednictvím Active Directory.

2.9.6 Kryptografie (A.10)

Kryptografická opatření

Cíl: Zajistit řádné a efektivní používání kryptografie k ochraně důvěrnosti, autentičnosti a integrity informací.

Opatření: 10.1.1 Politika používání kryptografických opatření
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS
Komentář: Tyto bezpečnostní opatření obsahují přímo používané systémy, ať už se jedná o Active Directory, Windows či systém Bakaláři.

Opatření: 10.1.2 Správa klíčů
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS
Komentář: Je řešeno prostřednictvím Active Directory, Windows a Bakaláři.

2.9.7 Fyzická bezpečnost a bezpečnost prostředí (A.11)

Zabezpečené oblasti

Cíl: předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace

Opatření: 11.1.1 Fyzický bezpečnostní perimetr
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Školní řád, Organizační řád školy
Komentář: Omezení přístupu pro žáky a využívání školní vrátnice a přítomnost bezpečnostního pracovníka toto opatření pokrývá, ale není to z hlediska bezpečnosti dostatečné, více se o tomto opatření vyjadřuji v kapitole 3.7.1

Opatření: 11.1.2 Fyzické kontroly vstupu
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Školní řád, Organizační řád školy
Komentář: Řešeno v kapitole 3.7.2

Opatření: 11.1.3 Zabezpečení kanceláře a vybavení
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Školní řád, Organizační řád školy
Komentář: Z důvodu pohybu žáků je nežádoucí uzamykat všechny učebny a kanceláře, z tohoto důvodu jsou určeny učebny s vybavením, které jsou uzamykány a žáci je využívají jen za přítomnosti učitele (např. učebna informatiky) a učebny bez zvláštního vybavení, které umožňují žákům trávit zde přestávku či volnou hodinu. Více v kapitole 3.7.3.

Opatření: 11.1.4 Ochrana před vnějšími a přírodními hrozbami
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Škola se nenachází v záplavové oblasti ani v oblasti se zvýšenou tektonickou aktivitou, na ostatní hrozby je potřeba reagovat.

Opatření: 11.1.5 Práce v zabezpečených oblastech
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: V dané organizaci se nenachází.

Opatření: 11.1.6 Oblasti pro nakládku a vykládku
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Jako oblast pro nakládku a vykládku slouží školní dvůr viz obr. 12. V této oblasti se můžou subjekty třetích stran nacházet jen za přítomnosti zaměstnanců školy.

Zařízení

Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiva či přerušení činnosti organizace.

Opatření: 11.2.1 Umístění zařízení a jeho ochrana
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Navazuje na 11.1.3, více se tomuto opatření věnuji v kapitole 3.7.4.

Opatření: 11.2.2 Podpůrné služby
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Nejdůležitější data (na serveru) jsou chráněny pomocí UPS.

Opatření: 11.2.3 Bezpečnost kabelových rozvodů
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS, mapa sítě, plány rozvodů
Komentář: Jelikož škola dodělávala datovou síť postupně a od různých dodavatelů, je tato síť v nevyhovujícím stavu a sama škola plánuje její celkovou renovaci. Více o problémech s kabelovými rozvody v kapitole 3.7.5.

Opatření: 11.2.4 Údržba zařízení
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS, Organizační řád školy, SLA
Komentář: O údržbu zařízeni se stará dodavatelská firma dle potřeb a pokynů správce ICT.

Opatření: 11.2.5 Přemístění aktiv
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS, Pracovní řád, Školní řád, Seznam aktiv
Komentář: Aktiva není možné přemisťovat bez povolení pověřené osoby, vynášení aktiv z budovy školy má za úkol zabránit bezpečnostní pracovník a vrátná.

Opatření: 11.2.6 Přemístění zařízení a aktiv mimo prostory organizace
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Pracovní řád, Seznam aktiv
Komentář: Aktiva schválená pro pohyb mimo prostory organizace mají v seznamu aktiv přidělena odpovědnou osobu, která musí zajistit požadovanou bezpečnost i mimo prostory organizace, doporučuji vypracovat předávací formulář, kde bude osoba využívající zařízení mimo organizaci poučena o možných hrozbách a kde potvrdí, že za aktivum přebírá plnou zodpovědnost.

Opatření: 11.2.7 Bezpečná likvidace nebo opakované použití zařízení
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: SLA, příručka ISMS
Komentář: Media typu cd apod. likvidují v organizaci samy, stará a vysloužilá zařízení jsou v organizaci skladována a jednou za čas jsou zlikvidována firmou obstarávající ICT.

Opatření: 11.2.8 Neobsluhovaná uživatelská zařízení
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: příručka ISMS
Komentář: Nastavit v Active Directory, že v případě neaktivity počítače po přihlášení znovu vyžadovat heslo po určitém časovém intervalu bez uživatelovy aktivity.

Opatření: 11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: E-learningový kurz
Komentář: Doporučuji vytvořit pro žáky a zaměstnance e-learningový kurz, kde bude mimo jiné prezentována i zásada prázdného stolu a prázdné obrazovky.

2.9.8 Bezpečnost provozu (A.12)

Provozní postupy a odpovědnosti

Cíl: Zajistit správný a bezpečný provoz vybavení pro zpracování informací

Opatření: 12.1.1 Dokumentace provozních postupů
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: E-learningový kurz
Komentář: Doporučuji vytvořit pro žáky a zaměstnance e-learningový kurz, kde bude mimo jiné prezentována i dokumentace pracovních postupů.

Opatření: 12.1.2 Řízení změn
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Provozní řád
Komentář: Při každé změně dbát i na bezpečnost informací.

Opatření: 12.1.3 Řízení kapacit
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Organizační řád školy
Komentář: Správce ICT používá, monitoruje, vyhodnocuje, optimalizuje a plánuje výkon systému.

Opatření: 12.1.4 Princip oddělení prostředí vývoje, testování a provozu
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: V dané organizaci se nenachází.

Ochrana před malwarem

Cíl: Zajistit ochranu informací a vybavení na jejich zpracování adekvátní ochranou.

Opatření: 12.2.1 Opatření proti malwaru
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS
Komentář: Pro ochranu proti virům a malwaru je na stanicích nainstalován Eset Endpoint Antivirus s centrální správou ze serveru. Na serveru je použit Eset File security. Internetový provoz je kontrolován pomocí antiviru SOPHOS ve firewallu Kerio Control.

Zálohování

Cíl: Ochrana před ztrátou dat

Opatření: 12.3.1 Zálohování informací
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS
Komentář: Soubory jsou uloženy na serveru na zrcadlených discích v poli RAID1 (dva disky), jejich záloha probíhá 1x měsíčně na externí síťový disk. Zálohy z počítačů ředitele, ekonomky a kanceláře školy probíhají odděleně na jiný externí síťový disk.

Zaznamenávání formou logů a monitorování

Cíl: Zaznamenávat události a generovat důkazy.

Opatření: 12.4.1 Zaznamenávání událostí formou logů
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Zaznamenávání logů nad službou Active Directory na Windows Server 2008 R2, logování musí být zapnuto, vhodné nastavení logování ponecháno na správci ICT.

Opatření: 12.4.2 Ochrana logů
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Stanovit takový interval kontroly logů, aby nebyla překročena kapacita média pro záznamu logů.

Opatření: 12.4.3 Ochrana logů
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Stanovit takový interval kontroly logů, aby nebyla překročena kapacita média pro záznamu logů, umístění logů na serveru zabraňuje přístupu uživatelů.

Opatření: 12.4.3 Logy o činnosti administrátorů a operátorů
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Vzhledem k chybějící vyšší autoritě, jsou sice administrátorské činnosti logovány, kontrolují je, ale správci navzájem.

Opatření: 12.4.4 Synchronizace hodin
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS
Komentář: Synchronizace probíhá z vnějšího autorizovaného zdroje. Synchronizace probíhá přes server.

Správa provozního softwaru

Cíl: Zajistit integritu provozních systémů

Opatření: 12.5.1 Instalace softwaru na provozních systémech
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS
Komentář: Instalaci pouze autorizovaného softwaru zajišťuje fakt, že uživatelé nemají práva instalovat software a veškerý software je tak instalován správcem.

Správa a řízení technických zranitelností

Cíl: Zabránit využívání technických zranitelností

Opatření: 12.6.1 Správa a řízení technických zranitelností
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Navrhuji udržovat aktualizovaný software a ovladače zařízení. Více v kapitole 3.8.2.

Opatření: 12.6.2 Omezení instalace softwaru
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS
Komentář: viz SoA 12.5.1 pouze správci mají práva instalovat software.

Hlediska auditu IS

Cíl: Minimalizovat dopady auditních činností na provozní systémy

Opatření: 12.7.1 Opatření k auditu informačních systémů
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Správa z interního auditu IS
Komentář: Interní audity IS.

2.9.9 Bezpečnost komunikací (A.13)

Správa bezpečnosti sítě

Cíl: Zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací.

Opatření: 13.1.1 Opatření v sítích
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty:
Komentář: Aktuálně špatný stav sítě, v blízké době je plánováno předělání celé sítě, chybí mapa sítě, výhoda je, že připojení k síti je v současné době omezeno.

Opatření: 13.1.2 Opatření v sítích
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Jako velký nedostatek vnímám chybějící mapu sítě.

Opatření: 13.1.3 Princip oddělení v sítích
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty:
Komentář: Není využíváno, s výstavbou nové sítě doporučuji zavést

Opatření: 13.1.3 Princip oddělení v sítích
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty:
Komentář: Není využíváno, s výstavbou nové sítě doporučuji zavést.

Přenos informací

Cíl: Zajistit bezpečnost informací během jejich přenosu k externímu subjektu a naopak.

Opatření: 13.2.1 Politiky a postupy při přenosu informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Politik bezpečnosti informací
Komentář: Doporučuji zakomponovat do připravované politiky bezpečnosti informací.

Opatření: 13.2.2 Dohody o přenosu informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty:
Komentář: Nepopiratelnost by měl zajistit podpis, jak klasický tak digitální při elektronické komunikaci. Klasický podpis je v organizaci při komunikaci využíván, jeho digitální ekvivalent už ale o poznání méně.

Opatření: 13.2.3 Elektronické předávání zpráv
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Příručka ISMS
Komentář: Používání šifrovaných kanálů pro přenos informace by měli zajistit důvěrnost informace

Opatření: 13.2.4 Dohody o důvěrnosti nebo mlčenlivosti
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Dohoda o mlčenlivosti
Komentář: Doporučuji s dodavateli, u kterých je to relevantní, zakomponovat do smluv a podepsat dohodu o mlčenlivosti.

2.9.10 Akvizice, vývoj a údržba systému (A.14)

Bezpečnostní požadavky IS

Cíl: Zajistit aby se bezpečnost informací stala nedílnou součástí IS v celém jejich životním cyklu (to zahrnuje i požadavky na IS poskytující služby ve veřejných sítích).

Opatření: 14.1.1 Analýza a specifikace bezpečnostních požadavků
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Politika bezpečnosti informací
Komentář: Aktuálně vnitřní systém řeší systém Bakaláři, který má tyto požadavky politiky bezpečnosti informací pokryty.

Opatření: 14.1.2 Zabezpečení aplikačních služeb ve veřejných sítích
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Politika bezpečnosti informací
Komentář: Aktuálně vnitřní systém řeší systém Bakaláři, který má tyto požadavky politiky bezpečnosti informací pokryty.

Opatření: 14.1.3 Ochrana transakcí aplikačních služeb
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Politika bezpečnosti informací
Komentář: Používání elektronických podpisů a šifrované komunikace.

Bezpečnost v procesech vývoje a podpory

Cíl: Zajistit aby bezpečnost informací byla navrhována a implementována v životním cyklu vývoje IS.

Opatření: 14.2.1 Politika bezpečného vývoje
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: V organizaci k žádnému vývoji softwaru a systému nedochází.

Opatření: 14.2.2 Postupy řízení změn systémů
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: V organizaci k žádnému vývoji softwaru a systému nedochází.

Opatření: 14.2.3 Technické přezkoumání aplikací po změnách provozní platformy
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: V organizaci k žádnému vývoji softwaru a systému nedochází.

Opatření: 14.2.4 Omezení změn softwarových balíků
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: V organizaci k žádnému vývoji softwaru a systému nedochází.

Opatření: 14.2.5 Principy budování bezpečných systémů
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: V organizaci k žádnému vývoji softwaru a systému nedochází.

Opatření: 14.2.6 Prostředí bezpečného vývoje
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: V organizaci k žádnému vývoji softwaru a systému nedochází.

Opatření: 14.2.7 Outsourcovaný vývoj
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: Organizace má zakoupeno krabicové řešení, dohled nad vývojem není možný.

Opatření: 14.2.8 Testování bezpečnosti systémů
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: V organizaci k žádnému vývoji softwaru a systému nedochází.

Opatření: 14.2.9 Testování akceptace systémů
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: V organizaci k žádnému vývoji softwaru a systému nedochází.

Data pro testování

Cíl: Zajistit ochranu dat používaných pro testování.

Opatření: 14.3.1 Ochrana dat pro testování
Vyloučeno: Ano
Aplikováno: Ne
Dokumenty:
Komentář: V organizaci k žádnému testování nedochází.

2.9.11 Dodavatelské vztahy (A.15)

Bezpečnost informací v dodavatelských vztazích

Cíl: Zajistit ochranu aktiv, ke kterým má dodavatel přístup

Opatření: 15.1.1 Politika bezpečnosti informací pro dodavatelské vztahy
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: SLA, Politika bezpečnosti informací
Komentář: Odpovídající bezpečnost informací by měla být s dodavateli dohodnuta a zdokumentována v SLA.

Opatření: 15.1.2 Bezpečnostní požadavky v dohodách s dodavateli
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Politika bezpečnosti informací, smlouvy třetích stran
Komentář: Úprava smluv s dodavateli, aby odpovídali požadavkům na bezpečnost informací.

Opatření: 15.1.3 Řetězec dodavatelů informačních a komunikačních technologií
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: SLA, smlouvy s dodavateli
Komentář: Řešeno v SLA je-li vytvořeno, pokud ne rizika a povinnosti uvést ve smlouvách s dodavateli.

Řízení dodávek služeb dodavatelů

Cíl: Udržení dohodnuté úrovně BI a dodávky služeb ve shodě s dodavatelskými smlouvami.

Opatření: 15.2.1 Monitorování a přezkoumání služeb dodavatelů
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Zápis o přezkoumání
Komentář: Přezkoumání dodavatelů každých 12 měsíců vedením organizace.

Opatření: 15.2.2 Monitorování a přezkoumání služeb dodavatelů
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Provozní řád
Komentář: Případné změny dodávky služeb musí být schváleno vedením organizace.

2.9.12 Řízení incidentů bezpečnosti informací (A.16)

Řízení incidentů BI a zlepšování

Cíl: Zajistit odpovídající a efektivní přístup ke zvládání incidentů bezpečnosti informací zahrnující komunikaci ohledně bezpečnostních událostí a slabých míst.

Opatření: 16.1.1 Odpovědnosti a postupy
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Řízení incidentů bezpečnosti informací
Komentář: Proškolení odpovědné osoby v organizaci

Opatření: 16.1.2 Podávání zpráv o událostech bezpečnosti informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Řízení incidentů bezpečnosti informací
Komentář: Proškolení proškolená osoba školí ostatní zaměstnance a hlásí události bezpečnosti informací této osobě

Opatření: 16.1.3 Podávání zpráv o slabých místech bezpečnosti informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Řízení incidentů bezpečnosti informací
Komentář: Proškolení proškolená osoba školí ostatní zaměstnance a zaměstnanci hlásí slabá místa bezpečnosti informací této osobě.

Opatření: 16.1.4 Posuzování a rozhodování o událostech bezpečnosti informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Řízení incidentů bezpečnosti informací
Komentář: Kontaktní místo posuzuje každou událost bezpečnosti informací pomocí odsouhlasené klasifikační stupnice určené v Řízení incidentů bezpečnosti informací.

Opatření: 16.1.5 Odezva na incidenty bezpečnosti informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Řízení incidentů bezpečnosti informací
Komentář: Na incidenty bezpečnosti informací by mělo být reagováno v souladu s dokumentovanými postupy.

Opatření: 16.1.6 Ponaučení z incidentů bezpečnosti informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Řízení incidentů bezpečnosti informací
Komentář: Znalosti získané z analýzy a řešení incidentu by měli sloužit ke snížení pravděpodobnosti či snížení dopadu dalších případných incidentů.

Opatření: 16.1.7 Shromažďování důkazů
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Řízení incidentů bezpečnosti informací
Komentář: Měly by být definovány postupy, které by mohli sloužit pro identifikaci, shromažďování, získávání a uchovávání informací.

2.9.13 Aspekty řízení kontinuity činností organizace z hlediska BI (A.17)

Cíl: Zajistit, aby kontinuita bezpečnosti informací byla součástí systémů řízení kontinuity činnosti organizace.

Opatření: 17.1.1 Plánováni kontinuity bezpečnosti informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Řízení kontinuity činností
Komentář: Je potřeba definovat požadavky a kontinuitu řízení bezpečnosti informací v nepříznivých a nenadálých situacích.

Opatření: 17.1.2 Implementace kontinuity bezpečnosti informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Řízení kontinuity činností
Komentář: Udržovat procesy, postupy a opatření během nepříznivých a nenadálých situací.

Opatření: 17.1.3 Verifikace, přezkoumání a vyhodnocení kontinuity BI
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Řízení kontinuity činností
Komentář: Přezkoumání každých 12 měsíců, že stanovena a zavedená opatření kontinuity BI jsou stále aktuální a použitelná.

Redundance

Cíl: Zajistit dostupnost vybavení pro zpracování informací.

Opatření: 17.2.1 Verifikace, přezkoumání a vyhodnocení kontinuity BI
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Řízení kontinuity činností
Komentář: Škola má dva servery, kdy v případě incidentu může být jeden nahrazen druhým a disponuje skladem s výpočetní technikou, kde se nachází náhradní komponenty, které mohou být v případě potřeby vyměněny za vadné komponenty

2.9.14 Soulad s požadavky

Soulad s právními a smluvními požadavky

Cíl: Zamezit porušení zákonných, předpisových nebo smluvních povinností týkajících se bezpečnosti informací a jakýchkoliv bezpečnostních požadavků.

Opatření: 18.1.1 Identifikace příslušné legislativy a smluvních požadavků
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Portál veřejné zprávy
Komentář: Doporučuji zpracovat registr právních požadavků.

Opatření: 18.1.2 Ochrana duševního vlastnictví
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS, DML, seznam aktiv
Komentář: Jak již bylo zmíněno v opatření 8.1.1, všechny licenční čísla jsou uložena a v opatření 12.5.1, že software může instalovat pouze správce, který ručí za to, že je software legální a není porušeno autorské právo.

Opatření: 18.1.2 Ochrana duševního vlastnictví
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS, DML, seznam aktiv
Komentář: Jak již bylo zmíněno v opatření 8.1.1, všechny licenční čísla jsou uložena a v opatření 12.5.1, že software může instalovat pouze správce, který ručí za to, že je software legální a není porušeno autorské právo.

Opatření: 18.1.3 Ochrana záznamů
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Příručka ISMS, DML, seznam aktiv
Komentář: Jak již bylo zmíněno v opatření 8.1.1, všechny licenční čísla jsou uložena a v opatření 12.5.1, že software může instalovat pouze správce, který ručí za to, že je software legální a není porušeno autorské právo.

Opatření: 18.1.4 Soukromí a ochrana osobních údajů
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Zákon na ochranu osobních údajů, školský zákon
Komentář: Soukromí a ochrana osobních údajů musí být zajištěny v souladu s odpovídající legislativou a s předpisy, pokud je to použitelné. Ve výsledku to znamená, že organizace může uchovávat jen ty osobní údaje, které skutečně potřebuje a jen po dobu, po kterou je potřebuje.

Opatření: 18.1.5 Regulace kryptografických opatření
Vyloučeno: Ne
Aplikováno: Ano
Dokumenty: Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti
Komentář: Kryptografická opatření mohou být užívána jen s příslušnými úmluvami a legislativou. Vyhláška nám ukládá používat pouze bezpečné algoritmy, ale jelikož je z roku 2014 je dobré si aktuálnost těchto algoritmů ověřit.

Přezkoumání bezpečnosti informací

Cíl: Zajistit, že bezpečnost informací je implementována a provozována v souladu s politikami a postupy organizace.

Opatření: 18.2.1 Nezávislá přezkoumání bezpečnosti informací
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Zpráva z auditu
Komentář: Přístup organizace k řízení a implementaci bezpečnosti informací musí být nezávisle přezkoumáván v plánovaných intervalech nebo v případě, že nastane významná změna.

Opatření: 18.2.2 Shoda s bezpečnostními politikami a normami
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Zpráva z auditu
Komentář: Odpovědní pracovníci musí pravidelně přezkoumávat shodu zpracování informací v rozsahu jejich odpovědnosti s odpovídajícími bezpečnostními politikami, normami a dalšími požadavky na bezpečnost.

Opatření: 18.2.3 Přezkoumání technické shody
Vyloučeno: Ne
Aplikováno: Ne
Dokumenty: Zpráva z auditu
Komentář: Přezkoumání interních systému zda jsou stále v souladu s bezpečnostními normami a politikami bezpečnosti organizace. Doporučuji toto přezkoumání provádět v rámci interního auditu.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

V této kapitole vycházím z analytické části, kde jsem zabýval aktuálním stavem bezpečnosti informací v organizaci a zjistil tak i slabá místa. K těmto zranitelnostem navrhnu konkrétní opatření, jak danou situaci zlepšit. Závěrem kapitoly provedu ekonomické zhodnocení.

3.1 Politika bezpečnosti informací (A.5)

Bezpečnostní politika představuje závazek vedení, že se ztotožňuje se záměrem zvyšovat bezpečnost informací a poskytnout k tomu potřebné zdroje. Doporučuji aplikovat mnou navrhovanou bezpečnostní politiku viz příloha I.

3.2 Organizace bezpečnosti informací (A.6)

Rámec pro bezpečnost informací představuje z velké části organizační řád školy, ten by ale potřeboval rozšířit, případně doplnit o kapitoly pokrývající problematiku ISMS z detailnější úrovně. V případě kybernetického incidentu, doporučuji pak do komunikační matice doplnit kontakt na Národní centrum kybernetické bezpečnosti.

3.3 Bezpečnost lidských zdrojů (A.7)

Již před vznikem pracovního vztahu je třeba myslet na bezpečnost informací, dle role, kterou bude subjekt v organizaci vykonávat.

Nově přijímaný zaměstnanec musí projít řádným ISMS školením uvnitř organizace. Ostatní zaměstnanci se musí účastnit pravidelných školení ISMS, které doporučují provádět interním zaměstnancem, který bude pro tuto roli vyškolen. Pokud je zaměstnanec proškolen, je seznámen se sankcemi, plynoucími z porušování ISMS.

Při ukončení či pracovního vztahu je potřeba vyřešit otázku jak bude nakládáno s aktivy, která byla zaměstnanci svěřena, se svěřenými oprávněními, která musí být řešena ihned po ukončení či změně pracovního poměru. V případě, že byla se zaměstnancem uzavřena dohoda o mlčenlivosti, tak tato dohoda platí i po ukončení či změně pracovního vztahu.

3.4 Řízení aktiv (A.8)

Doporučuji zlepšit identifikaci aktiv v organizaci, seznam aktiv aktualizovat každý rok nebo při významné změně v aktivech. Pro jednotlivá aktiva stanovit vlastníka nebo odpovědnou osobu.

Veškeré informace by měli být v rámci organizace klasifikovány a příslušně označeny, k tomu doporučuji využít tři základní kategorie:

1. Veřejné – informace, které jsou k dispozici široké veřejnosti a jsou zveřejněny například na stránkách školy,
2. interní – informace, sloužící pouze uvnitř organizace, v tomto případě se bude jednat o informace přístupné zaměstnancům školy,
3. chráněné – do této kategorie patří citlivé informace například výplaty jednotlivých zaměstnanců nebo informace spadající pod zákon o ochraně osobních údajů.

3.5 Řízení přístupu (A.9)

Řízení přístupu probíhá na základě práv přidělených v Active Directory. Jsou dvě základní skupiny uživatelů a to:

Správci – do této kategorie patří interní a externí správce ICT

Uživatelé – do této kategorie spadají všichni ostatní učitelé a zaměstnanci školy s přístupem k ICT a žáci

Vytváření uživatelských účtů probíhá ručně ICT správcem a stejně jeho rušení, které by mělo být kontrolováno. Proto navrhuji alespoň jednou za rok překontrolovat počet aktivních účtů, případně porovnat seznam aktivních účtů se seznamem skutečně oprávněných uživatelů a v případě nesouladu provést nápravu.

3.6 Kryptografie (A.10)

Měla by být vypracována a aplikována politika použití kryptografických opatření na ochranu informací. Doporučuji šifrovat harddisk ekonomky školy, kde se nachází velká část citlivých dat.

Správa a distribuce hesel je vyřešena dobře i díky používání softwaru Bakaláři, kde musí o žákovo zapomenuté heslo zažádat učitel a systém mu vygeneruje nové dočasné heslo.

3.7 Fyzická bezpečnost a bezpečnostní prostředí (A.11)

V případě bezpečnosti prostředí můžeme fyzickou bezpečnost rozčlenit na tři úrovně:

1. Vnější prostředí školy
2. Vnitřní prostředí školy
3. Místa uvnitř školy s omezeným přístupem

3.7.1 Fyzický bezpečnostní perimetr (A.11.1.1)

Oddělení vnějšího a vnitřního prostředí školy je nejlépe vidět na obr. 6, ze kterého vyplývá, že vstup do budovy školy je možné realizovat prostřednictvím tří cest. Hlavní vstup školy je přes den otevřen a je kontrolován vrátnou, která je v pracovní době přítomna u hlavního vchodu ve vrátnici a monitoruje vstup. Dále se za hlavním vstupem pohybuje bezpečnostní pracovník, který je zde, aby zabránil případnému fyzickému útoku na žáky či zaměstnance školy. Ve večerních hodinách je tento vchod uzamčen a přepnut do režimu stráženo, kdy při případném narušení je odeslána SMS zpráva dvěma pověřeným osobám, které následně mohou místo fyzicky zkontrolovat nebo zavolat hlídku státní či městské policie, která sídlí shodou okolností v téže ulici Jana Palacha.

Nouzový východ se nachází v režimu stráženo neustále a je možné ho použít pouze z vnitřní strany školy, z té vnější je k jeho otevření použít klíč.

Třetí vchod do budovy školy je tzv. průchod do tělocvičny, jelikož jsou budova školy a budova tělocvičny fyzicky oddělené, existuje zde průchod ze školy přes část školního dvora do tělocvičny. Dveře se z venku dají otevřít opět pouze pomocí klíče. Zde však nastává problém, když se bude neoprávněná osoba chtít dostat do budovy školy a uvnitř bude mít komplice, může mu ten jít dveře zevnitř otevřít a není možnost, jak to zpětně zjistit. I žáci by pak tudy mohli nepozorovaně opustit budovu školy a další problém je, že kvůli snazšímu pohybu učitelů, aby nemuseli dveře žákům odemykat, instaloval někdo do západky dveří klínek na provázku, který zamezuje automatické zavírání dveří (viz obr. 17), takže většinu dne by se tímto vchodem do školy mohla neoprávněná osoba dostat.

Obr. 17: Klínek v zámku dveří [Zdroj: Vlastní zpracování]

3.7.2 Fyzické kontroly vstupu (A.11.1.2)

Kontrola vstupu do školy je koncipována vcelku dobře, jediné slabé místo jsou dveře umožňující průchod do tělocvičny. Zde by pomohla možnost otevření těchto dveří pouze za použití klíče a proškolit personál, který tyto dveře používá, o svých povinnostech, aby se používání podobného mechanismu na obr. 10 znovu neopakovala.

Místa s omezeným přístupem, která by při narušení mohla narušit chod školy, jsou tato: ředitelna školy, kde je mimo jiné umístěn počítač Cermatu pro maturitní zkoušky, dvě místnosti, kde se nachází servery školy a kancelář ekonoma školy.

Do kanceláře ředitele nebo ekonoma školy se bez jejich vědomí nebo bez vědomí jejich zástupců neměl nikdo dostat.

U serverů je situace složitější, protože nemají vyhrazenou svou místnost. Server 1 je umístěn ve společné místnosti se skladem prádla, server 2 pak v místnosti s archivem místní knihovny. Jedná se o místnosti, kam žáci nemají přístup za žádné okolnosti, ovšem první tři kategorie uživatelů se do těchto prostor mohou nemonitorovaně dostat, doporučuji proto sloučit místění serverů do vyhrazené místnosti s označením serverovna, kde budou mít přístup pouze uživatelé třídy správci.

Dále doporučuji zavést viditelné označení pro návštěvy a jejich evidenci na vrátnici školy. Pro evidenci bych doporučoval zavést knihu návštěv. Pro označení návštěv pak visačku se šňůrou na krk viz obr. 18.

Obr. 18: Visačka [Zdroj: Vlastní zpracování]

3.7.3 Zabezpečení kanceláří, místností a vybavení (A.11.1.3)

Každá z učeben obsahuje počítač zapojený do školní sítě, ať už kvůli obsluze interaktivní tabule nebo k využívání aplikace bakaláři, konkrétně modulu třídní kniha. Pokud se v učebně nachází notebook, je umístěn v uzamykatelné skříni, počítače typu desktop ale uzamykány nejsou. Žáci mají do těchto učeben o přestávce přístup a nejsou permanentně dozorováni. Funguje zde pouze učitelský dozor v rámci patra. Do specializovaných učeben s dražším vybavením žáci v době přestávky přístup nemají. Kabinety učitelů nejsou volně přístupné, volně přístupná je pouze sborovna školy a tam se po dobu výuky neustále nachází učitelé, takže není hrozba neoprávněného vniknutí.

Doporučuji rozšířit využívání uzamykatelných skříní i na volně stojící počítače a tiskárny (viz obr. 11) a umisťování ostatních prvků mimo dosah žáků, případně tato zařízení pevně uchytit (šrouby, vruty) ke zdi, či stropu učebny.

Obr. 19: Uzamykatelný učitelský stůl [Zdroj: Vlastní zpracování]

Obr. 20: Tiskárna ve třídě [Zdroj: Vlastní zpracování]

3.7.4 Umístění zařízení a jeho ochrana (A.11.2.1)

Jak už bylo zmíněno v analýze, aktuálním problémem se servery je nekoordinované umístění v budově školy v místnostech, které plní kromě umístění serveru i další využití. Navíc se tyto místnosti nacházejí ve vrchním patře budovy, kde se mají servery v létě tendenci přehřívat, díky nedokonalé střešní izolaci a špatně řešenému odvodu tepla. Řešením je tedy vytvoření místnosti serverovna, kde budou oba servery na jednom místě. Požadavky na tuto místnost jsou:

1. Čistost a bezprašnost prostředí – toho bývá docíleno oddělením od okolního prostředí a použitím vzduchových a prachových filtrů,
2. kvalitní zdroj energie – zajistit přívod elektřiny ideálně od dvou dodavatelů, zde bude stačit zapojení již používané UPS,
3. kvalitní zapojení do sítě internet – opět ideálně od dvou poskytovatelů připojení, již nyní škola využívá dvě internetové přípojky, ADSL linku od O2 a bezdrátovou přípojku od společnosti PODA,
4. klimatizace – správný odvod teplého vzduchu a přívod vzduchu studeného je pro servery a jejich životnost velice důležitý, v minulosti měla škola právě s přehříváním serverů problémy a doporučuji jim tedy zvážit instalaci klimatizace, která by tento problém eliminovala,
5. zdvojená podlaha – ideální způsob umístění kabelových rozvodů hojně využívaný u velkých datacenter, v staré budově školy se ji ale kvůli vyšším finančním nárokům asi nedočkáme,
6. hašení – k serverovně doporučuji umístit plynový hasicí přístroj, ten totiž případný požár uhasí a nepoškodí další zařízení,
7. zabezpečení objektu – do serverovny mají přístup pouze správci.

3.7.5 Bezpečnost kabelových rozvodů (A.11.2.3)

Jak již bylo zmíněno v analytické části, síťová infrastruktura je ve špatném stavu, což je zapříčiněno zejména postupným dodělávaním jednotlivých částí sítě dle potřeb a různými dodavateli, kteří neměli všechny potřebné informace o aktuálním stavu sítě. Často proto zvítězilo řešení, které sice funguje či fungovalo, ale z hlediska času je neudržitelné. Na obrázcích můžete vidět například amatérskou instalaci Wi-Fi routeru, kde k němu vedou sice tři kabely, ale pouze jedna lišta. Navíc se lze jen těžko domnívat, že takové umístění routeru doporučuje výrobce daného zařízení, viz obr. 21.

Obr. 21: Umístění Wi-Fi routeru [Zdroj: Vlastní zpracování]

Další problém s vedením kabeláže můžeme objevit ve školní knihovně, kde byl pro studenty vytvořen studijní ostrůvek se šesti počítači. Ovšem pro zapojení těchto počítačů do školní sítě, bylo zvoleno ne zrovna ideální řešení, kdy je lišta se síťovým kabelem vedena uprostřed místnosti od stropu do počítačového ostrůvku. Toto řešení bylo zvoleno zřejmě z důvodu, aby žáci přes lištu vedenou po zemi nezakopávali nebo po ní nešlapali, ovšem výsledek působí velice neprakticky a je náchylný na fyzické poškození viz obr. 22. Škola si ale nevyhovující stav síťové infrastruktury uvědomuje a plánuje nápravu ještě během roku 2016 v závislosti na projektové výzvě č. 33, Infrastruktura středních škol a vyšších odborných škol, u které by ráda byla úspěšným žadatelem a posléze příjemcem dotace v rámci integrovaného regionálního operačního programu Evropského fondu pro regionální rozvoj a Ministerstva pro místní rozvoj ČR.

Obr. 22: Lišta ve školní knihovně [Zdroj: Vlastní zpracování]

Tato lišta vede ke switchi (viz obr. 15), který je také umístěn na nevyhovujícím místě. V případě, že mají žáci nekontrolovaný přístup k aktivním prvkům síťové infrastruktury, doporučuji používat klíčované konektory, aby nebylo možné přepojovat jednotlivé plugy či případně používat blokátory pro zamezení neautorizovaného přístupu do sítě. Vedení kabeláže v zamykatelných žlabech či ve zdech budovy by pak mělo zajistit, že nebude narušena pasivní vrstva sítě. Tyto návrhy by mělo vedení zvážit ještě před plánovanou rekonstrukcí sítě a do projektu rekonstrukce je zahrnout.

3.7.6 Bezpečnost zařízeni a aktiv mimo prostory organizace (A.11.2.6)

Bezpečnost aktiv by neměla končit na hranici organizace, ale v případě, že je aktivum použito vně organizaci je potřeba dodržovat stejná či dokonce přísnější opatření s ohledem na různá rizika, bezpečnostní pravidla, jako když se aktivum nachází uvnitř organizace. Toto zařízení by nemělo být ponecháno bez dozoru, měly by být dodržovány pokyny výrobce o ochraně zařízení. Dále by mělo být v organizaci vedeno,

kdo je za zařízení či aktivum aktuálně zodpovědný a měla by na něj být přenesena odpovědnost za dané zařízení dle zákoníku práce. Mnou navrhovaný dokument pro přenesení odpovědnosti lze nalézt v Příloze II.

3.8 Bezpečnost provozu (A.12)

3.8.1 Zaznamenávání událostí formou logů

K auditování událostí nad Active Directory doporučují použít nástroj Directory Service Access. I když tento nástroj není úplně jednoduchý, nabízí spoustu možnosti toho co sledovat, ať už jde o podezřelé operace, failed operace, či dohled nad správou účtů. Toto nastavení je velice efektivní, protože můžeme sledovat tisíce údajů a při špatné volbě si pouze zaplníme log. Za správné nastavení považuji logování událostí typu změna konfigurace systému, instalace aplikace, přihlášení a odhlášení ze systému, přístup ke sdíleným souborům, aktivace a deaktivace ochranných systémů aj. Bližší nastavení bude záležet na správci.

3.8.2 Správa a řízení technických zranitelností (A.12.6.1)

Udržovat aktualizovaný a záplatovaný operační systém je jedním ze základních stavebních požadavků bezpečnosti informací. V této organizaci tvoří výjimku aktualizovaného a záplatovaného systému volně přístupné počítače ve vestibulu školy, na nichž je nainstalován operační systém Microsoft Windows XP, který již není výrobcem aktualizován a záplatován, proto doporučuji přejít na novější verzi tohoto operačního systému. Ideální by byl přechod na systém Microsoft Windows 10, kterému končí podpora až v říjnu 2025. Zároveň doporučuji u těchto počítačů zavést řízení uživatelských účtů prostřednictvím AD, jako je tomu u všech počítačů ve škole.

3.9 Zvyšování bezpečnostního povědomí

Pro bezpečnost provozu je důležité, aby všechny třídy uživatelů, kteří se dostávají do kontaktu s ICT, dodržovali bezpečnostní postupy, byli si vědomi možných hrozeb a věděli jak s informacemi nakládat. Kvůli zvýšení bezpečnostního povědomí bych doporučil proškolit žáky a zaměstnance z bezpečnostního povědomí. Pro toto školení doporučuji zavést e-learningový kurz, jehož prostřednictvím by se žáci

i zaměstnanci školili ze základních dovednostní a pojmů v oboru bezpečnosti informací. Kurz bude zakončen testem z probírané látky a bez jeho absolvování nebudou žáci moci využívat školní ICT technologie. Dále bych doporučoval v návaznosti na mou práci vypracovat příručku ISMS, která bude jasně definovat pravidla a odpovědnosti vůči stanoveným opatřením. Hlavním cílem těchto dokumentů je pak předání informací dalším uživatelům a už jen z tohoto důvodu by měli být veřejně přístupné všem uživatelům v dané organizaci.

Několik základních bezpečnostních zásad, které by bylo dobré v těchto dokumentech zmínit:

1. Používejte silné heslo, bez významu, vyvarujte se obvyklých kombinací (password, 123456, kombinací křestního jména a příjmení),
2. heslo si zapamatujte, nikam nepište (pokuste se ho zapamatovat mnemotechnickou pomůckou),
3. heslo pravidelně měňte (doporučený a hojně využívaný interval je 3 měsíce),
4. dodržujte zásadu prázdného stolu a obrazovky při odchodu z pracoviště,
5. neotevírejte podezřelé e-maily a v žádném případě jejich přílohy,
6. pravidelně zálohujte,
7. na internetu nenavštěvujte podezřelé stránky, které by mohly být nebezpečné, nestahujte neznámé soubory,
8. používejte jen legální a aktualizovaný software,
9. nevypínejte firewall,
10. používejte antivir (pravidelně ho aktualizujte),
11. bezpečnostní problémy okamžitě hlaste příslušné osobě.

Další část zvýšení bezpečnostního povědomí se týká zaměstnanců, kteří přicházejí do styku s ICT při vykonávání náplně své práce; bude se jednat hlavně o učitele a administrativní pracovníky. Tyto zaměstnance bude z problematiky bezpečnosti informací školit externě vyškolený manažer systému řízení bezpečnosti informací, který ve škole zastává funkci CISO. Poslední část školení se týká zaměstnanců, kteří během vykonávání své pracovní náplně nepoužívají ICT. Tito zaměstnanci budou proškoleni pouze na obecné úrovni bezpečnosti informací.

3.10 Ekonomické zhodnocení plánovaných opatření

Ztráty, které by mohly nastat při narušení integrity, dostupnosti a důvěrnosti informací, by mohly pro školu znamenat především poškození dobrého jména u rodičů žáků a vlastně i ohrožení bezpečnosti žáků. Dalším možným dopadem je ztráta finančních prostředků při nefunkčnosti ekonomického systému. Jakákoliv ztráta klíčových dat by měla negativní dopad na chod školy. Proto zde uvádím cenový odhad navrhovaných opatření, která by měla přispět k zvýšení bezpečnosti organizace a zároveň by tato opatření posloužila při na případné certifikaci ISMS. Mnou navrhovaný a konzultovaný cenový odhad vypadá takto:

Tab. 2: Náklady na zavedení opatření [Zdroj: Vlastní zpracování]

Opatření	Cena v Kč bez DPH
Vyškolení správce ICT na Manažera systému řízení bezpečnosti informací	21000
Vytvoření místnosti serverovna a přemístění obou serverů do této místnosti	
Úprava místnosti	15000
Zakoupení dodatečného vybavení	22000
Instalace klimatizace	24000
Přemístění serveru a úprava kabeláže	14900
Pořízení uzamykatelných boxů pro zabezpečení vybavení	36000
Vytvoření e-learningového kurzu	24500
Celkem	**157400**

Nutno podotknout, že v nákladech v tabulce není započtena rekonstrukce síťové infrastruktury, kterou řeší jiný projekt a taky náklady na změnu interních procesů v organizaci, jelikož jsou tyto náklady obtížně vyčíslitelné. Některé položky se mohou zdát na první pohled vysoké, je ovšem důležité si uvědomit, že při selhání bezpečnosti informací by ztráty pro organizaci byly ještě daleko větší.

Pro ohodnocení přínosu mnou navrhovaných opatření jsem vycházel z obdobné studie provedené na České zemědělské univerzitě, kde jsou ohodnoceny ceny jednotlivých částí zavádění ISMS. Při porovnání obou studií a odborné konzultaci jsem dospěl k těmto cenovým odhadům:

Tab. 3 Finanční ohodnocení [Upraveno dle 21]

Položka	Cena v Kč bez DPH
Vypracování bezpečnostní politiky	20000
Plán navrhovaných opatření	30000
Prohlášení o aplikovatelnosti	25000
Celkem	75000

ZÁVĚR

V této práci jsem vytvořil návrh na zavedení bezpečnostních opatření, která jsem doporučil s ohledem na analýzu, kterou jsem zpracoval na základě metod rozhovorů a pozorování. Díky tomu jsem poznal skutečný stav bezpečnosti informací ve škole. Po celou dobu vypracování práce jsem vycházel z platných norem ISO/IEC 27000. V návrhové části jsem se zaměřil na nejvýraznější nedostatky, které jsem zjistil a doporučil jejich řešení prostřednictvím zavedením bezpečnostních opatření, v případě, že budou některé z mnou navrhovaných opatření realizovány, věřím, že dojde ke zvýšení bezpečnosti ICT. To povede i ke zlepšení fungování celé organizace. Součástí analytické části práce je i hotové Prohlášení o aplikovatelnosti. Dále uvádím i doporučení pro Příručku ISMS, kterou je možné upravit na základě doporučení v mé práci. Oba tyto dokumenty mohou být prvním krokem při snaze o audit a následnou certifikací systému řízení bezpečnosti informací. Dalším přínosem mé práce jsou dokumenty, které mají škole pomoci nejen s řízením informační bezpečnosti a můžeme je nalézt v přílohách.

Bezpečnost ICT je velice rozsáhlé téma, které svou obsáhlostí výrazně přesahuje rámec této diplomové práce,. V některých částech jsem se tedy méně významnými opatřeními zabýval spíše stručným doporučením a věnoval jsem se několika klíčovým oblastem, které jsem v organizaci diskutoval a vyšly jako problémové.

Pevně věřím, že všechny cíle práce, které jsem v úvodu definoval jsem splnil a výstupy mé práce, v případě, že budou akceptovány, povedou ke zvýšení bezpečnosti ve škole.

SEZNAM POUŽITÉ LITERATURY

[1] ČSN ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy řízení informací - Přehled a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[2] ČSN ISO/IEC 27005. Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Řízení rizik bezpečnosti informací. 2013. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

[3] KOCH, Miloš a Bernard NEUWIRTH. Datové a funkční modelování. Vyd. 4., rozš. Brno: Akademické nakladatelství CERM, 2010. ISBN 978-80-214-4125-5.

[4] HRŮZA, Petr. Kybernetická bezpečnost II. Brno: Univerzita obrany, 2013. ISBN 978-80-7231-931-2.

[5] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013, 377 s. ISBN 978-80-7204-872-4.

[6] DRASTICH, Martin. Systém managementu bezpečnosti informací. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9.

[7] ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky. 2014. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

[8] ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Soubor postupů pro opatření bezpečnosti informací. 2014. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

[9] GRASSEOVÁ, Monika, Radek DUBEC a Roman HORÁK. Procesní řízení ve veřejném sektoru: teoretická východiska a praktické příklady. Brno: ComputerPress, 2008. ISBN 978-80-251-1987-7.

[10] RAM SINGHAL, Keshav. Quality Concepts and ISO 9001:2008 QMS Awareness. In: ISO 9001:2008 QMS Awareness [online]. 2014 [cit. 2016-05-

20]. Dostupné z: http://iso9001-2008awareness.blogspot.cz/2014/04/pdca-cycle.html

[11] ITIL. Axelos: Global best practise [online]. 2011 [cit. 2016-05-07]. Dostupné z: https://www.axelos.com/best-practice-solutions/itil

[12] PVC Cap for RJ-45 UTP Connector. Ri-vier.eu [online]. 2016 [cit. 2016-01-15]. Dostupné z: https://ri-vier.eu/pvc-cap-for-rj45-utp-connector-grey-p-302.html

[13] Panduit [online]. [cit. 2016-01-15]. Dostupné z: http://www.panduit.com/

[14] RAC ISMS: Zavedení systému řízení bezpečnosti informací. Risk Analysis Consultants [online]. 2016 [cit. 2016-05-23]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/ISMS

[15] O škole. SZŠ a VOŠZ Znojmo [online]. 2009 [cit. 2016-01-14]. Dostupné z: http://www.szsz.cz/o-skole/

[16] Organizační řád. Znojmo: Střední zdravotnická škola a Vyšší odborná škola zdravotnická, Znojmo, Jana Palacha 8, 2013.

[17] Bakaláři software [online]. [cit. 2016-01-16]. Dostupné z: http://www.bakalari.cz

[18] Stapro: Informace v ceně života [online]. 2016 [cit. 2016-05-16]. Dostupné z: http://www.stapro.cz

[19] VOKÁČ, Petr. Školský zákon: zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání. 5. přepracované vydání. Třinec: RESK, spol. s r.o., 2015. ISBN 978-80-87675-03-8.

[20] Zaměstnavatel jako správce osobních údajů. Úřad pro ochranu osobních údajů [online]. 2013 [cit. 2016-05-20]. Dostupné z:

[21] BRECHLEROVÁ, Dagmar a Michal MORAVEC. Bezpečnostní politika univesity [online]. 2006 [cit. 2016-05-23]. Dostupné z: http://uninfos.ukf.sk/documents/zbornik_uninfos2006.pdf. Česká zemědělská univerzita.

SEZNAM POUŽITÝCH ZKRATEK

AD	*Active Directory*
BI	*Bezpečnost informací*
ČSN	*Česká technická norma*
ČR	*Česká republika*
EU	*Evropská unie*
HDD	*Hard disk drive*
HW	*Hardware*
ICT	*Informační a komunikační technologie*
IEC	*Mezinárodní elektrotechnická komise*
IS	*Informační systém*
ISMS	*Systém řízení bezpečnosti informací*
ISO	*Mezinárodní organizace pro standardizaci*
IT	*Informační technologie*
ITIL	*Information Technology Infrastructure Library*
MS	*Microsoft*
PC	*Osobní počítač*
RAID	*Vícenásobné diskové pole nezávislých disků*
RAM	*Random access memory*
SLA	*Service Level Agreement*
SoA	*Prohlášení o aplikovatelnosti*
SW	*Software*
UPS	U*ninterruptible power supply*

SEZNAM OBRAZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Politika informační bezpečnosti

Střední zdravotnická škola a Vyšší odborná škola zdravotnická Znojmo, příspěvková organizace si je vědoma, jak důležitou roli hrají informace v současném světě v pracovním i v soukromém životě. Rozhodla se proto dodržovat systém řízení bezpečnosti informací, aby chránila svá informační aktiva a aby svým žákům i zaměstnancům poskytla odpovídající míru jistoty.

Orientace na výsledky

Důsledně zajišťujeme ochranu informací na potřebné úrovni tak, aby k nim měly přístup pouze oprávněné osoby (princip důvěrnosti), aby byla zajištěna správnost a úplnost informací, byly jasně stanoveny pravomoci a práva k jejich pozměňování (princip integrity) a aby informace byly uživatelům přístupné v okamžiku jejich potřeby (princip dostupnosti).

Vedení a stálost záměrů a cílů

Vedení organizace podporuje a motivuje zaměstnance a žáky k zajištění bezpečnosti informací, a to i nad rámec požadavků platné legislativy. Na základě důsledného zvážení všech dostupných informací a zkušeností iniciuje změny v procesech, činnostech a vztazích se všemi zainteresovanými stranami s cílem dlouhodobě naplňovat deklarovanou strategii společnosti v oblasti informační bezpečnosti.

Řízení na základě procesů a faktů, inovace a zlepšování

Naše procesy a činnosti spjaté s ochranou informací systematicky monitorujeme, vyhodnocujeme a neustále zlepšujeme. Jednotlivé bezpečnostní cíle naplňujeme pomocí adekvátních opatření určených v rámci procesu řízení rizik s dopadem na bezpečnost informací. Naše opatření přitom zahrnují veškeré relevantní oblasti života společnosti: organizaci bezpečnosti, klasifikaci informací, personální a fyzickou bezpečnost, bezpečnost řízení komunikací a provozu, řízení přístupů, bezpečnost vývoje a údržby systémů a řízení kontinuity provozu.

Soulad s legislativními a smluvními požadavky

Naše procesy a činnosti řídíme tak, aby byla zajištěna kontinuita a soulad s platnou legislativou České republiky i Evropské unie, mezinárodními smlouvami a jinými požadavky na ochranu bezpečnosti informací.

Odpovědnost

Systematicky zvyšujeme povědomí našich zaměstnanců o problematice informační bezpečnosti, aby si uvědomovali důsledky a dopady vykonávaných činností a byli schopni účinné prevence. Poskytujeme jim informace o naplňování naší politiky a cílů v oblasti bezpečnosti informací.

Prohlášení

Vedení školy, se tímto zavazuje, v souladu s přijatou a schválenou strategií společnosti, jejíž nedílnou součástí je trvalá ochrana aktiv organizace a výše uvedenou politikou bezpečnosti informací, k plnění všech aplikovatelných požadavků a k neustálému zlepšovaní řízení bezpečnosti informací ve společnosti.

Ve Znojmě 1. 9. 2016 RNDr. Bc. Karel Pigl, ředitel školy

Potvrzení o převzetí a dohoda o odpovědnosti za ztrátu svěřených předmětů dle § 255 zákoníku práce

Uzavřená mezi
Střední zdravotnická škola a Vyšší odborná škola zdravotnická Znojmo, příspěvková organizace
se sídlem Jana Palacha 956/8, 669 33 Znojmo
IČ: 00638081
DIČ:CZ00638081
(dále jen „zaměstnavatel“)

a

Pan[í]

……
(dále jen „zaměstnanec“)

Zaměstnanec tímto potvrzuje, že oproti podpisu tohoto potvrzení a dohody převzal od zaměstnavatele následující předmět[y], které potřebuje k výkonu práce pro zaměstnavatele:

(dále jen souhrnně „svěřené předměty“)

Zaměstnavatel a zaměstnanec se tímto dohodli, že i) zaměstnanec od zaměstnavatele přebírá a zaměstnavatel zaměstnanci svěřuje výše uvedené svěřené předměty a ii) zaměstnanec odpovídá zaměstnavateli za ztrátu výše uvedených svěřených předmětů ve smyslu § 255 a násl. Zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (dále jen „Zákoník práce”). Zaměstnanec se zprostí své odpovědnosti za ztrátu svěřených předmětů zcela, popřípadě zčásti, jestliže prokáže, že ztráta vznikla zcela nebo zčásti bez jeho zavinění.

V případě ztráty svěřených předmětů se zaměstnanec zavazuje škodu vzniklou takovou ztrátu zaměstnavateli nahradit do 30 dnů ode dne, kdy ho k tomu zaměstnavatel vyzval, pokud nebylo dohodnuto jinak.

Dne:

…… ……..
Zaměstnavatel Zaměstnanec