ICT koordinátor – studium k výkonu specializované činnosti

Zabezpečení informačních technologií ve škole

Závěrečná práce

Mgr. Jiří Hablawetz

Ostrava

2024

Prohlášení

Prohlašuji, že předložená závěrečná práce je mým původním autorským dílem, které jsem vypracoval/a samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal/a, v práci cituji a jsou uvedeny v seznamu použité literatury.

V Ostravě – Koblově, dne 29. 10. 2024

Mgr. Jiří Hablawetz

Anotace

Dokument závěrečná práce s názvem Zabezpečení informačních technologií ve škole se zabývá důležitostí implementace technologických řešení, procesů a osvědčených postupů pro kybernetickou bezpečnost ve školním prostředí. Upozorňuje na vytváření a provádění efektivních bezpečnostních politik, stanovení jasných bezpečnostních cílů, definování odpovědností a vytváření plánů reakce na incidenty. Zdůrazňuje význam školení zaměstnanců a studentů v oblasti povědomí o kybernetické bezpečnosti a potřebu škol vytvářet a provádět školicí programy. Prozkoumává technická opatření a software pro zvýšení kybernetické bezpečnosti, s důrazem na výběr a implementaci řešení odpovídajících potřebám a rozpočtu školy. Monitorování a reagování na bezpečnostní incidenty je klíčové pro rychlou detekci a řešení. Nakonec se dokument zabývá procesem auditu a revize bezpečnostních procedur a politik, zdůrazňuje potřebu škol pravidelně hodnotit a aktualizovat své bezpečnostní strategie, aby odpovídaly nejnovějším hrozbám a nejlepším postupům.

Seznam klíčových slov abecedně:

- Audit
- Bezpečnostní incidenty
- Bezpečnostní politika
- Kybernetická bezpečnost
- Opatření
- Osvěta
- Plán reakce na incidenty
- Procesy
- Školení
- Technologická řešení
- Zabezpečení dat

Obsah

Úvod:

Zvolil jsem si téma Zabezpečení informačních technologií ve škole kvůli rostoucímu množství kybernetických útoků na počítače a IT systémy po celém světě. Školy se často stávají terčem útoků kvůli slabšímu zabezpečení a velkému množství citlivých údajů, které spravují.

Mým cílem je vytvořit ucelený plán, jak zvýšit úroveň zabezpečení ICT technologií ve škole a zároveň podpořit osvětu mezi žáky a pedagogy. To zahrnuje prevenci, identifikaci zranitelných míst a návrh konkrétních opatření.

Chci se zaměřit na:

1. **Technická opatření**: Zlepšení firewallů, antivirových programů a ochrany sítě.
2. **Organizační opatření**: Pravidelné školení pedagogů i žáků v oblasti kybernetické bezpečnosti.
3. **Právní aspekty**: Zajištění souladu s GDPR a legislativou týkající se školních dat.
4. **Přístupy pro zajištění kontinuity výuky**: Zavedení zálohovacích systémů, obnovení dat při výpadcích a ochrana cloudových úložišť.

1. Kapitola: Digitální technologie a kybernetická bezpečnost ve vzdělávání

1.1. Úvod do digitálních technologií ve vzdělávání

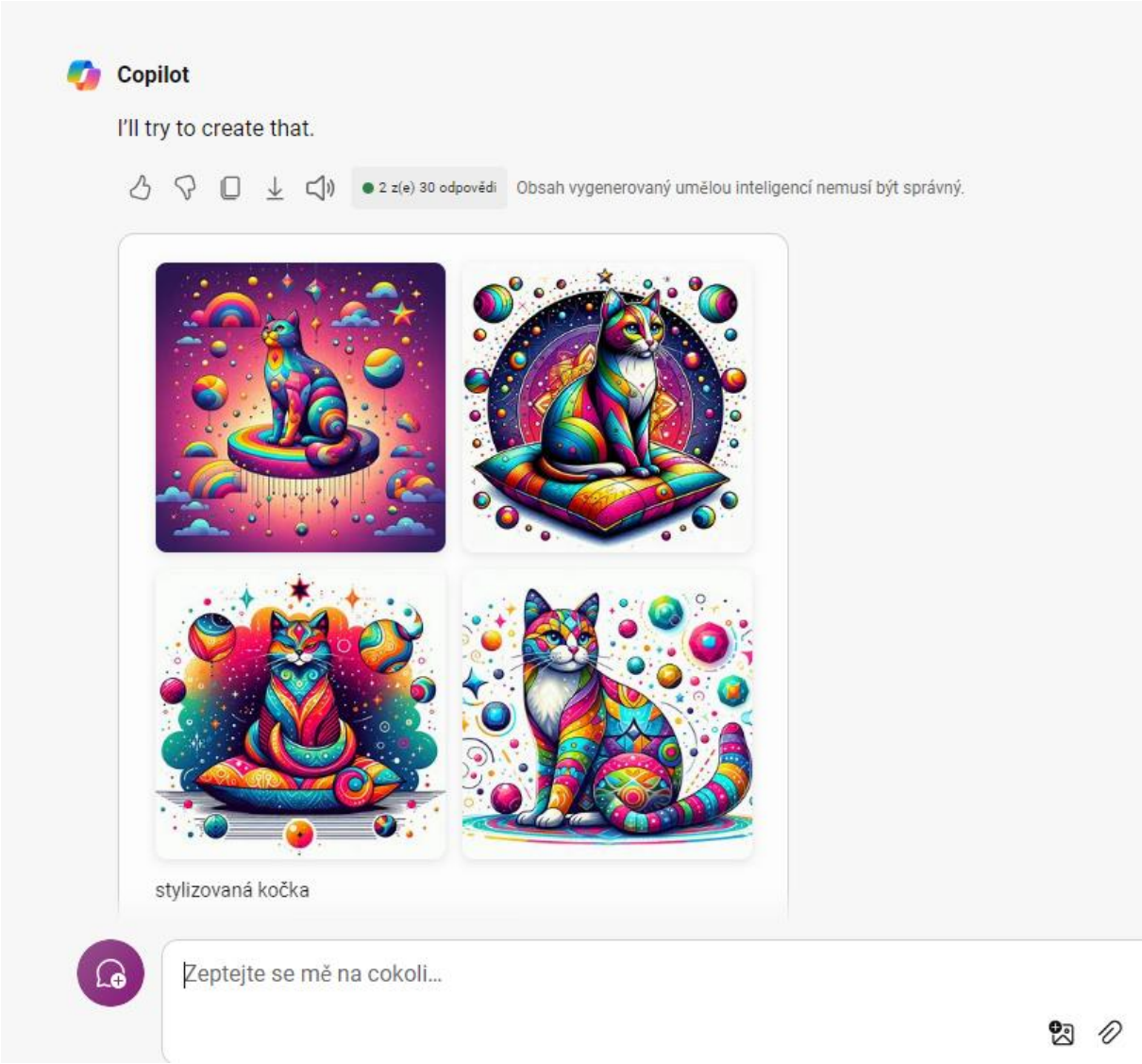
V úvodu kapitoly se zaměříme na základní principy a definice digitálních technologií a jejich roli ve vzdělávacím procesu. Představíme, jak digitální nástroje transformují tradiční učební metody a jaký mají dopad na pedagogiku. Diskutujeme o tom, jak se digitální dovednosti staly nezbytnou součástí vzdělávacích cílů a jak vzdělávací instituce integrují technologie do svých programů.

1.2. Historický vývoj a současný stav digitálních technologií

V této části se podrobněji zaměříme na historii a vývoj digitálních technologií a jejich vliv na vzdělávací prostředí. Od prvních počítačů, které vstoupily do tříd, až po dnešní sofistikované online vzdělávací platformy, digitální technologie prošly dlouhou cestou.

- **Počátky digitálních technologií ve vzdělávání** Historie digitálních technologií ve vzdělávání sahá až do 60. let 20. století, kdy byly počítače poprvé zavedeny do školních tříd. Tyto rané počítače byly velké, drahé a obtížně přístupné, ale přesto položily základ pro budoucí integraci technologie do vzdělávání.
- **Éra osobních počítačů** V 80. letech přinesla éra osobních počítačů revoluci ve vzdělávání. Počítače se staly dostupnějšími a začaly se objevovat v domácnostech i školách. Software pro vzdělávání, jako jsou interaktivní vzdělávací hry a programy, začal měnit způsob, jakým studenti učí a učitelé vyučují.
- **Internet a online vzdělávání** 90. léta přinesla internet a s ním novou éru informací a komunikace. Školy začaly využívat internet pro výzkum a jako zdroj materiálů. Vznik online vzdělávacích kurzů a materiálů umožnil studentům učit se nezávisle na čase a místě.
- **Interaktivní a mobilní technologie** S příchodem nového tisíciletí se objevily interaktivní tabule a mobilní technologie, které dále rozšířily možnosti vzdělávání. Tablety a chytré telefony umožnily studentům přístup k vzdělávacím aplikacím a zdrojům odkudkoliv. Ve škole využíváme při výuce interaktivní velkou dotykovou tabuli v jazykové učebně. Vzdělávací materiály v mobilní aplikaci školního informačního systému Bakaláři jsou k dispozici kdykoliv a kdekoliv našim žákům.
- **Současný stav a trendy** Dnes jsou digitální technologie neodmyslitelnou součástí vzdělávacího procesu. Online vzdělávací platformy, jako je Khan Academy nebo Coursera, nabízejí širokou škálu kurzů pro studenty všech věkových kategorií. Virtuální a rozšířená realita přináší nové způsoby interakce a učení. Umělá inteligence a personalizované učení se stávají stale běžnějšími a otevírají dveře k novým metodám vzdělávání.

- Aktuálně pedagogové ve škole začínají využívat různých nástrojů umělé inteligence AI jako Chat GPT, Google Gemini, Microsoft Copilot.



Obrázek 1 - Generativní AI Microsoft Copilot

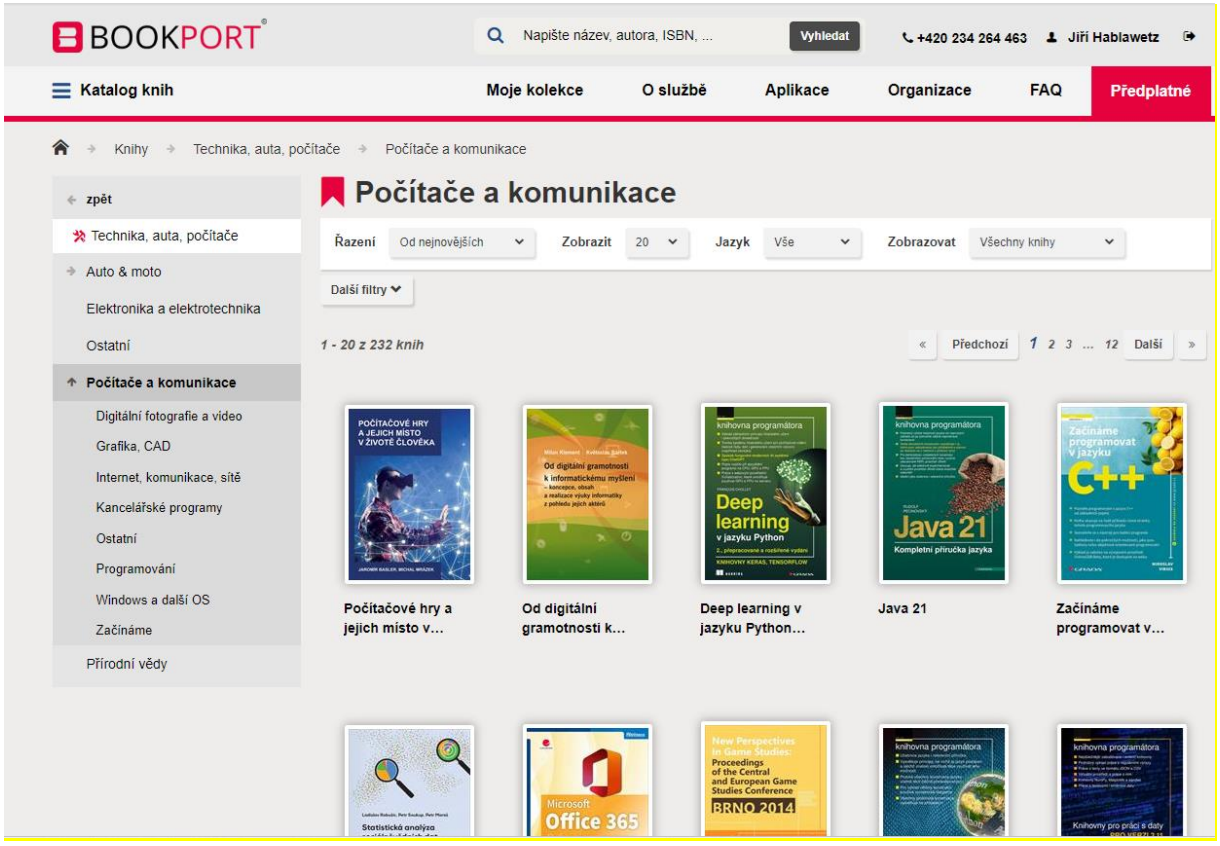
- **Výzvy a budoucí směřování** Přestože digitální technologie nabízejí mnoho výhod, přinášejí také výzvy, jako je potřeba zabezpečení dat a ochrana soukromí. Budoucí směřování bude zahrnovat nejen integraci nových technologií do vzdělávacích systémů, ale také zajištění, aby tyto technologie byly přístupné a bezpečné pro všechny studenty.

1.3. Význam digitálních technologií pro moderní vzdělávací procesy

Zde se zaměříme na to, jak digitální technologie obohacují vzdělávací procesy a jak přispívají k rozvoji nových forem učení. Diskutujeme o tom, jak technologie umožňují personalizované a adaptivní učení a jak podporují rozvoj kritického myšlení a kreativity.

Přizpůsobení vzdělávání individuálním potřebám Digitální technologie umožňují vytváření personalizovaných učebních plánů, které respektují individuální tempo a styl učení každého studenta. S pomocí adaptivního softwaru mohou studenti pracovat na úkolech, které jsou přizpůsobeny jejich konkrétním schopnostem a potřebám, což vede k efektivnějšímu a smysluplnějšímu učení. Každý student se může individuálně vracet k předchozím kapitolám v rámci učebních platforem jako je např. kurzy na moodle. Kolegové vyučující ve škole využívají platformu moodle pro vytváření kurzů jednotlivých předmětů jako psychologie, ošetřovatelství apod. V rámci kurzu moodle mají studenti k dispozici různé učební formy jako videa, prezentace, testy…

- **Zvýšení zapojení a motivace** Interaktivní nástroje a multimediální obsah, které digitální technologie nabízejí, mohou zvýšit zapojení studentů tím, že učiní učební materiál více vizuálně atraktivním a interaktivním. Hry, simulace a virtuální realita mohou učinit učení zábavnějším a zároveň podporovat hlubší porozumění učivu. Vizuální podoba prezentací, grafika aj. interaktivní prvky vytvořené umělou inteligencí mohou zvýšit zájem studentů o studium předmětu. Kolegové využívají např. možnosti Canvy.
- **Rozvoj digitální gramotnosti** V dnešním digitálně propojeném světě je digitální gramotnost nezbytnou dovedností pro osobní i profesní život. Školy využívají digitální technologie k výuce programování, bezpečného používání internetu a kritického hodnocení online informací, což připravuje studenty na budoucí výzvy. V předmětu matematika si studenti mohou např. zkontrolovat výsledek zadaného příkladu pomocí aplikace Photomath.
- **Podpora spolupráce a komunikace** Digitální technologie usnadňují spolupráci mezi studenty, ať už jsou kdekoli. Online nástroje jako jsou diskusní fóra, sdílené dokumenty a komunikační platformy umožňují studentům pracovat společně na projektech a sdílet myšlenky, což podporuje rozvoj komunikačních dovedností a týmové práce. Studenti se zúčastňují různých projektů, kde spolupracují na různých školních projektech jako je Prezentiáda, laboratorní konference.
- **Přístup k širokému spektru zdrojů** Internet a digitální knihovny poskytují studentům přístup k obrovskému množství informací a vzdělávacích zdrojů. To umožňuje studentům prozkoumat různá témata a získat hlubší porozumění předmětům, které je zajímají. Studenti mají možnost využívat digitální zdroje jako je např. digitální knihovna Bookport.cz, učební materiály v škol. systému Bakaláři.



Obrázek 2 - digitální knihovna Bookport

- **Flexibilita a dostupnost vzdělávání** Digitální technologie umožňují studentům učit se kdykoliv a kdekoliv, což je zvláště důležité pro distanční vzdělávání a pro ty, kteří nemohou navštěvovat tradiční výukové instituce. Online kurzy a vzdělávací programy nabízejí flexibilní možnosti pro pokračování ve vzdělávání bez ohledu na geografickou polohu nebo časová omezení. Časovou flexibilitu nabízejí právě nástroje jako Bookport, platforma moodle AGEL SZŠ Ostrava.
- **Příprava na budoucí kariéru** Vzhledem k tomu, že digitální dovednosti jsou stále více vyžadovány na pracovním trhu, školy hrají klíčovou roli v přípravě studentů na budoucí kariéru. Vzdělávací programy, které zahrnují práci s digitálními nástroji a technologiemi, pomáhají studentům získat dovednosti potřebné pro úspěch v různých oborech. Praxi např. v ošetřovatelství si naši studenti mohou nacvičit pomocí 3D brýlí s virtuální realitou.

1.4. Přehled hlavních výhod digitálních technologií ve vzdělávání

Digitální technologie přinášejí do vzdělávacího procesu řadu výhod, které mohou zásadně ovlivnit způsob, jakým studenti učí a učitelé vyučují. Zde je podrobný přehled některých z nejvýznamnějších výhod:

- **Zvýšení zapojení studentů**
- **Interaktivní učení:** Digitální technologie, jako jsou interaktivní tabule a vzdělávací aplikace, zvyšují zapojení studentů tím, že učební proces činí více interaktivním a vizuálně atraktivním. Studenti využívají velkoplošnou interaktivní dotykovou tabuli při výuce.
- **Herní prvky ve vzdělávání (gamifikace):** Využití herních prvků může učení proměnit v zábavnou aktivitu, což může vést k lepší motivaci a zapamatování učiva. Vyučující někdy využívají aplikaci Kahoot pro lepší motivaci k učení u žáků.
- **Personalizace vzdělávání**
- **Adaptivní učební platformy:** Tyto platformy umožňují přizpůsobit učební obsah a tempo individuálním potřebám každého studenta, což podporuje efektivnější učení.
- **Zpětná vazba v reálném čase:** Učitelé mohou využívat technologie pro poskytování okamžité zpětné vazby, což studentům pomáhá rychleji pochopit a opravit své chyby.
- **Přístup k rozmanitým zdrojům informací**
- **Digitální knihovny a databáze:** Studenti mají díky internetu přístup k širokému spektru knih, článků a vzdělávacích videí, což rozšiřuje jejich možnosti pro výzkum a učení. Škola využívá online knihovnu Bookport.cz.
- **Online kurzy a workshopy:** Možnost vzdělávat se online od expertů z celého světa nabízí studentům unikátní příležitosti pro rozvoj a specializaci. Ve škole často probíhají projekty jako např. Konference laborantů, soutěže v První pomoci, projekt Agel School Awards.
- **Flexibilita a dostupnost**
- **Distanční vzdělávání:** Studenti, kteří nemohou fyzicky navštěvovat výukové instituce, mohou využívat online kurzy a programy, což zajišťuje větší dostupnost vzdělání. V případě potřeby mohou studenti využívat platformou MS Teams pro distanční výuku.
- **Asynchronní učení:** Možnost učit se podle vlastního časového rozvrhu umožňuje studentům lépe sladit studium s osobním životem a pracovními povinnostmi.
- **Rozvoj digitální gramotnosti a příprava na budoucí kariéru**

- **Důraz na IT dovednosti:** Vzhledem k tomu, že digitální dovednosti jsou stále více vyžadovány na trhu práce, vzdělávací systémy, které začleňují výuku těchto dovedností, lépe připravují studenty na budoucí zaměstnání. Sociálně znevýhodněným žákům škola zapůjčila notebooky z projektu Digitální propast.
- **Inovativní a technologické kurzy:** Kurzy zaměřené na programování, data science, umělou inteligenci a další technologické obory jsou stále dostupnější a poskytují studentům potřebné znalosti pro technologicky orientované kariéry.
- **Podpora inkluzivního vzdělávání**
- **Nástroje pro studenty se speciálními vzdělávacími potřebami:** Technologie, jako jsou čtecí programy nebo aplikace pro komunikaci, umožňují studentům se speciálními potřebami lépe se zapojit do vzdělávacího procesu.
- **Jazykové nástroje**: Digitální překladače a jazykové aplikace pomáhají studentům, kteří se učí cizí jazyk nebo jsou méně zběhlí v jazyce vyučování.
- **Zlepšení administrativní efektivity**
- **Správa školních systémů:** Digitální nástroje pro správu škol zjednodušují administrativní procesy, jako je sledování docházky, hodnocení a komunikace s rodiči. Škola využívá školní informační systém Bakaláři, který výrazně usnadňuje komunikaci s rodiči a žáky. Pro správu kurzů Sanitář, Ošetřovatel využívá škola platformu Edupage.com.

1.5. Diskuse o výzvách a nerovnostech přístupu k digitálním technologiím

Zde se zaměříme na výzvy spojené s implementací digitálních technologií, jako jsou otázky rovnosti přístupu a digitální propasti. Diskutujeme o tom, jak tyto výzvy ovlivňují různé demografické skupiny a jaké kroky mohou školy podniknout k jejich překonání.

1.6. Analýza rizik a kybernetických hrozeb ve vzdělávacím prostředí

V této části se zaměříme na potenciální rizika a hrozby, které přináší využívání digitálních technologií ve školách, včetně kybernetických útoků, zneužití dat a porušování soukromí. Probereme, jak mohou školy identifikovat a řešit tyto hrozby. Ve škole jsme řešili případ kyberšikany zobrazení vulgárních komentářů na příspěvcích na oficiálním profilu školy na sociálních sítích. Proto pravidelně školíme žáky na kyberšikanu.

1.7. Důležitost kybernetické bezpečnosti ve školách

Zde zdůrazníme, proč je kybernetická bezpečnost klíčová pro ochranu studentů a školních informačních systémů. Probereme, jaké kroky mohou školy podniknout k zajištění bezpečného využívání digitálních technologií.

Pravidelně provádíme údržbu na škol. stolních počítačích, kdy mažeme staré uživatelské profily studentů, které pak zabírají hodně místa na systém. disku OS Windows 10. Zvýší se tak výkon počítače a uvolní volné místo pro ukládání dat. Na všech škol. počítačích a NTB je nastaveno šifrování disku pomocí nástroje Bitlocker. Veškeré detekce škodlivého software a souborů AV software Eset jsou monitorovány a zasílány AGEL IT bezpečnostnímu týmu k prověření. Veškerá data ve složce dokumenty uživatelů žáků i pedagogů jsou pravidelně zálohovány na AGEL serveru. Mnoho problémů s ICT technikou uživatelů pedagogů jsme schopni vyřešit rychle přes vzdálený nástroj TeamViewer.

Na škole jsme nainstalovali další kopírku Konica Minolta pro studenty, kdy studenti si mohou tisknout soubory ze škol. počítače přes ISIC student. karty. Dávka se vytiskne na tiskárně až po ověření uživatele přes ISIC kartu z důvodu bezpečnosti.

Pro přístup do školy využívají žáci student. karty ISIC navedené do docházkového systému ID-Karta. Vyučující využívají pro vstup učitel. TTIC karty. Přístup do školy je tak dobře zabezpečen a je pořád přehled o žácích i vyučujících v budově.

Vstup do budovy školy a hlavní chodba jsou monitorovány kamerami se záznamem.

Žáci mají přístup pouze do svých osobních složek dokumenty na škol. počítačích. Vyučující také, vyučující mají ještě přístup do společného sdíleného úložiště, kde jsou uloženy důležité základní dokumenty školy.

Ve školním informačním systému Bakaláři mají učitelé definovány role učitele, kdy mají přístup pouze k údajům žáků své třídy, svého předmětu, podle funkce. Nejvíce oprávnění má samozřejmě vedení školy (ředitel, zástupce ředitele).

Z důvodu bezpečnosti je při přerušení nebo ukončení studia studentovi ihned zablokován škol. počítačový účet v Active Directory, škol. e-mail, přístup do Bakalářů. To samé je nastaveno u zaměstnanců – učitelů.

AV software Eset je nainstalován na každém škol. počítači, personální FW blokuje nebezpečné útoky přes síť jako např. DDOS. AV software Eset pravidelně aktualizuje svou virovou databázi.

Dle škol. řádu je všem žákům zakázáno

> Používat mobilní telefon, MP3 přehrávače nebo jiná audio zařízení v době výuky. Tato zařízení musí být v době vyučování uložena ve školních taškách žáků v takovém režimu, aby nerušila akustickými projevy, nebo v osobních (uzamykatelných) šatních skříních. Nedodržení této povinnosti je bráno jako závažné porušení školního řádu, v takovém případě má vyučující právo žákovi odebrat mobilní telefon pro zbytek vyučovací hodiny*.

Veškeré důležité informace ke studiu a aktuality školy jsou publikovány na webových stránkách školy a na oficiálních profilech SZŠ Agel Ostrava na sociálních sítích FB, Twitter.

Pravidla pro chování žáků při práci na škol. počítačích jsou pak definovány ve škol. řádu ICT učebny.

1.8. Příklady efektivního využití digitálních technologií ve vzdělávání

Na závěr první kapitoly poskytneme konkrétní příklady úspěšného využití digitálních technologií ve vzdělávání, včetně studijních případů a příběhů z praxe, které ilustrují, jak mohou technologie pozitivně ovlivnit vzdělávací proces.

Využívání umělé inteligence pro kontrolu překladu do angličtiny v předmětu anglický jazyk.

Zobrazování trojrozměrných modelů lidského těla a orgánů pomocí 3D brýlí v předmětu biologie, ošetřovatelství.

Využívání cloudového školního účtu Microsoft Offfice 365 online – Wordu, Powerpointu pro např. referáty, prezentace, seminární práce, domácí úkoly z různých předmětů jako český jazyk, angličtina, biologie.

2. Kapitola: Bezpečnostní hrozby a strategie ochrany

2.1. Identifikace běžných kybernetických hrozeb ve školním prostředí

V této sekci se zaměříme na identifikaci a pochopení různých typů kybernetických hrozeb, kterým čelí školy. Prozkoumáme, jak phishing, malware, ransomware a DDoS útoky mohou ohrozit školní

sítě a jaké jsou nejnovější trendy v kybernetických útocích. Diskutujeme o tom, jak mohou být školy zranitelné vůči těmto hrozbám a jaké jsou běžné slabiny v jejich bezpečnostních systémech. Kybernetická bezpečnost je pro školy stále důležitější, protože se stávají cílem různých typů kybernetických hrozeb. Zde je podrobný přehled běžných hrozeb, kterým školy čelí:

- **Phishingové útoky**

  Emailový phishing: Nejčastější formou útoku, při kterém útočníci posílají emaily, které vypadají jako legitimní komunikace od známých institucí, ale ve skutečnosti jsou pokusem o získání citlivých informací, jako jsou hesla a uživatelská jména.

    - Na školní emailový účet některým kolegům občas přijde podvodný email, který ale zachytí SPAM filter a AV software.

  Spear phishing: Cílenější forma phishingu, kde útočníci personalizují své útoky na konkrétní jedince nebo skupiny v rámci školy, často využívají informace získané z veřejných zdrojů nebo sociálních sítí.

- **Malware a ransomware**

  Viry a trojské koně: Škodlivý software, který může být maskován jako legitimní software nebo přiložen k emailům, může po spuštění poškodit systémy nebo ukrást data.

  Ransomware: Typ malware, který šifruje soubory na infikovaném systému a vyžaduje výkupné za jejich odemčení. Školy jsou často cílem těchto útoků kvůli citlivosti a důležitosti dat, která uchovávají.

- **DDoS útoky**

  Distributed Denial of Service (DDoS): Útoky, které přetěžují školní servery a síťovou infrastrukturu tím, že na ně současně posílají obrovské množství požadavků, což může vést k dočasnému nebo trvalému výpadku služeb.

- **Úniky dat**

Porušení datové ochrany: Neoprávněný přístup k osobním údajům studentů a zaměstnanců může vést k jejich úniku a zneužití. To může zahrnovat informace jako adresy, telefonní čísla, zdravotní záznamy a další citlivé informace. Veškeré školní tisky jsou v případě nepotřebnosti zkartovány.

- **Insider threats**

Hrozby zevnitř: Někdy mohou být bezpečnostní incidenty způsobeny zaměstnanci nebo studenty, kteří mají legitimní přístup k systémům, ale zneužívají jej pro osobní zisk nebo z jiných důvodů.

- **Bezpečnostní slabiny v softwaru a hardware**

Zastaralý software: Neaktualizovaný software může obsahovat bezpečnostní chyby, které mohou útočníci využít k proniknutí do systémů. Operační systémy Windows 10, 11 škol. počítačů a NTB ad. software jako Microsoft Office jsou pravidelně aktualizovány centrálně pomocí IT oddělení spol. AGEL. Vyučující a žáci nemají oprávnění na škol. počítačích instalovat jakýkoliv software.

Nekvalitní hardware: Zařízení bez dostatečných bezpečnostních funkcí mohou být snadným cílem pro kybernetické útočníky. Starší škol. počítače a NTB jsou pravidelně obměňovány za novější.

- **Sociální inženýrství**

Manipulace: Útočníci mohou využívat techniky sociálního inženýrství k manipulaci s lidmi, aby získali přístup k systémům nebo informacím, které by jinak nebyly dostupné.

Setkali jsme se na škole s incidentem, kdy se někteří žáci 2. roč. SZŠ dopustili kyberšikany vůči svým spolužákům na oficiálních stránkách školy na sociální síti Facebook. Tito žáci byli poučeni o nevhodném chování na sociálních sítích a celá třída si prošla školením o kyberšikaně. Z důvodu běžpečnosti jsme omezili využívání sociálních sítí Facebook, Twitter atd. na veřejné wifi síti ve škole.

Další incident bylo, kdy jeden žák zjistil přístupové údaje do škol. počítačového účtu spolužáka a zneužil jeho materiály do předmětu. Všichni žáci jsou pravidelně školeni na kyberbezpečnost, aby si zamykali svůj škol. počítačový účet, když odcházejí od počítače.

Kolegyně se setkala s podvodným telefonátem požadujícím získání přístupu ke škol. počítači. Tento incident jsme dále řešili s Agel manažerem ICT bezpečnosti.

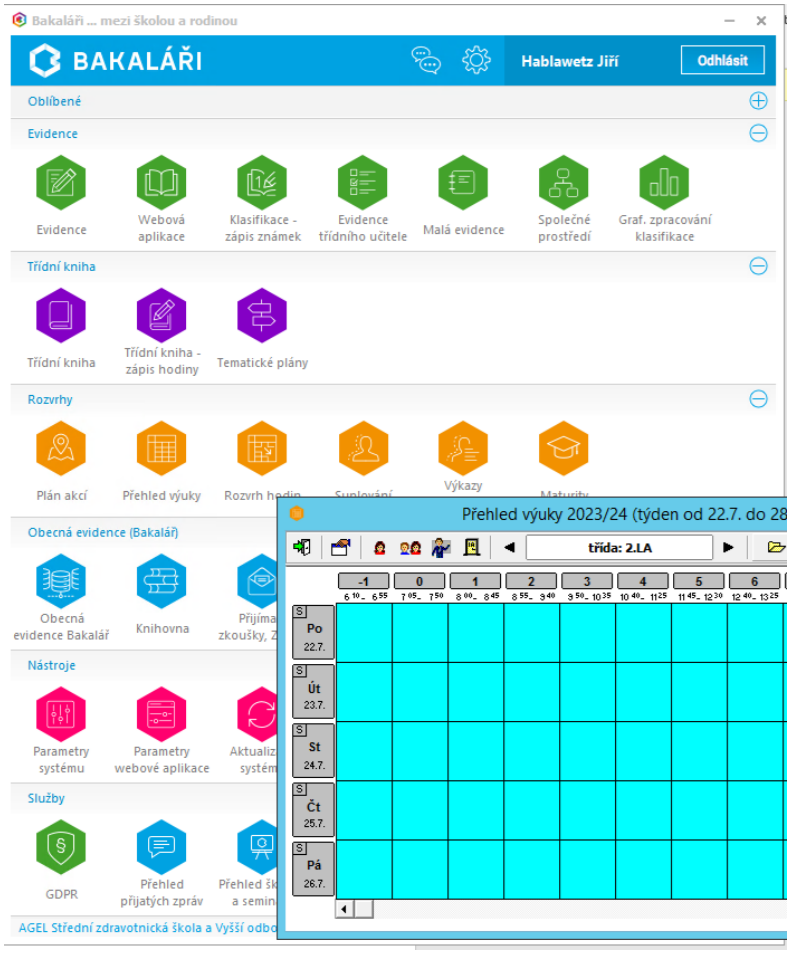
- **Bezpečnostní vědomí**

  Nedostatečné školení: Nedostatek školení a povědomí o kybernetické bezpečnosti mezi zaměstnanci a studenty může vést k tomu, že se stanou nevědomými nástroji útoků.

Identifikace a pochopení těchto hrozeb je prvním krokem k jejich předcházení a ochraně školních systémů. Školy musí být proaktivní ve vzdělávání svých zaměstnanců a studentů o těchto hrozbách a v implementaci efektivních bezpečnostních opatření.

2.2. Ochrana osobních údajů studentů a zaměstnanců

Zde se podíváme na důležitost ochrany osobních údajů a jak školy mohou zajistit, aby byly informace o studentech a zaměstnancích chráněny před neoprávněným přístupem a zneužitím. Probereme zákony a regulace, jako je GDPR, a jak tyto předpisy ovlivňují politiky škol. Diskutujeme o nejlepších postupech pro zabezpečení dat a o tom, jak mohou být implementovány v školním prostředí. Školní informační systém Bakaláři podporuje standardy a zákonné požadavky na GDPR.



Obrázek 3 - školní IS Bakaláři

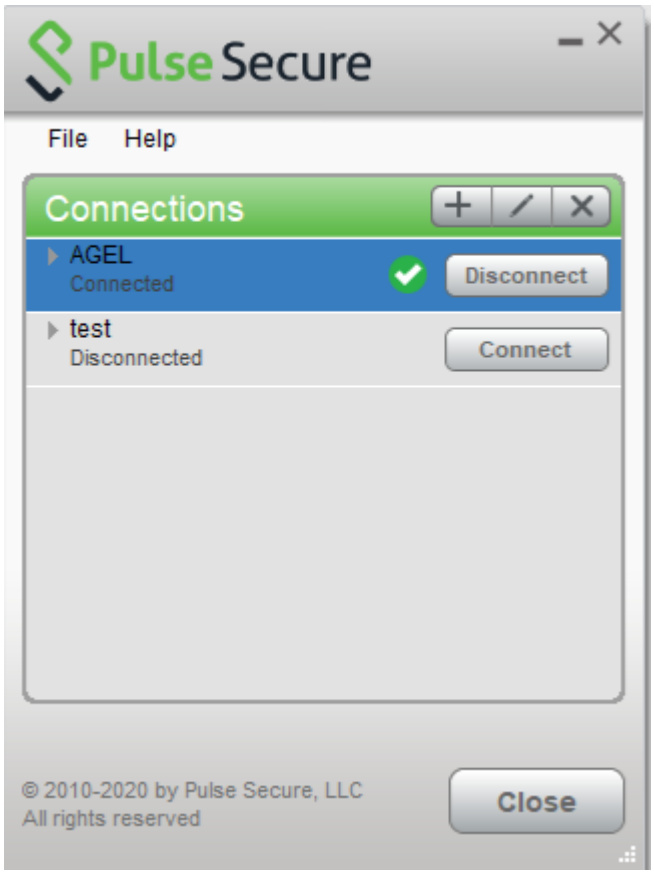
2.3. Metody prevence kybernetických útoků a zabezpečení dat

V této části se zaměříme na preventivní opatření, která mohou školy

přijmout pro ochranu před kybernetickými útoky. Prozkoumáme různé technologie a postupy, jako jsou firewally, antivirové programy, šifrování dat a dvoufaktorová autentizace. Diskutujeme o významu pravidelných aktualizací softwaru a o tom, jak mohou školy vytvářet robustní zálohovací a obnovovací plány. Přístupy do IS Cermat Certis, DIPSY jsou zabezpečeny dvoufaktorovým ověřováním.

Metody prevence kybernetických útoků a zabezpečení dat jsou klíčové pro ochranu osobních I firemních informací v digitálním světě. Zde je několik osvědčených postupů a technologických řešení, které mohou pomoci chránit vaše data:

1. **Aktualizace softwaru a operačních systémů**: Pravidelné aktualizace softwaru a operačních systémů jsou nezbytné pro opravu bezpečnostních chyb a zlepšení ochrany1.
2. **Silná hesla a pravidelná změna hesel:** Vytváření silných hesel, která jsou dostatečně dlouhá a kombinují písmena, čísla a speciální znaky, a jejich pravidelná změna může výrazně zvýšit bezpečnost2.
3. **Dvoufázové ověření:** Používání dvoufázového ověření, kde je kromě hesla vyžadován další kód nebo biometrický údaj, snižuje riziko neoprávněného přístupu2. Dvoufaktorové ověření pro přístup do škol. digitální kanceláře MS Office 365 online je v procesu přípravy.
4. **Šifrování dat:** Šifrování citlivých dat, jak na přenosových cestách, tak na úložištích, zabraňuje neoprávněným osobám v přístupu k těmto datům3. K přístupu k datům ve školní sítí z domu využívají pedagogové VPN klienta Pulse Secure.
5. **Bezpečnostní software:** Používání antivirového softwaru a firewallů může zabránit nebo detekovat škodlivý software a neoprávněné pokusy o přístup4. Veškeré školní počítače jsou chráněny AV softwarem Eset s FW.



Obrázek 4 - VPN klient Pulse Secure

6. **Osvěta a školení zaměstnanců:** Vzdělávání zaměstnanců o kybernetických hrozbách a bezpečných online praktikách je zásadní pro prevenci sociálního inženýrství a phishingových útoků.
7. **Monitorování a detekce:** Implementace systémů pro monitorování sítě a detekci neobvyklého chování může pomoci rychle identifikovat a reagovat na bezpečnostní incidenty.
8. **Plán reakce na incidenty:** Mít připravený plán reakce na bezpečnostní incidenty, včetně postupů pro obnovu dat a komunikaci s dotčenými stranami, je nezbytné pro minimalizaci škod.
9. **Fyzická bezpečnost:** Zajištění fyzické bezpečnosti zařízení a datových center je také důležité, protože útočníci mohou využít fyzický přístup k provádění útoků5.

Tyto metody by měly být součástí komplexní strategie kybernetické bezpečnosti, která zahrnuje technologická řešení, procesy a osvědčené postupy pro ochranu před širokou škálou kybernetických hrozeb. Je důležité si uvědomit, že žádný systém není stoprocentně bezpečný, ale správným používáním těchto metod lze riziko kybernetických útoků výrazně snížit.

2.4. Vytvoření a implementace školní bezpečnostní politiky

Zde se podíváme na proces vytváření efektivní školní bezpečnostní politiky. Diskutujeme o tom, jak mohou školy stanovit jasné bezpečnostní cíle, definovat odpovědnosti a vytvořit plány pro reakci na incidenty. Probereme, jak mohou být tyto politiky komunikovány a jak mohou být začleněny do každodenního provozu školy. Pravidelně aktualizujeme školní řád, zej. s využíváním soukromých mobilních telefonů při výuce. Žáci nesmí používat mobil v hodině.

2.5. Školení zaměstnanců a studentů v oblasti kybernetické bezpečnost

V této sekci se zaměříme na význam školení a osvěty v oblasti kybernetické bezpečnosti. Diskutujeme o tom, jak mohou školy vytvářet a provádět školicí programy, které zvyšují povědomí o bezpečnostních hrozbách a učí zaměstnance a studenty, jak se chovat bezpečně online.

2.6. Technická opatření a software pro zajištění bezpečnosti

Zde prozkoumáme různé technické nástroje a software, které mohou školy použít pro zvýšení své kybernetické bezpečnosti. Diskutujeme o výběru a implementaci správných řešení, která odpovídají potřebám a rozpočtu školy.

Z důvodu zvýšení bezpečnosti jsme rozdělili připojení k wifi síti na naší SZŠ Agel Ostrava na wifi síť SZS-Zamestnanci pro zaměstnance (pedagogové) a na wifi síť volnou SZS-free pro osobní

využití a pro žáky. Wifi síť SZS-Zamestnanci je více zabezpečena šifrováním a heslem. Wifi síť SZS-free má také určitá omezení nastavena na firewallu. IT oddělení spol. AGEL zajišťuje pravidelnou aktualizaci operačních systému platformy Windows 10/11 na školních pracovních stanicích a noteboocích. Žáci SZŠ Agel Ostrava jsou pravidelně školeni, jak se vyvarovat nevhodného chování na sociálních sítích Facebook, Twitter školy. Všichni zaměstnanci SZŠ Agel Ostrava jsou pravidelně školeni v oblasti kyberbezpečnosti. Starší počítače s méně výkonným hardware se snažíme postupně obnovovat za novější. Emailová pošta z externích zdrojů mimo spol. Agel je označena a scanována z důvodu vzrůstajícího počtu kybernetických útoků. Každý školní počítač je chráněn AV software spol. Eset a využíváním VPN klienta pro šifrování provozu počítačové sítě. Zásady kybernetické bezpečnosti jsme implementovali také do školního řádu, zvláště využívání osobních mobilních telefonů ve výuce. Žáci by neměli využívat mobil ve výuce, pokud se nejedná o součást výuky z důvodu prevence kyberšikany.

2.7. Sledování a reakce na bezpečnostní incidenty

V této části se zaměříme na důležitost monitorování sítí a systémů pro včasnou detekci bezpečnostních incidentů. Diskutujeme o tom, jak mohou školy reagovat na bezpečnostní incidenty a jak mohou být vyšetřovány a řešeny.

> Škola při kybernetickém incidentu postupuje podle postupů a procesů ICT bezpečnosti spol. AGEL.

2.8. Audit a revize bezpečnostních postupů a politik

Na závěr kapitoly se podíváme na proces auditu a revize bezpečnostních postupů a politik. Diskutujeme o tom, jak mohou školy pravidelně hodnotit a aktualizovat své bezpečnostní strategie, aby zajistily, že jsou v souladu s nejnovějšími hrozbami a nejlepšími postupy. Škola provádí pravidelnou revizi ICT bezpečnosti všech zařízení (počítačů, notebooků, tabletů, mobilních zařízení). Zastaralý hardware počítačů, dataprojektorů postupně nahrazujeme novými ICT systémy.

2.9. Zákony a směrnice

Kybernetická bezpečnost na středních školách v České republice se řídí několika zákony a směrnicemi. Zde jsou základní legislativní a regulatorní rámce:

1. **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti**

Tento zákon upravuje práva a povinnosti fyzických a právnických osob, státních orgánů a orgánů územních samosprávných celků při zajišťování kybernetické bezpečnosti.

2. **Zákon č. 101/2000 Sb., o ochraně osobních údajů**
   Tento zákon zajišťuje ochranu osobních údajů fyzických osob a stanovuje povinnosti správců a zpracovatelů osobních údajů.

3. **Zákon č. 365/2000 Sb., o informačních systémech veřejné správy**
   Tento zákon stanoví pravidla pro provozování informačních systémů veřejné správy, včetně školských informačních systémů.

4. **Nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR)**
   Obecné nařízení o ochraně osobních údajů (GDPR) reguluje zpracování osobních údajů a chrání práva občanů EU na soukromí.

5. **Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti**
   Tato vyhláška doplňuje zákon o kybernetické bezpečnosti a specifikuje technické a organizační opatření pro zajištění kybernetické bezpečnosti.

2.10. Základní body pro zabezpečení počítačů a ICT techniky na školách

1. **Pravidelné aktualizace softwaru a operačních systémů**
   Zajistit pravidelné aktualizace všech softwarových aplikací a operačních systémů, aby se minimalizovala zranitelnost vůči novým hrozbám.

2. **Antivirová ochrana**
   Instalovat a pravidelně aktualizovat antivirové a antimalware programy na všech počítačích.

3. **Silná autentizace**
   Implementovat silné hesla a vícefaktorovou autentizaci pro přístup k systémům a datům.

4. **Pravidelné zálohování dat**
   Provádět pravidelné zálohování důležitých dat a ověřovat obnovitelnost záloh.

5. **Šifrování dat**
   Šifrovat citlivá data, zejména osobní údaje studentů a zaměstnanců, při přenosu i v úložišti.

6. **Přístupová práva**

   Omezit přístupová práva k datům a systémům pouze na ty zaměstnance a studenty, kteří je skutečně potřebují k výkonu svých povinností.

7. **Bezpečnostní školení**

   Pravidelně školit zaměstnance a studenty v oblasti kybernetické bezpečnosti a bezpečného používání ICT techniky.

8. **Firewall a síťová bezpečnost**

   Používat firewally a další síťové bezpečnostní opatření k ochraně před neoprávněným přístupem zvenčí.

9. **Monitorování a audit**

   Monitorovat síťovou aktivitu a provádět pravidelné audity bezpečnostních opatření a procesů.

10. **Incident Response Plan (IRP)**

    Vypracovat a pravidelně aktualizovat plán pro reakci na bezpečnostní incidenty, který zahrnuje kroky pro detekci, oznamování, analýzu a obnovu.

Tato opatření by měla být součástí komplexní strategie kybernetické bezpečnosti na školách, která zajistí ochranu dat, systémů a uživatelů před kybernetickými hrozbami.

3. Závěr

Během naší analýzy jsme identifikovali několik kritických slabin v zabezpečení ICT zařízení na naší škole. Patří sem absence dvoufaktorového ověřování při přihlašování do cloudových služeb Microsoft Office, což výrazně zvyšuje riziko neoprávněného přístupu k citlivým datům. Dále jsme zjistili nedostatečné školení žáků v oblasti kyberbezpečnosti. Tento nedostatek povědomí o bezpečnostních hrozbách může vést k nezodpovědnému chování při používání ICT zařízení a služeb.

Dalším problémem je nejasná politika ohledně používání soukromých mobilních telefonů ve škole, což může vést k bezpečnostním rizikům spojeným s nechráněnými zařízeními připojujícími se

ke školní síti. Kromě toho je používání zastaralého a nevyhovujícího školního hardwaru významným bezpečnostním rizikem, protože starší zařízení často postrádají nejnovější bezpečnostní aktualizace a funkce.

Vzhledem k současné globální bezpečnostní situaci je nezbytné posilovat ochranu ICT zařízení na školách proti kybernetickým útokům. To zahrnuje zavedení dvoufaktorového ověřování pro všechny školní účty, pravidelné školení žáků a zaměstnanců o kyberbezpečnosti a správném chování online, a jasnou politiku pro používání soukromých zařízení ve školním prostředí.

Dále je nutné investovat do modernizace školního hardwaru, aby byl v souladu s aktuálními bezpečnostními standardy. Pravidelná aktualizace softwaru a hardwaru je klíčová pro ochranu před novými typy kybernetických hrozeb. Také doporučujeme implementaci centrálního systému správy zařízení, který umožní efektivní monitorování a správu všech ICT prostředků v rámci školy.

Zajištění robustní ochrany a pravidelná aktualizace bezpečnostních protokolů jsou nezbytné kroky ke zvýšení bezpečnosti a ochraně citlivých dat před neoprávněným přístupem. Zlepšení těchto oblastí pomůže nejen chránit data školy a jejích žáků, ale také přispěje k vytvoření bezpečnějšího a efektivnějšího vzdělávacího prostředí.

4. Seznam použité literatury

- Černý, Miroslav. Windows 11. 1. vydání. Brno: Computer Press, 2022. ISBN 978-80-251-5207-9. Dostupné z: https://www.bookport.cz/kniha/windows-11-10927/
- Drahotský, Ivo. Bezpečný internet. Praha: Computer Press, 2013. ISBN 978-80-251-3521-7.
- Kopřivová, Barbora. Nebojte se počítače. Praha: Computer Media, 2018. ISBN 978-80-7402-355-8.
- Vondráková, Marcela. ECDL: manuál pro začátečníky a příprava ke zkouškám. 1. vydání. Brno: Computer Press, 2010. ISBN 978-80-251-3120-3. Dostupné z: https://www.bookport.cz/kniha/ecdl-manual-pro-zacatecniky-a-priprava-ke-zkouskam-233/
- Využití umělé inteligence (AI) – Google. Google Gemini, Microsoft. Microsoft Copilot. OpenAI. Chat GPT.

5. Seznam obrázků: