Metodika pro zavedení základních bezpečnostních opatření pro střední školy dle VKB (Vyhlášky o kybernetické bezpečnosti)

Vypracoval: Ing. Petr Sedlák

Ústav informatiky

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Kolejní 2906/4
612 00 Brno

+420 602 738 320
e-mail: sedlak01@vutbr.cz
www.fbm.vutbr.cz

Spolufinancováno Evropskou unií

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

Obsah materiálu

1 Myšlenková mapa

Myšlenková mapa metodiky pro zavedení základních bezpečnostních opatření pro střední školy dle VKB je logickým schématem stěžejních témat potřebných k vytvoření relevantních postupů. Postupy mají vést k zavedení základních bezpečnostních opatření pro střední školy dle Vyhlášky o kybernetické bezpečnosti. Zadání s cílem zpracování interního dokumentu zaměřeného na implementaci opatření kybernetické bezpečnosti a bezpečnosti informací má vést ke zlepšení stavu ve střední škole.

1.1 Bezpečnostní strategie

V návaznosti na poslání (strategii s misí a vizí) ve středním školství lze implementovat bezpečnostní strategii (**BS**) pro střední školy s aktuálním výstupem.

1.2 Minimální bezpečnostní standard

Minimální bezpečnostní standard (**MBS**) je vhodným krokem k realizaci bezpečnostní strategie pro střední školy.

1.3 Budování bezpečnostního povědomí

Účinnou obranou proti zneužití informací a kybernetickým útokům je budování bezpečnostního povědomí u všech věkových kategorií uživatelů informačních a komunikačních technologií. Pozornost bude zaměřena na tři cílové skupiny – žáky, pedagogy a vedení střední školy.

1.3.1 Security Awarenes and Education (**SAE**)

Cíl budování bezpečnostního povědomí (Security Awareness Education, angl. zkratka SAE) tkví v představě, že organizace nemohou chránit důvěrnost, integritu a dostupnost informací v dnešním světě moderních informačních technologií zapojených do sítě, aniž by zajistily, že všichni lidé, podílející se na používání těchto technologií a jejich řízení:

- porozumí své roli a budou si vědomi své zodpovědnosti vůči organizaci a okolí;
- pochopí bezpečnostní zásady a postupy organizace v oblasti řízení a správy informačních technologií a informačních systémů;
- budou mít alespoň základní znalosti o řídicích, provozních a technických mechanismech používaných k zajištění ochrany informačních zdrojů, za které odpovídají a se kterými pracují.

V říjnu roku 2003 vydal Národní institut standardů a technologie speciální publikaci pod označením NIST Special Publication 800-50 věnující se tématu vybudování programu pro zvyšování bezpečnostního povědomí a školení o informačních technologiích (oficiální název „Building an Information Technology Security Awareness and Training Program“). Tato norma poskytuje návod na vybudování účinného bezpečnostního programu v oblasti informačních technologií.

1.3.2 Cyber Security Awareness (**CSA**)

Kybernetické nebezpečí dané masivní digitální transformací nabízí obrovské ekonomické a sociální příležitosti, ale zároveň mění povahu a rozsah kybernetických rizik a vytváří nová zranitelná místa, která se kybernetičtí útočníci snaží využít. V rámci povědomí o kybernetické bezpečnosti (Cyber Security Awareness, ang. zkratka CSA) jsou nastaveny pravidla pro celou řadu akcí, opatření a iniciativ zavedených s cílem zlepšit kybernetickou odolnost a reakce na ně.

1.3.3 Kybernetická hygiena

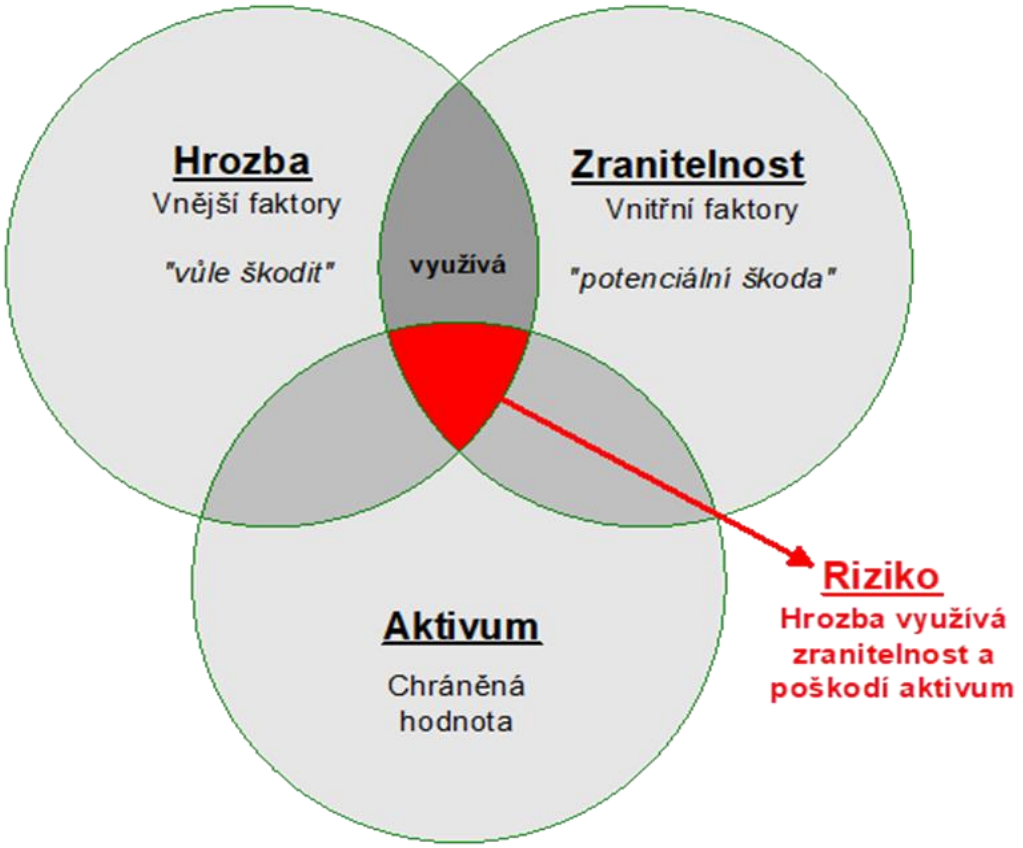
Je nedílnou součástí povědomí o kybernetické bezpečnosti. Tento koncept funguje podobně jako osobní hygiena, kdy si jedinec udržuje své zdraví přijímáním preventivních opatření, která by mu pomohla zajistit zdraví. Pokud jedinec zanedbává své zdraví, může se nachladit. Pokud organizace zanedbá kybernetickou hygienu, může to vést k napadení virem a úniku dat. Kybernetická hygiena (neboli hygiena kybernetické bezpečnosti) je postup, který udržuje základní stav a bezpečnost používaného hardwaru a softwaru. Kybernetická hygiena je společné preventivní opatření prováděné bezpečnostním pracovníkem organizace, správcem počítačového systému a uživateli, které pomáhá chránit před útoky. Tento základní postup pomáhá udržovat a chránit již správně fungující zařízení a zajišťuje jejich ochranu před hrozbami.

1.4 Zranitelnosti

Veškerá bezpečnost (informační a kybernetická) se snaží chránit aktiva. Základní vlastností je bezpečnostní problém, který se nazývá zranitelnost aktiva. Jedná se o jakékoliv slabé místo aktiva ve formě vnitřního faktoru, nebo potenciálu ke vzniku škody. Zdrojem zranitelností je informovanost o bezpečnostním stavu aktiva a jeho slabých místech ve formě databází a zveřejnění nejlepších praktických zkušeností (Best Practicies).

1.5 Hrozby

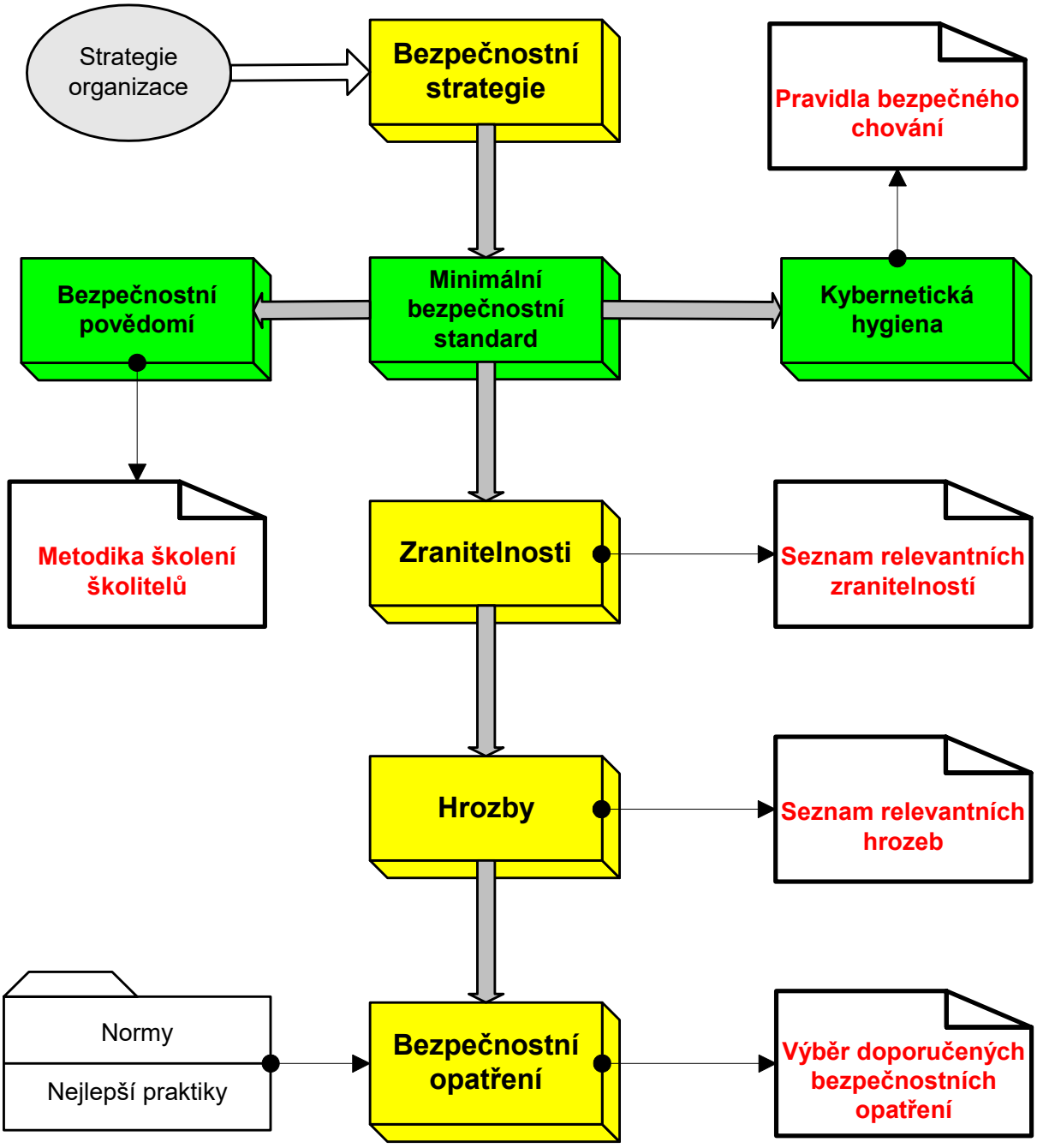
Vnějším faktorem vzniku škody je hrozba. Jedná se o akci nebo událost, která může ohrozit bezpečnost aktiva zneužitím zranitelnosti aktiva. Zdrojem hrozeb je databáze ve formě zpráv a prezentací a je založena na podrobné analýze nově se objevujících rizik a trendů z celého světa. Ty jsou klasifikovány a zveřejněny ve zpravodajstvích o kybernetických hrozbách.



Obrázek 1: Množinové vyjádření rizika a vzniku škody

1.6 Bezpečnostní opatření

Bezpečnostní opatření je jakákoliv aktivita, zařízení, technika či postup snižující sílu hrozby nebo zabránění jejímu účinku (dopadu). Seznam bezpečnostních opatření je k dispozici v normách, doporučeních a nejlepších praktických zkušenostech. Pro bezpečnostní opatření obecně platí, že jsou členěna oborově, takže mechanismus výběru bezpečnostních opatření je postaven na relevantních vztazích zranitelnost – hrozba – bezpečnostní opatření. Myšlenková mapa ilustruje jednotlivé kroky použité v metodice pro zavedení základních bezpečnostních opatření pro střední školy dle VKB.



Obrázek 2: Myšlenková mapa navrhované metodiky

Implementace

Pro zavádění minimálního bezpečnostního standardu je vhodné uvažovat o adekvátním SW nástroji pro implementaci a následné udržování a zlepšování bezpečnostní úrovně ve školském prostředí. Jako vhodný se jeví SW nástroj ESKO-KB, který splňuje základní požadavky na zavedení minimálního bezpečnostního standardu.

Kontext

Organizace se ocitají ve stále složitějším prostředí kybernetických hrozeb a musí čelit mnohostranným kybernetickým rizikům, a to jak interním, tak externím. Tato rizika ovlivňují kontinuitu podnikání, duševní vlastnictví a osobní a profesní integritu. Vzdělávací systém je ve spoustě zemí na prvních příčkách v počtu útoků.

Útočníci často vidí učitele a rodiče dětí, žáků a studentů jako snadný cíl, protože nebývají vhodně vybaveni, aby dokázali kybernetickým útokům, a často nedisponují ani znalostmi z této oblasti. Na černém webu jsou však citlivé údaje, shromažďované ve školském sektoru lukrativní. Na uvedených příkladech z různých zemí i České republiky lze pozorovat podobné charakteristiky. Navíc je oblast vzdělávání v oblasti bezpečnosti finančně, odborně i legislativně podhodnocena.

Používané pojmy

Bezpečnostní strategie	Bezpečnostní strategie kybernetické bezpečnosti organizace stanovuje vize a priority v zajišťování kybernetické a informační bezpečnosti.
Bezpečnostní povědomí	Bezpečnostní povědomí je souhrn procesů, které mají za cíl: Rozvíjet ve firmě kulturu bezpečného chování a zacházení s informacemi. Rozvíjet odbornost osob, které kybernetickou bezpečnost ve firmě navrhují a řídí Snižovat rizika lidského charakteru.
Kybernetická hygiena	Základní princip kybernetické hygieny je myšlen jako analogie osobní hygieny. Cílem je minimalizace kybernetických rizik.

2 Bezpečnostní strategie na období 2023 až 2028

Strategie kybernetické bezpečnosti střední školy stanovuje vize a priority v oblasti zajišťování kybernetické bezpečnosti. Střední škola, jakožto poskytovatel vzdělávání, čelí mnoha kybernetickým bezpečnostním hrozbám a rizikům a informační infrastruktura všech klíčových systémů musí být za všech okolností stabilní a bezpečná.

Strategie proto určuje, jak tohoto stavu dosáhnout, a jakým způsobem a nástroji se bude střední snažit snižovat rizika a zmírňovat hrozby plynoucí z kybernetického prostoru, aniž by jakkoliv omezovala výhody jeho využívání.

Strategie byla formulována s přihlédnutím k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025 a k Akčnímu plánu k Národní strategii kybernetické bezpečnosti pro období let 2021 až 2025, zpracovaným Národním úřadem pro informační a kybernetickou bezpečnost a schváleným Vládou České republiky.

Cílem tohoto strategického dokumentu je vymezení základní vize v oblasti kybernetické bezpečnosti a v návaznosti na tuto vizi stanovení strategických cílů a konkrétních programů a projektů vedoucích k realizaci této vize.

Strategie bude procházet každoroční evaluací, v jejímž rámci bude vyhodnocen pokrok v naplňování strategických cílů, případné změny v okolním prostředí a jejich dopad do vize a definovaných strategických cílů, včetně zpracování akčního plánu na následující období.

2.1 Principy

Strategie kybernetické bezpečnosti Organizace stanovuje základní principy a hodnoty, jejichž dodržováním chce Organizace dosáhnout požadovaného zajišťování kybernetické bezpečnosti.

2.1.1 Ochrana základních lidských práv a svobod

Organizace dodržuje při zajišťování kybernetické bezpečnosti základní lidská práva, demokratické principy a hodnoty demokratického právního státu. Respektuje charakter otevřeného a neutrálního prostředí internetu, dbá na dodržování svobody projevu, ochrany osobních dat a soukromí. Při zajišťování kybernetické bezpečnosti proto usiluje o maximální otevřenost přístupu k informacím a minimalizaci zásahů do práv občanů a soukromých subjektů. Jedním ze základních principů činnosti v oblasti kybernetické bezpečnosti je ochrana základních informačních práv.

2.1.2 Komplexní přístup ke kybernetické bezpečnosti

Komplexní přístup ke kybernetické bezpečnosti je založený na principu subsidiarity a spolupráce. Cílem strategie je zajištění podmínek pro spolehlivě fungující informační systém Organizace schopný čelit kybernetickým hrozbám. Strategie je postavena na principu nedělitelnosti bezpečnosti, kde kybernetickou bezpečnost Organizace nelze oddělovat od kybernetické bezpečnosti resortní, regionální a národní. Organizace bude cíleně koordinovat aktivity v této oblasti v rámci resortu i na regionální a národní úrovni.

Hlavním gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast je NÚKIB, který koordinuje úsilí v této oblasti a poskytuje metodické vedení ostatním zainteresovaným subjektům. NÚKIB je zodpovědný za rozhodnutí o předkládaných návrzích a návodech na přijetí

opatření při předcházení i řešení kybernetických bezpečnostních incidentů a probíhajících kybernetických útoků.

2.1.3 Budování důvěry

Budování důvěry a spolupráce mezi všemi aktéry poskytování zdravotních služeb je klíčovou součástí zajišťování kybernetické bezpečnosti. Bezpečnostní politika v této oblasti je proto založena na inkluzivní spolupráci všech zainteresovaných partnerů. Zásadní je zde důvěryhodné prostředí, ve kterém je možno účinně spolupracovat. Důvěra mezi managementem a pracovníky organizace, jejími partnery i zákazníky (pacienty), stejně jako důvěra k národním autoritám v oblasti zdravotnictví a kybernetické bezpečnosti je nezbytná k efektivnímu zajišťování kybernetické bezpečnosti.

Vzhledem k tomu, že se stále více stírají rozdíly mezi vnitřními a vnějšími hrozbami a riziky, respektive vnitřní a vnější bezpečností, bude Organizace rozvíjet koordinaci úsilí a posilovat důvěru mezi zainteresovanými subjekty na lokální i národní úrovni.

2.1.4 Rozvoj kapacit k zajišťování kybernetické bezpečnosti

Vzhledem ke značné závislosti společnosti na informačních a komunikačních technologiích a neustálým změnám povahy současných kybernetických hrozeb a rizik závisí kybernetická bezpečnost Organizace nejen na neustálém budování robustnější, odolnější informační infrastruktury, ale i na Organizaci jako celku. Proto Organizace podporuje rozvoj problematiky kybernetické bezpečnosti ve všech rovinách – od vzdělávání a osvěty koncových uživatelů, přes péči o profesní růst odborných zaměstnanců Organizace, až po účinné nástroje a opatření pro naplnění požadavků kybernetické bezpečnosti.

2.2 Vize

Vize strategie kybernetické bezpečnosti je postavena za několika základních bodech:

2.2.1 Nastavení pravidel pro MBS

Minimální bezpečnostní standard (MBS) je vhodným krokem k realizaci bezpečnostní strategie pro střední školy.

Střední škola zabezpečí podmínky a zdroje pro zavedení Minimálního bezpečnostního standardu do školního prostředí.

2.2.2 Ochrana základních lidských práv a svobod

Střední škola zajistí podmínky pro bezproblémové fungování a rozvoj informačních služeb, zejména prostřednictvím zajištění hladkého fungování komponent informačního systému.

2.2.3 Osvěta a výuka kybernetické bezpečnosti

Střední škola bude podporovat rozvoj kultury informační společnosti pomocí osvěty svých pracovníků a výuky svých žáků.

2.2.4 Šíření bezpečnostního povědomí

Střední škola svou výchovou a výukou žáků o kybernetické bezpečnosti bude budovat prostředí znalé v oboru informační a kybernetické bezpečnosti. Forma výchovy bude postavena na principu SAE, forma výuky bude postavena na principu SAE a CSA včetně kybernetické hygieny.

2.2.5 Rozšiřování expertní základny

Střední škola zaměří své úsilí na nepřetržité rozšiřování expertní základny v oblasti kybernetické bezpečnosti a schopností čelit nejnovějším kybernetickým hrozbám.

2.2.6 Spolupráce s bezpečnostními komunitami

Znalostní databáze, měkké dovednosti a systémová integrace kybernetické bezpečnosti do všech oborů lidské činnosti vyžadují sdílení informací s externími spolupracujícími subjekty na partnerské úrovni.

2.2.7 Spolupráce s navazujícími vzdělávacími institucemi

Profil žáka střední školy v návaznosti na další vzdělávání v oboru kybernetické bezpečnosti vyžaduje minimálně tři stupně znalostí se čtvrtým stupněm tzv. přidanou hodnotou:

- Základní technické znalosti,
- Základní znalosti v oblasti software, zejména aplikací,
- Základní znalosti v oblasti komunikace,
- Základní znalosti kybernetické bezpečnosti.

2.3 Výzvy

Základní výzvou je snižování kybernetických rizik v rámci školní výuky na všech úrovních. K tomu je třeba přímé podpory a výuky problematiky:

2.3.1 Vybudování odolné infrastruktury

Se zvýšeným počtem žáků střední školy roste závislost školních procesů na informačních a komunikačních technologiích. Narůstá však kritičnost jejich selhání z pohledu dostupnosti a ochrany dat.

2.3.2 Dynamický rozvoj technologií

Kybernetické nebezpečí dané masivní digitální transformací a dynamickým technologickým rozvojem nabízí obrovské ekonomické a sociální příležitosti, ale zároveň mění povahu a rozsah kybernetických rizik a vytváří nová zranitelná místa, která se kybernetičtí útočníci snaží využít.

2.3.2.1 internet věcí (IoT – internet of Things)

Počet zařízení připojených k internetu neustále narůstá, velké části uživatelů chybí povědomí o nezbytné kybernetické hygieně, tedy jak se v online prostředí pohybovat a jak zabezpečit používaná zařízení.

2.3.2.2 Velká dat (Big Data)

Spojená problematika s prostředím internetu věcí, což je nedostatek úložišť v celosvětovém měřítku dává podněty k různým řešením. Začaly se proto využívat nové formy ukládání dat, např. cloudová úložiště, on-line zálohy a využívání technologie block chain. Zvýšené používání těchto online služeb a cloudů však vede mnohdy k netransparentnímu řešení zabezpečení, jehož důvěryhodnost je minimálně sporná. Další vlnou dat je možno označit produkty a činnosti fenoménu umělé inteligence.

2.3.2.3 Umělá inteligence (AI – Artificial Inteligence)

Umělá inteligence je na vzestupu. Bude měnit náš život zlepšováním zdravotní péče (umožní např. stanovení přesnější diagnózy či lepší prevenci nemocí), zvyšováním účinnosti zemědělství, přispíváním ke zmírňování změny klimatu a přizpůsobování se této změně, zlepšováním účinnosti výrobních systémů prostřednictvím prediktivní údržby, zvyšováním bezpečnosti Evropanů a mnoha jinými způsoby, které si zatím umíme představit pouze v náznacích. Umělá inteligence zároveň zahrnuje řadu potenciálních rizik, jako je netransparentní rozhodování, diskriminace na základě pohlaví nebo jiné druhy diskriminace, narušování našeho soukromí nebo může být zneužita k páchání trestné činnosti.

2.3.3 Kybernetická bezpečnost

Všichni cítíme potřebu internetu ve všech oblastech života. V oblasti vzdělávání je internet nesmírně důležitý a také jeho využívání neustále roste.

Potřeba výuky kybernetické bezpečnosti pro žáky je obrovská. Pouze z pohledu na technickou stránku věci, kybernetická bezpečnost je potřebná, protože nabízí obranný mechanismus pro všechny druhy zařízení připojených k internetu před kybernetickými útoky. Před těmito kybernetickými útoky není v bezpečí ani sektor vzdělávání. Výzkumem bylo zjištěno, že kybernetická bezpečnost je obor, kde jsou vysoké šance na růst a kde je také velmi vysoký rozdíl mezi nabídkou a poptávkou.

2.3.4 Rizika spojená s lidským faktorem

Vzhledem k otevřenému, anonymnímu charakteru internetu narůstají i možnosti obchodování s citlivými informacemi, snadná dostupnost, či dokonce volné nakupování kriminálních služeb. V souvislosti s pokračujícím pronikáním informačních technologií do běžného života a fungování společnosti dochází také k rychlému přesunu řady kriminálních aktivit do virtuálního prostředí, které pachatelům slibuje rychlý účinek při výrazně sníženém riziku postihu. K tomu přispívá zejména anonymita a prostorová neuchopitelnost internetu. To vše umožňuje jak vysoce cílené, tak masové a plošné útoky.

2.3.5. Nedostatek odborníků

Objektivní skutečností na pracovním i dodavatelském trhu je nedostatek odborníků na kybernetickou bezpečnost. S tím souvisí výzvy v oblasti zajištění odpovídajících odborných kapacit a nutnost revize vzdělávacích programů v oblasti kybernetické bezpečnosti pro vlastní pracovníky i žáky střední školy tak, aby odpovídaly v současné podobě aktuálním požadavkům a trendům.

2.4 Implementace bezpečnostní strategie

Na základě hlavních cílů Bezpečnostní strategie bude vypracován podrobný Akční plán, který definuje konkrétní kroky, stanoví u nich zodpovědnost, termíny jejich plnění a kontrolu. Tento akční plán bude po projednání předložen ke schválení poradě vedení.

2.5 Závěrečná ustanovení

Tato strategie nabývá účinnosti dnem 30.6.2024.

3 Minimální bezpečnostní standard – MBS

Je určen pro subjekty nespadající pod zákon o kybernetické bezpečnosti. Je vhodný především tam, kde s nastavováním zabezpečení teprve začínají, protože ke kybernetické bezpečnosti přistupuje návodným doporučením. Minimální bezpečnostní standard (MBS) lze pojmout ve dvou částech.

První část bude zaměřena manažersky, oblasti popisované v této části jsou zaměřeny procesně, zpravidla zahrnují popisy postupů, které je potřeba v rámci organizace zavést a dodržovat.

Druhá část bude zaměřena technicky a je určena spíše pro IT a bezpečnostní specialisty, obsahuje konkrétní návody, jak zajistit minimální úroveň zabezpečení.

3.1 Manažerská část

Struktura manažerské části je postavena na stěžejních bodech postavených na systematickém přístupu vedoucího o ke zvyšování kybernetické bezpečnosti, včetně požadavků na vrcholové vedení v oblasti organizační bezpečnosti a určení odpovědností v oblasti kybernetické bezpečnosti.

Základním předpokladem systematického přístupu ke kybernetické bezpečnosti je podpora ze strany vrcholového vedení při jejím prosazování. Je potřeba vyčlenit potřebné zdroje, stanovit bezpečnostní role, vytvořit přiměřené bezpečnostní politiky a dokumentaci, včetně jejich schválení a následně kontrolovat jejich dodržování.

Vrcholové vedení musí projevit dostatečnou podporu a přidělit přiměřené zdroje (finanční, lidské, technické) potřebné k zavedení a udržování principů vedoucích ke zvyšování kybernetické bezpečnosti a určit osobu odpovědnou za kybernetickou bezpečnost, včetně stanovení jejích povinností, odpovědností a pravomocí.

Tato role je odpovědná za řízení a rozvoj kybernetické bezpečnosti, průběžnou kontrolu stavu kybernetické bezpečnosti, dohlížení na naplňování plánu zavádění bezpečnostních opatření a komunikaci v oblasti kybernetické bezpečnosti s vrcholovým vedením.

Je vhodné zajistit dostatečnou zastupitelnost bezpečnostních rolí, ale není nutné vytvářet speciální pozice pro osoby zastupující bezpečnostní role. Je důležité, aby příslušné činnosti byly řádně vykonávány i v případě, že odpovědná osoba nebude v daný okamžik k dispozici, anebo bude mít v náplni práce i další činnosti.

Administrátoři a osoby zastávající bezpečnostní role by měli mít uzavřenou dohodu o zachování mlčenlivosti buď přímo ve formě smlouvy (NDA) nebo doložky k pracovní smlouvě.

Dále je potřeba vytvořit přiměřené bezpečnostní politiky a bezpečnostní dokumentaci. Tyto politiky a dokumenty musí být dostatečně návodné, aby bylo zajištěno, že výsledky budou reprodukovatelné, a tedy aby jiná osoba byla po jejich nastudování schopna postupovat shodným způsobem.

Při výběru vhodných politik a dokumentace je vždy nutné zohlednit jejich relevanci pro konkrétní prostřední organizace.

Bezpečnostní politiky a dokumentace musí být schváleny na stejné úrovni jako jiné interní akty organizace (tedy nejčastěji vrcholovým vedením), a to mimo jiné i z toho důvodu, aby byla zajištěna jejich vymahatelnost.

Politiky a dokumentace by měly být v přiměřených intervalech aktualizovány tak, aby vždy reflektovaly aktuální stav.

Všechny činnosti spojené se zajišťováním kybernetické bezpečnosti by měly být v souladu se zákony a interními předpisy organizace.

Mezi bezpečnostní dokumentaci patří mimo jiné i plán zavádění bezpečnostních opatření, který je stěžejním dokumentem sloužícím k plánování zavádění bezpečnostních opatření, a tedy i k zajištění kontinuálního zlepšování.

3.1.1 Struktura manažerské části

Plán zavádění bezpečnostních opatření
Klasifikace a ochrana informací (viz GDPR)
Řízení dodavatelů
Řízení lidských zdrojů
Řízení změn
Řízení kontinuity činnosti
Audit kybernetické bezpečnosti

3.1.2 Doporučené bezpečnostní politiky

1. Politika organizační bezpečnosti

    a. Určení bezpečnostních rolí a jejich práv a povinností.

2. Politika řízení informací

    a. Identifikace, hodnocení a evidence informací.
    b. Pravidla ochrany jednotlivých úrovní informací.
    c. Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií.
    d. Pravidla a postupy pro ochranu předávaných informací.
    e. Způsoby ochrany elektronické výměny informací.
    f. Pravidla pro využívání kryptografické ochrany.

3. Politika řízení dodavatelů

    a. Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.
    b. Pravidla pro provádění kontroly zavedení bezpečnostních opatření u dodavatele.

4. Politika bezpečnosti lidských zdrojů

    a. Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení.
    b. Bezpečnostní školení nových zaměstnanců.
    c. Pravidla pro řešení případů porušení bezpečnostní politiky.
    d. Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice.

5. Politika řízení změn

    a. Způsob a principy řízení změn v procesech a informačních nebo komunikačních systémech.

6. Politika řízení kontinuity činností

    a. Práva a povinnosti zúčastněných osob.
    b. Cíle řízení kontinuity činností.
    c. Určení a obsah potřebných plánů kontinuity činností a havarijních plánů.

7. Politika řízení dokumentace

8. Politika fyzické bezpečnosti

    a. Pravidla pro ochranu objektů.
    b. Pravidla pro kontrolu vstupu osob.
    c. Pravidla pro ochranu zařízení.
    d. Detekce narušení fyzické bezpečnosti.

9. Politika řízení provozu a komunikací

    a. Postupy bezpečného provozu.
    b. Požadavky a standardy bezpečného provozu.

10. Politika řízení přístupu

    a. Princip minimálních oprávnění/need-to-know.
    b. Požadavky na řízení přístupu.
    c. Životní cyklus řízení přístupu.
    d. Řízení privilegovaných oprávnění.
    e. Řízení přístupu pro mimořádné situace.
    f. Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.

11. Politika bezpečného chování uživatelů

    a. Pravidla pro bezpečné nakládání s informacemi.
    b. Bezpečné použití přístupového hesla.
    c. Bezpečné použití elektronické pošty a přístupu na internet.
    d. Bezpečný vzdálený přístup.
    e. Bezpečné chování na sociálních sítích.
    f. Bezpečnost ve vztahu k mobilním zařízením.

12. Politika zálohování a obnovy a dlouhodobého ukládání

    a. Pravidla a postupy pro zálohování a obnovu.

13. Politika řízení technických zranitelností

14. Politika bezpečného používání mobilních zařízení

15. Politika akvizice, vývoje a údržby

    a. Bezpečnostní požadavky pro akvizici, vývoj a údržbu.
    b. Řízení zranitelností.
    c. Politika poskytování a nabývání licencí programového vybavení a informací.

16. Politika zvládání kybernetických bezpečnostních incidentů

a. Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů
b. Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti.
c. Evidence incidentů.

3.1.3 Doporučená dokumentace

1. Plán zavádění bezpečnostních opatření

a. Popis bezpečnostních opatření, osoby odpovědné za zavedení jednotlivých bezpečnostních opatření, potřebné zdroje a termíny.

2. Síťová topologie

3. Přehled používaných zařízení

4. Zprávy z auditu

3.1.4 Doporučená administrátorská dokumentace

1. Informace o informačním nebo komunikačním systému jako celku (schéma začlenění informačního nebo komunikačního systému a komunikační mapa na úrovni L2-L3 topologie).

2. Základní popis provozní technologie vztahující se k danému informačnímu nebo komunikačnímu systému.

3. Zásady a doporučení k organizaci práce s informačním nebo komunikačním systémem.

4. Popis instalace, konfigurace a ovládání informačního nebo komunikačního systému.

5. Popis dohledu nad funkčností informačního nebo komunikačního systému a administrace informačního nebo komunikačního systému.

6. Popis řešení nestandardních stavů.

3.2 Technická část

Struktura technické části je postavena na zlepšení odolnosti a dostupnosti používaných systémů pomocí zavádění relevantních a přiměřených bezpečnostních opatření.

3.2.1 Struktura technické části

Fyzická bezpečnost
Řízení přístupů
Síťová bezpečnost
Aplikační bezpečnost

Ochrana před škodlivým kódem
Kybernetické bezpečnostní události a incidenty
Zajištění úrovně dostupnosti informací
Cloudové služby

3.2.2 Fyzická bezpečnost

Je postavena na stanovení základních požadavků a principů pro zajištění bezpečnosti informací z pohledu fyzické bezpečnosti. Definuje nový či rozšiřuje stávající soubor opatření předcházející poškození, krádeži či zneužití informací či majetku nebo přerušení poskytování služeb informačního nebo komunikačního systému, vymezuje fyzický perimetr.

3.2.3 Řízení přístupů

Je postaveno na základě rolí a evidence přidělování nebo odebírání přístupových oprávnění. Specifikace parametrů pro hesla a využívání vícefaktorové autentizace. V rámci politiky řízení přístupu se musí definovat pravidla a postupy potřebné pro omezení a kontrolu používaného softwaru a hardwaru, který by mohl narušit systémovou a aplikační bezpečnost. Jedná se např. o kontrolu připojovaných USB, antivir apod.

3.2.4 Síťová bezpečnost

Je postavena na stanovení základních požadavků a principů pro oblast síťové bezpečnosti a jejího neustálého monitorování. Síťová bezpečnost je činnost, jejímž účelem je zachovávat dostupnost a integritu sítě pomocí hardwarové i softwarové technologie. Efektivní zabezpečení sítě řídí i přístup do ní. Cílí na široké spektrum hrozeb a blokuje jejich průnik nebo šíření v síti.

3.2.5 Aplikační bezpečnost

Je postavena na stanovení základních požadavků a principů pro oblast aplikační bezpečnosti a jejího testování. Tyto opatření mimo jiné říkají, kdy provádět penetrační testování důležitých prvků informační a komunikační infrastruktury, jak zabezpečit aplikace atd.

3.2.6 Ochrana před škodlivým kódem

Je postavena na snížení pravděpodobnosti napadení škodlivým kódem, případně snížení dopadů při napadení škodlivým kódem.

V rámci informačního nebo komunikačního systému musí být navržen a implementován způsob řešení ochrany před škodlivým kódem. Správce informačního nebo komunikačního systému (společně s případným dodavatelem/provozovatelem) musí zhodnotit všechny směry, vstupy/výstupy dat a jejich uložení či další zpracování v informačním nebo komunikačním systému a navrhnout způsob ochrany před škodlivým kódem.

3.2.7 Kybernetické bezpečnostní události a incidenty

Jsou postaveny na stanovení postupů při vzniku nestandardní situace, včetně stanovení eskalačního procesu uvnitř organizace a auditních požadavků (logování). Za incident je považováno nejen narušení integrity či důvěrnosti ale i nedostupnost informace či služby. V organizaci by měl být stanoven proces, dle kterého se bude řídit hlášení nestandardního chování informačního nebo komunikačního systému. Zaměstnanci by měli být seznámeni s tím, co mají hlásit (např. neobvyklé či podezřelé chování informačního nebo komunikačního systému, nevyžádané e-maily, problémy s dostupností informací či služeb atd.) a mít k dispozici konkrétní kontakty, na koho se v rámci organizace obracet. Současně by také měl fungovat eskalační proces, v rámci, kterého budou přesně definovány v rámci organizace osoby, které budou o situaci informovány, a případně na ně bude přenesena odpovědnost za její řešení.

3.2.8 Zajištění úrovně dostupnosti informací

Je postaveno na zajištění dostupnosti informačního nebo komunikačního systému a dat. Při stanovení dostupnosti je nutné brát zřetel na efektivnost celého řešení, neboť nadhodnocené požadavky na dostupnost mají významný dopad na architekturu řešení a v konečném důsledku pak dopad na finanční stránku. Na základě definice požadavků na dostupnost se stanoví architektura celého informačního nebo komunikačního systému.

3.2.9 Cloudové služby

Je postaveno na zajištění kybernetické bezpečnosti při využívání cloudových služeb. V případě, že je využíváno cloudových služeb pro provoz informačního nebo komunikačního systému, zajistit kybernetickou bezpečnost i z pohledu těchto služeb, a to bez ohledu na to, jaký typ cloudové služby je používán (IaaS, PaaS, SaaS). Na poskytovatele cloudových služeb je potřeba vztáhnout stejná pravidla jako pro ostatní dodavatele.

Používané pojmy

Dostupnost	Vlastnost přístupnosti a použitelnosti v požadovaném čase na žádost autorizované entity.
Důvěrnost	Vlastnost, že informace není dostupná nebo není odhalena neautorizovaným jednotlivcům, entitám nebo procesům.
Integrita	Vlastnost ochrany přesnosti a úplnosti aktiv.
Kybernetická bezpečnostní událost	Událost, která může způsobit narušení bezpečnosti informací v informačních nebo komunikačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
Kybernetický bezpečnostní incident	Narušení bezpečnosti informací v informačních nebo komunikačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.
Plán kontinuity činností	Dokumentovaný soubor postupů a informací, který je vytvořen sestaven a udržován v pohotovosti pro užití při

incidentu za účelem umožnění organizaci uskutečňovat své kritické činnosti na přijatelné, předem stanovené úrovni.

4 Metodika SAE (Security Awareness and Education)

Kapitola dokumentu „SAE“ má za cíl vybudovat program na zvyšování bezpečnostního povědomí na střední škole. Do práce byly zahrnuty i požadavky stanovené školou.

4.1 Fáze programu

V této kapitole jsou popsány jednotlivé fáze programu, které vychází z SAE, a jejich cíle.

4.1.1 Povědomí

Jak vyplývá z tabulky, fáze budování povědomí je společná pro všechny uživatele – od vedení školy, až po zákonné zástupce. Jedná se o nejrozsáhlejší část. Cílem této fáze je vzbudit zájem účastníků, kteří na základě získaných informací jsou schopni detekovat hrozbu či riziko z oblasti informační bezpečnosti, reagovat na něj odpovídajícím způsobem, případně umět s informacemi dále zacházet.

Pro tuto fázi je vhodné využít co nejvíce atraktivní metody. Vzbudíme-li zájem u pedagogů školy, je velice pravděpodobné, že budou dále schopni toto nadšení předávat svým studentům a ti se problematice budou více věnovat. K neosobním materiálům můžeme počítat různé letáčky, reklamy, emaily, informace na stránkách školy. Pro potenciální lepší výsledek je však dobré mít také osobní kontakt, tedy rozhovory. Na základě poznatků od zaměstnanců je možné lépe specifikovat dílčí cíle, které se ve fázi školení mohou využít. Stejně tak je vhodné zavést osobní kontakt se žáky školy, školním psychologem a zákonnými zástupci, což je možné primárně během třídních schůzek. Žáci vyšších stupňů se mohou zapojit v rámci různých projektů. Tímto způsobem dochází k nenásilnému předání informací, které pomáhá budovat povědomí o dané problematice.

4.1.2 Školení

Školení se účastní všichni zaměstnanci školy. Je nutné zahrnout i zaměstnance školní jídelny, neboť pracují s osobními daty žáků. Cílem je předat (dle potřeb) bezpečnostní znalosti a dovednosti. V této fázi programu již rozdělujeme uživatele na začátečníky, mírně pokročilé a pokročilé. Ke každé skupině je přistupováno individuálně a na základě jejich potřeb jsou sestavené speciální metodiky. Pro testování znalostí a rozřazení do úrovně je vhodné vybrat projekt **ECDL**. Tento projekt je zavedený i návrhu řešení budování bezpečnostního povědomí na gymnáziu, přičemž pro tento projekt vycházíme z požadavku, aby jednotlivé fáze na sebe navazovaly a žáci tak dostali během studia na základní, následně střední, škole komplexní informace pro bezpečnou práci s daty. Rozdílné jsou ovšem doporučené moduly, které jsou přizpůsobené výuce na škole.

Učitelé a administrativní zaměstnanci mají dle rozhodnutí ředitelky školy požadavek na splnění minimálně úrovně mírně pokročilí, učitelé specializovaní na výuku ICT potom výrazné doporučení na splnění úrovně pokročilí.

Stupeň pokročilosti a název kurzu	Témata	Výstupy
Začátečníci e-Citizen	- Řešení běžných situací a každodenních problémů - Bezpečné využívání online služeb - Komunikace na internetu - Vyhledávání informací a relevantnost dat	Po ukončení kurzu uživatel umí řešit běžně dennodenní situace, zvládá komunikovat skrze email a jiné komunikační portály, umí vyhledat data na internetu a zhodnotit důvěryhodnost vyhledaných dat.
Mírně pokročilí ECDL Start	Složení čtyř zkoušek z následujících modulů: - Internet a komunikace - Bezpečné používání IT - Počítač a soubory - Informace na internetu - Zpracování textu - Práce s tabulkami - Spolupráce na internetu Pozn.: doporučený je výběr prvních čtyř možností	Po ukončení kurzu uživatel umí zacházet s daty z webových stránek s ohledem na bezpečnost, rozumí pojmu záloha dat a je schopen činnost provádět, umí zabezpečit počítač před útoky škodlivého softwaru, dokáže třídit a vyhodnocovat informace z internetu pomocí podpůrných SW nástrojů.
Pokročilí ECDL Profile	Složení nejméně jedné zkoušky z nabízených modulů ECDL Core, ECDL Advanced, Digitální fotografie, e-Citizen a řady dalších.	Po ukončení kurzu uživatel umí tvořit webové stránky dle aktuálních požadavků trhu/upravit fotografie podle platných legislativních zákonů a norem/pracovat s tabulkami pro
	Doporučené moduly: - Webové stránky - Úpravy obrázků - Práce s tabulkami - Prezentace	následné využití analyzovaných dat/vytvářet prezentace na podporu výuky a možných projektových řešení.

Tabulka 4. 1.: Příklad programu ECDL

4.1.3 Vzdělávání

Vzdělávání v oblasti inovací ICT je jeden ze základních požadavků vedení školy. Cílem této fáze je získat odborné znalosti z oblasti informační a kybernetické bezpečnosti, znalosti o hrozbách a technologických změnách. Na jejich základě je uživatel schopen včasné detekce a proaktivní reakce. Z důvodu menšího počtu účastníků je vhodné vybrat externího školitele, neboť vytváření vlastních materiálů či objednání hromadného školení by bylo neefektivní a neekonomické. Kurzů nabízených dodavateli je celá řada a je jen na vedení školy, případně vedení či správci sítě, kterou dodavatelskou firmu zvolí. Kurzy je vhodné navštívit jedenkrát ročně a doplnit si znalosti v případě změn legislativy či vzniku nových hrozeb.

4.1.4 Profesní rozvoj

Profesní rozvoj je nad rámec požadovaných znalostí většiny účastníků programu. Je však nutné zmínit, že správce sítě a vedení školy jsou v pozici, kdy by bylo vhodné znát aktuální legislativní podmínky a hrozby, kterým musí čelit. Vedení je zároveň odpovědné za chod střední školy.

4.2 Rozsah programu

Podle požadavků střední školy je třeba naplnit požadavky programu SAE zejména v těchto oblastech:

- Základy a zásady informační bezpečnosti (včetně možných rizik a odpovědností).
- Ochrana osobních údajů, včetně klasifikace dat.
- Bezpečné využívání internetu (podvodné zprávy, nevhodné stránky).
- Zásady bezpečné komunikace (email, messenger).
- Bezpečné využívání informačních a komunikačních technologií.
- Zásady správného zálohování dat.
- Správa hesel.
- Antivirové programy a jejich využití.
- Pravidla pro využívání ICT ve výuce.
- Bezpečné používání sociálních sítí.

Všechny požadavky musí odpovídat aktuální legislativě.

4.3 Role a odpovědnosti programu SAE

Pověřená osoba – CISO provádí školení zaměstnanců, kteří následně školí žáky školy.

V následující tabulce jsou přehledně zpracovány jednotlivé role a odpovědnosti v programu.

	Řízení	Vývoj	Realizace	Vyhodnocení
CISO	x	x	x	x
Ředitel	x		x	x
Učitelé			x	x
Žáci				x
Ostatní uživatelé				

Tabulka 4.2: Role a odpovědnosti v programu SAE

4.3.1 CISO

CISO má na starosti vytvoření programu, což zahrnuje vytvoření strategie zavedení, přípravu a provedení školení. Jeho úkolem je dostatečně informovat účastníky o přínosech školení a zároveň zdůraznit důležitost školení o kybernetické bezpečnosti. Následně dohlíží na správný průběh implementace a zajišťuje zpětnou vazbu programu. Na střední škole může být CISO pověřená osoba, externista, jehož úkolem je mimo jiné podrobná analýza školy, neboť je nutný mít celkový přehled o zázemí, kde daný program bude zavádět.

4.3.2 Ředitel/ka

Jako hlava školy je ředitel/ka nedůležitějším článkem mezi školitelem a zaměstnanci. Jeho hlavním úkolem je zajištění zdrojů (finančních, lidských), které jsou potřebné pro správný průběh vytvoření a zavedení programu. V jeho moci je také výběr kompetentní osoby, která bude zodpovídat za kontrolu a dohled. Ředitel je také v pozici kontrolora, kdy je nutné zkontrolovat, zdali se požadavky školy shodují s metodikou školení, a je tedy možné program uvést do praxe.

4.3.3 Učitelé

Stěžejní a nejvíce sledovanou skupinou uživatelů je učitelský sbor. Učitele ve škole můžeme rozdělit na dva typy. Třídní a ty, co vlastní třídu v současné době nemají. Nicméně to neznamená, že v budoucnu ji mít nebudou, z čehož vyplývá, že náplň školení je pro všechny stejná. Z důvodu implementační povinnosti školení pro žáky je nutné, aby každý pedagog uměl vzbudit v žácích zájem, dokázal jim vysvětlit důležitost školení a pravidla, kterými je třeba se řídit.

Profil učitele střední školy vychází z toho, že běžný učitel má vyšší znalosti práce s PC než většina populace. Každý učitel musí připravovat věci do výuky a ty se dnes již bez výjimky dodávají v digitální, někdy tištěné podobě, včetně ověření na internetu. Musí tedy ovládat Office a v řadě předmětů ještě specializované aplikace. K tomu řada škol využívá elektronický vzdělávací systém.
Pochopitelně používá stravovací objednávkový systém, intranet školy a e-mailovou komunikaci. Samozřejmostí je k tomu elektronická klasifikace, je-li třídním učitelem, pak i docházka, a na většině středních škol kompletní elektronická třídní kniha.

BĚŽNÝ UČITEL
Nepotřebuje znát technické podrobnosti nastavení sítě, ani svého počítače. Od toho má správce sítě. Pokud tedy neučí předměty, spojené s IT, vystačí se základními zásadami péče o software, zálohováním a archivací a zásadami tvorby hesel.

UČITEL, KTERÝ SE ZABÝVÁ KOMUNIKAČNÍ STRÁNKOU VĚCI A MÁ PŘESAH DO IT OBLASTI
Učí tedy všeobecný společenský základ nebo právní nauky, popřípadě jazyky. Musí znát přesah do trestního zákoníku, tedy autorský zákon, postihy za neoprávněné využití výpočetní techniky, zejména dat a další podrobnosti. Současně by měl znát i nástroje sociálního inženýrství a techniky fake news, kterým se nelze vyhnout. Těžiště jeho práce a znalostí tedy bude v oblasti cybercrime, nikoliv v technických podrobnostech. Nesmí se pokoušet jevy, které do oblasti cybercrime patří, řešit. To spadá do kompetence metodika prevence nebo výchovného poradce. Je nutné jevy pouze vysvětlit, zasadit do společenského kontextu a popřípadě zdokumentovat a ohlásit jejich výskyt.
Tady už nevystačíme s kurzem pro běžné učitele. Je dobré znát alespoň základy techniky.

UČITEL OBECNÉHO PŘEDMĚTU IT
Musí znát i technické podrobnosti, a to do takové hloubky, aby dokázal předvídat reakce žáků na různé restrikce a hrozby. Měl by umět vysvětlit jednotlivé typy útoků, a to včetně následků a popsat přesně typy závadového chování. Aby učitel šel s dobou a měl přehled, je vhodné sledovat jednak Informační servis NÚKIB, jednak další servery.

Je nutné mít stále na paměti, že **učitel IT není správce sítě a ani ICT koordinátor**. Na tyto činnosti musí mít uzavřeny další smlouvy a neměl by své povinnosti přenášet do výuky a už vůbec ne na žáky. Obvyklá praxe, že žáci pomáhají s nastavením stanic, je cestou k vytvoření velkých problémů.

4.3.4 Žáci

Vycházíme z toho, že žáci umí vše, co měli umět ze základní školy. Současně je obecný materiál určen pouze pro výuku všeobecného základu. Předměty, zaměřené na komunikační techniku v rámci odbornosti je nutné uzpůsobit konkrétnímu zaměření a specializaci oboru.

Dále je třeba vzít v potaz dokument NÚKIBu s názvem „Profil žáka střední školy“ pro žáky s různou hodinovou dotací na středních školách.

4.3.5 Ostatní uživatelé

Do této kategorie spadají další zaměstnanci školy. Jedná se o nejrozsáhlejší a nejrizikovější skupinu. Je nutné dbát speciální pozornost na to, aby uživatelé správě chápali své povinnosti, možná rizika a odpovědnost za vzniklé chyby.

4.4 Rozdělení uživatelů

Jedním z prvních kroků je jednoznačně rozdělení uživatelů. To je nutné provést ve dvou fázích. V první fázi dochází k rozdělení podle pracovního nasazení, ve druhé potom do příslušného stupně pokročilosti (platí pouze pro fáze školení a vzdělávání). Na základě ověřených znalostí mohou být uživatelé přiřazeni do skupiny začátečníci, mírně pokročilí nebo pokročilí. Ke každé ze skupin se přistupuje individuálně a s ohledem na jejich potřeby. Rozřazení probíhá na základě odpovědí v dotazníku, který vychází z ECDL certifikátů. Začátečníkem je automaticky nově příchozí zaměstnanec, který se poprvé seznamuje s IS školy.

V následující tabulce je znázorněno rozřazení uživatelů do jednotlivých fází programu i s jejich povinnostmi.

	Povědomí		Školení		Vzdělávání	Profesní rozvoj	
	Základní bezpečnost	Bezpečnostní gramotnost	Normy a nařízení	Prohloubení vědomostí	Inovace v oblasti ICT	Obecná certifikace	Technická certifikace
Vedení školy	x	x	x	x	x	x	
Učitelé	x	x	x	x	x		
Správce sítě	x	x	x	x	x		x
Údržba	x	x					
Školní jídelna	x	x	x				
Žáci	x	x					
Zákonní zástupci	x	x					

Tabulka 4.3: Program SAE

Obecná certifikace není pro uživatele povinná, nicméně například pro vyučující ICT je velmi doporučená.

Technická specifikace je povinná pro správce sítě.

Na zvolené škole není v současné době o profesní rozvoj zájem, ale vedení školy si ponechává možnost tuto část v budoucnu využít.

Zároveň byl vznesen požadavek na vzdělávání učitelů i v oblasti novinek ICT, neboť mnozí z nich vyučují již několik let a je potřeba doplnit a rozšířit jejich znalosti o aktuální dění.

4.5 Podpůrné a školící materiály

V momentě, kdy je odsouhlasena vize budování bezpečnostního povědomí v organizaci a je vytvořena základní strategická dokumentace pro tuto oblast včetně zajištění alokace potřebných finančních prostředků, mohou být zpracovány podpůrné a školicí materiály.

Při tvorbě materiálů je potřeba zohlednit:

- jaké chování chceme posílit (v případě zvyšování povědomí);
- jakou dovednost, příp. dovednosti by si uživatelé měli osvojit a v praxi aplikovat (v případě školení).

V obou případech musí být obsah podpůrných i školicích materiálů zpracován pro konkrétní cílovou skupinu, a to tak, aby sloužil jako pomyslný průvodce s nápovědou, jak se ve specifických případech zachovat a co vykonat. Materiály zpracované na obecné úrovni mohou na účastníky působit zmatečně a neosobně. Lehce se tak může stát, že si uživatel bude myslet, že se ho daná informace netýká a pojme

zvyšování povědomí nebo školení jako akci, na které musí být a ze které si nic neodnese. SAE program bude účinný za předpokladu, že vytvořené podpůrné a školicí materiály budou zajímavé a aktuální.

Mezi příjemce zvyšování povědomí by měli patřit všichni uživatelé v organizaci. Zprávy, které se mají šířit na první úrovni zvyšování povědomí, by měly informovat každého jednotlivce o společných sdílených odpovědnostech v oblasti bezpečnosti informací. Na druhém stupni v rámci školení už je problematika bezpečnosti zaměřena vždy na konkrétní cílovou skupinu. Školicí materiál by měl obsahovat vše, co souvisí s bezpečnostní úrovní, na kterou se konkrétní uživatelé musí dostat, aby mohli vykonávat své pracovní činnosti. Materiály vytvořené pro školení jdou do větší hloubky oproti podpůrným materiálům připraveným pro zvyšování povědomí.

4.5.1 Zpracování materiálů pro zvyšování povědomí (témata, zdroje)

Zásadní otázka, na kterou je třeba najít odpověď v době příprav podpůrných materiálů pro zvyšování povědomí, zní: Čeho si mají být všichni uživatelé v oblasti informační a kybernetické bezpečnosti vědomi?

Plán pro zvyšování povědomí by měl obsahovat seznam témat budování bezpečnostního povědomí na této úrovni a přehled zdrojů, ze kterých lze čerpat inspiraci.

Existuje mnoho témat, která se dají řešit na této úrovni budování bezpečnostního povědomí. Mezi ty základní patří:

- bezpečnostní politika v organizaci a důsledky jejího nedodržení;
- použití a správa hesel včetně jejich tvorby a frekvence změn;
- ochrana před viry, trojskými koni a jiným nebezpečným kódem;
- přijetí e-mailu, ev. přílohy od neznámé osoby, spamy;
- používání webových stránek (povolené versus zakázané);
- zálohování a ukládání dat (centralizovaný versus decentralizovaný přístup);
- sociální inženýrství (manipulace osob za účelem provedení určité akce nebo získání specifických informací);
- reakce na incident (koho kontaktovat a co udělat);
- tzv. shoulder surfing (typ sociálního inženýrství používaného k získání informací, jako např. heslo, identifikační číslo a další důvěrná data při pohledu přes rameno);
- rizika systému z vnějšího prostředí (voda, požár, prach, nečistoty aj.);
- inventura majetku (odpovědná osoba a odpovědnosti jednotlivých uživatelů);
- rizika při využití informačních technologií pro osobní použití;
- přenos citlivých a důvěrných informací prostřednictvím internetu (postupy, kontakty pro pomoc);
- problémy související s omezením softwarové licence;
- povolený software v systémech organizace;
- problémy s kontrolou přístupu (přidělení oprávnění dle pracovního zařazení a pracovních povinností);
- individuální odpovědnost (dopad jednání jedince);
- kontrola hostů organizace a fyzický přístup k prostorům (fyzická bezpečnost a zásady zacházení s majetkem organizace);
- zabezpečení plochy obrazovky (šetřiče obrazovky, omezení přístupu kolemjdoucích k informacím na obrazovce a další);
- etiketa používání e-mailů (např. velikost a množství připojených souborů).

4.5.2 Zdroje pro tvorbu školicích materiálů

Prvním krokem při určování zdrojů výcvikového materiálu musí být rozhodnutí, zda budou materiály pro jednotlivé kurzy a školení vytvářeny interně nebo externě. Disponuje-li organizace vlastními odbornými zdroji, může si dovolit je přidělit na přípravu a vývoj školicích materiálů. Při rozhodování o způsobu tvorby výcvikových materiálů je třeba vzít v úvahu odpovědi na níže uvedené otázky:

- Má organizace k dispozici dostatek vlastních zdrojů pro vývoj materiálů? Patří sem počet osob a jejich odborné znalosti, dovednosti a zkušenosti.
- Je nákladově efektivnější vytvářet a vyvíjet školicí materiál v rámci organizace, nebo formou outsourcingu?
- Disponuje organizace zaměstnancem schopným monitorovat činnost dodavatele?
- Existuje dostatečný objem finančních prostředků?
- Dokáže organizace vyčlenit zdroje (především finanční a lidské) potřebné k zajištění udržení materiálů, pokud jsou vypracovány dodavatelem?
- Odpovídá obsah citlivosti údajů možnosti použití dodavatele?

4.5.3 Příklad – Bezpečnostní desatero

Pro výčet základních pravidel bezpečnosti je nutné zmínit, že neexistuje jednotný seznam, který by byl centrálně využíván. Pro potřeby této práce bylo tedy zvoleno bezpečnostní desatero, které je uzpůsobené jak žákům střední školy, tak i učitelům a dalším uživatelům programu.

1. Neotvírejte neznámé odkazy.
2. Využívejte antivirové programy – a to nejen na notebooku či stolním PC, ale i na mobilním telefonu a tabletu.
3. Pro práci s citlivými údaji nevyužívejte veřejných sítí Wi-Fi.
4. Pozorně čtěte požadovaná povolení při instalaci aplikací.
5. Pravidelně zálohujte.
6. Svá hesla nikomu nesdělujte, ani je nezapisujte.
7. Nenechávejte svá zařízení přihlášená bez dozoru, hrozí krádež dat.
8. Ověřujte si informace, které na internetu nacházíte, neboť ne vše je pravdivé.
9. Informace, které sdělujete, si pečlivě rozmyslete. Sdělte jen to, co jste schopni vyvěsit na vlastní vchodové dveře.
10. Pokud narazíte na něco, co se vám nezdá, informujte o tom.

Zvláště je nutné specifikovat práci s hesly, neboť tato část je velmi rizikovým faktorem:

- Základní pravidla pro vytváření hesel (délka, složitost, důvěrnost).
- Základní pravidla pro správu hesel (pravidla změn, frekvence změn).

V současné době nejvíce času tráví žáci (a mnohdy i ostatní uživatelé) na sociálních sítích. Je tedy vhodné uvést základní pokyny pro bezpečnou práci mířené právě na tuto oblast:

- Nastavte si soukromí a pravidla sdílení (váš obsah uvidí jen ti, kterým to umožníte).
- Bezpečně se odhlašujte.
- Pravidelně obměňujte přihlašovací heslo.
- Čtěte pravidla pro používání sociální sítě pečlivě.

- Do okruhu přátel schvalujte pouze ty lidi, které znáte.
- Pokuste se omezit sdílení fotek v reálném čase.
- Nenahrávejte intimní a hanlivé fotografie, které by mohly poškodit vás, nebo jinou osobu.
- Nezveřejňujte osobní údaje.

Proti škodlivému softwaru se většina uživatelů neumí, nebo nechce bránit. Útočníci jsou vždy krok napřed oproti těm, co se snaží vybudovat ochranu proti poškození (nejprve musí vzniknout slabina, než je opravena). Velmi častým současným trendem je také neinformovanost o možnosti pořídit si antivirový program na mobilní zařízení. Součástí programu by tedy mělo být i informování o škodlivém softwaru, a to:

- Základní dělení škodlivého softwaru (zaměření na viry).
- Behaviorální analýza.
- Příklady nejznámějších virů (historie, současnost).
- Detekce a protiopatření.

Častým problémem, se kterým se setkává většina populace, je dezinformovanost. Uživatel neumí přesně odhadnout, co je pravdivé a co už ne. Na základě pravidel je ale možné zvýšit šanci odhalení falešné zprávy. Touto problematikou se v současné době zabývá autor knihy Fake News, která se stala velmi populární. Autor realizuje mnohá školení na středních školách, která se problematiky týkají. Se studenty diskutuje o příčinách, následcích a učí je detekovat hoaxy.

Mezi nejpoužívanější jednoduché metody patří prohlížení EXIFu fotografií (který je ovšem možné při exportu smazat, případně to lze i dodatečně v programech tomu uzpůsobených), vyhledávání částí textu, reverze obrázků a zdravý rozum.

Součástí updatů materiálů by mohl být seznam aktuálních hoaxů na internetu.

4.5.4 Techniky budování programu SAE

Mezi běžně používané techniky budování bezpečnostního povědomí na úrovni školení patří:

- Interaktivní video výcvik – jedná se o jednu z několika metod distančního učení. Tato technologie podporuje obousměrné interaktivní audio i video instrukce. Interaktivní funkce činí techniku užitečnější, ovšem na druhou stranu také dražší.
- Trénink založený na webové aplikaci – tato technika je v současné době jednou z nejoblíbenějších pro distribuovaná prostředí. Účastníci webové relace mohou studovat samostatně a učit se vlastním tempem. Testovací a odpovědnostní funkce mohou být postaveny na měření výkonnosti. Některé testovací modely, zahrnující tuto techniku, začínají poskytovat další přínos, a to interakci mezi instruktorem a žákem nebo mezi žáky.
- Trénink prostřednictvím informačních technologií (zejména počítače) bez přístupu k internetu – tato technika je navzdory dostupnosti dat prostřednictvím webových aplikací stále populární. I nadále se považuje za účinnou metodu pro distribuci školicích materiálů. Stejně jako předchozí technika, ani tato neumožňuje vzájemnou interakci mezi instruktorem a žákem, ev. více žáky.
- Školení na pracovišti prováděné instruktorem (včetně odborné prezentace a mentoringu) – jedná se o jednu z nejstarších a současně stále jednu z nejoblíbenějších metod pro šíření školicích materiálů cílové skupině.

Bezesporu největší výhodou této techniky je interaktivní povaha výcviku. Na druhou stranu má i svá negativa. Ve velké organizaci mohou nastat při plánování rozdělení uživatelů potíže se zajištěním prostor pro účast všech cílových skupin. V organizacích, které mají zastoupení v různých eografických oblastech, mohou být v souvislosti s potřebou přemístění vysoké cestovní náklady pro instruktory i žáky. Navzdory všem nevýhodám stále většina uživatelů upřednostňuje tuto tradiční metodu oproti ostatním.

Sloučením a kombinací různých technik výcviku lze déle udržet pozornost účastníků školení. To může v organizaci vést k vyšší efektivitě při budování bezpečnostního povědomí. Například zobrazování videí během školení vedeného instruktorem umožňuje účastníkům soustředit se na jiný zdroj informací. Video záznam může zvýšit důraz na problematiku, kterou instruktor předkládá.

4.6 Bezpečnostní politika

Politika bezpečnosti je právní dokument, který popisuje, jakým způsobem organizace zaštiťuje bezpečnost. Musí být aktuální, srozumitelný, závazný a právně vymahatelný, zároveň musí existovat v písemné podobě a musí být dostupný. Je důležitou součástí obchodních podmínek. Šablona bezpečnostní politiky slouží mimo jiné i k vytvoření školících a podpůrných materiálů.

Politika bezpečnosti typicky obsahuje následující části:

1) Cíle bezpečnosti

2) Šíření působnosti a politiky bezpečnosti ve třech oblastech

   a) Fyzická a objektová bezpečnost

   b) Personální bezpečnost

   c) Informační bezpečnost (klasifikace dat, řízení oprávnění)

3) Odpovědnosti pracovníků

4.7 Post-implementační fáze projektu SAE

Podle programu SAE je poslední, a nedílnou, součástí post-implementační fáze. Zde je nutné vyhodnotit získané výsledky a získat zpětnou vazbu. Tato fáze se týká také počtu opakování školení a aktualizací, případně úprav, výukových materiálů.

Sledování shody realizace SAE programu s původním plánem zahrnuje posouzení stavu programu budování bezpečnostního povědomí a jeho mapování z pohledu protnutí se směrnicemi organizace a používanými normami. Zprávy o stavu a dílčích aktivitách SAE programu lze z databáze generovat a používat k identifikaci mezer, ev. problémů. V návaznosti na zjištění neshod mohou být podniknuty nápravné kroky. Ty mohou mít podobu formálních připomínek, potřeby další osvěty ve zvyšování bezpečnostního povědomí či školení nebo nabídky vzdělávání, anebo zavedení opravného plánu s harmonogramem realizace a plánovaným termínem dokončení.

4.7.1 Dokumentace

Dokumentaci je nutné vytvořit pro doložení výuky a pro uchování zpětné vazby uživatelů. Dokument musí být uložen v zabezpečeném archivu školy. Obsahem je každá část programu SAE. Školení, která

proběhla, je nutné doložit podpisy na prezenčních listinách, popřípadě vyplněnými testy. Certifikát, který účastníci získávají, se jako kopie ukládá do archivu školy. Vyhodnocení materiálů se ukládá v listinné formě a obsahuje kompletní historii proběhlých změn.

4.7.2 Hodnocení SAE programu a zpětná vazba

Formální hodnocení a mechanismy zpětné vazby jsou kritickými součástmi jakéhokoliv programu budování bezpečnostního povědomí. Proces neustálého zlepšování nemůže nastat bez dobrého úmyslu vedoucího k zajištění fungování stávajícího SAE programu. Mechanismus zpětné vazby musí být nastaven tak, aby řešil původní stanovené cíle programu budování bezpečnostního povědomí. Strategie zpětné vazby může být navržena a implementována teprve poté, co jsou ustáleny a zakotveny základní požadavky. Následující obrázek znázorňuje různé mechanismy hodnocení a získávání zpětné vazby, které lze k aktualizaci SAE programu a jeho plánu použít.

Strategie zpětné vazby musí obsahovat prvky, které se budou zabývat jakostí, rozsahem, metodou zavádění (metody realizace školení – např. trénink založený na webové aplikaci, interaktivní video výcvik nebo školení na pracovišti prováděné instruktorem a další), úrovní obtížnosti, vhodností použití, délkou trvání dané vzdělávací akce, relevancí, náklady a návrhy na změnu.

4.7.3 Četnost opakování, aktualizace materiálů

Vzhledem k faktu, že SAE je nikdy nekončící činnost, je třeba školení opakovat. Doporučená frekvence je jedenkrát ročně, pro učitele v tzv. přípravném týdnu (poslední týden prázdnin, standardně poslední týden v srpnu), pro žáky je rozhodnutí na vedení školy. Během letních prázdnin dochází k aktualizaci výukových materiálů a možným změnám požadavků vedení školy. V případě náhlých změn je třeba školení zahrnout dříve, nejlépe na nejbližší možné schůzi pedagogů, které se konají pravidelně – například jedenkrát měsíčně, vždy v pondělí.

4.7.4 Správa změn

Řízení změn je součástí programu budování bezpečnostního povědomí, jehož cílem je zajistit, aby zvyšování povědomí, školení a vzdělávání se nestaly stagnujícími, a v důsledku toho pozbyly relevance pro skutečně vznikající problémy, kterým organizace čelí. Systém řízení změn je navržen takovým způsobem, aby řešil změny v bezpečnostní politice a postupech, které se odrážejí v kultuře organizace.

Do budoucna je potřeba zajistit, aby byl SAE program stále stejně strukturován a průběžně aktualizován z důvodu stále se objevujících nových a nových informačních technologií a s tím souvisejících bezpečnostních problémů. Požadavky na zvyšování povědomí a školení rozvíjejí o nové znalosti a dovednosti nezbytné k tomu, aby uživatelé dokázali reagovat na nové technologické změny. Změny v poslání organizace, příp. jejích cílech, mohou také ovlivnit smysl, rozložení a obsah jednotlivých vzdělávacích akcí.

Stále aktuálnější problémy, jako je např. obrana vlasti, budou také mít vliv na povahu a rozsah činností týkajících se povědomí o bezpečnosti, které jsou nezbytné k tomu, aby byli uživatelé informováni o nejnovějších praktikách a uplatňovaných protiopatřeních. Zároveň nové zákony a normy mohou mít také dopad na agendu budování bezpečnostního povědomí a obsah podpůrných a školicích materiálů. Dalším faktorem, který se v průběhu času vyvíjí a mění, jsou změny směrnic v organizaci. Tyto změny by se taktéž měly odrazit v obsahu vzdělávacích materiálů.

4.7.5 Neustálé zlepšování SAE programu

Tato fáze programu budování bezpečnostního povědomí je zaměřena na vytváření vyšší úrovně bezpečnostního povědomí a excelence řešených témat, které se dosahuje prostřednictvím všudypřítomného vnímání této problematiky v organizaci. Procesy, které poskytují jednotlivým cílovým skupinám zvyšování povědomí, školení a vzdělávání, by měly být zcela začleněny do celkové strategie organizace. Vyvinutý SAE program definuje soubor metrik pro tuto oblast a stanovuje, že by měly být zavedeny automatizované sledovací systémy, které by podporovaly zachycování kvantitativních i kvalitativních dat a poskytovaly informace odpovědným osobám a vedoucím jednotlivých úseků v předem stanovených pravidelných intervalech. V této fázi organizace začleňují do svého programu budování bezpečnostního povědomí formální mechanismy pro průběžný výzkum v oblastech technologického pokroku, osvědčených postupů a příležitostí pro srovnávání.

4.7.6 Ukazatele úspěšnosti SAE programu

Správce SAE programu a osoba odpovědná za přípravu a správu školení by měli být primární obhájci a iniciátoři neustálého zlepšování a podpory programu budování bezpečnostního povědomí v organizaci. Klíčovým faktorem úspěchu SAE programu je, aby každý byl schopen a ochoten vykonávat svěřenou bezpečnostní roli v organizaci.

Pravidlo „organizace je tak silná jako její nejslabší článek“ platí i v oblasti bezpečnosti. Zabezpečení informací a infrastruktury organizace je týmovým úsilím. Níže jsou uvedeny některé klíčové ukazatele pro posouzení podpory a přijetí SAE programu. Mezi ně patří:

- dostatečné finančních prostředky na realizaci strategie SAE programu;
- vhodné přidělení rolí a odpovědností, které umožní osobám s klíčovými povinnostmi efektivně implementovat strategii SAE programu;
- podpora různých distribučních kanálů (např. web, e-mail, tištěné a propagační materiály a další) a zveřejňování informací o informační a kybernetické bezpečnosti;
- zprávy zaměstnancům o budování bezpečnostního povědomí (obsah může být sdělován i prostřednictvím schůzek);
- použití metrik (např. označení poklesu bezpečnostních incidentů nebo porušení značí, že se zmenšuje rozdíl mezi stávajícím povědomím a záměrem realizovaných výcviků a vzdělávacích akcí a zjištěnými potřebami, zvyšuje se procento uživatelů vystavených podpůrným a školicím materiálům a procento uživatelů s náležitě vyškolenými bezpečnostními povinnostmi);
- vedoucí jednotlivých úseků nepoužívají svůj status v organizaci, aby se vyhnuli bezpečnostním kontrolám, které jsou důsledně dodržovány;
- úroveň účasti na povinných bezpečnostních vzdělávacích akcích;
- uznávání dodržení bezpečnostních pravidel (např. ocenění, plakety);
- motivace demonstrovaná osobami, které hrají klíčovou roli při řízení a koordinaci programu budování bezpečnostního povědomí.

4.8 Koordinace SAE programu s ostatními

Pro zvýšení efektivnosti budování bezpečnostního povědomí lze s výhodou začlenit do programu SAE další programy. Každý má své uplatnění v členění v jednotlivých fázích programu budování bezpečnostního povědomí SAE.

4.8.1 Koncept REP

Prvním z nich je program založený na konceptu REP vycházejícího z teorie digitálního občanství.

Respect, Educate and Protect (REPs) je výuková metoda k výchově digitálního občana od mateřské školy. Metoda obsahuje 3 témata:

- Respect Your Self/Respect Others – REP 1 (R-R) Téma lze definovat jako „respektuj sebe, ale také respektuj ostatní".

- Educate Your Self/Connect with Others – REP 2 (E-C) Téma znamená „vzdělávání sebe sama/spojení s ostatními".

- Protect Your Self/Protect Others – REP 3 (P-P) Téma říká „ochraňuj sebe, ale také ostatní před sebou samým".

4.8.1 Koncept ECDL

Druhým z nich je evropský program založený na konceptu ECDL – European Computer Driving Licence, dnes European Certification of Digital Literacy. Lze volně přeložit jako „digitální řidičské oprávnění".

Přínos konceptu ECDL spočívá zejména v tom, že prostřednictvím mezinárodně jednotných sylabů definuje vzdělávací obsah, který odráží aktuální potřeby trhu práce a běžného života jedince ve společnosti, a to zejména v oblasti přenositelných digitálních znalostí a dovedností, a současně nabízí mezinárodně uznávanou, standardizovanou, objektivní a nezávislou metodu ověřování výsledků vzdělávání (tzv. ECDL zkoušky).

Koncept ECDL svým rozsahem pokrývá prakticky všechny oblasti, ve kterých se digitální technologie v běžném životě využívají. Zahrnuje celou škálu vzdělávacích a certifikačních programů v oblasti digitálních kompetencí, od programů pro žáky a studenty základních a středních škol, přes programy pro zaměstnané, nezaměstnané nebo digitálně vyloučené osoby, až po programy určené široké veřejnosti nebo naopak pro odborníky z různých oborů.

Ověřování digitálních znalostí a dovedností probíhá formou praktických zkoušek v reálném prostředí s využitím běžných stolních počítačů, notebooků, tabletů či mobilních telefonů, různých operačních systémů, běžně používaných aplikací, lokálních sítích a internetu.

<u>Základní moduly ECDL / ICDL:</u>

M15 – Vyhledávání, vyhodnocování a zpracování informací z internetu	(Information Literacy)
M14 – Spolupráce a výměna informací na internetu	(Online Collaboration)
M12 – Bezpečné používání informačních technologií	(IT Security)
M7 – Práce s internetem a komunikace	(Online Essentials)
M27 – Práce s počítačem a internetem	(Computer&Online Essentials)
M346 – Práce s webovými aplikacemi	(Application Essentials)
M4 – Práce s tabulkami	(Spreadsheets)
M3 – Zpracování textu	(Word Processing)
M2 – Práce s počítačem a správa souborů	(Computer Essentials)

Standardní moduly ECDL / ICDL:

M19 – Robotika	(Robotics)
M17 – Využívání digitálních technologií v marketingu	(Digital Marketing)
M16 – Informatické myšlení a programování	(Computing)
M13 – Plánování projektů	(Project Planning)
M10 – Tvorba webových stránek	(Web Editing)
M9 – Úpravy digitálních obrázků	(Image Editing)
M6 – Prezentace	(Presentation)
M5 – Použití databází	(Using Databases)

Pokročilé moduly ECDL / ICDL:

AM8 – Analýza a vizualizace dat	(Data Analytics)
AM7 – Finanční tabulky	(Financial Spreadsheets)
AM6 – Pokročilé prezentace	(Advanced Presentation)
AM5 – Pokročilé použití databází	(Advanced Databases)
AM4 – Pokročilá práce s tabulkami	(Advanced Spreadsheets)
AM3 – Pokročilé zpracování textu	(Advanced Word Processing)

4.8.3 Program CSA

Třetím modelem do skládačky je CSA – Cyber Security Awareness, v překladu povědomí o kybernetické bezpečnosti.
Součástí povědomí o kybernetické bezpečnosti je uvědomění si nebezpečí při prohlížení webu, kontrole e-mailů a interakci online.
Školení pro technické i netechnické pracovníky podle rolí je nejlepší způsob, jak připravit správné lidi na správné hrozby kybernetické bezpečnosti.
Jakékoli školení a zvyšování povědomí o kybernetické bezpečnosti může významně ovlivnit chování zaměstnanců, od formálního programu školení o bezpečnosti až po měsíční e-mail s tipy a triky v oblasti kybernetické bezpečnosti, a dokonce může podnítit kulturní změnu v pohledu zaměstnanců na kybernetickou bezpečnost. Skutečná změna začne, jakmile si jednotlivci osvojí myšlenku, že kybernetická bezpečnost je jednou z jejich pracovních povinností.

4.8.4 Kybernetická hygiena

Kybernetická hygiena vychází z oficiálního doporučení evropské bezpečnostní agentury ENISA. Základní princip kybernetické hygieny je myšlen jako analogie osobní hygieny. Cílem je minimalizace kybernetických rizik. Jedná se o návyky navazující na metodiku bodování bezpečnostního povědomí (SAE).
Kybernetická hygiena je základem kybernetické bezpečnosti. Návyky kybernetické hygieny pomáhají předcházet rizikovým situacím a umožňují bránit se lépe kybernetickým hrozbám.

4.9 Obsahová část školení

Příklady obsahu školení jsou uvedeny v materiálech:
„A Základní školení: Vzdělávání zaměstnanců“, který uvádí základní body pro koncept obsahu školení.
„B Povědomí o kybernetické bezpečnosti“ zabývající se základním bezpečnostním povědomí v kybernetickém prostoru.

A Základní školení: Vzdělávání zaměstnanců

Díky těmto bodům budou vaši zaměstnanci připraveni podílet se na ochraně vaší organizace. V kombinaci se správnými bezpečnostními nástroji budete mít solidní začátek budování pevných bezpečnostních základů.

Ochrana identity

- ☐ Používejte dlouhá a složitá hesla, která jsou jedinečná a nelze je uhodnout.
- ☐ Nikdy nepoužívejte hesla opakovaně.
- ☐ Používejte správce hesel.
- ☐ Všude, kde je to možné, zapněte funkci MFA (Multifaktorová autentizace).
- ☐ Pro změnu hesla vždy přejděte na skutečnou webovou stránku. Pozor na žádosti o změnu hesla v e-mailu.

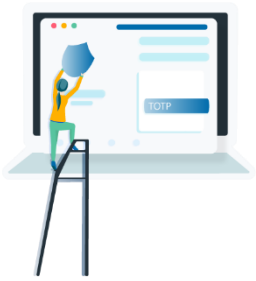
Zabezpečená koncová zařízení

- ☐ Pracujte pouze na svém koncovém zařízení.
- ☐ Ujistěte se, že je vždy aktualizován nejnovějšími aktualizacemi a bezpečnostními záplatami.
- ☐ Na všech pracovních zařízeních je vyžadováno dodržování zásad (tj. antivirový program, šifrování celého disku, zámek obrazovky systému, zakázané účty hostů atd.)
- ☐ Za svá zařízení jste zodpovědní vy, proto vždy myslete na to, jak je zabezpečit. Musíte vědět, kde jsou a kdo k nim má přístup.
- ☐ Pokud zjistíte, že vaše zařízení zmizelo, neprodleně kontaktujte odpovědnou osobu.

Spolufinancováno Evropskou unií
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
jihomoravský kraj

- Kdykoli se od notebooku vzdálíte, zamkněte jej.
- Pokud je to možné, musí být na všech noteboocích zapnuta funkce MFA.
- Nikdy nepoužívejte USB disk, který jste nezakoupili vy nebo společnost, a nikdy nepoužívejte disk, který vám dal někdo mimo společnost. Pokud náhodou najdete USB disk na ulici nebo v kavárně, zahoďte jej.
- Všechna zařízení uchovávejte na bezpečném místě 24 hodin denně, 7 dní v týdnu, buď pod dohledem, nebo bezpečně uzamčená.

Ochrana dat



- Neukládejte firemní data na jiné než firemní disky nebo webové stránky.
- Dávejte pozor, kam ukládáte citlivá data, a dbejte na to, jaké druhy oprávnění jsou nastaveny pro jednotlivé složky a soubory. Pokud je to možné, udělujte přístup individuálně.
- Ujistěte se, že jsou všechna data zálohována na vhodném místě.
- Pokud to má smysl, data šifrujte nebo je umístěte do souborů a složek s velmi přísnými oprávněními.
- Nepovažujte e-mail za bezpečné komunikační médium. Snažte se zdržet zasílání příloh nebo citlivých informací, které byste nechtěli zveřejnit.
- Pokud se nacházíte ve veřejném prostoru, buďte opatrní při přihlašování a ujistěte se, že vám při tom nikdo nekouká přes rameno.

Zabezpečený e-mail

- Pro e-mail je vyžadována MFA.
- E-mail je středobodem autentizačního prostoru organizace, proto je nutné neztratit nad ním kontrolu. Pokud se domníváte, že jste ztratili kontrolu nad svým e-mailem, neprodleně kontaktujte odpovědnou osobu.
- Neklikejte na odkazy v e-mailech. Pokud je to možné, přejděte na web ručně, abyste dokončili jakoukoli akci, kterou e-mail požaduje.
- Nevěřte, že e-mail je od toho, za koho se vydává.
- Neotevírejte přílohy e-mailů, které nečekáte, a držte se sdílení souborů prostřednictvím určeného postupu pro sdílení souborů.

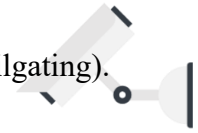
Bezpečný prohlížeč

- Používejte Chrome.
- Nepoužívejte bezdůvodně pluginy.
- Vyhýbejte se webovým stránkám, které používají protokol HTTP, a nikoli HTTPS, ale nespoléhejte se pouze na zelený zámek, který určuje, zda jste v bezpečí, nebo ne. Věnujte pár sekund dvojité kontrole zbytku url adresy.

Zabezpečení telefonu

- Telefony musí být chráněny heslem nebo pinem a v ideálním případě se telefon po určitém počtu nesprávných pokusů o přihlášení vymaže.
- V telefonu by mělo být povoleno vzdálené vymazání.
- Udržujte telefon v aktuálním stavu s nejnovějšími bezpečnostními záplatami.

Zabezpečení kanceláře



- Pro zabezpečení kanceláře máme k dispozici prostředky typu ostraha, kamery, čidla.
- Zabezpečení vniknutí cizích osob v okamžiku, kdy se zavírají dveře (tailgating).
- Po skončení práce vymažte obsah na tabulích.
- Když si v kanceláři všimnete neznámé osoby, neváhejte se jí zeptat a zjistit, co potřebuje. V případě potřeby je nechte počkat v prostoru určeném pro návštěvníky.

Zabezpečení duševního vlastnictví

- Vše, co pro společnost vyvinete, patří společnosti.
- Nestahujte ani neukládejte duševní vlastnictví na osobní disky.
- Nehovořte o duševním vlastnictví s nikým mimo společnost.

Zabezpečená WiFi

- Pokud je to možné, vyhněte se používání veřejné Wi-Fi.
- Pokud veřejnou WiFi bezpodmínečně musíte použít, použijte virtuální privátní síť (VPN).
- Mobilní zařízení připojujte pouze k ověřené a důvěryhodné síti.
- Pracovní stanice připojujte pouze k firemní síti.

Bezpečné interakce s veřejností

- Vždy vězte, s kým mluvíte.
- Dávejte si pozor na interakce, které jste neiniciovali, a nikdy v těchto situacích neposkytujte informace.
- Pokud se někdy dostanete do interakce s někým, kdo na vás bude vyvíjet tlak, abyste mu ihned poskytli odpověď, odpovězte ne.
- Nesdělujte soukromé informace veřejnosti.
- Dávejte si pozor na škodlivé odkazy v komunikaci na sociálních sítích.
- Dávejte si pozor na to, jaké informace zveřejňujete na sociálních sítích.

Co dělat v případě problému?

- Ihned kontaktujte odpovědnou osobu.
- Bezpečnostní školení se koná pravidelně (např. čtvrtletně, pololetně atd.] a je povinné.
- Je velmi důležité, abyste v případě problému zapojili bezpečnostní tým. Pokud uděláte chybu nebo špatné rozhodnutí, nedostanete se do potíží; do potíží se však dostanete, pokud o tom nikomu neřeknete.

B Povědomí o kybernetické bezpečnosti

Cílem Cyber Security Awareness (CSA) neboli Povědomí o kybernetické bezpečnosti je dosáhnout základního bezpečnostního povědomí při využívání internetu a kybernetického prostoru. Tento materiál zmíněnou problematiku uchopil jako prostý dotaz – „Co dělat a co nedělat“ - ✓ versus ✗.

E-mail

- ✓ Před kliknutím na odkaz zaslaný e-mailem zkontrolujte adresu URL.
- ✓ Nahlaste všechny podezřelé aktivity a kybernetické incidenty příslušnému orgánu.
- ✓ Oficiální e-mailový účet by měl být používán pouze pro oficiální účely.
- ✓ Úřední e-mail by neměl být přeposílán na osobní e-mailový účet.
- ✗ Neodpovídejte na e-maily přijaté od cizích lidí.
- ✗ Neklikejte na odkazy z neznámého nebo nedůvěryhodného zdroje.
- ✗ Neposílejte žádné osobní nebo citlivé informace, jako jsou čísla kreditních karet, hesla nebo jiné údaje prostřednictvím e-mailu.

Heslo

- ✓ Vždy dodržujte zásady pro vytváření hesel, abyste se vyhnuli rizikům.
- ✓ Používejte těžko odhadnutelná hesla nebo přístupové fráze.
- ✓ Pravidelně měňte heslo.
- ✓ Používejte různá hesla pro různé účty.
- ✓ Udržujte svá hesla nebo přístupové fráze v tajnosti.
- ✓ Okamžitě změňte heslo, pokud máte podezření, že bylo prozrazeno či jinak kompromitováno.
- ✓ Při zadávání hesla buďte vždy opatrní (například sedí-li někdo poblíž).
- ✗ Hesla nesdílejte s ostatními ani si je nezapisujte.
- ✗ Nepoužívejte heslo, které již bylo použito dříve.
- ✗ Jako heslo k účtu nepoužívejte názvy věcí, které se nacházejí ve vašem okolí.
- ✗ Nepoužívejte slova ze slovníku (lze je snadno rozluštit).

Počítač

- ✓ Pokud počítač nebo notebook nepoužíváte, zamykejte je.
- ✓ Notebooky a počítače fyzicky zabezpečte.
- ✓ Dojde-li ke ztrátě nebo odcizení zařízení, neprodleně to nahlaste příslušnému orgánu.
- ✓ V počítači by měl být nainstalován antivirový software a měl by být aktualizován.

- Neinstalujte do svého pracovního počítače nebo notebooku neautorizované programy.
- Nenechávejte zařízení bez dozoru.

Mobil

- Nepoužívaný mobilní telefon zamykejte.
- Udržujte mobilní telefony fyzicky zabezpečené.
- Osobní údaje nebo údaje o účtu by měly být řádně střeženy.
- Pokud dojde ke ztrátě nebo odcizení zařízení, neprodleně to nahlaste příslušnému orgánu.
- Vždy zkontrolujte, jaká oprávnění požaduje mobilní aplikace, kterou chcete nainstalovat.
- Před instalací aplikace je vhodné zkontrolovat její důvěryhodnost.
- Buďte opatrní při používání geolokačních služeb. Pronásledovatelé mohou snadno získat přístup k vaší poloze.
- Neodpovídejte na telefonáty s žádostí o důvěrné údaje.
- Nenechávejte mobilní telefon bez dozoru.
- Nenechte se oklamat a neprozraďte důvěrné informace. Neautorizovaná osoba se může vydávat za zaměstnance nebo obchodního partnera.

Přenosná média

- Přenosná média s citlivými informacemi ochraňujte, zamykejte je.
- Pokud již informace nepotřebujete, řádně je zničte.
- Používejte oficiální přenosná paměťová média pro úřední účely.
- V případě ztráty oficiálních přenosných paměťových médií je třeba tuto skutečnost nahlásit příslušnému orgánu co nejdříve.
- Nenechávejte přenosná média s citlivými informacemi volně na stole.
- Nepřipojujte přenosná zařízení bez povolení a ověření (může obsahovat viry nebo může být poškozeno).
- Přenosná média by neměla být předávána neoprávněné osobě.

Připojení k bezdrátové síti

- Pamatujte, že bezdrátové připojení je ze své podstaty nezabezpečené.
- Pokud musíte používat Wi-Fi, použijte k ochraně dat a zařízení síť VPN.
- Ujistěte se, že jsou bezdrátová rozhraní ve výchozím nastavení zakázána.

- Nenechávejte bezdrátové připojení nebo Bluetooth zapnuté, pokud je nepoužíváte.
- Zabezpečené webové stránky využívající veřejnou Wi-Fi by neměly být používány.
- Vyhněte se používání veřejných hotspotů Wi-Fi.

Použití internetu

- Používejte nejnovější verzi internetového prohlížeče.
- Před ukončením relace prohlížeče se odhlaste z webových služeb, například z webové pošty.
- Po dokončení činnosti v aktuálním webové aplikaci zavřete relaci prohlížeče.
- Soubory cookie by měly být povoleny pouze z důvěryhodných webových stránek.
- Nepovolujte funkce prohlížeče "uložit heslo" a automatické dokončování.
- Nestahujte ani nešiřte škodlivý software ani jiné nástroje.
- Nestahujte data chráněná licencemi a autorským zákonem.

Ochrana před viry a škodlivým kódem

- Zajistěte, aby byl klientský systém nakonfigurován s autorizovaným centrálně spravovaným antivirovým softwarem.
- Ujistěte se, že antivirový software je aktuální.
- V případě, že se virus neodstraní, musí být incident nahlášen příslušnému orgánu.

Zabezpečení internetového prohlížeče

- Nezapomeňte odstranit historii procházení, čímž se odstraní všechny soubory cookie, dočasné soubory, historie a filtrování ActiveX.
- Nezapomeňte ve svém webovém prohlížeči vypnout podporu JavaScriptu nebo ActiveX, než začnete navštěvovat neznámé webové stránky.
- Na nedůvěryhodných odkazech neuvádějte žádné osobní údaje.
- Nepovolujte vyskakovací okna a zásuvné moduly (zakažte je v nastavení prohlížeče).

Webové aplikace

- Bezpečnostní záplaty a aktualizace softwaru by měly být nainstalovány ihned, jakmile jsou k dispozici.

Tiskové výstupy / faxy

- ✓ Tiskové výstupy obsahující citlivé informace uzamykejte, abyste snížili riziko neoprávněného vyzrazení.
- ✓ Při tisku citlivých informací dávejte pozor na své okolí.
- ✓ Vyzvedávejte včas výstupy z tiskáren a kopírek.
- ✗ Nenechávejte citlivé informace ležet v kanceláři.
- ✗ Nenechávejte na stole výtisky nebo přenosná média obsahující soukromé informace.

Sociální sítě

- ✓ Používejte nastavení soukromí na sociálních sítích, abyste omezili přístup ke svým osobním údajům.
- ✓ Přidávejte si pouze lidi, které znáte off-line.
- ✓ Pokud přidáváte cizí osoby, mějte se na pozoru.
- ✓ Dávejte pozor na přesvědčivé napodobeniny bank, karetních společností, charitativních organizací a vládních agentur.
- ✓ Je třeba zkontrolovat nastavení soukromí profilu a ujistit se, že je nastaveno na správnou úroveň.
- ✓ Buďte opatrní se sdílenými příspěvky.
- ✓ I když je sociální síť nastavena jako soukromá, nezaručuje to, že informace jsou zcela soukromé.
- ✗ Netolerujte nepohodlí.
- ✗ Nezveřejňujte žádné soukromé nebo citlivé informace, jako jsou čísla kreditních karet, hesla nebo jiné údaje na veřejných stránkách, včetně stránek sociálních médií.
- ✗ Nepřehánějte to se sdílení informací. Citlivé informace, jako je datum narození, rodné číslo matky, jméno a příjmení matky, jméno domácího mazlíčka nebo jiné identifikační údaje by neměly být sdíleny na sociálních sítích a platformách, jako je Facebook, LinkedIn nebo Twitter

Vždy mějte na paměti, že jakmile se na internet dostane osobní nebo citlivá informace, nemáte nad ní žádnou kontrolu. Cokoli, může být zveřejněno a zachyceno, zkopírováno a uloženo v cizím počítači a zrcadleno na jiných stránkách.

5 SW nástroj

Stručné seznámení s nástrojem Esko-SW

5.1 Komu je nástroj primárně určen

Typickými aktivními uživateli nástroje Esko-SW jsou:

- manažer kybernetické bezpečnosti (MKB),
- ředitel informační bezpečnosti (CISO),
- garanti nebo vlastníci informačních aktiv (dle zvolené metodiky),
- členové výboru pro řízení kybernetické bezpečnosti (VŘKB).

5.2 Komu jsou určeny výstupy z nástroje

Typickými konzumenty tiskových výstupů a vizualizací z nástroje Esko-SW jsou:

- architekt informační bezpečnosti,
- auditor kybernetické bezpečnosti,
- pracovník NÚKIB (v případě auditu NÚKIB),
- vyšší management organizace a/nebo její vedoucí pracovníci.

5.3 Podpora metodik

Nástroj Esko-SW podporuje práci ve dvou rozdílných režimech, tj. podporuje dvě různé metodiky řízení informační bezpečnosti:

- shoda s vyhláškou o kybernetické bezpečnosti (VKB),
- systém řízení bezpečnosti informací (ISMS, ISO/IEC 27001).

Mezi oběma metodikami nelze volně přecházet, ale je možno Esko-SW využít pro podporu obou metodik v rámci jedné organizace.

5.4 K čemu Esko-SW primárně slouží

Cílem nasazení nástroje Esko-SW je docílit větší transparentnosti procesů řízení informační bezpečnosti v organizaci. Přínosy nástroje spočívají především v těchto oblastech:

- názorná vizualizace informací řízení informační bezpečnosti od úrovně abstraktního konceptu až po úroveň konkrétních fyzických nebo logických informačních aktiv;
- přehledná inventarizace informačních aktiv;
- zavedení jasně stanovených odpovědností jednotlivých účastníků zavádění informační bezpečnosti a jejich názorná vizualizace;
- usnadnění procesu analýzy rizik prostřednictvím expertních funkcí založených na Best Practicies;
- podpora koncepčního myšlení v oblasti informační bezpečnosti;
- automatizace Prohlášení o aplikovatelnosti (PoA);

- automatizace Plánu zvládání rizik (RTP);
- podpora řízení kontinuity informační bezpečnosti v organizaci.

5.5 Podpora řízení kontinuity informační bezpečnosti

Velkou výhodu přináší nástroj Esko-SW do oblasti řízení kontinuity informační bezpečnosti. Data evidovaná v nástroji jsou neustále tzv. "živá" a jsou křížově vzájemně propojená do interaktivního systému, kterému se poněkud nesrozumitelně říká "sukcesivní hierarchie". Plně postačí, když si zapamatujete, že mezi daty uloženými do nástroje automaticky (tj. bez nutnosti zásahu uživatele) vznikají užitečné logické dynamické vazby, které samy o sobě jsou již jistou formou automatizace procesů v Esko-SW. Tyto dynamické vazby zajišťují, že některé úkony nutné k zajištění kontinuity řízení informační bezpečnosti v organizaci budou téměř bezpracné. Vhodným, jednoduchým případem je ukončení provozu nějakého informačního aktiva. V takovém případě prostě aktivum jednoduše vymažete z evidence aktiv a toto odstranění daného aktiva z evidence se plně automaticky promítne do všech návazných agend (Analýza rizik, Výběr bezpečnostních opatření PoA, RTP apod.). Jiným případem je situace, kdy například změníte hodnotu aktiva nebo upřesníte zdroje (lidé nebo finance) v RTP plánu. Tyto změny se automaticky a bezprostředně promítnou do PoA apod. Rovněž když upřesníte Analýzu rizik, automaticky aktualizuje PoA i RTP.

5.6 Esko-SW jako místo sdílení informací mezi profesními skupinami

Většina velkých organizací se vyznačuje přítomností různorodých profesionálních skupin s odlišnými pohledy na kybernetickou a informační bezpečnost. Tyto skupiny zahrnují výkonný management, který si je obvykle uvědomuje důležitost kybernetické bezpečnosti, avšak prioritně se soustředí na obchodní nebo operativní cíle. Dále jsou tu provozní zaměstnanci a nižší management, kteří mohou vnímat bezpečnostní opatření dokonce jako praktickou překážku své každodenní činnosti. Dále jsou to obvykle např. prodejní a marketingové týmy, které usilují o maximální zapojení zákazníků, a v důsledku toho obvykle stojí na straně méně striktních bezpečnostních zásad. Velmi významnou skupinou z hlediska informační bezpečnosti jsou vývojáři a IT specialisté, kteří jsou prioritně zaměření na inovace a rychlost, což často komplikuje striktní dodržování bezpečnostních standardů. Nakonec jsou zde bezpečnostní profesionálové, kteří se soustředí na prevenci hrozeb a ochranu dat. Mezi těmito skupinami často chybí společná terminologie informační bezpečnosti a omezená je i vzájemná komunikace skupin v důsledku rozdílných cílů a priorit. Akcentace různých priorit ze strany těchto skupin je přirozenou a nedílnou součástí života organizace a stává se významným faktorem, se kterým je nutné realisticky počítat při uplatňování bezpečnostních standardů. Nástroj Esko-SW si klade za jeden ze svých cílů umožnit zlepšení sdílení klíčových bezpečnostních informací napříč skupinami a hledá, pokud možno jednoduchý názorný společný jazyk pro jejich sdílení zejména mezi managementem, odborníky na kybernetickou bezpečnost a IT specialisty.

6 Relevantní zranitelnosti

6.1 Obecné zranitelnosti

	OBECNÉ ZRANITELNOSTI
id	
1	nevhodné nastavení přístupových oprávnění
2	nedostatečné monitorování činnosti uživatelů
3	neschopnost odhalit nevhodné nebo závadné způsoby chování
4	neschopnost včasného odhalení pochybení ze strany zaměstnanců
5	nedostatečné bezpečnostní povědomí uživatelů a administrátorů
6	nedostatečné monitorování činnosti uživatelů
7	nedostatečná ochrana aktiv (dat)
8	nedostatečná ochrana aktiv (dat)
9	nevhodná bezpečnostní architektura
10	chybějící nebo nedostatečné řízení zranitelností
11	nedostatečná malwarová ochrana
12	zastaralost informačního a komunikačního systému
13	nedostatečná údržba informačního a komunikačního systému
14	nedostatečná SW údržba (patch management)
15	chybějící nebo nedostatečná strategie zálohování a archivace dat
16	chybějící nebo nedostatečné řízení kontinuity činnosti organizace
17	nedostatečná ochrana vnějšího perimetru
18	nedostatečná údržba podpůrných aktiv
19	nedostatečná údržba podpůrných aktiv
20	nedostatečná ochrana aktiv
21	nedostatečná ochrana aktiv
22	nedostatečná míra nezávislé kontroly
23	nedostatečné bezpečnostní povědomí uživatelů a administrátorů
24	chybějící nebo nedostatečné řízení kontinuity činnosti organizace
25	nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů
26	nedostatečná ochrana aktiv
27	nedostatečná ochrana aktiv
8	nedostatečná ochrana aktiv
29	nedostatečné bezpečnostní povědomí uživatelů a administrátorů
30	nedostatečné bezpečnostní povědomí uživatelů a administrátorů
31	nedostatečná vymahatelnost bezpečnostních pravidel a rolí
32	chybějící licenční politika pro SW

6.2 Zranitelnosti dle VKB

	Zranitelnosti dle opatření ve VKB	
id		
1	není vytvořena politika řízení přístupů	§12
2	není vytvořena politika fyzické bezpečnosti	§17
3	není zaručena mlčenlivost (NDA)	§6
4	není zajištěno oznamování zaměstnanců o nestandardním chování	§14
5	není zajištěno oznamování zaměstnanců o nestandardním chování	§14
6	není zajištěno oznamování zaměstnanců o nestandardním chování	§14
7	není vytvořena politika bezpečného používání šifrování	§26
8	není vytvořena politika bezpečného předávání a výměny informací	§10
9	není řízena komunikace uvnitř a vně perimetru	§18
10	není nasazena ochrana proti DDoS útokům	§27
11	není vytvořena politika ochrany před škodlivým kódem	§21
12	není vytvořena politika řízení technických zranitelností	§10
13	nejsou stanoveny postupy pro řízení technických zranitelností	§10
14	není zavedena centrální správa instalovaného SW	§12
15	není vytvořena politika zálohování a archivace vč. obnovy záloh	§10
16	není zajištěna redundance důležitých aktiv (server)	§27
17	není zajištěna redundance důležitých aktiv (vpn router)	§27
18	nejsou k dispozici dva nezávislé přívody elektrické energie	§27
19	není zajištěna redundance důležitých aktiv	§27
20	není nainstalován EPS a hasící systém	§17
21	nejsou aplikovány standardy opatření proti přírodním katastrofám	§17
22	nejsou nastaveny pravidla pro logování a logování není prováděno	§22
23	nejsou přijímaná opatření k odvrácení a zmírnění dopadu incidentů	§14
24	není vytvořena politika řízení lidských zdrojů	§9
25	nejsou nastavena pravidla pro používání výměnných zařízení a nosičů	§21
26	není zajištěna ochrana aplikací, informací a transakcí	§25
27	není vytvořena politika fyzické bezpečnosti	§17
8	nejsou zmapována a ošetřena rizika související s umístěním aktiv	§17
29	zaměstnanci nejsou upozorňováni na hrozby a trendy KB	§9
30	nejsou stanovena pravidla pro připojení zařízení do sítě	§10
31	není kontrolováno dodržování bezpečnostních politik	§9
32	není prováděn audit (SW) v pravidelných intervalech	§16

7 Relevantní hrozby

7.1 Obecné hrozby

Hrozby

id	
1	Neoprávněný přístup k aktivu (systému/datům)
2	Neoprávněný přístup k aktivu (systému/datům)
3	Zneužití práv – neoprávněná akce uživatelem, neautorizované použití informací
4	Zneužití práv – neoprávněná akce uživatelem, neautorizované použití informací
5	Zneužití systémových zdrojů
6	Popření akce
7	Napadení komunikace
8	Napadení komunikace
9	Přerušení komunikace
10	Kybernetický útok z vnější sítě
11	Škodlivý SW
12	Technické selhání HW
13	Technické selhání HW
14	Selhání SW
15	Selhání externí služby
16	Selhání externí služby
17	Selhání externí služby
18	Selhání napájení (elektrická energie)
19	Selhání klimatizace
20	Požár
21	Voda
22	Úmyslná chyba uživatele/administrátora
23	Neúmyslná chyba uživatele/administrátora
24	Nedostatek zaměstnanců
25	Prozrazení informací z vyřazeného aktiva
26	Ztráta aktiva
27	Krádež aktiva
28	Úmyslné poškození aktiva
29	Sociální inženýrství
30	Odposlech, sledování
31	Nedodržení bezpečnostních politik…
32	Užívání programového vybavení v rozporu s licenčními podmínkami

7.2 Popis hrozby – scénář

Popis hrozby – scénář

id	
1	Použití cizího uživatelského účtu – hádání nebo krádež přihlašovacích údajů (hesla)
2	Použití cizího uživatelského uživatele počítače po přihlášení oprávněného uživatele
3	Porušení mlčenlivosti – prozrazení důvěrných informací neoprávněným osobám
4	Úmyslná změna záznamů/informací
5	Použití techniky pro nepovolené účely (stahování/přehrávání médií, soukromé aplikace)
6	Popření provedení akce uživatelem
7	Odposlech komunikace pro získání dat – narušení důvěrnosti dat
8	Infiltrace komunikace pro změnu dat – narušení integrity dat
9	Úmyslné nebo neúmyslné fyzické přerušení komunikačních linek
10	Útok na interní zařízení z vnější sítě (DDOS, zneužití zranitelností)
11	Zavedení/spuštění škodlivého SW – z externího média, přílohy mailu apod.
12	Technické selhání HW způsobené stářím/dobrou provozu
13	Technické selhání HW způsobené nedostatečnou údržbou/monitoringem
14	Selhání SW (modrá smrt, chyba/padání SW)
15	Selhání zálohování IT
16	Selhání wmware IT (podpůrné servery MaR – Historian, WSUS, Webserver)
17	Selhání VPN přístupů (interních i externích)
18	Selhání/výpadek napájení
19	Selhání/výpadek klimatizace
20	Poškození zařízení ohněm
21	Poškození zařízení vodou (záplava/povodeň/technologická voda)
22	Úmyslná chybná manipulace, konfigurace systému
23	Neúmyslná chyba při obsluze, údržbě, opravách, změnách apod.
24	Nedostatek zaměstnanců s požadovanou odborností, nedostatečná zastupitelnost
25	Prozrazení informací z vyřazené komponenty/média/dokumentu
26	Ztráta zařízení, média, dokumentů
27	Krádež zařízení/média/dokumentu
28	Úmyslné poškozeni aktiva, vandalismus
29	Manipulace se zaměstnanci/dodavateli za účelem získání informací apod.
30	Odposlech rozhovoru, sledování obrazovky, umístění neautorizovaného HW zařízení do USB apod.
31	Nedodržování předepsaných politik
32	Užívání SW bez zajištění odpovídajících licencí

8 Vazby Hrozby – zranitelnosti

Hrozba	**Popis hrozby – scénář**
Neoprávněný přístup k aktivu (systému/datům)	Použití cizího uživatelského účtu – hádání nebo krádež přihlašovacích údajů (hesla)
Neoprávněný přístup k aktivu (systému/datům)	Použití cizího uživatelského uživatele počítače po přihlášení oprávněného uživatele
Zneužití práv – neoprávněná akce uživatelem, neautorizované použití informací	Porušení mlčenlivosti – prozrazení důvěrných informací neoprávněným osobám
Zneužití práv – neoprávněná akce uživatelem, neautorizované použití informací	Úmyslná změna záznamů/informací
Zneužití systémových zdrojů	Použití techniky pro nepovolené účely (stahování/přehrávání médií, soukromé aplikace)
Popření akce	Popření provedení akce uživatelem
Napadení komunikace	Odposlech komunikace pro získání dat – narušení důvěrnosti dat
Napadení komunikace	Infiltrace komunikace pro změnu dat – narušení integrity dat
Přerušení komunikace	Úmyslné nebo neúmyslné fyzické přerušení komunikačních linek
Kybernetický útok z vnější sítě	Útok na interní zařízení z vnější sítě (DDOS, zneužití zranitelností)
Škodlivý SW	Zavedení/spuštění škodlivého SW – z externího média, přílohy mailu apod.
Technické selhání HW	Technické selhání HW způsobené stářím/dobrou provozu
Technické selhání HW	Technické selhání HW způsobené nedostatečnou údržbou/monitoringem
Selhání SW	Selhání SW (modrá smrt, chyba/padání SW)
Selhání externí služby	Selhání zálohování IT
Selhání externí služby	Selhání wmware IT (podpůrné servery MaR – Historian, WSUS, Webserver)
Selhání externí služby	Selhání VPN přístupů (interních i externích)
Selhání napájení (elektrická energie)	Selhání/výpadek napájení
Selhání klimatizace	Selhání/výpadek klimatizace
Požár	Poškození zařízení ohněm
Voda	Poškození zařízení vodou (záplava/povodeň/technologická voda)
Úmyslná chyba uživatele/administrátora	Úmyslná chybná manipulace, konfigurace systému
Neúmyslná chyba uživatele/administrátora	Neúmyslná chyba při obsluze, údržbě, opravách, změnách apod.
Nedostatek zaměstnanců	Nedostatek zaměstnanců s požadovanou odborností, nedostatečná zastupitelnost
Prozrazení informací z vyřazeného aktiva	Prozrazení informací z vyřazené komponenty/média/dokumentu

Hrozba	Popis hrozby – scénář
Ztráta aktiva	Ztráta zařízení, média, dokumentů
Krádež aktiva	Krádež zařízení/média/dokumentu
Úmyslné poškození aktiva	Úmyslné poškozeni aktiva, vandalismus
Sociální inženýrství	Manipulace se zaměstnanci/dodavateli za účelem získání informací apod.
Odposlech, sledování	Odposlech rozhovoru, sledování obrazovky, umístění neautorizovaného HW zařízení do USB apod.
Nedodržení bezpečnostních politik…	Nedodržování předepsaných politik
Užívání programového vybavení v rozporu s licenčními podmínkami	Užívání SW bez zajištění odpovídajících licencí

OBECNÉ ZRANITELNOSTI	Zranitelnosti dle opatření ve VKB	
nevhodné nastavení přístupových oprávnění	není vytvořena politika řízení přístupů	§12
nedostatečné monitorování činnosti uživatelů	není vytvořena politika fyzické bezpečnosti	§17
neschopnost odhalit nevhodné nebo závadné způsoby chování	není zaručena mlčenlivost (NDA)	§6
neschopnost včasného odhalení pochybení ze strany zaměstnanců	není zajištěno oznamování zaměstnanců o nestandardním chování	§14
nedostatečné bezpečnostní povědomí uživatelů a administrátorů	není zajištěno oznamování zaměstnanců o nestandardním chování	§14
nedostatečné monitorování činnosti uživatelů	není zajištěno oznamování zaměstnanců o nestandardním chování	§14
nedostatečná ochrana aktiv (dat)	není vytvořena politika bezpečného používání šifrování	§26
nedostatečná ochrana aktiv (dat)	není vytvořena politika bezpečného předávání a výměny informací	§10
nevhodná bezpečnostní architektura	není řízena komunikace uvnitř a vně perimetru	§18
chybějící nebo nedostatečné řízení zranitelností	není nasazena ochrana proti DDoS útokům	§27
nedostatečná malwarová ochrana	není vytvořena politika ochrany před škodlivým kódem	§21
zastaralost informačního a komunikačního systému	není vytvořena politika řízení technických zranitelností	§10
nedostatečná údržba informačního a komunikačního systému	nejsou stanoveny postupy pro řízení technických zranitelností	§10
nedostatečná SW údržba (patch management)	není zavedena centrální správa instalovaného SW	§12
chybějící nebo nedostatečná strategie zálohování a archivace dat	není vytvořena politika zálohování a archivace vč. obnovy záloh	§10
chybějící nebo nedostatečné řízení kontinuity činnosti organizace	není zajištěna redundance důležitých aktiv (server)	§27
nedostatečná ochrana vnějšího perimetru	není zajištěna redundance důležitých aktiv (vpn router)	§27

nedostatečná údržba podpůrných aktiv	nejsou k dispozici dva nezávislé přívody elektrické energie	§27
nedostatečná údržba podpůrných aktiv	není zajištěna redundance důležitých aktiv	§27
nedostatečná ochrana aktiv	není nainstalován EPS a hasící systém	§17
nedostatečná ochrana aktiv	nejsou aplikovány standardy opatření proti přírodním katastrofám	§17
nedostatečná míra nezávislé kontroly	nejsou nastaveny pravidla pro logování a logování není prováděno	§22
nedostatečné bezpečnostní povědomí uživatelů a administrátorů	nejsou přijímaná opatření k odvrácení a zmírnění dopadu incidentů	§14
chybějící nebo nedostatečné řízení kontinuity činnosti organizace	není vytvořena politika řízení lidských zdrojů	§9
nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů	nejsou nastavena pravidla pro používání výměnných zařízení a nosičů	§21
nedostatečná ochrana aktiv	není zajištěna ochrana aplikací, informací a transakcí	§25
nedostatečná ochrana aktiv	není vytvořena politika fyzické bezpečnosti	§17
nedostatečná ochrana aktiv	nejsou zmapována a ošetřena rizika související s umístěním aktiv	§17
nedostatečné bezpečnostní povědomí uživatelů a administrátorů	zaměstnanci nejsou upozorňováni na hrozby a trendy KB	§9
nedostatečné bezpečnostní povědomí uživatelů a administrátorů	nejsou stanovena pravidla pro připojení zařízení do sítě	§10
nedostatečná vymahatelnost bezpečnostních pravidel a rolí	není kontrolováno dodržování bezpečnostních politik	§9
chybějící licenční politika pro SW	není prováděn audit (SW) v pravidelných intervalech	§16

9 Checklist opatření dle VKB – GAP analýza

ID	VKB		Aplikováno		
			ano	částečně	ne
01	§3	Je vytvořena politika řízení IB			
02	§3	Je stanoven rozsah ISMS			
03	§3	Je schválena a aktualizována bezpečnostní politika			
04	§3	Je prováděno pravidelné vyhodnocování			
05	§4	Je vytvořena politika aktiv			
06	§4	Probíhá identifikace a hodnocení aktiv			
07	§4	Je vytvořena politika ochrany osobních údajů			
08	§4	Jsou určeni garanti aktiv			
09	§5	Je vytvořena politika řízení rizik			
10	§5	Probíhá identifikace a hodnocení rizik			
11	§5	Je prováděno v pravidelných intervalech			
12	§5	Jsou zaváděná bezpečnostní opatření v souladu s RTP			
13	§6	Je vytvořena politika organizační bezpečnosti			
14	§6	Je kybernetická bezpečnost součástí procesů organizace			
15	§6	Jsou zajištěny dostatečné zdroje na KB			
16	§6	Je zaručena mlčenlivost (NDA) adminů a bezpečnostních rolí			
17	§6	Jsou přiděleny dostatečné pravomoci			
18	§6	Je zastupitelnost bezpečnostních rolí			
19	§6	Je určen výbor KB, ustanoven a funkční			
20	§7	Je určen manažer KB			
21	§7	Je určen architekt KB			
22	§7	Je určen auditor KB			
23	§8	Je vytvořena politika řízení dodavatelů			
24	§8	Jsou evidování významní dodavatelé a informováni o KB			
25	§8	Jsou dodavatelé seznamováni s bezpečnostními pravidly			
26	§8	Je v SLA s dodavateli zohledněn výběr bezpečnostních opatření			
27	§8	Probíhá předsmluvní hodnocení rizik			
28	§8	Je určena smluvní odpovědnost za vedení a kontrolu bezp. opatření			
29	§8	Je reagováno na nedostatky při řízení dodavatelů			
30	§8	Jsou nahlášeny dle §34 aktuální kontaktní údaje			
31	§9	Je vytvořena politika řízení lidských zdrojů			
32	§9	Jsou prováděna školení adminů, uživatelů a bezpečnostních rolí			
33	§9	Je vytvořena politika bezpečného chování uživatelů			
34	§9	Účastní se bezpečnostní role školení dle SAE			
35	§9	Je kontrolováno dodržování bezpečnostních politik			
36	§9	Je zajištěno předání odpovědností při ukončení smluvního vztahu			
37	§9	Jsou zaměstnanci upozorňováni na hrozby a trendy KB			
38	§10	Je vytvořena politika řízení provozu a komunikací			
39	§10	Je vytvořena politika zálohování a archivace vč. obnovy záloh			
40	§10	Je vytvořena politika bezpečného předávání a výměny informací			
41	§10	Je vytvořena politika řízení technických zranitelností			

ID	VKB		Aplikováno		
			ano	částečně	ne
42	§10	Je vytvořena politika bezpečného používání mobilních zařízení			
43	§10	Jsou stanoveny postupy pro řízení technických zranitelností			
44	§10	Jsou stanovena pravidla pro připojení zařízení do sítě			
45	§11	Je vytvořena politika řízení změn a významných změn			
46	§11	Jsou přezkoumávány dopady změn			
47	§11	Je řízen proces změny včetně testování			
48	§11	Je prováděno penetrační testování a skenování zranitelností			
49	§12	Je vytvořena politika řízení přístupů			
50	§12	Je přístup řízen na základě skupin a rolí			
51	§12	Jsou uživatelům a adminům přidělována jedinečná ID			
52	§12	Jsou řízeny ID, přístupová práva a oprávnění			
53	§12	Je zavedena centrální správa mobilních zařízení			
54	§12	Dochází ke změně nebo odebrání přístupových oprávněni			
55	§12	Jsou stanovena pravidla a postupy pro používání BYOD			
56	§12	Je zaveden princip need-to-know			
57	§12	Je zaveden princip minimálních oprávnění			
58	§12	Je zavedena centrální správa instalovaného SW			
59	§12	Probíhají revize přidělených oprávnění			
60	§13	Je vytvořena politika akvizice vývoje a údržby			
61	§13	Jsou stanoveny bezpečnostní požadavky na vývoj a údržbu			
62	§13	Je zajištěno oddělení vývoje, provozu a testování			
63	§14	Jsou vytvořeny politiky nástroje pro detekci kybernetické události			
64	§14	Je zajištěno oznamování zaměstnanců o nestandardním chování			
65	§14	Jsou incidenty posuzovány a kategorizovány			
66	§14	Jsou přijímaná opatření k odvrácení a zmírnění dopadu incidentů			
67	§14	Jsou incidenty řádně hlášeny			
68	§14	Jsou vedeny záznamy o incidentech a jejich zvládání			
69	§15	Je vytvořena politika kontinuity činností			
70	§15	Je zpracována dopadová analýza			
71	§15	Je zajištěno pravidelné testování havarijních plánů a kontinuity			
72	§16	Je prováděn audit v pravidelných intervalech			
73	§16	Je stanoven proces a plán provádění auditů			
74	§16	Jsou zpracovány zprávy z auditu			
75	§16	Existují záznamy o provedených auditech, kontrolách a přezkumu			
76	§16	Jsou výsledky přezkumů a auditu zohledněny v plánování			
77	§17	Je vytvořena politika fyzické bezpečnosti			
78	§17	Je vymezen a chráněn fyzický perimetr			
79	§17	Je zabezpečen fyzický perimetr (EZS, EPS, CCTV,)			
80	§17	Je nainstalována EPS a hasící systém			
81	§17	Jsou prostory chráněny mechanickými zábranami			
82	§17	Je nainstalována detekce pohybu a průniku (EZS)			
83	§17	Je používán a kontrolován systém pro kontrolu vstupu			

ID	VKB		Aplikováno		
			ano	částečně	ne
84	§17	Jsou aktiva chráněna kamerovými systémy s ukládáním			
85	§17	Je používáno nošení identifikačního prvku			
86	§17	Je prováděna identifikace osob na vstupu			
87	§17	Jsou zařízení zabezpečena při krátkodobém opuštění pracoviště			
88	§17	Jsou důležitá aktiva zavírána při dlouhodobé nepřítomnosti do trezoru			
89	§17	Jsou zmapována a ošetřena rizika související s umístěním aktiv			
90	§17	Jsou aplikovány standardy opatření proti přírodním katastrofám			
91	§17	Je vedena evidence přístupů do zabezpečených prostor			
92	§17	Je zaveden klíčový režim s fyzickými klíči			
93	§18	Je vytvořena politika bezpečnosti komunikačních sítí			
94	§18	Je provedena segmentace sítě			
95	§18	Je řízena komunikace uvnitř a vně perimetru sítě			
96	§18	Je zřízena VPN pro vzdálený přístup			
97	§18	Dochází k aktivní blokaci nežádoucí komunikace			
98	§18	Je řízena komunikace mezi jednotlivými segmenty sítě			
99	§19	Je implementován nástroj pro ověření identity uživatele			
100	§19	Je zavedena dvoufaktorová autentizace (2FA)			
101	§19	Je používán nástroj pro ověření identity pomocí šifrovacích klíčů			
102	§19	Jsou autentizační údaje chráněny (šifrování, hash)			
103	§19	Je vynucována změna prvotních a obnovovacích hesel			
104	§20	Je nastaven proces bezpečného přístupu dodavatelů do sítě			
105	§20	Je zavedeno oddělení admin a uživatelských oprávnění			
106	§20	Je zavedeno centralizované řízení přístupových oprávnění (ACL)			
107	§21	Je vytvořena politika ochrany před škodlivým kódem			
108	§21	Je antivirová ochrana nasazena na důležitých aktivech			
109	§21	Jsou nastavena pravidla pro používání výměnných zařízení a nosičů			
110	§21	Je antivirová ochrana pravidelně aktualizována			
111	§21	Jsou prováděny pravidelné antivirové testy záloh			
112	§21	Je řízeno oprávnění ke spouštění kódu			
113	§22	Jsou nastaveny pravidla pro logování a je logování prováděno			
114	§22	Jsou logy zabezpečeně uchovávány			
115	§22	Je prováděna synchronizace jednotného času min. 1x za 24 hodin			
116	§23	Jsou nastavena pravidla pro detekci KBU (IDS, IPS.)			
117	§24	Je využíván log management			
118	§24	Je využíván SIEM			
119	§24	Jsou nástroje pro KBI ošetřeny personálními kapacitami			
120	§25	Jsou prováděny penetrační testy před uvedením aktiv do provozu			
121	§25	Je zajištěna ochrana aplikací, informací a transakcí			
122	§26	Je vytvořena politika bezpečného používání šifrování			
123	§26	Jsou používány odolné algoritmy dle NÚKIB			
124	§26	Je využíván systém pro správu klíčů a certifikátů			
125	§27	Je nasazena ochrana proti DDoS útokům			

ID	VKB		Aplikováno		
			ano	částečně	ne
126	§27	Je internetová konektivita zajištěna od dvou různých poskytovatelů			
127	§27	Jsou k dispozici dva nezávislé přívody elektrické energie			
128	§27	Je k dispozici alternativní zdroj napájení (UPS, MG)			
129	§27	Je nainstalována přepěťová ochrana			
130	§27	Je zajištěna redundance důležitých aktiv			
131	§28	Je v organizaci nasazen SCADA IS (ICS prostředí)			
132	§33	Jsou plněna reaktivní opatření dle NÚKIB			
133		Je nasazeno řešení DLP			

10 Vzory bezpečnostních směrnic

Příklady relevantních směrnic jsou uspořádány do následujícího řazení:

11 Rejstřík pojmů a zkratek

APT Advanced Persistent Threat
Pokročilá trvalá hrozba

ASM Attack Surface Management
Správa povrchu útoků (ASM) je nepřetržité monitorování, náprava a snižování všech bezpečnostních rizik v rámci útočného povrchu organizace.

AV Antivirus
Antivirus je zjednodušené označení bezpečnostního programu, který vyhledává, detekuje, blokuje a odstraňuje kybernetické hrozby

BEC Business Email Compromise
Ohrožení zabezpečení podnikových e-mailů (BEC) je typ kybernetické trestné činnosti, kdy podvodník pomocí e-mailu někoho oklame tak, aby odeslal peníze nebo vyzradil důvěrné firemní informace.

BCM Business Continuity Management
Řízení kontinuity organizace

BCP Business Continuity Planning
Plánování kontinuity činnosti

BIA Business impact analysis
Analýza dopadů na činnosti organizace

CERT Computer Emergency Response Team
Skupina pro reakci na kybernetické hrozby

CIA Confidentiality, Integrity and Availability
Důvěrnost, integrita a dostupnost (bezpečnostní triáda ISMS)

CIO Chief Information Officer
Vedoucí oddělení IT

CISO Chief Information Security Officer
Manažer informační bezpečnosti

CSA Cybersecurity Awareness
CSA je princip budování povědomí o kybernetické bezpečnosti.

CSF Cybersecurity Framework
CSF je soubor pokynů pro zmírnění rizik kybernetické bezpečnosti organizací, který vydal americký Národní institut pro standardy a technologie (NIST) na základě stávajících norem, doporučení a postupů.

CSIRT Cyber Security Incident Response Team
Skupina pro reakci na kybernetické bezpečnostní incidenty

Spolufinancováno Evropskou unií
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
jihomoravský kraj

CVE Common Vulnerability and Exposure
Systém CVE představuje referenční metodu pro veřejně známé zranitelnosti a odhalení v oblasti informační bezpečnosti.

DR Diaster Recovery
Obnova po havárii

ECSF European Cybersecurity Skills Framework
ECSF je praktický nástroj na podporu identifikace a vyjádření úkolů, kompetencí, dovedností a znalostí spojených s rolemi evropských odborníků v oblasti kybernetické bezpečnosti.

ENISA The European Union Agency for Cybersecurity
Agentura Evropské unie pro kybernetickou bezpečnost ENISA je agenturou Unie, jejímž úkolem je dosáhnout vysoké společné úrovně kybernetické bezpečnosti v celé Evropě.

GRC Governance, Risk and Compliance
Kontrola, rizika a dodržování předpisů GRC je oblast procesů a manažerských aktivit, jejímž cílem je zajištění souladu všech aktivit organizace napříč kontrolou, řízením rizik a shodou s legislativou, standardy nebo dalšími požadavky.

IAM Identity and Access Management
Je řešení zajišťující autentizaci, autorizaci a SSO (Single Sign On) uživatelů.

IoC Indicators of Compromise
Indikátory kompromitace slouží k identifikaci kompromitovaného zařízení.

ICT Information and Communication Technology

ISO International Organization for Standardization
Mezinárodní organizace pro normalizaci

IT Information Technology

MFA Multi-Factor Authentication
Je způsob ověření uživatele při autentizaci vůči systému nebo službě vícero na sobě nezávislými faktory.

NIS2 Network and Information Security 2
Je celoevropská směrnice o kybernetické bezpečnosti, tedy bezpečnosti informačních systémů, počítačových sítí, aplikací, software a informací.

NIST National Institute of Standards and Technology
Národní institut standardů a technologie NIST je laboratoř měřicích standardů při ministerstvu obchodu USA.

NÚKIB Národní úřad pro kybernetickou a informační bezpečnost

PII	Personally Identifiable Information Osobně identifikovatelné informace (údaje)
PoC	Proof of Concept Proof of Concept je termín používaný v mnoha oborech, včetně IT a software vývoje, kde se jedná o realizaci určité metody nebo myšlenky, aby se prokázala jeho proveditelnost
RPO	Recovery Point Objective Bod obnovy dat
RTO	Recovery Time Objective Doba obnovy činnosti
SAE	Security Awareness and Education SAE je metodika budování bezpečnostního povědomí v organizaci.
SOC	Security Operations Center SOC je bezpečnostní dohledové centrum kybernetické bezpečnosti, které zajišťuje služby detekování a eliminaci aktivit kyberútočníků dřív, než ohrozí data, informace, finance a pověst organizace.
TI	Threat Intelligence Cyber threat intelligence je proces sběru, analýzy a využití informací o kybernetických hrozbách.
VKB	Vyhláška o kybernetické bezpečnosti
VM	Vulnerability Management Řízení zranitelností je neustálý proces identifikace a vyhodnocování zranitelností napříč operačními systémy, aplikační software a síťovými zařízeními.
VPN	Virtual Private Network Vrtuální privátní síť je technologie umožňující vytvoření zabezpečeného a šifrovaného spojení mezi zařízením uživatele a vzdáleným serverem.
WAF	Web Application Firewall WAF poskytuje centralizovanou ochranu webových aplikací před běžným zneužitím a ohrožením zabezpečení.
ZKB	Zákon o kybernetické bezpečnosti

12 Použité zdroje

Seznam použitých zdrojů pro tento dokument je v následujícím členění:

12.1 Normy

ČSN EN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky, 2023. [Praha]: Česká agentura pro standardizaci.

ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti, 2023. [Praha]: Česká agentura pro standardizaci.

ČSN ISO/IEC 27003 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny, 2018. [Praha]: Česká agentura pro standardizaci.

ČSN ISO/IEC 27005 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Pokyny pro management rizik informační bezpečnosti, 2023. [Praha]: Česká agentura pro standardizaci.

NIST SP 800-50. Computer Security: Building an Information Technology Security Awareness and Training Program, 2023. [Gaithersburg]: National Institute of Standards and Technology.

NIST SP 800-16. Information Security: A Role-Based Model for Federal Information Technology/ Cyber Security Training, 2013. [Gaithersburg]: National Institute of Standards and Technology.

12.2 Publikace

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2019. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing. ISBN isbn978-80-88260-39-4.

SEDLÁK, Petr a KONEČNÝ, Martin, 2023. Přeměna ISMS v manažerské informatice. Brno: CERM, akademické nakladatelství. ISBN 978-80-7623-110-8.

SEDLÁK, Petr a KONEČNÝ, Martin, 2021. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, akademické nakladatelství. ISBN 978-80-7623-068-2.

SEDLÁK, Petr a KONEČNÝ, Martin, 2024. Případové studie řízení kybernetické bezpečnosti. Brno: CERM, akademické nakladatelství.

12.3 Doporučení NÚKIB (www.nukib.cz)

Minimální bezpečnostní standard v 1.2 - podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti

Bezpečně v kyber! - brožura kurzu pro učitele a ředitele škol

Profil učitele střední školy

Profil žáka střední školy

12.4 Podpůrné materiály

ENISA, 2022. ECSF – European Cybersecurity Skills Framework. ISBN 978-92-9204-584-5.

ENISA, 2022. User Manual - European Cybersecurity Skills Framework (ECSF). ISBN 978-92-9204-583-8.

TEHRAIK Sonali, 2022. Cybersecurity in school education.

NIC-WCD, 2021. Cyber Security Awareness.