FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Zadání bakalářské práce

Název:	E-learningová aplikace pro rozvoj kybernetické bezpečnosti
Student:	Markéta Petrtýlová
Vedoucí:	Ing. David Buchtela, Ph.D.
Studijní program:	Informatika
Obor / specializace:	Informační systémy a management
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	do konce letního semestru 2023/2024

Pokyny pro vypracování

E-learningová aplikace pro rozvoj kybernetické bezpečnosti

Práci zadává společnost KPCS, která vnímá potřebu vzdělávat své zaměstnance v oblasti kybernetické bezpečnosti. Zaměřit se chce především na rozvoj znalostí v oblasti útoků phishing a sociálního inženýrství.

Hlavním cílem bakalářské práce bude společnosti umožnit vzdělávat své zaměstnance efektivní metodou v předem zmíněných oblastech. Součástí práce bude sepsat edukativní materiál, který bude tvořit podklad pro obsah vzdělávacích kurzů. Dále také vytvořit aplikaci, která bude zaměstnance společnosti formou kurzů vzdělávat a bude je testovat z nově nabytých znalostí po dokončení vzdělávací části kurzu v aplikaci. Následovat bude samotná implementace a testování vzniklého řešení společně se získáním zpětné vazby na rozvoj znalostí uživatelů. Shrnuté bude také ekonomicko-manažerské vyhodnocení, kde budou popsány přínosy tohoto řešení pro společnost KPCS a přehled nákladů.

Elektronicky schválil/a Ing. David Buchtela, Ph.D. dne 12. prosince 2022 v Praze.

Bakalářská práce

E-LEARNINGOVÁ APLIKACE PRO ROZVOJ KYBERNETICKÉ BEZPEČNOSTI

Markéta Petrtýlová

Fakulta informačních technologií
Katedra softwarového inženýrství
Vedoucí: Ing. David Buchtela, Ph.D.
9. května 2023

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů kódu

Chtěla bych poděkovat především vedoucímu práce Ing. Davidu Buchtelovi, Ph.D., oponentce práce Ing. Daně Vynikarové, Ph.D. a společnosti KPCS za možnost konzultovat moje poznatky a cenné rady během vypracovávání práce. Dále bych ráda poděkovala své rodině a přátelům za podporu během psaní této práce a celého studia.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací. Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen " Dílo"), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 9. května 2023 Markéta Petrtýlová

Abstrakt

Tato bakalářská práce se zabývá návrhem, realizací, implementací, nasazením a testováním aplikace pro rozvoj znalostí v oblasti sociálního inženýrství. Zahrnuta je také analýza požadavků společnosti požadující vzdělávací aplikaci a podpora společnosti při nasazení i prvním používání aplikace. Obsah vzdělávacích kurzů v aplikaci je vytvořen na základě analýzy oblasti sociálního inženýrství, která tvoří teoretickou část této práce. Tato aplikace pomáhá společnosti, pro kterou je aplikace tvořena, rozvíjet znalosti zaměstnanců v oblasti sociálního inženýrství. Aplikace také připravuje uživatele na rozpoznání útoků phishing v e-mailové komunikaci. Hlavním přínosem bakalářské práce je pomocí vzdělávacích kurzů proškolit zaměstnance, aby se dokázali ubránit před útoky sociálního inženýrství, a tak ochránili sebe i společnost. V příloze práce lze nalézt přípravy a zápisy z jednání se zadavatelem. Také je zde pomocí fotografií představeno vývojové prostředí aplikace a uživatelské rozhraní aplikace.

Klíčová slova e-leraningová aplikace, firemní školení, phishing, sociální inženýrství, Microsoft Power Platform

Abstract

This bachelor's thesis deals with the design, realization, implementation, deployment and testing of an e-learning application for improving knowledge in the field of social engineering. The thesis includes a requirement analysis of the company requesting the educational application, and its support during deployment and first use of the application. The content of the educational courses in the application is created based on the analysis of the field of social engineering, which forms the theoretical part of this work. This application helps the company for which the application is created to develop the knowledge of employees in the field of social engineering. The application

also prepares users to recognize phishing attacks in e-mail communication. The main benefit of the bachelor's thesis is to use educational courses to train employees so that they can defend themselves against social engineering attacks and thus protect themselves and their company. In the appendix of this thesis, you can find preparations and summaries from consultations with the company requesting the application. The development environment of the application and the user interface of the application are also presented here with the help of photos.

Keywords e-leraning application, on-the-job training, phishing, social engineering, Microsoft Power Platform

Seznam zkratek

BEC	Kompromitace podnikových e-mailů (z anglického Business Email Compromise)
DPH	Daň z přidané hodnoty
EUR	Euro
FBI	Federální úřad pro vyšetřování (z anglického Federal Bureau of Investigation)
ČR	Česká republika
IT	Informační technologie
Kč	Koruna česká
KPCS	KPCS CZ, s.r.o.
MD	Jeden člověkoden, označení pro jeden pracovní den (z anglického man-day)
OSINT	Open Source Intelligence neboli zpravodajství z otevřených zdrojů
PIN	Osobní identifikační číslo (z anglického Personal identification number)
SDLC	Životní cyklus vývoje softwaru (z anglického software development life cycle)
SI	Sociální inženýrství
SMS	Krátké textové zprávy (z anglického Short message service)
URL	Jednotný lokátor zdroje (z anglického Uniform Resource Locator)
USB	Univerzální sériová sběrnice (z anglického Universal Serial Bus)

Úvod

Dle výsledků výzkumu organizace Arlington Research publikovaných společností Egress se v roce 2021 až 94 % organizací potýkalo s nechtěným únikem dat. V 84 % případů způsobila únik lidská chyba, a tedy neznalost, oklamaní či nepozornost lidí. (Přel. Petrtýlová Markéta) [1]

Na základě reportu amerického Federálního úřadu pro vyšetřování (FBI) se internetoví útočníci v roce 2021 zmocnili okolo 6,9 miliard dolarů. Toto číslo je dvakrát větší než suma o dva roky dříve a téměř pětinásobek obnosu, který byl obětem odcizen v roce 2017. S rostoucí meziroční částkou odcizených peněz je vidět i rostoucí počet útoků, mezi kterými je nejčastějším typem phishing. (Přel. Petrtýlová Markéta) [2]

Kvůli rostoucí částce odcizených peněz, možné ztrátě tajných či citlivých informací a mnoha dalším rizikům spojených s úspěšně provedeným kybernetickým útokem se některé firmy snaží zaměstnance pravidelně školit a mít přehled o jejich znalostech. Mimo seznámení se s bezpečnostními protokoly jim nabízí, a někdy i vyžadují, splnění řady různých kurzů, kvízů a certifikací v oblasti kybernetické bezpečnosti. Tato snaha má díky lepším znalostem zaměstnanců v oblasti této problematiky snižovat možnost lidské chyby, a tak minimalizovat možné dopady útoků.

Společnost KPCS CZ, s. r. o. již 17 let pomáhá svým zákazníkům růst a rozvíjet se v digitálním světě. Důraz klade zejména na obchodní procesy, týmovou spolupráci, bezpečné cloudové služby a měřitelné přínosy. Tato společnost vnímá potřebu vzdělávat své zaměstnance o kybernetické bezpečnosti. Zaměřit se chce především na rozvoj znalostí v oblasti útoků sociálního inženýrství. Motivací pro tuto práci je tedy vytvořit pro společnost KPCS řešení, které jí pomůže eliminovat lidské chyby řádným proškolením zaměstnanců a současně umožní mít přehled o znalostech pracovníků. [3]

Vzdělávat se o kybernetické kriminalitě je důležité nejen pro uchování pracovních a osobních dat, ale i pro ochránění osobní identity lidí kolem nás. U mnoha mých kamarádů a rodinných příslušníků vidím, jak některé jejich zvyky mohou vést k potížím. Příkladem těchto zvyků je

odcházení od nezamčeného počítače, klikání na odkazy bez přemýšlení o možných důsledcích a sdělování osobních údajů neověřeným osobám skrze telefon.

Cílem této práce je podpořit snahu společnosti KPCS o vzdělávání v oblasti sociálního inženýrství vytvořením interaktivní aplikaci pro vzdělávání a testování znalostí.

Následujících devět kapitol obsahuje analýzu oblasti sociálního inženýrství a následný popis procesu vývoje vzdělávací aplikace. První kapitola popisuje cíle bakalářské práce, které dělí na teoretické a praktické. Druhá kapitola je úvodem do oblasti sociálního inženýrství. Jsou zde vysvětleny základní pojmy této oblasti a rozepsané typy útoků sociálního inženýrství. Ve třetí kapitole je představeno, jaké typy nebezpečí se skrývají za útoky sociálního inženýrství a na koho je nejčastěji cíleno. Dále se práce zaměřuje na to, jak předejít sociálnímu inženýrství, a jak se zachovat při napadení. Šestá kapitola se zaměřuje na vývoj vlastní e-learningové aplikace a analýzu konkurence. Sedmá kapitola pak shrnuje realizaci aplikace včetně nasazení, testování a podpory. Jsou zde uvedené také vize pro možný rozvoj nad rámec této práce. Poslední kapitolou před závěrem je ekonomicko-manažerské zhodnocení shrnující nejdůležitější informace z pohledu manažera včetně přehledu nákladů, harmonogramu, vize projektu a rizik.

Kapitola 1

Cíl práce

Cílem teoretické části bakalářské práce je analyzovat oblast sociálního inženýrství. Na základě této analýzy poté vytvořit osnovy pro obsah vzdělávacích kurzů pro společnost KPCS, později i texty kurzů. Dílčím cílem je analyzovat již existující školící řešení, požadavky společnosti KPCS a možné nástroje pro vytváření výukových aplikací. Na základě této analýzy je cílem navrhnout vlastní školící aplikaci.

Cílem praktické části bakalářské práce je vytvořit aplikaci, která bude zaměstnance společnosti KPCS formou kurzů vzdělávat v oblasti sociálního inženýrství a bude je testovat z nově nabytých znalostí. Následovat bude testování a samotná implementace vzniklého řešení společně se získáním zpětné vazby na rozvoj znalostí uživatelů. Vytvořeno bude také ekonomicko-manažerské vyhodnocení, kde budou popsány přínosy tohoto řešení pro společnost KPCS a přehled nákladů na vývoj aplikace.

Kapitola 2

Úvod do sociálního inženýrství

Hardware i software se za poslední desítky let vyvíjely rapidní rychlostí. S tímto vývojem se rozvíjelo také zabezpečení, které je nyní v obou zmíněných oblastech na takové úrovni, že je pro kybernetické útočníky v mnoha případech nejjednodušší předpokládat lidskou chybu. První kapitola popisuje základní pojmy v oblasti sociálního inženýrství a analyzuje nejčastější typy útoků sociálního inženýrství, tedy kybernetických útoků, kde se cílí na nepozorné a neproškolené uživatele, které útočník zvládne oklamat.

2.1 Kybernetický prostor a kybernetická kriminalita

Kybernetická kriminalita je odvozena od pojmu kybernetický prostor, neboli kyberprostor. Kyberprostor je virtuální prostředí, které nemá začátek ani konec, nezná hranice států a tedy nelze přesně určit, jak rozsáhlý je. Kybernetická kriminalita, dříve také označována jako informační kriminalita, je definována Policií ČR jako trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání. [4]

2.2 Kybernetická kriminalita v ČR

Policie ČR od roku 2011 sleduje počet trestných činů spáchaných v kyberprostoru. V uvedeném období je zaznamenán trend trvalého nárůstu evidovaných případů kybernetické kriminality. V roce 2019 bylo v oblasti kybernetické kriminality a kriminality páchané na internetu evidováno 8 417 trestných činů, což ve srovnání s rokem 2018, kdy bylo případů 6 815, potvrzuje nárůst

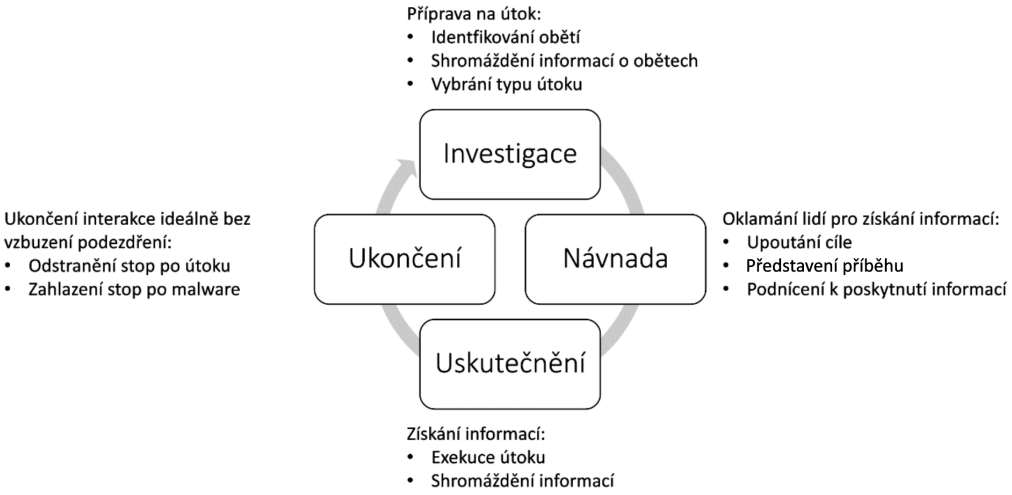
o více než 1 600 skutků. V roce 2011 se uskutečnilo trestných činů 1 502. Tradičně nejpočetnější skupinou v oblasti kybernetické kriminality a kriminality páchané na internetu jsou různé formy podvodného jednání (více než polovina všech evidovaných skutků), vedle kterých jsou nemalou měrou zastoupeny i pojistné podvody. [4]

2.2.1 Sociotechnika

Sociotechnika je forma ovlivňování a přesvědčovaní osob s cílem oklamat lidi tak, aby uvěřili, že osoba, která se je snaží oklamat, je totožností, kterou se pro potřeby manipulace jeví. Při úspěšném provedení této techniky dochází k využití přesvědčených osob či osoby pro získání hledaných informací. K tomu může dojít i za dodatečné pomoci technologických prostředků. (Přel. Petrtýlová Markéta) [5]

2.2.2 Sociální inženýrství

Dle Iana Manna, experta na kybernetickou bezpečnost, je definice sociálního inženýrství, jednoho z typů kybernetické kriminality, manipulace lidí pomocí sociotechniky za cílem získání informací nebo podnícení lidí k určité akci. Jedná se o útok na nedokonalou ochranu mezi fyzickou bezpečností a bezpečností v IT, tedy útok na lidi, kteří sami vydají citlivé informace. (Přel. Petrtýlová Markéta) [6] K útokům nemusí docházet pouze skrze internet, u některých sociotechnických metod může být použit telefon, dopis či také přímý osobní kontakt. Životní cyklus sociálního inženýrství je zachycen na obrázku 2.1.



Obrázek 2.1 Životní cyklus sociálního inženýrství [7]

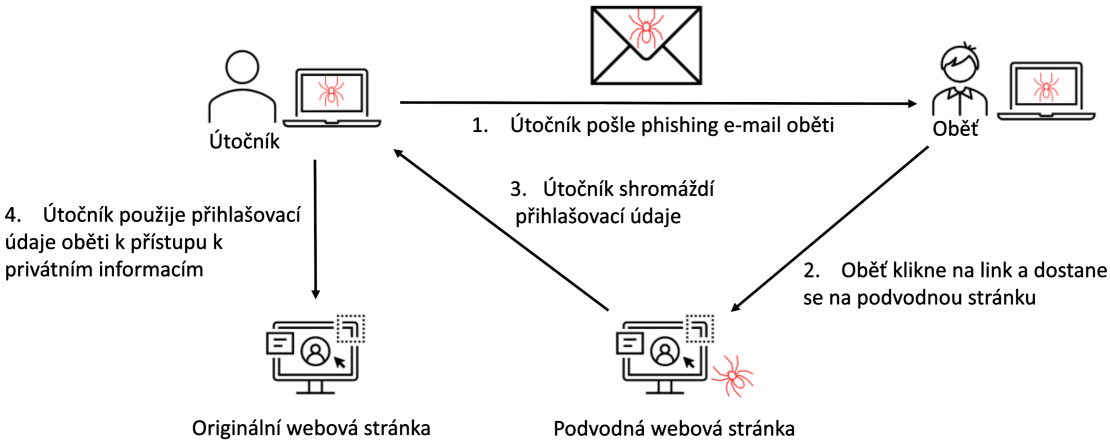
2.3 Typy útoků sociálního inženýrství

Existuje mnoho typů útoků sociálního inženýrství. V následující části práce jsou shrnuty ty, se kterými se v současné době mohou lidé nejčastěji setkat.

2.3.1 Phishing

První zmínku o konceptu tohoto typu útoku najdeme v dokumentu System Security: A hacker´s perspective od autorů Jerryho Felixe a Chrise Haucka. Dokument, který byl v roce 1987 představen na konferenci Iterex, se věnuje technice útoku, kdy útočník imituje důvěryhodnou autoritu nebo službu. Slovo phishing vzniklo úpravou anglického překladu pro lov ryb neboli fishing, v češtině se občas používá také pojem rhybaření. Analogie je zřejmá, útočník (lovec) nahodí háček s návnadou například v podobě výhodné nabídky a čeká na oběť. Záměna písmena f za ph má původ ve slově „phreaks“, což byla hackerská skupina v USA, která ilegálně experimentovala s telekomunikačními systémy v devadesátých letech minulého století. [8]

Phishing je útok využívající sociální inženýrství a technologií k odcizení osobní identity a přihlašovacích údajů neopatrných obětí. Oklamaní lidé jsou vystaveni nejčastěji e-mailové zprávě, která je navržena tak, aby co nejvíce napodobovala legitimní zprávu, avšak je odeslána z podvodné e-mailové adresy a v textu odkazuje na padělané webové stránky. Příjemci, kteří klam neodhalí, jsou vyzváni na webové stránce k zadání finančních údajů, přihlašovacích jmen a hesel. Tyto informace jsou následně shromážděny útočníky, kterými mohou být zneužity. (Přel. Petrtýlová Markéta) [9] Schéma phishing útoku je představeno na obrázku 2.2.



Obrázek 2.2 Schéma phishing útoku [10]

Ačkoliv se jedná o starší taktiku, díky své jednoduchosti a efektivitě je dnes phishing velice populární volbou útočníků. Dle výzkumu společnosti CISCO se tato metoda, kdy se útočník snaží vystupovat jako důvěryhodná osoba, velmi rozmohla v období koronavirové pandemie. V tomto období lidé prahli po informacích, které často z důvodu různých omezení hledali především online. To zapříčinilo fakt, že v roce 2021 se z 86 % organizací alespoň jeden uživatel pokusil o připojení se na podvodnou stránku. (Přel. Petrtýlová Markéta) [11]

Phishing má mnoho různých podob a typů, je to způsobeno především tím, že se útočníci stále snaží nacházet nové a efektivnější způsoby pro klamání lidí. Mezi ty nejhojněji používané však řadíme v daném pořadí tyto:

1. E-mail Phishing.
2. Spear Phishing.
3. Whaling.
4. Smishing.
5. Vishing. (Přel. Petrtýlová Markéta) [12]

Následující sekce se zaměřují na tyto jednotlivé typy, kromě útoku phishing v e-mailové komunikaci, který byl představen již v rámci předchozích odstavců jako nejčastější typ phishing útoku.

2.3.2 Cílený phishing neboli spear phishing

Tento typ útoku se oproti klasickému útoku liší specifickým cílením na individuální organizace nebo jedince. Pro tuto formu útoku pachatelé předem sbírají a kupují si data o obětech, díky kterým následně provedou personalizovaný útok. V současné době se jedná o nejúčinnější typ útoku typu phishing. (Přel. Petrtýlová Markéta) [13]

Útočníci si vyhradí čas pro získání minimálně jména, příjmení a e-mailové adresy budoucí oběti. Mohou však získat daleko více informací o oběti i lidech kolem ní a to dnes již jednoduchým vyhledáváním na sociálních sítích a internetu. Z těchto zdrojů lze získat informace o rodinných příslušnících, koníčcích a zálibách, jako je například sázení či závislost na hrách. Všechny tyto poznatky pak útočník použije při kontaktování oběti. Snaží se tak být věrohodnější osobou, která snáze oběť přesvědčí k nějaké akci. (Přel. Petrtýlová Markéta) [14]

2.3.3 Whaling

Tento typ útoku sociálního inženýrství je praktikou zaměřenou na vedoucí pracovníky společností. Whaling je velice sofistikovaný a spoléhá na OSINT, průzkumy obchodních praktik společnosti a dokonce i na hluboké proniknutí do účtů na sociálních sítích. (Přel. Petrtýlová Markéta) [15] Zkratka OSINT (Open Source Intelligence neboli zpravodajství z otevřených zdrojů) označuje sběr, zpracování a analýzu dat z volně dostupných zdrojů. K těm mohou patřit různé tištěné či elektronické sdělovací prostředky, nicméně dominantní je internet. OSINT nevyužívají jen zpravodajské agentury, ale také novináři a firmy při analýze obchodních partnerů a konkurentů nebo útočníci v počáteční fázi kybernetického útoku. (Přel. Petrtýlová Markéta) [16]

Zločinci se také mohou vydávat přímo za vedoucího pracovníka s rozhodovacími pravomocemi a pokud k účtu takového pracovníka získají přístup, posílají interní požadavky zaměstnancům na nižší úrovni. Této praktice se přezdívá BEC, což je zkratka pro Business Email Compromise neboli Kompromitace podnikových e-mailů. (Přel. Petrtýlová Markéta) [15]

2.3.4 Smishing

Smishing je typ phishing útoku, který probíhá formou textových zpráv (SMS). Tento typ útoku vyzývá oběť k okamžité akci tím, že obsahuje škodlivé odkazy, na které jste vedeni kliknout. Může také obsahovat falešné telefonní čísla, na která jste vedeni zavolat. Často jsou oběti požádány o sdělení osobních údajů, které mohou útočníci využít ve svůj prospěch. Útoky typu smishing vyvolávají pocit naléhavosti, aby přiměly oběti k rychlému jednání. (Přel. Petrtýlová Markéta) [17]

2.3.5 Vishing (Voice phishing)

Podvody používající sociotechniku nemusí být založené pouze na odeslání e-mailové zprávy a následném čekání na odpověď či akci, mohou také využívat například telefonní hovory.

Benefit metody Vishing spočívá v rychlosti odpovědi. Za krátký čas může útočník způsobit škodu více lidem než při použití předchozí metody. Během těchto hovorů se útočníci vydávají za zaměstnance firem, klienty či osoby vykonávající průzkum. Cílenou osobu se poté snaží přesvědčit k prozrazení informací nebo vykonání určité akce. (Přel. Petrtýlová Markéta) [18]

Z mé osobní zkušenosti se podvodníci mohou vydávat za zaměstnance banky, společnosti s energiemi nebo za technickou podporu mezinárodního technického giganta. Mezi běžnou otázkou bývá poptávka po sdělení dvou čísel z posledního čtyřčíslí rodného čísla, což je část, která

se nedá odvodit z data narození a pohlaví. Setkala jsem se také s pokusem o nabídku nevšedně výhodné smlouvy na energie, kterou musíte využít do 24 hodin.

2.4 Baiting

Baiting je technika, která spočívá v tom, že útočník nastraží návnadu (bait) na určitém místě, kde jej nalezne oběť. Návnadou bývá často USB klíč, neboli klíč univerzální sériové sběrnice, ale může jí být například i QR kód (zkratka z anglického quick response, což lze přeložit jako rychlá odpověď), který je nyní běžně dostupný na stolech v restauracích. Cílem tohoto útoku je, aby oběť nalezenou návnadu použila k načtení podvodné stránky či stažení malware, tedy škodlivého počítačového programu. Útočník se poté snaží oběť přimět k zadání citlivých informací a ukrást tak její osobní identitu. (Přel. Petrtýlová Markéta) [18]

2.5 Scareware

Scareware je škodlivý software, který uživatele přiměje navštívit webové stránky napadené malware. Tento software, známý také jako klamavý software, podvodný skenovací software nebo fraudware, způsobuje vyskakování oken. Ty se tváří jako legitimní varování od společností poskytujících antivirový software a tvrdí, že soubory vašeho počítače byly infikovány. Jsou provedeny tak chytře, že některé uživatele vyděsí a donutí je zaplatit poplatek za rychlé zakoupení softwaru, který údajně problém vyřeší. Stáhnou si však falešný antivirový software, který je ve skutečnosti malware určeným ke krádeži osobních údajů oběti. (Přel. Petrtýlová Markéta) [19]

Podvodníci používají i další taktiky, jakou je například rozesílání nevyžádané pošty k šíření scareware. Po otevření této zprávy jsou oběti oklamány, aby si zakoupily bezcenné služby. Zveřejnění osobních a bankovních údajů otevírá dveře pro budoucí krádeže identity. (Přel. Petrtýlová Markéta) [19]

2.6 Pretexting

Pretexting je taktika, která spočívá ve vytváření souborů informací, které zvyšují míru úspěšnosti budoucího útoku. Útok je prezentován pomocí legitimně vypadajících zpráv, obrázků (například vládních log), tónu a formulací. Útok může být proveden on-line, osobně nebo po telefonu. Cílem útočníka je načerpat informace, aby mohl v budoucnu provést přesvědčivější a cílenější útok. (Přel. Petrtýlová Markéta) [20]

Běžným příkladem této taktiky je, že pachatel někomu zašle e-mail, kde se vydává za legitimní autoritu (například vládní organizaci) nebo důvěryhodný kontakt, a snaží se získat přihlašovací údaje. (Přel. Petrtýlová Markéta) [20]

2.7 Honey trap

Honey trap, v překladu medová past, je druh sociálního inženýrství, kdy útočník láká oběť do zranitelné situace. Útočník tuto situaci následně využije jako příležitost k sexuálnímu nebo jinému typu vydírání. Sociální inženýři často nastražují pasti zasíláním nevyžádaných e-mailů, ve kterých tvrdí, že vás sledovali přes webovou kameru a chtějí zaslat peníze, aby záznam nezveřejnili na internetu. (Přel. Petrtýlová Markéta) [21]

Pokud takovouto zprávu obdržíte, zkontrolujte, zda je webová kamera zabezpečená. Pak jednoduše zachovejte klid a nahlaste zprávu jako pokus o podvod. Tento typ útoku se také nemusí vázat na e-mailovou komunikaci.

2.8 E-mail spamming

Rozesílání nevyžádané pošty je jednou z nejstarších forem sociálního inženýrství a je zodpovědné v podstatě za veškerou nevyžádanou poštu v e-mailových schránkách. V lepším případě je e-mailový spam obtěžující, v horším případě nejde jen o spam, ale o podvod s cílem získat osobní údaje. Mnoho e-mailových serverů automaticky prověřuje škodlivý spam, ale tento proces není dokonalý a někdy nebezpečné a nechtěné e-maily proklouznou. (Přel. Petrtýlová Markéta) [17]

Kapitola 3

Nebezpečí sociálního inženýrství

Třetí kapitola popisuje, v jaké podobě lze útoky sociálního inženýrství nejvíce očekávat, a kdo je jejich nejčastějším cílem. Uvedeny jsou pro poučení příklady nejdražších útoků v průběhu historie.

3.1 Příklady nejdražších útoků sociálního inženýrství

3.1.1 Colonial Pipeline

V květnu roku 2021 se skupině útočníků s názvem DarkSide gang podařilo pomocí e-mailové zprávy obsahující phishing získat heslo jednoho ze zaměstnanců Colonial Pipeline, amerického giganta obchodujícího s pohonnými hmotami. (Přel. Petrtýlová Markéta) [22]

Organizace byla nucena zastavit provoz poté, co byla ohrožena její obchodní síť a fakturační systém ransomware útokem provedeným pomocí získaného hesla. Firmu přišel tento útok na 3,4 miliardy EUR, z toho dešifrovací částka byla 4,4 milionů EUR a zbytek ztráty tvořily škody způsobené pozastavením provozu. (Přel. Petrtýlová Markéta) [22]

3.1.2 Facebook a Google

Mezi lety 2013 a 2015 byly dvě světové technologické firmy okradeny o 100 milionů dolarů poté, co se staly obětí podvodu s falešnou fakturou (Přel. Petrtýlová Markéta). [22]

Litvan Evaldas Rimasauskas si všiml, že obě organizace využívají tchajwanského dodavatele infrastruktury Quanta Computer. Poslal řadu falešných mnohamilionových faktur, které během dvou let replikovaly dodavatele. Faktury byly doplněné smlouvami a dopisy, které údajně podepsali vedoucí pracovníci a agenti společností Facebook a Google. (Přel. Petrtýlová Markéta) [22]

Podvod byl nakonec odhalen a společnosti Facebook a Google podnikly právní kroky. Získali necelou polovinu ukradených peněz, zatímco Rimasauskas byl zatčen a vydán z Litvy. V prosinci 2019 byl odsouzen k pěti letům vězení. (Přel. Petrtýlová Markéta) [22]

3.1.3 Sony Pictures

V listopadu 2014 ukradla hackerská skupina „Guardians of Peace“ 100 terabajtů dat z filmového studia Sony Pictures. (Přel. Petrtýlová Markéta) [22] Podle Stuarta McClurea, generálního ředitele společnosti Cylance pro počítačovou bezpečnost, který analyzoval uniklá data, útočníci nastražili past měsíce dříve. McClure zjistil, že mnoho vrcholových manažerů Sony obdrželo škodlivé e-mailové zprávy, které vypadaly jako zprávy od společnosti Apple. (Přel. Petrtýlová Markéta) [22]

Prostřednictvím odkazu v této zprávě byli přesměrováni na falešnou stránku, která zachytila jejich přihlašovací údaje. Díky těmto informacím se útočníci dostali k velkému množství firemních dat včetně podrobností o zaměstnancích Sony Pictures a jejich rodinách, soukromé korespondenci a informacím o tehdy nevydaných filmech. (Přel. Petrtýlová Markéta) [22]

Aby útočníci umocnili škody, použili malware k vymazání počítačové infrastruktury Sony. Útočníci byli později navázáni na státem podporovanou severokorejskou skupinu a požadovali, aby Sony stáhla svůj film The Interview, komedii o spiknutí s cílem zavraždit severokorejského vůdce Kim Čong-una. Hrozili také teroristickými útoky v kinech, kde se film promítal, což vedlo k tomu, že se mnoho řetězců kin rozhodlo jej nepromítat. (Přel. Petrtýlová Markéta) [22]

Vzhledem k neobvyklé povaze incidentu je těžké přesně vypočítat škody, ale Jim Lewis, vedoucí pracovník Centra pro strategická a mezinárodní studia, odhadl, že tento incident stál Sony Pictures více než 100 milionů dolarů. (Přel. Petrtýlová Markéta) [22]

3.2 Trendy u útoku typu phishing

Trendem této doby začínají být cílené útoky, které využívají umělé inteligence a volně získatelná data o uživatelích ze sociálních sítí. Jednou z novinek, o které vyšel nedávno článek na stránce Seznam Zprávy, jsou falešné syntetické spoty bank. [23]

Video-výzva je vytvořená pomocí umělé inteligence. Vygenerovaná postava se v ní pomocí syntézy hlasu a simulace pohybu úst při mluvení snaží přesvědčit cílenou reklamou k dokončení konkrétní transakce. Ve videu postava osloví oběť jejím celým jménem, aby vypadala co nejvíce důvěryhodně. [23]

Tyto zprávy jsou cílené tak, že odkaz na video v e-mailové zprávě dostali ti klienti, kteří před několika týdny na sociálních sítích reagovali na nabídku koupi akcií firmy RWE. [23]

„To, že se podvodník vydává za banku, je vcelku časté. Zatím to ale bylo hlavně ve formě e-mailu nebo SMS. Někdy útočníci zase klientům telefonují a dokonce i číslo, které se klientům zobrazí, vypadá jako naše. Tento případ, kdy podvodník vytvoří video-výzvu, v níž se zaštiťuje naším jménem, je ale zcela nový," říká Jakub Heřmánek, mluvčí Fio banky. Banka podle něj považovala za nutné, aby lidé o takovémto způsobu podvodného jednání věděli, měli možnost se na něj připravit a nenaletět na něj, a proto sama příspěvek s videem umístila na Twitter, kde se od něj distancovala. [23]

3.3 Na jaké typy lidí se nejvíce cílí

Znalostí toho, kdo je vůči útoku nejzranitelnější, může pomoci vhodně zaměřit vzdělávací kampaň a efektivně tak rozdělit zdroje společnosti. Kampaň, která je přizpůsobena starším lidem, vypadá totiž jinak než kampaň, která je určena spíše dospívajícím. Stejně tak, když jsou například muži více ohroženi útokem, mohou se společnosti zaměřit na osvětu znalostí této konkrétní skupiny a lépe ji zaujmout. (Přel. Petrtýlová Markéta) [24]

3.3.1 Věk

Díky obecně menším zkušenostem mladších lidí, ať již ve vzdělání či v profesním životě, by se dalo předpokládat, že mladiství budou častěji obětmi kybernetických útoků. Z následujících výzkumů se však dozvídáme, že se studie v tomto směru velmi rozchází.

Dle výzkumu FBI jsou všechny demografické skupiny ohroženy, zdá se však, že nejvíce jsou ohroženy osoby ve věku 40 let a více, ovdovělí a zdravotně postižení lidé. (Přel. Petrtýlová Markéta) [25]

K podobnému výsledku dospěl i výzkum civilistů na amerických univerzitách. Dle jejich studie je pravděpodobnost, že starší lidé kliknou na odkaz v e-mailové zprávě 3,2 %, zatímco u mladších uživatelů e-mailových služeb je pravděpodobnost rozkliknutí odkazu 2,9 %. [26]

Opačný výsledek však zaznamenala studie z Carnegie Mellon University ve spolupráci s Indraprastha Institute of Information Technology. Při této studii dospěli výzkumníci k tomu, že skupina lidí ve věku 18 až 25 let je nejvíce náchylná na podlehnutí útokům. (Přel. Petrtýlová Markéta) [27]

3.3.2 Pohlaví

Poslední dva zmíněné výzkumy dospěly k tomu, že ženy (především pak starší ženy) byly obzvláště náchylné k útokům typu spear phishing. (Přel. Petrtýlová Markéta) [26]

Naopak studie společnosti SecurityAdvisor zjistila, že ženy jsou mnohem bezpečnější než muži. 76 % mužských zaměstnanců se zapojuje do rizikového chování na internetu, zatímco jejich ženské protějšky se zapojují pouze ve 26 %. Kellie A. McElhaneyová, zasloužilá pedagožka a zakládající ředitelka Centra pro rovnost pohlaví a inkluzi (EGAL) na Kalifornské univerzitě v Berkeley, poskytla několik informací o důvodech rozdílů mezi muži a ženami. Profesorka vysvětlila, že muži vnímají riziko jako hru a od mládí jsou vedeni k tomu, aby za každou cenu vyhráli. Když jim hrozí ztráta nebo negativní výsledek, udělají vše pro to, aby se mu vyhnuli. Nepříznivé důsledky se týkají pouze těch, kteří riziko podstupují. (Přel. Petrtýlová Markéta) [28]

Totéž neplatí pro ženy nebo příslušníky nedominantních sociálních skupin na pracovišti. Podle studií si ženy více uvědomují dlouhodobé důsledky rizikového chování, protože jsou si vědomy, že jejich jednání může mít nepříznivý dopad na ostatní členy ve skupině. (Přel. Petrtýlová Markéta) [28]

Z rozdílných výsledků studií vyplývá, že každý musí být na pozoru, nehledě na pohlaví nebo věk, jelikož všichni můžeme být zasaženi a udělat chybu v přehlédnutí.

3.3.3 Odvětví povolání

Dle reportu Kepnet LABS z roku 2020 je patrné, že nejvíce phishing útoků bylo mířeno na poradenské společnosti, kde bylo zasaženo přes 83 % společností. Druhým nejvíce zasaženým odvětvím bylo bankovnictví s 70,7 %. V těsném závěsu byli téměř se stejným výsledkem okolo 65 % telekomunikace, transport a obchodní domy. (Přel. Petrtýlová Markéta) [29]

3.4 Důvody pro kliknutí a nekliknutí aneb pochopení zranitelnosti lidí

Více než 1200 respondentů se zapojilo do výzkumu v oblasti phishing na německých univerzitách, kde byl experiment proveden rozesláním e-mailových zpráv a zpráv na platformě Facebook s podvodným odkazem. 20 % respondentů kliklo na odkaz v e-mailové zprávě a 42,5 % na zprávu poslanou skrze Facebook. Odkaz měl vést na obrázky z fiktivní oslavy. Z výzkumu vyšlo najevo, že lidé nejčastěji kliknou na odkaz kvůli důvodům uvedeným v tabulce 3.1.

Naopak nejvíce od kliknutí respondenty odradilo, že byla adresa odesílatele pro ně neznámá. Z lidí, kteří odhalili podvod jej 50 % označilo za phishing, a to převážně právě kvůli neznámému odesílateli. (Přel. Petrtýlová Markéta) [30]

Tabulka 3.1 Důvody pro kliknutí na phishing

Důvod kliknutí	Kliklo	Popis
Zvědavost	34 %	Respondenti toužili po tom spatřit dané fotografie.
Kontext	27 %	Zpráva má odkazovat na fotky z akce typické pro období, kdy byl výzkum vykonáván.
Zkoumání	18 %	Přáli si zjistit více o situaci, která způsobila tuto zprávu.
Známý odesílatel	16 %	Jistota nebo domněnka, že odesílatele známe.
Technický kontext	11 %	Myšlenka, že technické zabezpečení dokáže zabránit případným hrozbám.
Strach	7 %	Strach z toho, že cizí osoba má fotografie dané osoby.
Automaticky	3 %	Impulsivní kliknutí bez přemýšlení.

Kapitola 4

Jak předejít sociálnímu inženýrství

Každý den jsou útočníky rozeslány miliony škodlivých zpráv, některé jsou detekovány a následně blokovány filtry. Především nové typy útoků ale nemusí být technickými ochrannými systémy zachyceny. Avšak mohou být zachyceny samotnými uživateli. Tato kapitola se zaměřuje na to, jak proškolit uživatele a nastavit zařízení, aby lidé dokázali identifikovat možné nebezpečí a ochránili se před ním.

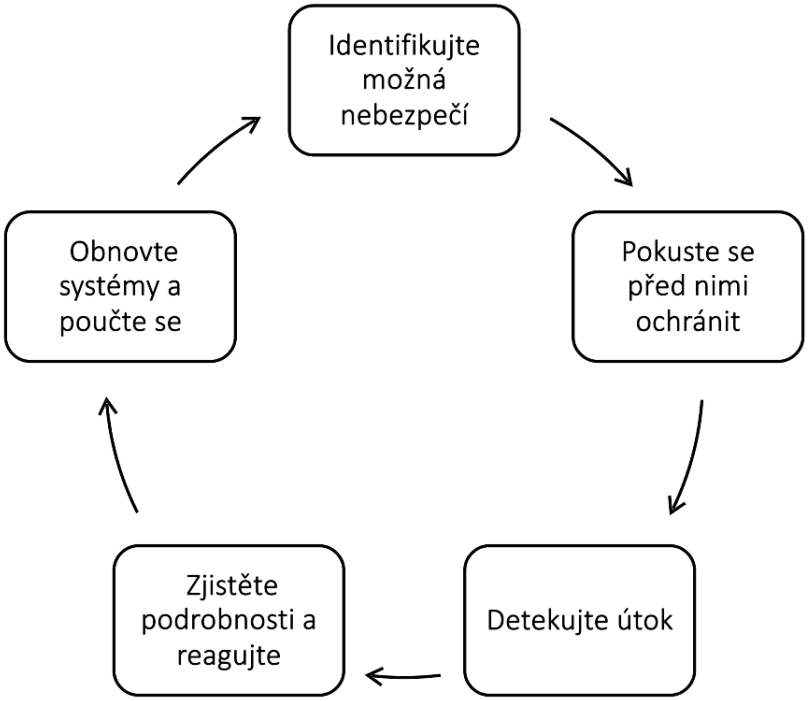
Kapitola je zaměřena na ochranu před útoky sociálního inženýrství a řešení škod po úspěšně provedeném útoku. Postup řešení vychází z frameworku nazvaného The Five Functions (v překladu Pět funkcí) [31]. Jeho cyklus je představen na obrázku 4.1.

4.1 Rozpoznání útoků díky vzdělávání

Vzdělávání v oblasti bezpečnosti by mělo být trvalou aktivitou v každé společnosti. Lidé si jednoduše nemusí být vědomi nebezpečí sociálního inženýrství nebo nemusí znát všechny jeho možné podoby. Neustálé obnovování povědomí o bezpečnosti mezi zaměstnanci je první linií obrany proti sociálnímu inženýrství ve společnostech.

4.1.1 Jak vzdělávat

Zaměstnanci na všech úrovních ve společnosti by měli být školeni, aby se vyhnuli nežádanému poskytování informací, a měli by mít zabezpečená svá zařízení. Studie však ukazují, že efektivita



Obrázek 4.1 Životní cyklus ochrany před sociálním inženýrstvím (Přel. Petrtýlová Markéta) [31]

různých způsobů vzdělávání se liší, a i když některé způsoby mohou vylepšit výsledek až o 40 %, některé jej naopak udělají ještě horším. (Přel. Petrtýlová Markéta) [27] Na co se tedy zaměřit?

1. Stále vylepšujte školení. Školení na téma sociální inženýrství by mělo být přístupné pro všechny zaměstnance. Vytvořte speciální školicí programy pro ty v první linii, kteří pravidelně jednají s návštěvníky, ti jsou nejvíce ohroženi. Zúčastnit se nějakého školení by měli zajisté i vedoucí pracovníci, kteří mají přístup k nejcitlivějším informacím a administrátorským právům.

   Ptejte se zaměstnanců na otázky o sociálním inženýrství založené na reálných scénářích, které by se skutečně mohli vyskytnout v jejich konkrétním prostředí. Udělejte to zajímavé a interaktivní. Pokud se firemní bezpečnostní tým necítí způsobilý ke školení, najměte si externího kouče.

2. Vytvořte firemní politiky, kterým zaměstnanci rozumí. Firemní politika sociálního inženýrství může zahrnovat cokoliv co pomůže zaměstnancům identifikovat, hodnotit, vyhýbat se a dokumentovat pokusy o sociální inženýrství. Nevytvářejte dlouhý dokument plný právních předpisů.

Zde je několik příkladů konkrétních zásad:

- Požádejte o ověření každého, kdo se pokouší vstoupit do zakázaných oblastí nebo k citlivým informacím.
- Dokumentujte podezřelé osoby a situace.
- Nikdy nepoužívejte USB klíč, pokud není získán přímo od IT oddělení.
- Ztracené/Odcizené zařízení nebo kreditní a přístupové karty nahlaste ihned.
- Nikdy neklikejte na odkaz, kde si nejste jisti jeho nefalšovaností.
- Diskutujte s manažerem a IT oddělením, pokud máte pocit, že jste se setkali s útokem.

3. Pravidelně na téma kybernetické bezpečnosti diskutujte, co nejdříve školte nové zaměstnance, věnujte tomuto tématu část v zaměstnaneckém zpravodaji nebo dejte tipy na nástěnky. Pravidelná pracovní rutina totiž usnadňuje zaměstnancům zapomenout na důležité bezpečnostní informace získané během školení.

4. Změňte kulturu firmy, aby se zaměstnanci nebáli ptát a útok nahlásit. Než se zaměstnanci vrhnou do rozhodnutí, měli by se vždy zamyslet nad zásadami a danou situací. V rámci zamyšlení by si měli položit otázky, jako jsou například:

   - Diskutuje se mnou běžně tento člověk na dané téma tímto způsobem?
   - Znám tohoto člověka?
   - Mám tomuto člověku dát svoje osobní údaje nebo půjčit přístupovou kartu? (Přel. Petrtýlová Markéta) [32]

Nejvíce kontroverzní je pak školení, kde se prvně testují znalosti zaměstnanců, kterému bude věnována celá pozdější sekce.

4.2 Naučte se základní principy rozpoznávání útoku

Následující sekce se zaměřuje na to, co by opravdu každý člověk měl znát, aby měl šanci útok sociálního inženýrství rozpoznat. Zde je několik situací, kdy by lidé měli být více obezřetní, jelikož se může jednat o útok.

- V e-mailové zprávě či v předmětu zprávy se vyskytuje naléhavý text.
- E-mailová adresa neodpovídá jménu odesílatele.
- Další příjemci jsou skryti či byl e-mail zaslán na několik neznámých adres.

- Nevšední doba odesílání zprávy.
- Odesílatel použil nevšední pozdrav.
- Jsou vyžadovány důvěrné informace.
- E-mailová zpráva obsahuje pravopisné chyby či je v jiném jazyce než je očekáváno.
- V URL odkazu je vynecháno písmeno nebo nekončí .net, .org nebo .com.
- Pokud e-mailová zpráva obsahuje přílohy typu .pif, .scr nebo .exe.
- Odesílatel takto běžně zprávy neukončuje. (Přel. Petrtýlová Markéta) [33]

Pokud si nejste jisti, zda se jedná o útok, okamžitě se spojte s někým, s kým to můžete prodiskutovat. Můžete také použít on-line stránky pro nalezení majitele domény jako whois.com (Přel. Petrtýlová Markéta) [34] nebo stránky, které ukazují, zda někdo danou webovou adresu nahlásil. Takovouto stránkou je například virustotal.com (Přel. Petrtýlová Markéta) [35]. Vzhledem ke stále novým typům útoků a rychlému jednání útočníků však webová adresa nemusí být ještě označena za podvodnou, a proto na nálezy na těchto stránkách nespoléhejte.

4.3 Testování znalostí

Určení kolik procent osob rozpozná škodlivou zprávu, jakým způsobem se zachovají, a jak bude reagovat IT oddělení, je možné pomocí rozeslání testovacích podvodných zpráv. Tato sekce popisuje, jaká skupina hackerů toto testování provádí a rozebírá různé pohledy na testování.

Hackery obecně dělíme do tří skupin:

Černý hacker je člověk, který útočí na interní sítě jiných společností za účelem vlastního zisku, zneškodnění konkurence nebo napadení funkční infrastruktury. Jedná se o nelegální činnost. [36]

Šedý hacker je člověk, který se sice pokouší dostat do interních sítí jiných firem, jeho záměrem však není vlastní finanční obohacení. Šedí hackeři většinou provádějí tuto činnost pro zábavu nebo pro osobní zviditelnění. Tak jako tak se jedná o činnost vykonávanou bez souhlasu majitele, a tudíž je nelegální. [36]

Bílý hacker neboli etický hacker se také snaží prolomit obranu a infiltrovat se do interních sítí společností. Od předchozích dvou se ale liší tím, že svoji činnost dělá legálně a se souhlasem společnosti. Bílí hackeři se tímto způsobem snaží odhalit trhliny nebo bezpečnostní chyby, které by mohly být napadeny a zneužity. Výsledky své práce pak předávají samotným

společnostem, které na jejich základě mohou lépe zabezpečit svoji síť nebo opravit potenciální bezpečnostní díry, o kterých nemusely mít předtím samy tušení. [36]

Tyto osoby mohou provádět takzvané penetrační testování, což je jeden ze způsobů proaktivní ochrany snažící se odhalit slabá místa v obraně dříve, než je někdo zneužije. Jedná se tedy o reálnou simulaci útoku, kdy dochází k pokusu proniknout do testovaného systému. Cílem penetračního testování je identifikovat zranitelnosti a navrhnout, jak tyto nedostatky odstranit. Na základě výsledků penetračního testování by mělo dojít k nasazení dodatečných nebo úpravě stávajících bezpečnostních opatření, a tedy ke zvýšení celkové úrovně zabezpečení. (Přel. Petrtýlová Markéta) [37]

Existuje nespočet kreativních způsobů jak proniknout do obrany organizace pomocí sociálního inženýrství. Použitím etického hackera k provádění penetračního testování umožníte jednotlivci s hackerskými dovednostmi identifikovat slabiny organizace. Když penetrační test uspěje v kompromitaci citlivých systémů, může pomoci objevit zaměstnance nebo systémy, na jejichž ochranu se má společnost zaměřit. Může také odhalit metody sociálního inženýrství, na které je organizace obzvláště náchylná. (Přel. Petrtýlová Markéta) [38]

Studie z roku 2021 z ETH Zurich, veřejná výzkumná univerzita ve Švýcarsku, však dospěla k závěru, že testování není velmi efektivní a ve skutečnosti může mít negativní vedlejší účinky. Testy dělají uživatele náchylnější k útokům, protože zaměstnanci buď získají falešnou sebedůvěru ze školení, nebo se začnou cítit méně zodpovědní za zastavení takových útoků. (Přel. Petrtýlová Markéta) [39]

Na druhou stranu výzkumníci zjistili, že simulace utoků phishing typu crowdsourcing jsou efektivní. (Přel. Petrtýlová Markéta) [39] V rámci typu crowdsourcing je přesunuta práce, kterou obvykle vykonává zaměstnanec, na větší počet lidí prostřednictvím otevřené výzvy. (Přel. Petrtýlová Markéta) [40] Účastníci experimentu dostali tlačítko, které upozornilo bezpečnostní tým na podezřelou zprávu. Správně nahlásili 68 % podvodných e-mailových zpráv, čímž pomohli bezpečnostnímu týmu v prevenci před útoky sociálního inženýrství. Studie však uvedla, že i crowdsource simulace by měly doplňovat další opatření na zvýšení povědomí o bezpečnosti. [39]

4.3.1 Etičnost testování znalostí

Navzdory své schopnosti identifikovat rizika zůstávají simulace útoků kontroverzní, a to i mezi bezpečnostními profesionály.

Železniční společnost West Midlands Trains (WMT) je kritizována za šokující trik poté, co v roce 2021 rozeslala e-mailovou zprávu v níž slíbila zaměstnancům bonus za nadstandardně

odvedenou práci během pandemie covid. Pokud však zaměstnanci klikli na odkaz pro další informace, obdrželi zprávu s vysvětlením, že to byl jen test. (Přel. Petrtýlová Markéta) [41]

WMT uvedla, že první zpráva byla navržena tak, aby napodobovala taktiku, kterou používají zločinecké gangy, aby se pokusily získat data společnosti. Manuel Cortes, generální tajemník odborového svazu Transport Salaried Staffs' Association (TSSA), řekl, že firma mohla použít jakýkoli jiný bezpečnostní test. Vyzval operátora, aby se omluvil a doručil bonus zaměstnancům, kteří si jej zaslouží. „Tímto způsobem může společnost začít napravovat křivdu, která zbytečně způsobila tolik zranění." řekl. (Přel. Petrtýlová Markéta) [41]

I když to může být legální, není to vždy morální. „Při provádění simulace musíte vzít v úvahu mnoho faktorů," řekla Jinan Budge, analytička společnosti Forrester Research. Před nasazením testu navrhla položit si následující otázky týkající se simulace útoku typu phishing:

1. Jak to ovlivní duševní zdraví zaměstnanců?
2. Je simulace nutná?
3. Jak bude sdělení vnímáno?
4. Prospívá to zaměstnancům?
5. Jsme samolibí nebo opravdu chceme změnit chování?
6. Existuje lepší způsob, jak tuto zprávu sdělit?

Položení těchto otázek pomáhá zabránit tomu, aby se bezpečnostní týmy odloučily ze zbytku organizace. Bezpečnost je totiž často vnímána jako problém IT. 70 % zaměstnanců se domnívá, že je odpovědností IT zajistit, aby nebyly napadeny firemní účty. Bez správného zacílení kampaně tyto simulace pouze posilují toto myšlení. (Přel. Petrtýlová Markéta) [42]

4.4 Buďte podezíraví

Pokud to zní příliš dobře, aby to byla pravda, pravděpodobně je něco špatně. Základní dovednosti kritického myšlení jsou jedním z nejlepších způsobů jak zabránit útoku sociálního inženýrství. Nedávné útoky sociálního inženýrství provedené na platformě Twitter zahrnovaly celebrity jako Elon Musk a Bill Gates, kteří „tweetovali" nabídky na rozdávání tisíců dolarů.

Pokud celebrity slibují, že rozdají tisíce dolarů, zní to až příliš dobře, než aby to byla pravda. V této formě útoku sociálního inženýrství může intuice a zdravý rozum jít daleko. Dávejte si pozor na nabídky, které nabízejí bohaté odměny výměnou za zdánlivě malý poplatek. A pokud se zdá, že žádost pochází od někoho, koho znáte, zeptejte se sami sebe: „Opravdu by mě požádali o informace tímto způsobem?" (Přel. Petrtýlová Markéta) [17]

4.5 Myslete na digitální stopu

Útočníkům může pomoci nadměrné sdílení osobních údajů on-line, například prostřednictvím sociálních sítí. Mnoho bank má jako možnou bezpečnostní otázku jméno vašeho prvního mazlíčka. Sdíleli jste to na platformě Facebook? Pokud ano, můžete být zranitelní! Některé útoky sociálního inženýrství se navíc pokusí získat důvěryhodnost odkazem na nedávné události, které jste mohli sdílet na sociálních sítích. (Přel. Petrtýlová Markéta) [43]

Přepněte nastavení sociálních sítí na „pouze přátelé“ a dávejte si pozor na to, co sdílíte. Pokud máte životopis vystaven on-line, měli byste zvážit umístění své adresy, telefonního čísla a data narození do životopisu. Jsou to totiž užitečné informace pro každého, kdo plánuje útok sociálního inženýrství. (Přel. Petrtýlová Markéta) [43]

4.6 Zohledněte své prostředí

Sociální inženýrství neprobíhá jen ve zdech organizací. Hackeři mohou ukrást informace v metru nebo odposlechem telefonního hovoru v obchodě s potravinami. (Přel. Petrtýlová Markéta) [32] Mohou také vyfotit obrazovku na počítači oběti v kavárně nebo na letišti.

4.7 Nepřipojujte cizí zařízení

Sociální inženýři mohou nechat zařízení, například typu USB klíče, na parkovišti. Pokud si jej někdo sebere a připojí do svého zařízení, může si stáhnout škodlivý software, který se pak může dostat do celého firemního systému. (Přel. Petrtýlová Markéta) [32]

4.8 Kontrolujte přístup a identitu lidí

Dalším způsobem, jak sociální inženýři využívají příležitosti ve svůj prospěch, je proplížení se neuzamčenými vchody nebo krádež zaměstnaneckých průkazů. (Přel. Petrtýlová Markéta) [32] Při vstupu do budovy jsou sociální inženýři sebevědomí, přátelští a obvykle spěchají. Vypadají, jako by do společnosti patřili, a používají nátlak, aby přiměli zaměstnance k poskytnutí informací. (Přel. Petrtýlová Markéta) [32]

4.9 Zabezpečení zařízení

Je důležité zabezpečit zařízení tak, aby útok, i když úspěšný, byl omezen v tom, čeho může dosáhnout. Základní principy jsou stejné, ať už jde o dotykový telefon, domácí síť nebo velký podnikový

systém. Zabránit útoku mohou i uživatelé pomocí správného zacházení s hesly a edukací v oblasti bezpečnostních systémů.

4.9.1 Používejte bezpečnostní software

Mějte anti-malware i antivirový software a udržujte je aktuální. To může pomoci zabránit tomu, aby se malware, který přichází prostřednictvím phishing e-mailů, sám nainstaloval. (Přel. Petrtýlová Markéta) [43]

4.9.2 Aktualizujte software a firmware

Udržujte software a firmware pravidelně aktualizovaný, aby měly všechny možné bezpečnostní záplaty. Vynucujte aktualizace u uživatelů, kteří si delší dobu nespustili aktualizaci, nebo alespoň o této potřebě uživatele informujte a přidejte povinnost aktualizace do své směrnice. (Přel. Petrtýlová Markéta) [43]

4.9.3 Buďte v uživatelském režimu

Nespouštějte svůj telefon, síť a počítač v režimu správce. I když útočník získá uživatelské heslo k vašemu účtu, nedovolí mu překonfigurovat systém ani na něj nainstalovat škodlivý software. Zároveň útočník nezíská data o ostatních zařízeních a uživatelných, ke kterým má mnoho administrátorů přístup. (Přel. Petrtýlová Markéta) [43]

4.9.4 Mějte unikátní hesla

Nepoužívejte stejné heslo pro různé účty. Pokud útok sociálního inženýrství získá heslo k vašemu účtu na sociálních sítích, nechcete, aby také mohl odemknout všechny vaše ostatní účty. (Přel. Petrtýlová Markéta) [43]

Pamatovat si PIN ke každé kartě, „silné“ heslo k sociálním sítím, k internetovému bankovnictví a ke každé další službě není však jednoduché. Kdybychom měli dodržovat všechny bezpečnostní zásady, museli bychom znát nazpaměť desítky až stovky složitých kombinací. Proto je lepší mít všechna hesla bezpečně uložená ve správci hesel neboli password manageru. To je aplikace pro mobilní telefon, tablet a počítač, která si pamatuje všechna hesla za vás. Sama také generuje nová vhodná hesla, a pokud chcete, sama je pak vyplňuje do jednotlivých služeb. [44]

Automatické vyplňování hesel a okének formulářů zvládají i internetové prohlížeče, slouží ale jen na internetová hesla. Plnohodnotní správci hesel toho umějí víc. Navíc je máte pořád u sebe v mobilním telefonu a uložíte do něj i další důležité údaje, třeba PIN ke kartě nebo číslo pasu. [44]

Srdcem aplikace je zašifrovaná databáze hesel kterou otevřete do čitelné podoby jen a jen ve správci hesel se znalostí master hesla. Obsahuje typicky přihlašovací jméno a heslo ke každé službě, kterou používáte. Databáze je uložená buďto na internetu (v cloudu provozovatele správce hesla nebo na Dropbox/Google Drive), případně přímo v mobilním telefonu nebo počítači. Dovnitř se dostanete jen pomocí svého správce hesel a jednoho hlavního hesla (anglicky master password). [44]

Hesla už dávno nejsou bezpečná. Je těžké si je zapamatovat a snadné je zaměnit. Jsou také cílem číslo jedna kybernetických zločinců, 81 % úspěšných útoků zahrnuje slabá nebo odcizená hesla. (Přel. Petrtýlová Markéta) [45]

Alternativou je použít autentizaci bez hesla, neboli passwordless. Namísto hesla používá tato technologie k ověření identity bezpečnější alternativy, jako jsou faktory vlastnictví (jednorázová hesla neboli one-time password generovaná například aplikací v telefonu, registrované chytré telefony) nebo biometrie (otisky prstů, skeny sítnice). (Přel. Petrtýlová Markéta) [45]

S redukcí uživatelských hesel může pomoci metoda ověřování jednotného přihlášení, neboli single sign-on (SSO), která uživatelům umožňuje bezpečně se autentizovat na vícero webů a aplikací pomocí jediné sady přihlašovacích údajů. (Přel. Petrtýlová Markéta) [46]

4.9.5 Používejte více-faktorové ověření

Alespoň u kritických účtů používejte také více-faktorové ověřování, anglicky Multi Factor Authentificator (MFA), aby k přístupu k účtu nestačilo mít pouze heslo. To může zahrnovat rozpoznávání hlasu, použití bezpečnostního zařízení či aplikace, otisky prstů, sken obličeje, potvrzovací SMS kódy, … (Přel. Petrtýlová Markéta) [43]

Dávejte si však pozor při odklikávání notifikací více-faktorového ověřování. I na to se totiž snaží zaměřit kybernetický zločinci a posílají svým obětem opakované notifikace, aby je přiměli ověřit jejich pokus o přihlášení a získali tak přístup k citlivým informacím. (Přel. Petrtýlová Markéta) [47]

Tento pokus může být úspěšný, zvláště když je cílová oběť rozptýlena, zahlcena oznámeními nebo nesprávně interpretuje legitimními požadavky na autentizaci. (Přel. Petrtýlová Markéta) [47]

4.9.6 Používejte princip nulové důvěry

Nulová důvěra, v angličtině zero trust, je strategie kybernetické bezpečnosti, ve které je bezpečnostní politika aplikována na základě nejméně privilegovaného přístupu. Máme tedy co nejmenší počet uživatelů s přístupem do důležitých systémů a účtů, a přísné autentizace uživatelů. Dobře

vyladěná architektura nulové důvěryhodnosti vede k jednodušší síťové infrastruktuře, lepší uživatelské zkušenosti a vylepšené obraně proti kybernetickým hrozbám. (Přel. Petrtýlová Markéta) [48]

Architektura nulové důvěry se řídí zásadou „nikdy nedůvěřuj, vždy prověřuj“. Tento hlavní princip existuje od doby, kdy tento termín vytvořil John Kindervag, tehdy ve společnosti Forrester Research. Architektura s nulovou důvěrou vynucuje zásady přístupu založené na kontextu, včetně role a umístění uživatele, jeho zařízení a dat. (Přel. Petrtýlová Markéta) [48]

4.9.7 Změna nastavení filtrů pro nevyžádanou poštu (spam)

Jedním z nejjednodušších způsobů jak se chránit před útoky sociálního inženýrství je upravit nastavení filtrování e-mailových zpráv. Můžete posílit své spamové filtry a zabránit tomu, aby podvodné e-maily sociálního inženýrství proklouzly do vaší doručené pošty. Postup nastavení spamových filtrů se může lišit v závislosti na e-mailovém klientovi, který používáte. (Přel. Petrtýlová Markéta) [17]

Označit lze také e-mailové adresy lidí a organizací, o kterých víte, že jsou legitimní. Kdokoliv se v budoucnu bude prohlašovat za tyto osoby nebo organizace a použije jinou adresu, pravděpodobně bude sociálním inženýrem. (Přel. Petrtýlová Markéta)[17]

4.9.8 Reagujte při prozrazení hesla

Pokud jste prozradili své heslo k účtu, okamžitě jej změňte a situaci nahlaste. To proveďte u všech účtů, které toto heslo používají. Nastavte nově na každé službě odlišné heslo a nastavte více-faktorové ověření. (Přel. Petrtýlová Markéta)[43]

Kapitola 5

Jak se zachovat při napadení

V minulé kapitole jsem popsala jak rozpoznat, zda se jedná o útok. Uvedla jsem také jak konat, pokud je útok včas rozpoznán. I přes všechna opatření a školení se však může stát, že budou útočníci úspěšní a útok nás poškodí. Pojďme si tedy nyní v sedmi krocích říci, co konat v této situaci, abychom eliminovali možné škody.

5.1 Zjistěte podrobnosti a reagujte

Následující body napomáhají k zorientování se v dané situaci a následné rychlé reakci.

5.1.1 Informujte bezpečnostní tým

První věc, kterou by společnost měla udělat, když je odhalen kybernetický útok, je mobilizovat tým určený pro reakci na kybernetickou hrozbu. Měl by to být tým odborníků z různých oborů. Je důležité, aby každý člen týmu byl řádně vyškolen ve své roli a přesně věděl, co dělat v případě útoku. [49]

5.1.2 Určete typ útoku

Aby tým pro kybernetickou bezpečnost reagoval správně, musí správně identifikovat typ útoku. Jakmile bude vědět, k jakému typu útoku dochází, ví, kam zaměřit svou pozornost. Tak lze eliminovat následující útok a zotavit se ze způsobených škod. Tým by měl znát nejen typ útoku, ale také pravděpodobný zdroj, rozsah útoku a jeho předpokládaný dopad. [49]

5.1.3 Určete rozsah

Většina útoků je navržena tak, aby útočníkům poskytla trvalá zadní vrátka do systémů, tak aby data mohla být i nadále extrahována v průběhu času. Je důležité identifikovat a zakázat veškerý přístup, který útočníci mohou mít k vašemu systému. [49] Ať už zažijete jakýkoli typ kybernetického útoku, bezpečnostní tým by měl okamžitě:

- Odpojit postiženou síť od internetu.
- Zakázat veškerý vzdálený přístup k síti.
- Přesměrovat síťový provoz.
- Změnit všechna zranitelná hesla.

Klíčem je zcela odepřít útočníkům přístup k vašemu systému. Poté lze pracovat na návratu systému do bezpečnějšího pracovního stavu. [49]

5.2 Obnovte systémy a poučte se

Po přesném určení typu a rozsahu útoku lze začít se zamezením dalšího rozšiřování útoku a opravou poškozených zařízení.

5.2.1 Posuďte a opravte poškození

Jakmile je útok pod kontrolou, měl by bezpečnostní tým určit, které kritické obchodní funkce byly ohroženy, jaká data byla narušena, ke kterým systémům bylo nezákonně přistupováno, a zda zůstaly nějaké neautorizované vstupní body. Možná bude nutné přeinstalovat systémy, obnovit ohrožená data ze záložních kopií a opravit nebo vyměnit jakýkoli poškozený hardware. (Přel. Petrtýlová Markéta) [49]

5.2.2 Nahlaste útok

Je důležité okamžitě nahlásit útok příslušným úřadům. Okamžitě kontaktujte státní a místní orgány činné v trestním řízení. Pokud má společnost pojištění kybernetické odpovědnosti, kontaktujte pojišťovnu. (Přel. Petrtýlová Markéta) [49]

5.2.3 Komunikujte se zákazníky

Spolupracujte se svým PR oddělením (public relations neboli oddělení pro vnitřní i vnější komunikaci), abyste zjistili, jak nejlépe řídit veřejný dopad události. Vaši zákazníci budou muset být informováni, zejména pokud útok zasáhl nějaká zákaznická data. Důležité je také vydat tiskovou zprávu k incidentu. Abyste si udrželi důvěru veřejnosti, musíte k útoku přistupovat otevřeně a transparentně. (Přel. Petrtýlová Markéta) [49]

5.2.4 Učte se ze zkušeností

A konečně, organizace se musí z této zkušenosti poučit. Proveďte důkladné šetření a určete, jak změnit systémy a postupy organizace, aby bylo zabráněno budoucím útokům. Využijte tento incident k tomu, abyste byli chytřejší a silnější v oblasti kybernetické bezpečnosti. (Přel. Petrtýlová Markéta) [49]

Kapitola 6

Návrh aplikace pro školení sociálního inženýrství

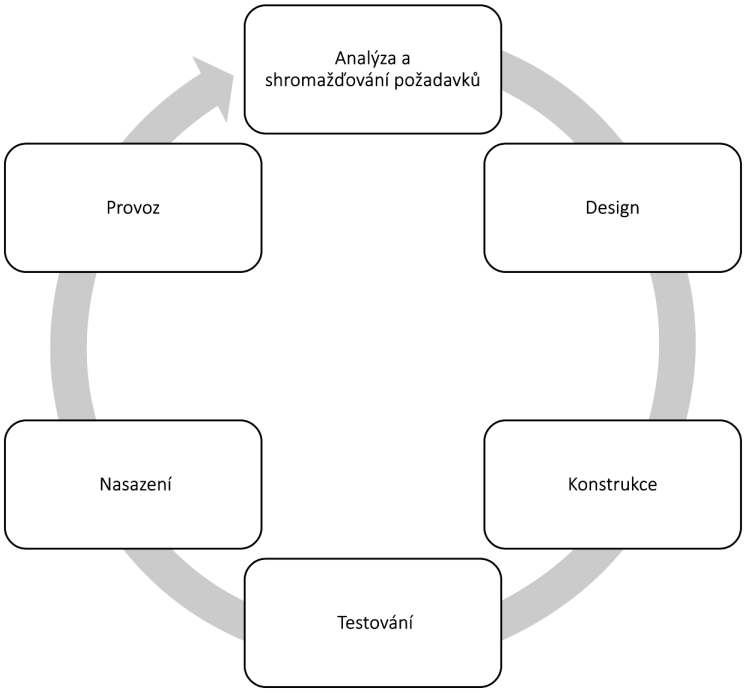
Společnost KPCS chce navrhnout aplikaci, která bude rozšiřovat znalosti všech jejich zaměstnanců v oblasti sociálního inženýrství a to především v odhalení potencionálně škodlivých e-mailových zpráv. V minulých kapitolách jsem rozebrala různé oblasti sociálního inženýrství. Poznatky jsem využila při tvorbě obsahu vzdělávacích kurzů. Tato kapitola popisuje současná řešení, které organizace ke školení a testovaní zaměstnanců mohou využívat, metody vývoje softwaru a návrh vlastní vzdělávací aplikace.

6.1 Životní cyklus vývoje softwaru

Životní cyklus vývoje softwaru neboli software development life cycle (SDLC) je proces plánování, psaní a úprav softwaru. Zahrnuje soubor postupů, metod a technik používaných při vývoji softwaru. Vývojáři tento přístup využívají při navrhování a psaní moderního softwaru pro počítače, cloudové nasazení, mobilní telefony, videohry a další. SDLC pomáhá zajistit, aby se do správných činností ve správný čas zapojili správní lidé. Umožňuje měřit pokrok ve vztahu k stanoveným cílům a poskytuje způsob, jak zajistit, že je vše na správné cestě. (Přel. Petrtýlová Markéta) [50]

Proces životního cyklu vývoje softwaru zahrnuje všechny aspekty procesu tvorby softwaru. Začíná stanovením rozsahu požadavků pro program, a končí jeho dodáním a správou protokolů údržby. Každá fáze SDLC má svůj vlastní soubor činností, které musí provádět členové týmu zapojení do vývojového projektu. Cyklus se může lišit společnost od společnosti a projekt od

projektu, ale obecně zahrnuje fáze zobrazené na obrázku 6.1. (Přel. Petrtýlová Markéta) [50] Tato kapitola představí první dvě fáze SDLC, ostatní budou popsány v následujících kapitolách.



Obrázek 6.1 Schéma SDLC (Přel. Petrtýlová Markéta) [51]

6.2 Analýza existujících konkurenčních řešení

První fáze SDLC je analýza a sběr požadavků. Tato fáze má hlavní pozornost projektových manažerů a zainteresovaných stran. Konají se schůzky s manažery, zainteresovanými firmami a uživateli za účelem stanovení požadavků jako jsou: Kdo bude systém používat? Jak budou systém používat? Jaká data by měla být vkládána do systému? Jaká data by měl systém vydávat? Toto jsou obecné otázky, které jsou zodpovězeny během fáze shromažďování požadavků. Po shromáždění požadavků jsou tyto požadavky analyzovány z hlediska jejich platnosti. Studována je také možnost začlenění požadavků do vyvíjeného systému. (Přel. Petrtýlová Markéta) [51]

Součástí první části životního cyklu vývoje softwaru je také analýza trhu, tedy funkcí a výhod již nabízených řešení. Jelikož firma KPCS projevila zájem o možnost prodávat vzniklé řešení, které chtějí používat pro vzdělávání svých zaměstnanců, jsou pro ně ostatní vzdělávací platformy používané ve firemních prostředí konkurencí [52]. Zde jsou uvedeny příklady často využívaných konkurenčních řešení.

6.2.1 Instructor

Společnost KPCS aktuálně používá vzdělávací platformu Instructor od společnosti Prevent. Toto řešení nabízí několik desítek před-připravených on-line kurzů, kurz na sociální inženýrství ani phishing však mezi nimi není. Některé z nich je možné po jejich zakoupení zdarma doplnit o konkrétní informace spojené s předpisy společnosti. Za poplatek pak nabízí zpracování doplňkových kurzů či zcela nových vzdělávacích kurzů. Tyto kurzy si však musí zákazník před-vytvořit v některých z nástrojů pro tvorbu prezentací, Prevent poskytuje vzorové šablony. (Přel. Petrtýlová Markéta) [53]

Na webových stránkách tohoto poskytovatele kurzů se firma označuje za jedničku na českém trhu a uvádí, že jejich služby používá více než 5 000 organizací. Interaktivní před-vytvořené kurzy jsou přístupné v českém jazyce a společnosti nabízí také dostupnost lektora pro dovysvětlení informací. (Přel. Petrtýlová Markéta) [53]

Co se týče ceny, tak ta se odvíjí od počtu dostupných a personifikovaných kurzů a počtu zaměstnanců. Balíček dvou před-vytvořených kurzů stojí pro společnost do 50 zaměstnanců 180 Kč na zaměstnance ročně s minimální cenou 1 800 Kč za organizaci. (Přel. Petrtýlová Markéta) [53]

6.2.2 LinkedIn learning

V rámci aplikace LinkedIn je možné zakoupit vzdělávací kurzy. Dle společnosti LinkedIn je na platformě nabízeno přes 16 000 kurzů v sedmi světových jazycích vytvořených experty v oboru, český jazyk však mezi nimi není. Je možné sledovat různé analýzy o pokrocích v učení, a to i ze strany zaměstnavatele, pokud tuto službu využíváte firemně. (Přel. Petrtýlová Markéta) [54]

Komunita podporuje zapojení uživatelů, takže LinkedIn Learning vytvořil nové a inovativní způsoby, jak se společně učit, včetně spojení s instruktory LinkedIn Learning a dalšími odborníky na témata napříč touto on-line vzdělávací platformou. (Přel. Petrtýlová Markéta) [54]

Tuto vzdělávací službu lze zakoupit běžně za 449 Kč na měsíc, pokud si budete za službu platit po celý rok. Druhou možností je jednorázová platba pouze na jeden měsíc za 889 Kč. (Přel. Petrtýlová Markéta) [55]

6.2.3 Viva Lerning

Mezi další nabízené možnosti spadá například Viva Learning. Kurzy jsou zde centralizované přímo v aplikaci Microsoft Teams pro rychlý přístup z tohoto populárního pracovního nastroje bez nutnosti jej opustit. Uživatelé se pomocí tohoto nástroje mohou učit, přidávat vlastní kurzy, sdílet kurzy i přidělovat kurzy pro splnění z pohledu manažera. (Přel. Petrtýlová Markéta) [56]

Součástí nabízených předem připravených kurzů je obsah z Microsoft Learn a Microsoft 365 Training, který je automaticky dostupný ve Viva Learning. Budete mít také volný přístup k sadě 125 kurzů z LinkedIn Learning. Kromě toho se do tohoto nástroje mohou integrovat vybrané kurzy a systémy pro management vzdělávání. Zdaleka ne všechny kurzy se však vyskytují v českém jazyce. (Přel. Petrtýlová Markéta) [56]

Microsoft Viva stojí 4 dolary (tedy k 24.02.2023 zhruba 22 Kč) na uživatele za měsíc, pro 50 uživatelů tedy zhruba 53 800 Kč za rok. Lze však zakoupit v Enterprise balíčku nebo s dalšími aplikacemi z rodiny Viva v rozšířeném balíčku. (Přel. Petrtýlová Markéta) [57]

6.2.4 Seduo.cz

Tato on-line vzdělávací platforma nabízí přes 360 kurzů, interaktivních webinářů a vzdělávacích programů v českém i slovenském jazyce. Zároveň nabízí různé soutěže a on-line setkání s experty pro zaměstnance, které prý přesvědčí až 70 % zaměstnanců zapojit se do vzdělávání. Toto řešení je používané ve více než 940 firmách. Platforma umožňuje náhled a administraci statistik o studiu zaměstnanců. Nenabízí však úpravu kurzů dle požadavků společnosti či možnost přidání vlastních kurzů. [58]

Pro 50 uživatelů za rok, což odpovídá počtu zaměstnanců společnosti KPCS, stojí platforma 164 150 Kč (bez DPH), tedy 3 283 Kč na uživatele ročně (bez DPH). [58]

6.2.5 Skillshare

Skillshare je platforma nabízející přes 35 000 kurzů v pěti světových jazycích, mezi kterými není jazyk český. Kromě běžných vzdělávacích kurzů pro společnosti se platforma zaměřuje na témata jako mentální zdraví, prezentační dovednosti a kreativní mysl. Součástí řešení jsou také analytiky zaměstnanců a možnosti přidělování kurzů konkretním zaměstnancům. Cena je 159 dolarů na uživatele na rok, tedy k 05.03.2023, kdy jeden dolar odpovídá zhruba 22 Kč, činí cena 3 498 Kč (pro 50 osob pak 174 900 Kč na rok). (Přel. Petrtýlová Markéta) [59]

6.2.6 Coursea

Tato vzdělávací platforma se odlišuje od ostatních zmíněných především tím, že nabízí kurzy od více než 275 předních univerzit na světe. Přes 3 000 firem po celém světě si vybralo tuto možnost vzdělávání. Platforma nabízí možnost dělení uživatelů do týmů dle jejich pracovní pozice a následné doporučovaní a přidělování kurzů pro splnění dle skupin. Umožňuje sledovat přehled pokroků zaměstnanců v analytikách. (Přel. Petrtýlová Markéta) [60]

Pro společnost do 125 zaměstnanců stojí portál 399 dolarů na uživatele na rok, což k 03.05.2023, kdy 1 dolar odpovídá zhruba 22 Kč, vyjde při 50 zaměstnancích společnost na 105 339 Kč ročně. (Přel. Petrtýlová Markéta) [61]

6.2.7 Knowee

Knowee je jednotným úložištěm, kde zaměstnanci naleznou všechny potřebné informace, od návodů přes podklady pro onboarding až po návody pro IT technologie. Vedle již obsažených kurzů lze do Knowee za pomoci intuitivního editoru snadno nahrávat i vlastní obsah včetně možnosti vkládat videa. Součástí Knowee je reporting pro možnost vyhodnocení zaměstnaneckého vzdělávání. Kromě toho je možné sledovat, který zaměstnanec se seznámil s jakým obsahem. S Knowee lze pracovat přímo v platformě Microsoft Teams. [62]

Aktuálně Knowee zahrnuje 100 videí a 250 textových návodů na osm technologií – Outlook, Teams, OneDrive, Forms, Stream, To Do, Planner a Sharepoint on-line. Knowee se před-připravenými kurzy zaměřuje na vzdělávání v oblasti kancelářského balíčku Microsoft 365. Kurzy jsou v českém i anglickém jazyce. [63]

6.2.8 Hodnocení konkurence

Jelikož společnost KPCS vidí jako jeden z hlavních benefitů vzdělávací platformy možnost k ní mít přístup přímo z komunikační platformy Micorsoft Teams [52], jak je později uvedeno v klíčových požadavcích, jediné z hojně používaných řešení pro vzdělávání nabízející tuto možnost je Viva Learning. Kurzy tu však nemají překlad do českého jazyka, a tak je nutné si vytvořit vlastní kurz, který si přidáte k ostatním kurzům na této platformě.

6.3 Požadavky společnosti KPCS

Stále součástí první fáze SDLC je také sběr požadavků, ten probíhal při této práci metodou polo-strukturovaného rozhovoru se čtyřmi zástupci společnosti KPCS, z čehož byli tři zástupci technických oddělení a jedna zástupkyně personálního oddělení. Nejdříve v této části představím klíčové požadavky a poté rozdělím požadavky KPCS na funkční a nefunkční.

6.3.1 Klíčové požadavky

Pro tento projekt byly definovány tři klíčové požadavky. Společnost KPCS požaduje řešení používat pro vzdělávání svých zaměstnanců, ale i jej prodávat, jak bylo uvedeno již v minulé sekci.

Hlavním požadavkem je, aby řešení bylo postavené na produktech z balíčku aplikací Microsoft Power Platform a platformě PowerBI od společnosti Microsoft. Tato řešení je totiž možné používat v rámci platformy pro firemní komunikaci Microsoft Teams i jako individuální webovou aplikaci. [52]

Jelikož se chce firma v následujícím období zaměřit na zlepšení vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti a především sociálního inženýrství, požaduje, aby vytvořené řešení obsahovalo kurzy, které budou tyto znalosti rozvíjet a testovat. [52]

Společnost chce mít přehled o pokrocích a učení zaměstnanců, a proto požaduje vytvořit také přehled, kde tyto informace může sledovat. [52]

6.3.2 Funkční požadavky

Funkční požadavky se zaměřují na to, jak musí software fungovat, a specifikují požadované chování systému. Příkladem těchto požadavků je, že při splnění specifické podmínky systém musí poslat uživateli e-mailovou zprávu. Dalším příkladem je, že údaje o mzdách mohou zobrazit pouze zaměstnanci na úrovni vedení. (Přel. Petrtýlová Markéta) [64] V tabulce 6.1 jsou uvedeny funkční požadavky tohoto projektu.

Tabulka 6.1 Přehled funkčních požadavků

F1	Ukládání úspěšných i neúspěšných dokončených pokusů o splnění kurzu. [65]
F2	K aplikaci mají přístup pouze uživatelé, kteří jsou zaměstnanci firmy KPCS. [52]
F3	Každý kurz lze ukončit vrácením se do menu v průběhu plnění kurzu. [66]
F4	Možnost vzdělávání přímo v Microsoft Teams pro rychlý přístup ke kurzu z komunikační platformy. [52]
F5	Vytvoření přehledu sebraných dat o studiu a výsledcích zaměstnanců. [52]
F6	Pro každý rok se dá zvolit libovolný den, do kterého musí zaměstnanci splnit jednotlivé kurzy. [65]
F7	Po splnění kurzu se zašle uživateli potvrzující e-mailová zpráva o splnění. [67]
F8	Řešení bude přístupné na tabletech i počítačích. [52]
F9	V aplikaci lze indikovat splnění kurzu podle získání odznaku. [66]
F10	Aplikace bude ukazovat požadované datum splnění pro splnění jednotlivých kurzů pro daný rok. [65]
F11	Kurz bude možné opakovat i po jeho splnění. [67]
F12	Po zadání tří špatných odpovědí v rámci jednoho plnění kvízu bude kvíz ukončen a uživatel bude přesměrován na stránku s oznámením o neúspěšném projití kurzu. [67]
F13	Otázky v kurzu Phishing se generují náhodně. [67]
F14	Ukládat seznamu otázek v kvízu zaměřeném na phishing, kde se otázky generují náhodně. [67]

6.3.3 Nefunkční požadavky

Nefunkční požadavky jsou zásadní pro použitelnost softwarového systému, a pokud nejsou definovány pečlivě, může to nepříznivě ovlivnit zkušenost koncových uživatelů. Příkladem nefunkčních požadavků je definování, jak rychle se musí webová stránka načítat, nebo určení, že webová stránka musí obsloužit 10 milionů uživatelů, aniž by měla nějaké problémy s výkonem. S bezpečností mohou souviset i nefunkční požadavky, například uživatel musí změnit své počáteční přihlašovací heslo při prvním přihlášení. (Přel. Petrtýlová Markéta) [64] Tabulka 6.2 obsahuje nefunkční požadavky tohoto projektu.

Tabulka 6.2 Přehled nefunkčních požadavků

N1	Aplikace bude obsahovat vzdělávací texty o sociálním inženýrství v českém jazyce. [52]
N2	Přístup k aplikaci budou mít všichni zaměstnanci. [52]
N3	Aplikace bude obsahovat dva kurzy zaměřené na sociální inženýrství a rozeznávaní e-mailových zpráv obsahujících phishing. [52]
N4	Barvy v aplikaci budou vycházet z poskytnuté palety barev společnosti KPCS. [52]
N5	Řešení má být postavené na platformě Microsoft Power Platform, na jejíž používání má již společnost zakoupené licence, její zaměstnanci s ní mají zkušenosti a KPCS plánuje v této oblasti růst. [52]
N6	Při vytváření obsahu kurzů preferuje společnost KPCS jako zdroj informací a podkladů především materiály od společnosti Microsoft. [52]

6.3.4 Součinnost

Úspěšnost projektu je podmíněna součinností ze strany společnosti KPCS. Součinnost je rozdělena do tří kategorií: lidské zdroje, ostatní projekty a infrastruktura.

6.3.4.1 Lidské zdroje

Jedná se o konkrétní součinnost zaměstnanců společnosti KPCS s dodavatelem. Především je nutné provést následující aktivity dle pracovních pozic.

Projektový manažer Společnost KPCS stanoví kompetentního zástupce s příslušnými pravomocemi pro řízení pracovníků zákazníka v rámci projektu. Během projektu bude projektový manažer ze společnosti KPCS pravidelně informován o stavu projektu, bude provádět klíčová rozhodnutí a finální akceptaci. Ideálně na tuto pozici zvolí osobu ze středního managementu, která bude schopna v rámci schůzek během práce na projektu definovat s dodavatelem detailní požadavky na součinnost.

Klíčoví a běžní uživatelé KPCS zajistí dostatečnou kapacitu odpovědných klíčových a běžných uživatelů. Ti budou během projektu průběžně, podle předem definovaného harmonogramu, spolupracovat s dodavatelem na analýze, návrhu a implementaci systému, včetně testování a akceptace výstupů projektu. Očekává se jejich účast na plánovaných schůzkách. Je nutné vybrat i zkušenější uživatele a vybrané zástupce managementu, kteří budou mít dostatečnou časovou kapacitu.

Testeři Společnost KPCS dedikuje dostatečně velký tým testerů, kteří budou schopni ve spolupráci s dodavatelem otestovat výstupy projektu. Testeři by měli být vybráni jak z oblasti klíčových, tak i běžných uživatelů, aby byly testy komplexní a věrohodné.

6.3.4.2 Ostatní projekty

Ve společnosti KPCS ani u dodavatele v současné době neprobíhá žádný souběžný projekt, který by výrazným způsobem mohl ovlivnit implementaci vzdělávací aplikace. [52]

6.3.4.3 Infrastruktura

Zadavatel zajistí technickou vybavenost společnosti společně s potřebnými licencemi pro přístup k aplikaci a připraví své prostředí i zaměstnance pro nasazení systému. [52]

6.3.4.4 Podpora systému po nasazení

V rámci reálného provozu bude společnosti KPCS ze strany dodavatele poskytována podpora funkčnosti systému v rozsahu 5 MD, kterou může KPCS využít pro drobné úpravy aplikace nebo školení uživatelů. Rozsáhlejší podpora a správa aktualizací a projektu do budoucna není zahrnuta.

6.3.4.5 Součinnost dle etap a počtu člověkodní (1. etapa)

V tabulce 6.3 je představena požadovaná součinnost zadavatele práce. Zobrazen je zde přehled objemu součinnosti v jednotlivých fázích projektu. Tento přehled navazuje na časový harmonogram ze sekce 6.7. Minimální požadovaná součinnost pro první etapu je dle tabulky 24 MD.

6.3.4.6 Součinnost dle etap a počtu člověkodní (2. etapa)

Dle harmonogramu projektu, který je detailně popsán v sekci 6.7, je v druhé etapě dodavatelem poskytnuto 5 MD na představení aplikace uživatelům a podporu. V rámci toho času bude dedi-

Tabulka 6.3 Součinnost v 1. etapě

Fáze projektu	Délka součinnosti
Definování a schválení zadání	2 MD
Schválení návrhu designu	1 MD
Schválení obsahu vzdělávacích kurzů	2 MD
Schválení návrhu aplikace	3 MD
Testování řešení před nasazením	5 MD
Akceptace řešení pro možnost nasazení aplikace	3 MD
Nasazení finální verze aplikace	3 MD
Testování nasazeného řešení	5 MD
Celkem	**24 MD**

kován minimálně jeden zaměstnanec společnosti KPCS pro školení o aplikaci a podporu systému po nasazení. Minimální požadovaná součinnost pro druhou etapu je 5 MD při komunikaci s jedním zaměstnancem společnosti. Celkem pak minimální požadovaná součinnost činí za obě etapy 29 MD.

6.3.5 Technologická a jiná omezení

Společnost KPCS požaduje použít pro vývoj primárně řešení Microsoft Power Platform, tedy sadu podnikových aplikací zaměřených na pomoc organizacím transformovat způsob, jakým zaměstnanci pracují. Kolekce aplikací zahrnuje Power Automate, Power Apps, Power Virtual Agents a Power Pages. (Přel. Petrtýlová Markéta) [68] Zaměstnanci KPCS jsou s tímto prostředím seznámeni, běžně s ním pracují a mají zakoupené potřebné licence pro všechny zaměstnance. [52]

6.4 Návrh řešení

Tento krok je již v druhé fázi SDLC, tedy Designu. V této fázi je návrh systému a softwaru připraven ze specifikací požadavků, které byly studovány v první fázi. Návrh systému pomáhá při specifikaci hardwarových a systémových požadavků a také při definování celkové architektury systému. Specifikace návrhu systému slouží jako vstup pro další fázi modelu. (Přel. Petrtýlová Markéta) [51]

Na základě požadavků získaných od zaměstnanců společnosti KPCS byla pro tento projekt navržena architektura vyobrazená na obrázku 6.2.

Obrázek 6.2 Návrh architektury

6.4.1 Obsah prvního kurzu

Po konzultaci se společností KPCS byla odsouhlasena následující osnova pro první vzdělávací kurz. Podkladem pro vzdělávací texty v aplikaci jsou první až pátá kapitola této bakalářské práce, které analyzují oblast sociálního inženýrství. Osnova prvního vzdělávacího kurzu je následující:

- Jak velký dopad mají útoky sociálního inženýrství.
- Příklad úspěšně provedeného útoku z posledních let.
- Představení jednotlivých typů sociálního inženýrství, a na co si u nich dávat pozor:
  - E-mail Phishing.
  - Spear Phishing.
  - Whaling.
  - Smishing.
  - Vishing.
  - Baiting.
  - Scareware.
  - Pretexting
  - Honey Trap.

- Spamming.

- Na koho jsou útoky mířeny.

- Jak postupovat v případě napadení.

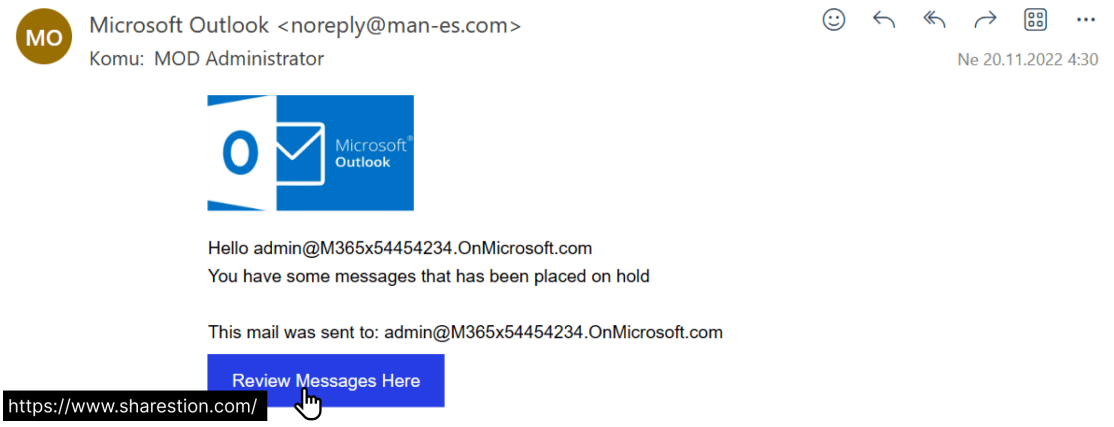
Kurz bude proložen deseti otázkami na právě probraná témata, ze kterých uživatel pro splnění kurzu bude muset správně zodpovědět osm. [66]

6.4.2 Obsah druhého kurzu

Druhý vzdělávací kurz bude zaměřený na rozpoznávání útoků typu phishing v e-mailové komunikaci [66], což je dle analýzy z předešlých kapitol nejčastější forma útoku sociálního inženýrství.

Pro vytvoření grafických podkladů k tomuto návrhu kurzu na rozpoznávání škodlivých e-mailových zpráv byl využit simulátor phishing útoků od společnosti Microsoft. Pomocí tohoto nástroje byly z pohledu administrátora vytvořené kampaně simulující různé druhy útoků. Ty jsou v běžném případě rozeslány zaměstnancům pro zjištění počtu lidí, kteří se na podvod nachytají a jejich následné možné cílené edukace. V tomto případě však z těchto před-připravených útoků byly pořízené podklady pro kurz na téma phishing, a zaslány tak byly jen samotnému administrátorovi. (Přel. Petrtýlová Markéta) [69]

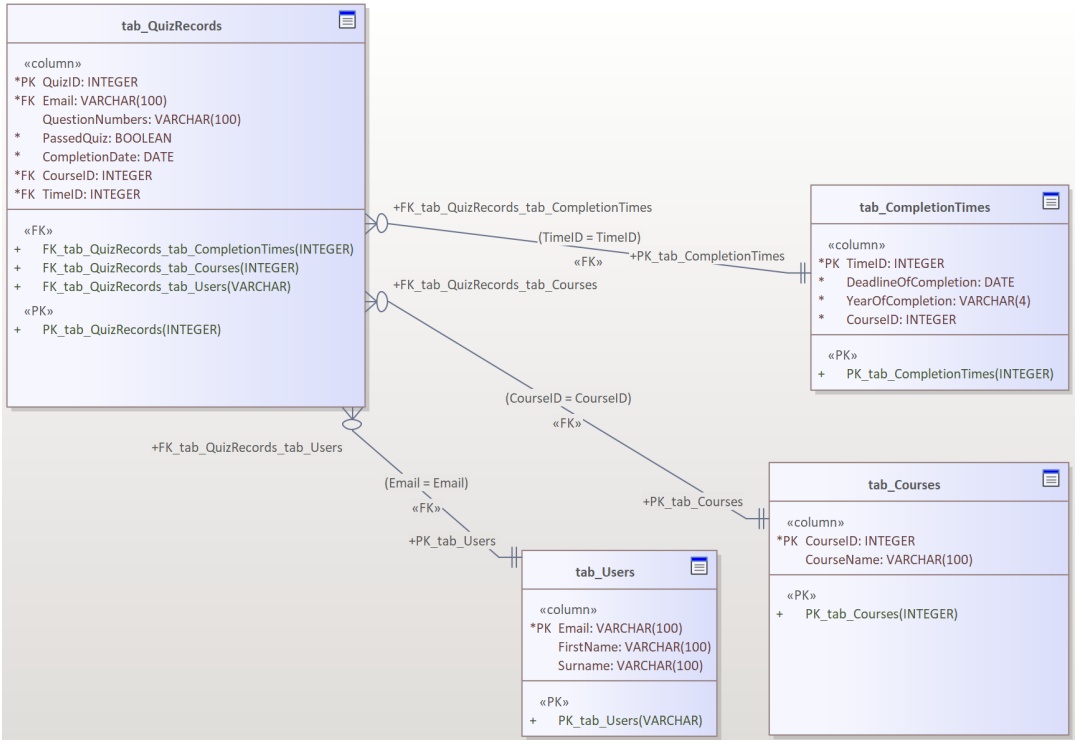
Provádět tyto simulace lze, pokud daná organizace má plán Microsoft 365 E5 nebo Microsoft Defender pro Office 365 Plán 2. Pro tvorbu tohoto projektu byl vygenerován zkušební tenant s plánem Microsoft 365 E5. (Přel. Petrtýlová Markéta) [70] Tenant je digitální reprezentace organizace a je primárně spojen s doménou, jako je Microsoft.com. Je to prostředí spravované prostřednictvím Azure Active Directory, které umožňuje přidělovat uživatelům oprávnění ke správě prostředků Azure a fakturace. (Přel. Petrtýlová Markéta) [71]



Obrázek 6.3 Příklad podvodné zprávy ze simulátoru

6.4.3 Databáze

Návrh databázového modelu byl vytvořen pomocí nástroje Enterprise Architect, celopodnikového řešení pro vizualizaci, analýzu, modelování, testování a údržbu systémů, softwaru, procesů a architektur. Zobrazuje jej obrázek 6.4.



Obrázek 6.4 Návrh databázového modelu

6.4.4 Grafický návrh aplikace

Efektivní návrh uživatelského rozhraní umožňuje uživatelům rychle a přehledně najít co hledají a snadno tak dosáhnout svého cíle. Při návrhu vzdělávací aplikace byl kladen důraz na několik následujících principů.

Udržujte jednoduchý design uživatelského rozhraní Nezapomeňte, pro koho aplikaci navrhujete a jaký má být její účel. Dobrý design uživatelského rozhraní je praktický, ne dekorativní. Dekorativní design odvádí pozornost od prvků, které jsou pro uživatele skutečně relevantní. (Přel. Petrtýlová Markéta) [72]

Předvídejte Ujistěte se, že plně rozumíte svému uživateli a jeho potřebám. Jakmile toho dosáhnete, budete moci předvídat, co bude uživatel chtít dělat dál. Tak mu můžete poskytnout přesně ty nástroje, informace a zdroje, které potřebuje. (Přel. Petrtýlová Markéta) [72]

Ponechte kontrolu uživateli Uživatel by měl cítit plnou kontrolu nad aplikací. Nikdy by neměl mít pocit, že ho rozhraní nutí k určité akci nebo dělá rozhodnutí za něj. I když některých případech to může být přesně to, co se děje. (Přel. Petrtýlová Markéta) [72]

Buďte konzistentní Důležité je nebýt konzistentní pouze v rámci daného projektu, ale také s průmyslovými standardy používanými jinde. Takto bude aplikace pro uživatele daleko intuitivnější. (Přel. Petrtýlová Markéta) [72]

Vyhněte se zbytečným složitostem Vždy se snažte o co nejmenší počet kroků, které uživatel musí udělat, aby se dostal k tomu, co hledá. (Přel. Petrtýlová Markéta) [72]

Přehledná navigace Navigace v aplikaci by neměla být v žádném případě zastrašující nebo matoucí, a to ani pro začátečníky. Místo toho by průzkum rozhraní měl být zábavný a probíhat téměř nevědomě. (Přel. Petrtýlová Markéta) [72]

Buďte tolerantní k chybám Chyby se stávají a uživatelé mění názor. Usnadněte přechod zpět či na domovskou stránku vždy, když by se to uživatelům mohlo hodit. Uchovávejte změny, které uživatel provedl. Nejen, že to pomůže vyhnout se frustraci ze ztracených dat a promarněného času, ale dává to uživatelům jistotu prozkoumat aplikaci a provádět změny beze strachu z negativních důsledků. (Přel. Petrtýlová Markéta) [72]

Poskytněte relevantní zpětnou vazbu Informujte uživatele o jejich pokroku. Poskytněte potvrzení, že jejich akce byly přijaty. Dejte jim vědět, že věci probíhají jak mají. (Přel. Petrtýlová Markéta) [72]

Určete prioritu funkcí Neschopnost vytvořit jasnou hierarchii je jednou z nejčastějších překážek, které lidem brání navrhnout skutečně minimální a efektivní uživatelské rozhraní. Každá položka na obrazovce by měla být pro uživatelskou zkušenost naprosto nezbytná. Přesto i mezi těmito základními položkami budou některé nevyhnutelně důležitější než jiné. Tato hierarchie by se měla jasně odrážet v návrhu uživatelského rozhraní. (Přel. Petrtýlová Markéta) [72]

Usnadněte práci s aplikací Nepředpokládejte, že všichni uživatelé jsou stejní jako vy a lidé, které znáte. To platí pro vše od technických znalostí a schopností až po světový rozhled. Aplikace používají lidé z velmi odlišného kulturního prostředí. I když realisticky nelze očekávat, že budete odpovídat za všechny možné variace ve společenské a kulturní konvenci, nepředpokládejte automaticky, že způsob, jakým věci děláte, je jediný logický způsob, jak je

dělat. Například v mnoha částech světa lidé čtou zprava doleva, takže umístění objektů zleva doprava nemusí nutně vést k tomu, že se s nimi všichni uživatelé setkají zleva doprava. (Přel. Petrtýlová Markéta) [72]

Před představením nástroje, který byl použit pro grafický návrh aplikace, je prvně důležité určit, co je to cloud. Tento termín nepředstavuje fyzický objekt, ale jedná se o rozsáhlou síť vzájemně propojených vzdálených serverů po celém světě, které fungují jako jeden ekosystém. Tyto servery jsou navržené buď k ukládání a správě dat, spouštění aplikací nebo doručování obsahu a služeb, jako je streamování videí, webová pošta, kancelářský software a sociální média. Namísto toho, aby byly k souborům a aplikacím získávány přístupy z místního nebo osobního počítače, lze k nim získat přístup on-line z jakéhokoli zařízení s podporou internetu – informace tak budou dostupné kdekoli a kdykoli. (Přel. Petrtýlová Markéta) [73]

Grafický návrh aplikace je vytvořen v kolaboračním nástroji pro návrh designu zvaný Figma. Toto řešení je založené na cloudových technologiích a odlišuje se tak od podobných nástrojů, které používáte většinou off-line na svém počítači nebo maximálně ukládáte do cloudu hotové soubory. (Přel. Petrtýlová Markéta) [74]

Ikony v aplikaci jsou vytvořené v prezentačním programu od společnosti Microsoft s názvem PowerPoint. Tento nástroj se nejčastěji používá k vytváření obchodních prezentací, ale může být také použit pro vzdělávací nebo neformální účely. (Přel. Petrtýlová Markéta) [75]

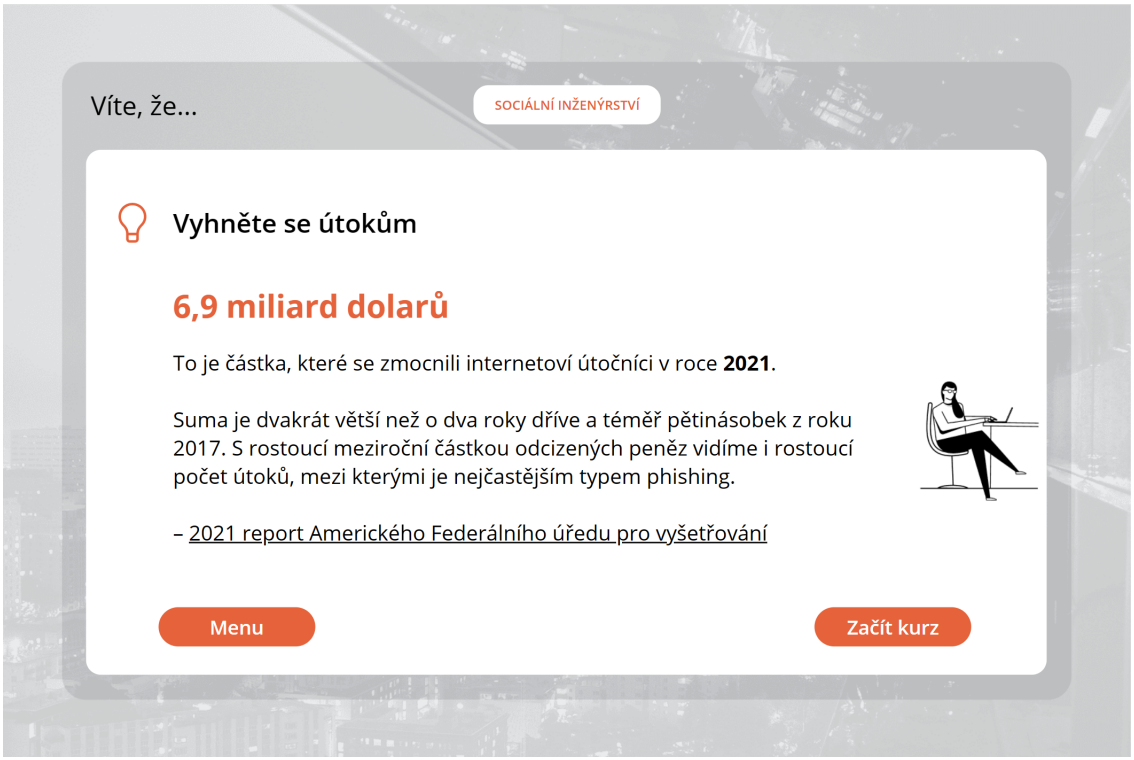
Grafický návrh byl vytvořen a následně i upravován dle požadavků společnosti KPCS, zápisy z těchto jednání i příprava na ně je součástí příloh této práce. Po odsouhlasení grafického návrhu začala práce na aplikaci. Více bude uvedeno v rámci příští kapitoly. Detailněji ukázané uživatelské rozhraní se nachází v příloze.

6.4.5 Návrh přehledu dat

Při návrhu přehledu dat je dobré dodržovat určitých zásad, aby přehled byl rychle a správně čitelný. Mezi ty nejdůležitějšími body, na které by měl každý před návrhem přehledu myslet, patří těchto deset:

Cíl přehledu Prvně je vhodné se zamyslet nad tím, pro koho je přehled vytvářen a za jakým účelem jej bude daná osoba či osoby využívat. Při tomto projektu bude přehled vytvořen pro manažery, personální oddělení či oddělení pro vzdělávání. Pro tyto osoby je požadavkem zobrazit data o tom, kolik lidí vzdělávací kurz splnilo, kdo jej nesplnil a kdo a kdy jej naopak již úspěšně ukončil.

Obrázek 6.5 Příklad první verze grafického návrhu



Obrázek 6.6 Příklad finálního grafického návrhu

Zobrazujte jen ta nejpotřebnější data Nezahlťte uživatele detaily, aby nepřehlédli důležité informace. V tomto reportu tedy nebude zobrazen konkretní den, kdy uživatel splnil kurz, ale postačí měsíc pro přehlednější zobrazení všech dat.

Snižte množství vizuálního šumu Odstraňte mřížky, barvy, ikony a popisky, které jsou nepotřebné a odvádí pozornost od čtených dat. Přehled bude tvořen v neutrálních barvách s důrazem na co nejméně zobrazených nadbytečných elementů.

Zaokrouhlete číselné údaje Zkrácení čísel zrychlí čtení. Zaokrouhlení na stejné množství desetinných míst čtení dat zpřehlední.

Používejte nejvíce vypovídající zobrazení dat Snažte se najít typ zobrazení, který data ukáže tak, že je bude možné co nejjednodušeji porovnávat. Sloupcový graf zobrazující dva podobně vysoké sloupce vedle sebe bude při malém rozdílu výšky lépe čitelný než malý rozdíl ve výřezu z koláčového grafu.

Seskupte data, která spolu souvisí Vizuálně seskupte data, která se ovlivňují nebo vypovídají o podobné věci. Naopak oddělte viditelně data, která spolu nesouvisí.

Buďte konzistentní Pokud zobrazujete spolu související data, zobrazujte je stejným způsobem.

Zobrazte hierarchii Ne všechna data jsou stejně důležitá. Nejdůležitějším údajům dedikujte větší prostor a směřujte je do levého horního rohu, kam běžně vedou první pohledy lidí.

Dejte číslům kontext Ukažte porovnání s výsledky z minulých let nebo ostatních sbíraných oddělení.

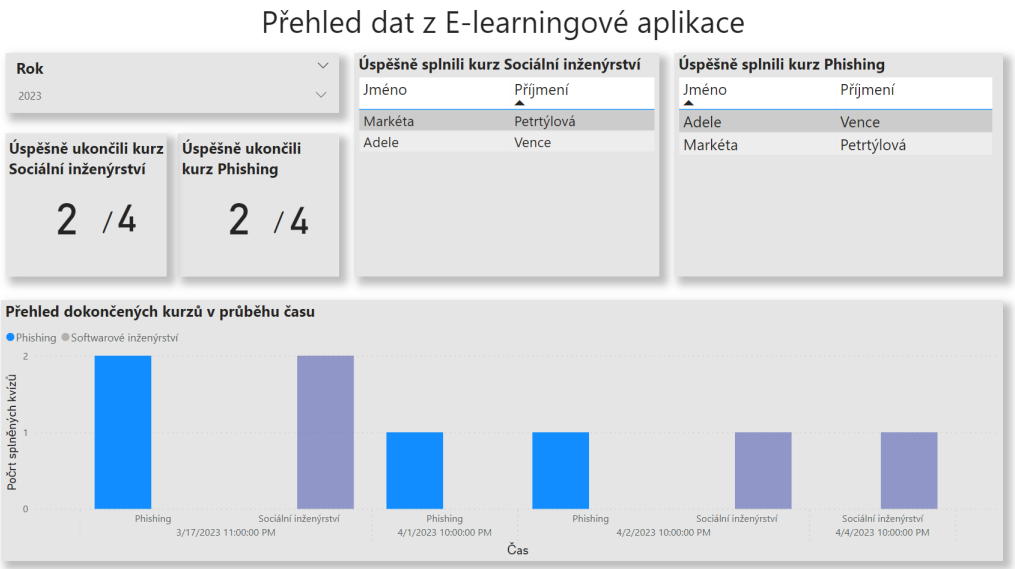
Používejte jednoduché popisy Přehledně ukažte, k čemu se data váží a jakému časovému úseku odpovídají. (Přel. Petrtýlová Markéta) [76]

Dle těchto bodů byl navržen přehled zobrazený na obrázku 6.7, který bude čerpá data z Dataverse, je vytvořen v prostředí PowerBI.

Při konzultaci se zákazníkem zákazník projevil zájem mít možnost filtrovat v přehledu dle uživatele, času a kurzu. [77] Dle těchto požadavků byl sestaven nový přehled. Konečná forma tohoto přehledu dat je představena v rámci následující kapitoly. 7.1.4

6.5 Change request (požadavky na změnu)

Oproti původnímu zadání je požadavkem do aplikace přidat e-mailové zprávy s potvrzením o úspěšném dokončení kurzu. Tato změna je zahrnuta v tomto projektu, a kvůli její nízké časové náročnosti neovlivní finanční část projektu. (Přel. Petrtýlová Markéta) [67]



Obrázek 6.7 Návrh přehledu dat

6.6 SWOT analýza

Tato analýza pomáhá identifikovat silné stránky, slabé stránky, příležitosti a hrozby pro konkrétní projekt nebo celý obchodní plán. Analýza je mocným nástrojem pro pomoc při identifikaci současného řešení a aktuálních tržních trendů. (Přel. Petrtýlová Markéta) [78]

6.7 Harmonogram projektu

V rámci přípravy na druhé jednání byla vytvořena tabulka 6.5 obsahující jednotlivé fáze projektu dělené dále do dvou etap. Harmonogram byl zákazníkovi představen v rámci druhé konzultace, jejíž příprava a zápis je součástí příloh této práce.

6.7.1 1. etapa (01.09.2022 až 30.04.2023)

Od počátku září 2022 začíná první etapa projektu. V této etapě bude provedena analýza konkurence i oblasti sociálního inženýrství. Dále bude navržena, implementována, nasazena a otestována aplikace.

Tabulka 6.4 SWOT analýza projektu

Silné stránky (Strengths)	▪ Snadná grafická úprava aplikace dle nároků zákazníka při prodeji tohoto řešení, i díky vyškoleným zaměstnancům KPCS v této oblasti. ▪ Možnost úpravy řešení do cizích jazyků. ▪ Možnost vytváření dalších kurzů v této aplikaci. ▪ Přístup k aplikaci skrze platformu Microsoft Teams. ▪ Přístup k aplikaci i analytikám z počítače i tabletu. ▪ KPCS má s technologiemi používanými při vývoji zkušenosti a plánuje se v této oblasti rozvíjet.
Slabé stránky (Weaknesses)	▪ Méně nabízených kurzů než nabízí jiné platformy. ▪ Společnost KPCS je v prodávání vzdělávacích aplikací o kybernetické bezpečnosti nováčkem.
Příležitosti (Opportunities)	▪ Příznivé podmínky na trhu, společnosti se zajímají o vzdělávání svých zaměstnanců a někdy poskytují kurzy zdarma jako benefit. ▪ Jen jeden konkurent, který se primárně zaměřuje na přidání vzdělávacího portálu přímo do platformy Microsoft Teams avšak nenabízí kurzy v českém jazyce. ▪ Kurzy jsou v českém jazyce, což je preference mnoha českých firem.
Hrozby (Threats)	▪ Zvýšení konkurence, která bude také nabízet možnost začlenit svoji platformu přímo do Microsoft Teams. ▪ Pokud by KPCS aplikaci prodávala, může se stát, že konkurence dokáže díky delšímu působení na trhu jít níže s cenou a zatraktivnit tak svoje řešení.

6.7.2 2. etapa (01.05.2023 až 05.05.2023)

Od počátku května 2023 začíná druhá etapa projektu zaměřená na servisní podporu a podporu uživatelů.

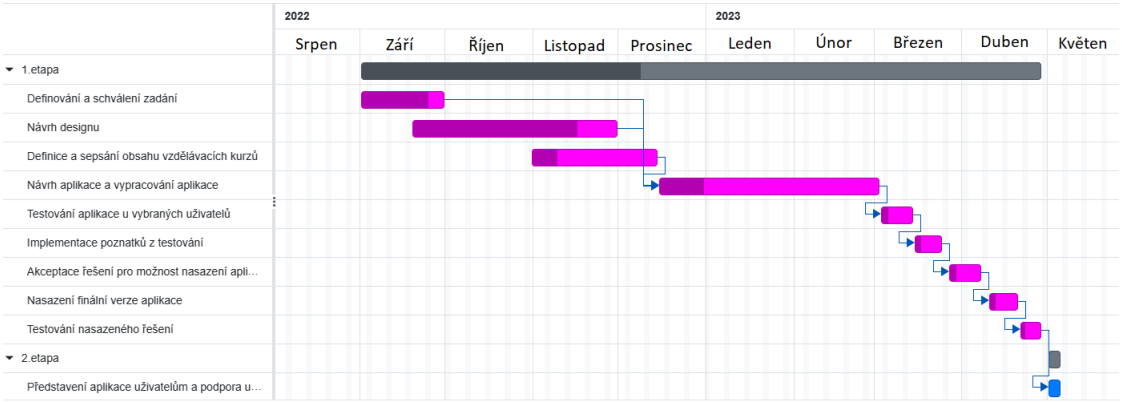
Podrobnější časový harmonogram je zobrazen na obrázku 6.8 v Ganttově diagramu. Ganttův diagram je jedním z nejoblíbenějších způsobů zobrazení aktivit v závislosti na čase. Vlevo na grafu je seznam aktivit a nahoře je vhodná časová škála. Každá činnost je znázorněna pruhem;

Tabulka 6.5 Harmonogram projektu

Fáze projektu	Délka trvání	Předběžné datum zahájení fáze
Definování a schválení zadání	5 MD	01.09.2022
Návrh designu	6 MD	19.09.2022
Definice a sepsání obsahu vzdělávacích kurzů	15 MD	31.10.2022
Návrh aplikace a vypracování aplikace	20 MD	15.12.2022
Testování řešení před nasazením	5 MD	03.03.2023
Implementace poznatků z testování	5 MD	15.03.2023
Akceptace řešení pro možnost nasazení aplikace	3 MD	27.03.2023
Nasazení finální verze aplikace	5 MD	10.04.2023
Testování nasazeného řešení	5 MD	21.04.2023
Představení aplikace uživatelům, podpora uživatelů	5 MD	01.05.2023
Celkem	**74 MD**	

pozice a délka pruhu odráží datum zahájení, trvání a datum ukončení aktivity. To umožňuje vidět na první pohled:

- Jaké jsou různé aktivity?
- Kdy každá činnost začíná a končí?
- Jak dlouho má každá aktivita trvat?
- Kde se aktivity překrývají s jinými aktivitami a do jaké míry?
- Datum zahájení a ukončení celého projektu. (Přel. Petrtýlová Markéta) [79]



Obrázek 6.8 Harmonogram v Ganttově diagramu

6.8 Cenová nabídka

Cenová nabídka je předběžná kalkulace ceny zakázky na zboží či službu, kterou si zákazník nechává vypracovat od potenciálního dodavatele před tím, než si službu či zboží objedná. Běžně si zákazník nechá vypracovat nabídky od rozdílných dodavatelů a následně se dle nich rozhoduje, kterého dodavatele pro zakázku zvolí. [80] Pro výpočty v této části sloužil jako podklad harmonogram projektu představený výše a poznatky z konzultací se společností KPCS. Zápisy z těchto konzultací jsou přílohami této práce. Ceny jsou počítány včetně DPH.

Náklady se definují jako spotřeba práce a prostředků v peněžním vyjádření. Lze říci, že náklady představují určité vstupy do podniku. Podnik tyto vstupy svými vnitřními mechanismy přetváří ve výstupy v podobě výrobků, prodaného zboží či vykonaných služeb. [81]

6.8.1 Mzdové náklady

Mzdové náklady jsou náklady přenesené na zaměstnavatele platbami do lidských zdrojů. Patří sem tedy mzda, příspěvek na sociální zabezpečení a soukromé pojištění, které zaměstnavatel svým zaměstnancům poskytuje. Lze také přenést výdaje jako odstupné, příspěvky, dopravu a samotné školení. [82]

Dle povahy projektu by se na projektu měli podílet především osoby na následujících pracovních pozicích:

Projektový manažer Řídí projekt, projektový tým, školení a komunikaci se zákazníkem. K 08.04.2023 je průměrný měsíční plat osob na této pozici v České republice 51 478 Kč [83].

UX/UI designér Podílí se na návrhu grafického designu aplikace a přehledu dat. K 08.04.2023 je průměrný měsíční plat osob na této pozici v České republice 59 676 Kč [84].

Programátor Pracuje na implementaci projektu, implementaci databáze a zhotovuje přehled dat. K 08.04.2023 je průměrný měsíční plat osob na této pozici v České republice 58 469 Kč [85].

Quality Engineer (Tester) Testuje řešení v rámci vývoje aplikace i po nasazení aplikace k zákazníkovi. K 08.04.2023 je průměrný měsíční plat osob na této pozici v České republice 47 873 Kč [86].

Jelikož na tomto projektu tyto role zastává jedna osoba, vypočteme její měsíční platové ohodnocení jako průměr měsíčních platových ohodnocení lidí na čtyřech zmíněných pracovních pozicích:

$$\text{Měsíční plat} = \frac{51\ 478 + 59\ 676 + 58\ 469 + 47\ 873}{4} = 54\ 365\ \text{Kč/měsíc}$$

V roce 2023 je 250 pracovních dní [87]. Vydělením tohoto čísla dvanácti, dle počtu měsíců, dostanete, že v jednom měsíci je necelých 21 dní. MD neboli man-day je jednotka která odpovídá jednomu pracovnímu dni jednoho člověka, tedy běžně 8 odpracovaných hodin.

Plat osoby pracující na tomto projektu za jeden den je poté měsíční plat vydělený průměrným počtem dní v měsíci neboli:

$$\text{Denní plat} = \frac{54\ 365}{21} \doteq 4\ 530\ \text{Kč/MD}$$

Jelikož vyšlo, že na projekt je nutné dedikovat 74 MD, vypočte se plat na celý projekt vynásobením denního platu počtem MD, za které by měl být projekt zhotoven:

$$\text{Plat za celé období práce na projektu} = 4\ 530 * 74 = 335\ 220\ \text{Kč}$$

Zaměstnavatelé však kromě platu za zaměstnance platí také sociální a zdravotní pojištění. Zdravotní pojištění je celkem 13,5 % ze mzdy, z toho jednu třetinu platí zaměstnanec a zbytek zaměstnavatel. Zaměstnavatel tedy platí 9 % ze mzdy. Sociální pojištění je celkem 31,5 % ze mzdy, z toho 6,5 % platí zaměstnanec, zbylých 25 % zaměstnavatel. [88] Výsledné mzdové náklady zaměstnavatele na jednoho zaměstnance se tedy skládají ze mzdy, ke které je připočteno 9 % ze mzdy na zdravotní pojištění a 25 % ze mzdy na sociální pojištění:

$$\text{Náklady za mzdu} = 335\ 220 + 335\ 220 * 0,09 + 335\ 220 * 0,25 \doteq 449\ 195\ \text{Kč}$$

6.8.2 Licence a prostory

Zákazník poskytl bezplatné prostředí pro vývoj aplikace, a tedy cena za licence v rámci vývoje je pro dodavatele nulová. Stejně tomu tak je i s prostory pro vývoj aplikace. Zákazník již vlastní všechny potřebné licence pro následné umožnění plného využívání aplikace pro všechny své zaměstnance.

6.8.3 Hardware

Společnost již obstarala všechna potřebná zařízení pro provoz aplikace, nikoliv však pro vývoj a podporu. Vývoj a podpora probíhala v rámci 9 měsíců (září 2022 až květen 2023). Pro vývoj aplikace lze využít například notebook Lenovo Yoga Slim 7 Pro 14IHU5 Slate, který je jeden z nejlevnějších notebooků v nabídce zařízení k zapůjčení na stránkách internetového obchodu

Alza a dostačuje pro vývoj, cena za měsíc je k 08.04.2023 476 Kč [89]. Za devět měsíců tedy pak 4 284 Kč.

6.8.4 Rezerva

K součtu cen za předchozí položky bude přičteno 20 % jako rezerva. Ta může být využitá také na drobné změnové požadavky zákazníka.

6.8.5 Celková cena

$$\text{Celkové náklady} = \text{Náklady za mzdu} + \text{Náklady za licence} + \text{Náklady za hardware} + \text{Rezerva}$$

$$\text{Celkové náklady} = 449\ 195 + 0 + 4\ 284 + (449\ 195 + 0 + 4\ 284) * 0,2 \doteq 544\ 175 \text{ Kč}$$

V ceně nejsou zahrnuty případné změnové požadavky neboli change requests, o které zákazník může projevit zájem. Ty budou řešeny vždy individuálně. Není zde také zahrnuté pořízení hardware, jelikož společnost již všechno potřebné vybavení obstarala. Maximální odchylka odhadu, s ohledem na definované požadavky a získané informace od společnosti KPCS, je ±20 %.

6.8.6 Porovnání s konkurencí

Cena odpovídá cenám středně velkých aplikací od společností nabízejících vývoj aplikace na zakázku. Za středně velkou ji můžeme dle konkurentů označit podle datových toků odesílajících e-mailové upozornění o dokončení kurzu nebo přehledu dat, který je vytvářen společně s aplikací. Společnost ThinkEasy prodává takovéto pokročilejší webové nebo mobilní aplikace od 350 000 Kč do 600 000 Kč. [90], [91] Firma Webfusion vyvíjí aplikace na míru od 100 000 Kč až po 3 000 000 Kč. [92]

6.9 Rizika

V této sekci jsou uvedena potenciální projektová rizika a potenciální rizika navrženého řešení.

6.9.1 Projektová rizika

Uvedená projektová rizika odpovídají rizikům, která se mohou při realizaci aplikace s nejméně malou pravděpodobností výskytu objevit.

Tabulka 6.6 Riziko RZ01: Neposkytnutí součinnosti zákazníka

Popis rizika:	Neposkytnutí součinnosti zákazníka.
Pravděpodobnost výskytu:	Malá.
Dopad:	Dopad na kvalitu projektu a termín jeho dodání.
Plán pro eliminování rizika:	Včasná eskalace problému na ostatní zaměstnance společnosti KPCS. Průběžné konzultace v rámci implementace projektu a reportování aktuálního stavu.
Krizový plán:	Dohoda se zákazníkem o posunutí termínu nebo změně rozsahu projektu. Zákazník uvedl, že nemá přesné časové požadavky na dodání projektu. [52]

Tabulka 6.7 Riziko RZ02: Zadrhávání komunikace mezi dodavatelem a zákazníkem

Popis rizika:	Zadrhávání komunikace mezi dodavatelem a zákazníkem.
Pravděpodobnost výskytu:	Malá.
Dopad:	Dopad na kvalitu projektu a termín jeho dodání.
Plán pro eliminování rizika:	Jasné určení pravidel stylu a nástrojů komunikace. Komunikace se zákazníkem probíhá přes e-mailové zprávy a konzultace přes platformu Microsoft Teams.
Krizový plán:	Dohoda se zákazníkem o změně komunikačních nástrojů či změně zaměstnance společnosti KPCS, se kterým dodavatel komunikuje.

6.9.2 Potenciální rizika navrženého řešení

Potenciální rizika navrženého řešení odpovídají rizikům, která mohou být způsobena výběrem daného návrhu aplikace. Tato rizika se vykytují nejméně s malou pravděpodobností výskytu.

Tabulka 6.8 Riziko RZ03: Možnost získání znalostí z jiného zdroje

Popis rizika:	Možnost získání znalostí z jiného zdroje.
Pravděpodobnost výskytu:	Střední. Řešení je pro zaměstnance postavené přímo na míru, avšak další výukové zdroje na toto téma se především v cizích jazycích vyskytují.
Dopad:	Nižší počet zaměstnanců, kteří jsou uživateli aplikace.
Plán pro eliminování rizika:	Seznámení zaměstnanců s možností vzdělávání a určení tohoto způsobu vzdělávání jako doporučeného jejich zaměstnavatelem. Komunikace se zadavatelem projektu o potřebách a preferencích jeho zaměstnanců.
Krizový plán:	Upravení kurzů dle zpětné vazby zaměstnanců společnosti KPCS pro spokojené používání aplikace.

Tabulka 6.9 Riziko RZ04: Nesprávný cenový odhad implementace projektu

Popis rizika:	Nesprávný cenový odhad implementace projektu.
Pravděpodobnost výskytu:	Střední.
Dopad:	Nutnost dalších investic nebo omezení funkčností aplikace.
Plán pro eliminování rizika:	Připravení detailního finančního plánu.
Krizový plán:	Do rozpočtu bude započítaná rezerva a zákazník bude obeznámen s možnými změnami konečné ceny od původního návrhu. Bude definována maximální odchylka odhadu ceny.

Tabulka 6.10 Riziko RZ05: Nasazení systému po plánovaném termínu

Popis rizika:	Nasazení systému po plánovaném termínu.
Pravděpodobnost výskytu:	Střední. Řešení je pro zaměstnance postavené přímo na míru, avšak další výukové zdroje na toto téma se především v cizích jazycích vyskytují.
Dopad:	Prodloužení aktuálního stavu plýtvání zdrojů. Další navýšení nákladů na implementaci řešení.
Plán pro eliminování rizika:	Vytvoření úvodní studie. Rozdělení projektu do etap. Klauzule ve smlouvě o nasazení systému po plánovaném termínu.
Krizový plán:	Včasné upozornění zadavatele a domluvení změny harmonogramu. Případné sankce pro dodavatele.

Kapitola 7

Realizace aplikace pro školení

Tato kapitola popisuje třetí až šestý bod SDLC, tedy vývoj, implementaci, testování a podporu. Kapitola se zaměřuje na to, jak bylo v jednotlivých krocích postupováno pro vytvoření školící aplikace. Zároveň jsou v této kapitole představeny další možné kroky vývoje aplikace, které jsou nad rámec vývoje v rámci této práce.

7.1 Implementace

Třetí fází SDLC je implementace neboli vývoj či konstrukce. Vzhledem k tomu, že v této fázi je vytvářen kód, v této části je zapotřebí především vývojářů. Jedná se běžně o nejdelší fázi životního cyklu vývoje softwaru. [51]

7.1.1 Implementace aplikace

Pro vývoj aplikace byla zvolena po konzultaci s KPCS platforma Power Apps. Jedná se o sadu aplikací, služeb, konektorů, a také datovou platformu, která poskytuje prostředí pro vývoj aplikací. Připojuje se k datům uloženým buď v základní datové platformě Microsoft Dataverse, nebo ke zdrojům dat jako je SharePoint, Microsoft 365, Dynamics 365, SQL Server,… Aplikace mají responzivní design a lze je spustit v prohlížeči i na mobilních zařízeních (telefonu nebo tabletu). (Přel. Petrtýlová Markéta) [93]

Aplikace je psaná v jazyce Power Fx, který je lze používat napříč platformou Microsoft Power Platform. Jde o silně typovaný, deklarativní a funkční programovací jazyk. (Přel. Petrtýlová Markéta) [94] Silně typovaný programovací jazyk je takový, ve kterém je každý typ dat, jako jsou celá čísla, znaky, desetinná místa, předdefinován jako součást programovacího jazyka a všechny kon-

Výpis kódu 7.1 Kolekce pro náhodné generování otázek

```
ClearCollect(col_randomNumber,FirstN(Shuffle(Sequence(var_questionCount)),
    var_questionGenerateCount));
Set(var_questionAnsweredCount,1);
Navigate(Scr_PhishingQuestions)
```

Výpis kódu 7.2 Ukládání dat do databáze

```
Patch(tab_QuizRecords,
      Defaults(tab_QuizRecords),
      {Email: User().Email,
      QuestionNumbers: Concat(col_randomNumber,Value & ","),
      PassedQuiz: If(var_numberOfTriesLeft >= 0, 1, 0),
      CourseID: 1001,
      CompletionDate: Today(),
      TimeID: LookUp(tab_CompletionTimes, YearOfCompletion = Text( Today(),
          "yyyy" ) && CourseID = 1000 ).TimeID
      }
);
```

stanty nebo proměnné definované pro daný program musí být popsány jedním z datových typů. (Přel. Petrtýlová Markéta) [95] Deklarativní programovací jazyk je typ programovacího jazyka, který nevyžaduje, aby programátor definoval kroky, které má stroj následovat, ale místo toho deklaruje a popisuje fakta a vztahy mezi datovými body a prvky. Koncový uživatel programu pak vytváří dotazy nebo hledá a přijímá výsledky na základě těchto dotazů. (Přel. Petrtýlová Markéta) [96] Funkční programování je přístup k vývoji softwaru, který používá funkce k vytvoření udržovatelného softwaru. (Přel. Petrtýlová Markéta) [97]

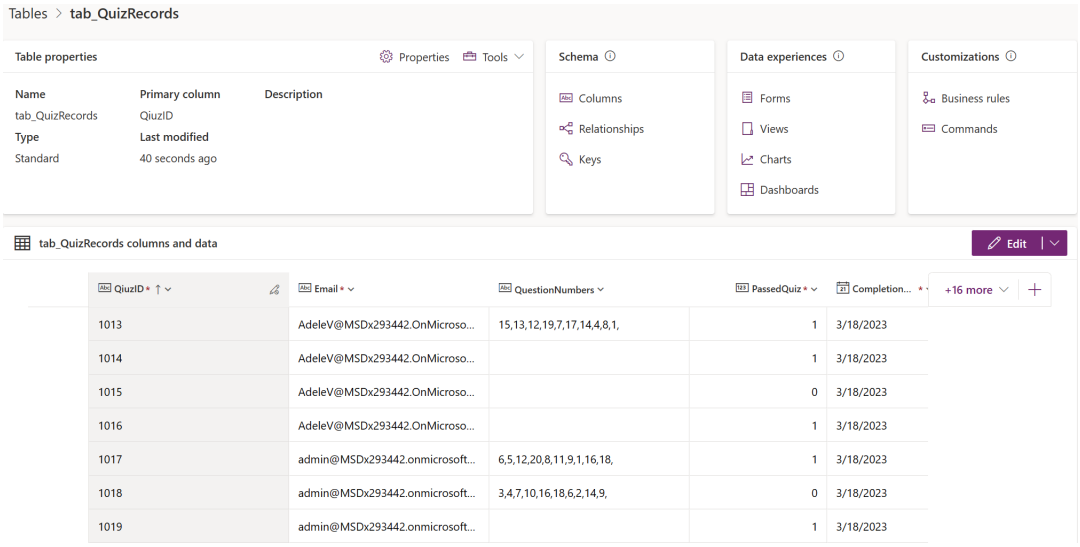
V následující části této kapitoly jsou příklady kódu aplikace napsané v jazyce Power Fx. Ukázka vývojového prostředí je poté umístěna v příloze M.1 společně s ukázkou vzniklé aplikace N.1. První ukázku kódu 7.1 je vybrání deset náhodných čísel z kolekce dvaceti čísel v náhodném pořadí. Tyto čísla vytvoří kolekci, díky které je poté v kurzu na phishing možné generovat náhodně deset otázek z dvaceti, na které mají uživatele v rámci kvízu odpovědět. Dále se v kódu nastavuje, že první otázka zobrazená uživateli bude pro něj v rámci kvízu označena jako první. Poslední řádek je poté ukázka přechodu na stránku aplikace, kde se zobrazí první otázka. Tento kód se v aplikaci spustí při kliknutí na tlačítko „Začít kurz".

Druhá ukázka kódu 7.2 představuje, jakým způsobem se odesílají data z aplikace do Dataverse. Konkrétně se jedná o zasílání údajů o kurzu na phishing v e-mailové komunikaci.

7.1.2 Implementace databáze

Dataverse umožňuje bezpečně ukládat a spravovat data, která používají podnikové aplikace. Data v Dataverse jsou uložena v sadě tabulek. Tabulka je sada řádků (dříve označovaných jako záznamy) a sloupců (dříve označovaných jako pole/atributy). Každý sloupec v tabulce je navržen tak, aby ukládal určitý typ dat, například jméno, věk, plat a tak dále. Dataverse obsahuje základní sadu standardních tabulek, které pokrývají typické scénáře, ale lze vytvořit vlastní tabulky specifické pro danou organizaci a naplnit je daty. Tvůrci aplikací pak mohou pomocí Power Apps vytvářet bohaté aplikace, které tato data využívají. (Přel. Petrtýlová Markéta) [98]

Pomocí Dataverse byly vytvořené čtyři tabulky odpovídající návrhu databázového modelu z minulé kapitoly 6.4. Ke specificky uloženým vlastním datům ukládá Dataverse automaticky metadata o záznamech jako jméno uživatele, který záznam vytvořil, čas vytvoření, čas poslední změny, ... Ukázka prostředí pro vývoj databáze s ukázáním tabulky pro ukládání záznamů o plnění kurzu je na obrázku 7.1.

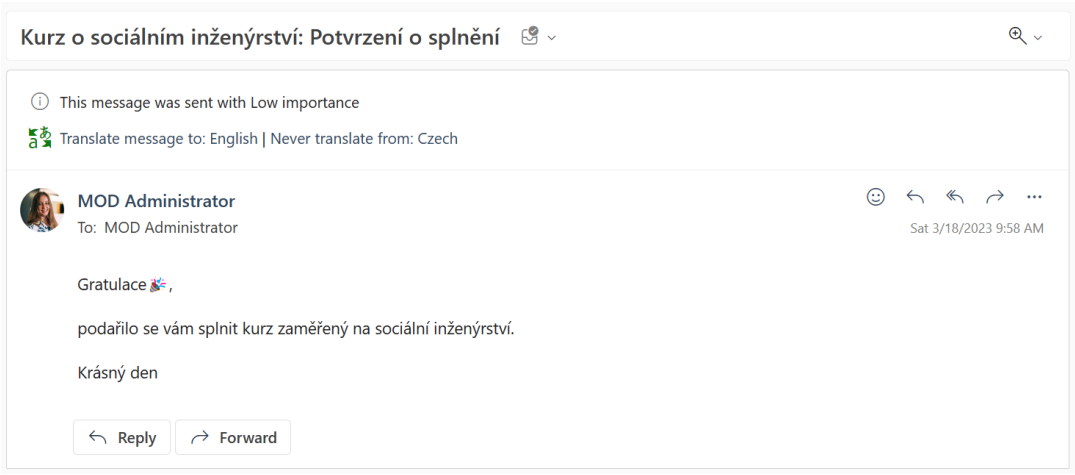


Obrázek 7.1 Ukázka prostředí pro vývoj databází

7.1.3 Pohyby s daty

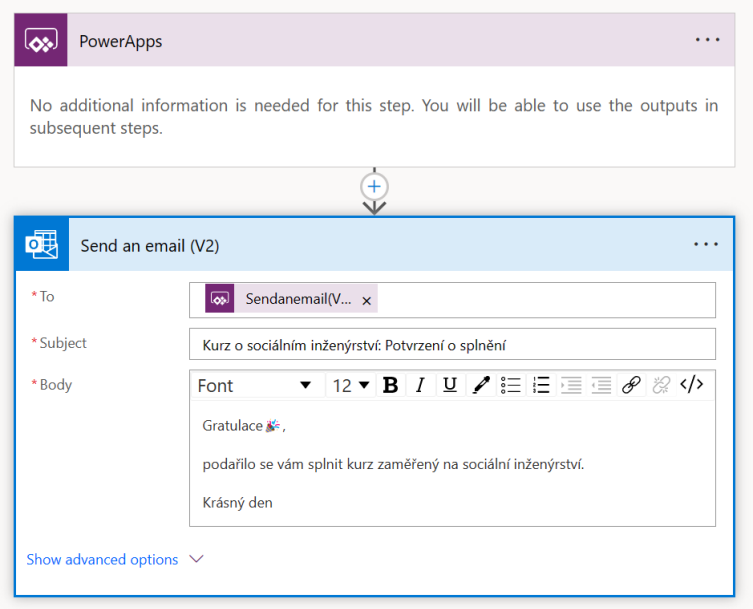
Datové toky jsou prováděny pomocí služby Power Automate. Tato služba pomáhá vytvářet automatizované pracovní postupy mezi aplikacemi a službami pro synchronizaci souborů, přijímání oznámení, shromažďování dat a další. [99]

E-mailová zpráva se odesílá pomocí Microsoft Outlook. Tento emailový klient se používá k odesílání a přijímání e-mailů, správě různých typů osobních údajů včetně schůzek v kalendáři a podobných záznamů, úkolů, kontaktů a poznámek. [100]



Obrázek 7.2 Ukázka e-mailové zprávy potvrzující splnění kurzu

Na obrázku 7.3 je zobrazen datový tok, který odešle e-mail s gratulacemi k dokončení kurzu o sociálním inženýrství.



Obrázek 7.3 Ukázka datového toku pro zaslání e-mailu po úspěšně dokončeném kurzu

Tento tok se zavolá v samotné školící aplikaci vytvořené v Power Apps. V ukázce kódu 7.3 je ukázána podmínka, kde se spustí datový tok, pouze pokud je kurz úspěšně dokončen.

Výpis kódu 7.3 Spuštění datového flow v aplikaci, pokud je kurz úspěšně ukončen

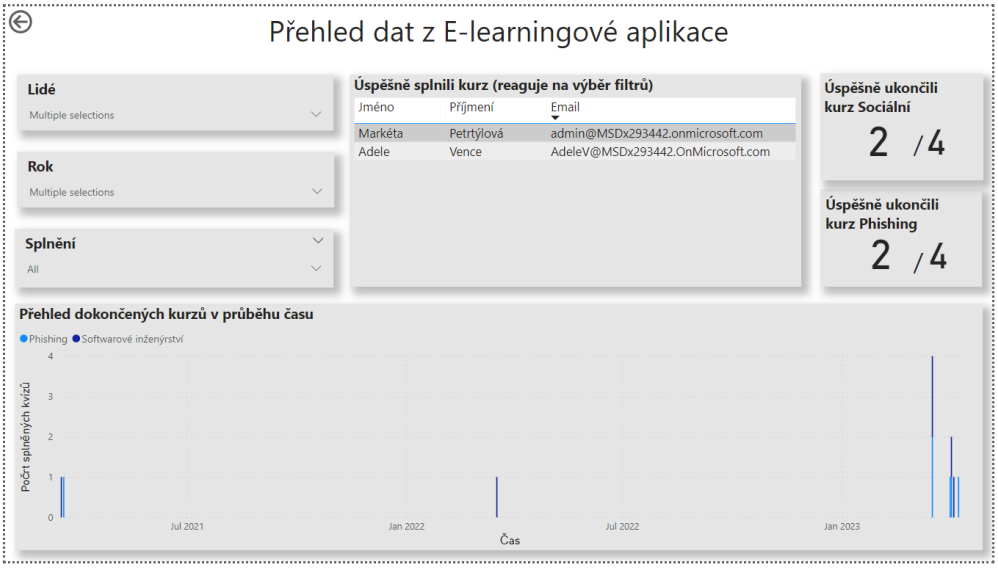
```
If(var_numberOfTriesLeft >= 0,CongratsPH.Run(User().Email, "","","));
```

7.1.4 Implementace přehledu analytik

K vytvoření přehledu analytik byl použit nástroj Power BI. Tento nástroj je kolekcí softwarových služeb, aplikací a konektorů, které spolupracují na přeměně nesouvisejících zdrojů dat na ucelené, vizuálně pohlcující a interaktivní přehledy. Data mohou být čerpána z Microsoft Excel, cloudu i na firemních serverech. (Přel. Petrtýlová Markéta) [101]

V power BI se používá jazyk Data Analysis Expressions (DAX). Tento jazyk se používá také v nástrojích Analysis Services a Power Pivot v Microsoft Excel. Vzorce jazyka DAX zahrnují funkce, operátory a hodnoty pro provádění výpočtů a dotazů na data v souvisejících tabulkách a sloupcích v tabulkových datových modelech. (Přel. Petrtýlová Markéta) [102]

Jak již bylo zmíněno v minulé kapitole u návrhu přehledu dat, zákazník měl výhrady k prvnímu návrhu přehledu a požadoval možnost filtrovat data dle uživatele, času a kurzu. [77] Na obrázku 7.4 je představena finální verze přehledu reflektující požadavky zákazníka.



Obrázek 7.4 Přehled analytik

7.1.5 Implementace regresních testů

Regresní testy se využívají při opětovném testování funkcí a vlastností aplikace. Jejich úkolem je ověřit, že provedené změny a implementace nových vlastností v aplikaci neměly žádný vliv na

stávající funkce a vlastnosti. Tedy především na oblasti, které zůstaly v kódu nezměněny. [103] V závislosti na velikosti a využití aplikace může stačit ruční testování nových změn. S rostoucí složitostí a pro veškeré kritické aplikace není však tato forma testování vždy vhodná, jelikož vyžaduje větší časovou investici. Regresní testování může trvat déle, než vývoj nových funkcí. Jednou z možností, jak zkrátit dobu potřebnou pro testování, je automatizace testování. Automatické testování pomáhá otestovat aplikaci s minimálním úsilím testerů, zkrátit dobu testování a identifikovat kritické problémy před nasazením. (Přel. Petrtýlová Markéta) [104]

K implementaci automatických regresních testů pro tento projekt bylo použito Power Apps Test Studio. Jedná se o řešení pro psaní, organizování a automatizaci testů pro aplikace vytvořené v prostředí Microsoft Power Platform. V Test Studio lze psát testy pomocí výrazů Power Apps nebo použít záznamník k uložení interakce s aplikací, aby se výrazy automaticky vygenerovaly. Písemné testy lze přehrávat v rámci Testovacího studia, pro ověření funkčnosti aplikace, lze také spouštět testy ve webovém prohlížeči a začlenit automatizované testy do procesu nasazení aplikace. [104]

Pro tento projekt bylo vytvořeno deset testů:

1. Test předčasného ukončení kurzu Phishing přejitím do okna Menu pomocí tlačítka s ikonou domu a odsouhlasením předčasného ukončení.

2. Automatické neúspěšné ukončení kurzu na téma phishing po zodpovězení třetí špatné odpovědi.

3. Úspěšné ukončení kurzu Phishing bez chybné odpovědi s odesláním dat do databáze a odesláním potvrzující e-mailové zprávy o dokončení kurzu.

4. Úspěšné ukončení kurzu Phishing s jednou chybnou odpovědí s odesláním dat do databáze a odesláním potvrzující e-mailové zprávy o dokončení kurzu.

5. Úspěšné ukončení kurzu Phishing s dvěma chybnými odpověďmi s odesláním dat do databáze a odesláním potvrzující e-mailové zprávy o dokončení kurzu.

6. Test předčasného ukončení kurzu o sociálním inženýrství přejitím do okna Menu pomocí tlačítka s ikonou domu a odsouhlasením předčasného ukončení.

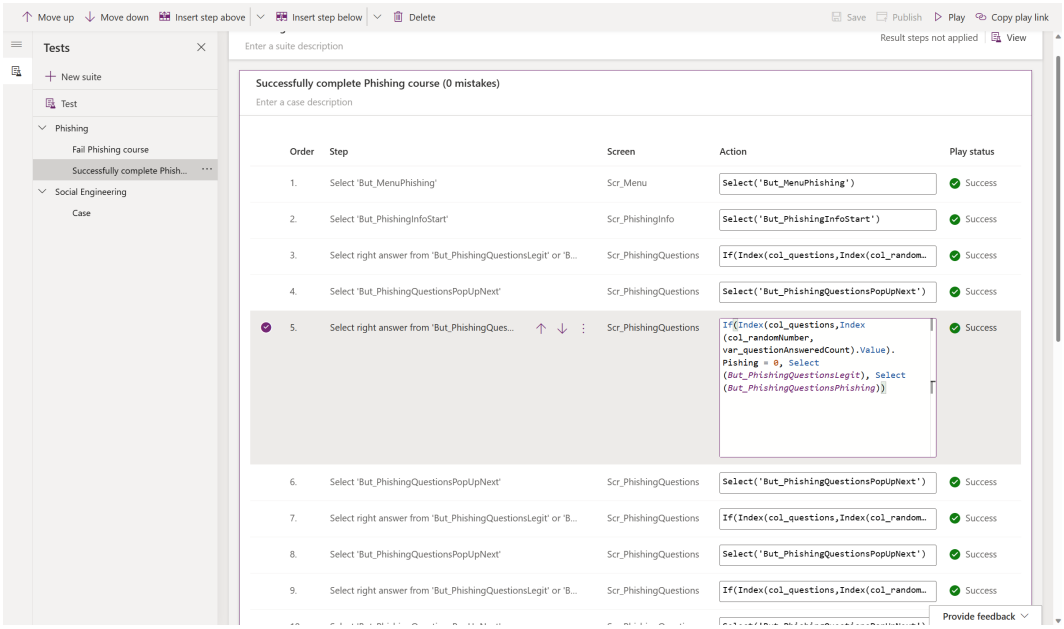
7. Automatické neúspěšné ukončení kurzu na téma sociální inženýrství po zodpovězení třetí špatné odpovědi.

8. Úspěšné ukončení kurzu Sociální inženýrství bez chybné odpovědi s odesláním dat do databáze a odesláním potvrzující e-mailové zprávy o dokončení kurzu.

9. Úspěšné ukončení kurzu Sociální inženýrství s jednou chybnou odpovědí s odesláním dat do databáze a odesláním potvrzující e-mailové zprávy o dokončení kurzu.

10. Úspěšné ukončení kurzu Sociální inženýrství s dvěma chybnými odpověďmi s odesláním dat do databáze a odesláním potvrzující e-mailové zprávy o dokončení kurzu.

Na následujících dvou obrazcích je ukázané vývojové prostředí pro tvorbu testů 7.5 a běh jednoho z testů 7.6



Obrázek 7.5 Ukázka prostředí pro vývoj testů

7.2 Nasazení

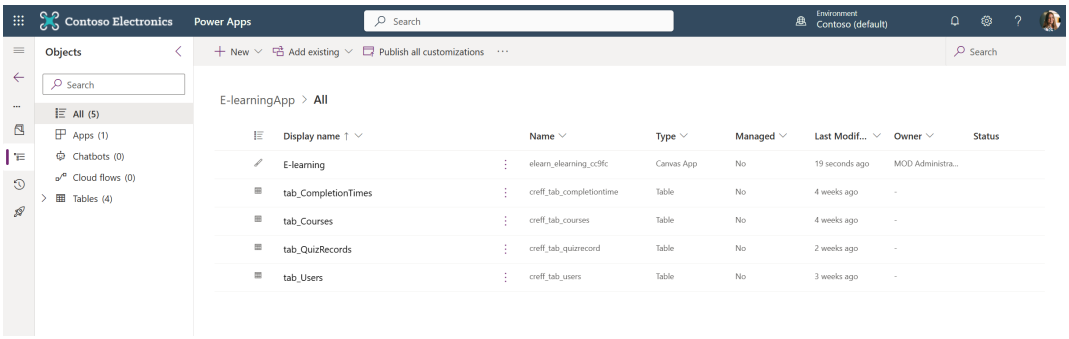
Následující postup pro nasazení aplikace reflektuje postup, který byl použit pro přenos aplikace včetně všech jejich komponent do prostředí zákazníka.

7.2.1 Příprava na nasazení a export aplikace

Pro nasazení byla aplikace, jejíž součástí jsou v tomto případě datové toky a regresní testy, společně s tabulkami v Dataverse, vložena do Solutions. Solutions (v překladu Řešení) se používají k přenosu aplikací a komponent z jednoho prostředí do druhého. Solutions může obsahovat jednu nebo více aplikací a také další komponenty, jako jsou mapy webu, tabulky, procesy, webové zdroje, volby, toky a další. (Přel. Petrtýlová Markéta) [105] Výhodou vložení komponent do tohoto balíčku je následný možný export celého balíčku jako celku, a tedy toto řešení umožňuje

Obrázek 7.6 Ukázka běhu testu

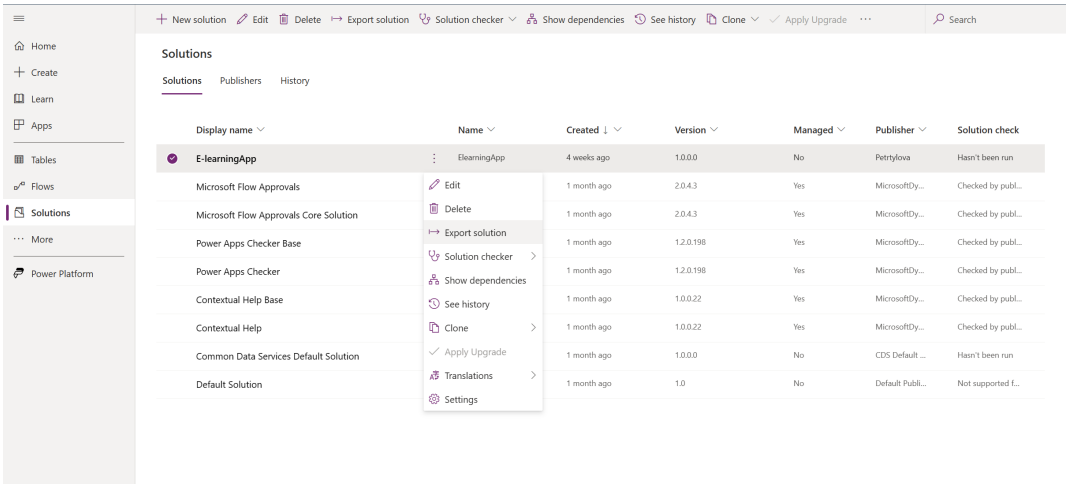
jednodušší přenos aplikací. Balíček se exportuje jako jedna zazipovaná složka s koncovkou .zip. Zazipované neboli komprimované složky zabírají menší místo a dají se jako jeden celek rychleji převádět do jiných počítačů než nekomprimované soubory (Přel. Petrtýlová Markéta) [106]. Vložené aplikace a tabulky do Solutions jsou zobrazené na obrázku 7.7 a export E-learningApp Solutions je zobrazen na obrázku 7.8.



Obrázek 7.7 Vložené aplikace a tabulky do Solutions

Jelikož tabulky se exportují bez dat, byly exportovány zvlášť data z tabulky „tab_Courses" do souboru tabulkového procesoru. Zde je uveden přehled o aktuálních kurzech v aplikaci.

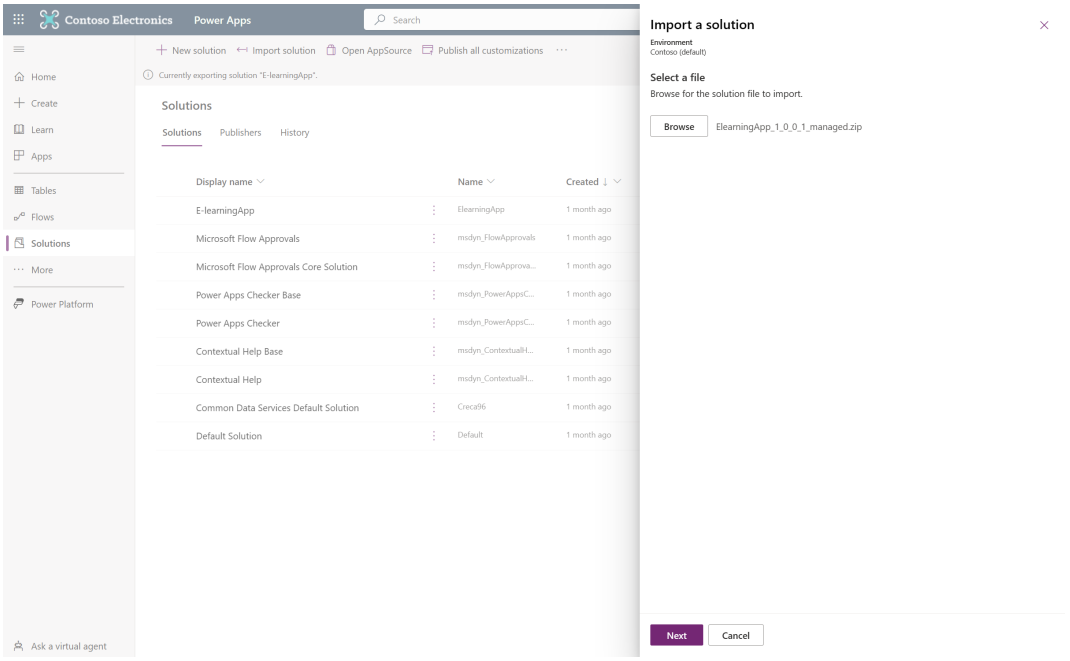
Samostatně se také společnosti KPCS předává přehled dat aplikace v souboru s koncovkou .pbix, což je soubor nástroje Power BI.



Obrázek 7.8 Export aplikace s tabulkami pomocí Solutions

7.2.2 Import aplikace

V prostředí Solutions v aplikaci Power Apps se provádí import pomocí tlačítka „Import solution" a následném zvolení zazipované složky. Proces importu je zobrazen na obrázku 7.9.



Obrázek 7.9 Import aplikace s tabulkami pomocí Solutions

V rámci tohoto projektu zákazník požadoval nasadit aplikaci do svého produkčního prostředí. Zakázáník chtěl vlastnoručně aplikaci do prostředí nasadit a chtěl tak provést v rámci hovoru,

kde bude asistovat dodavatel. [77] Takto bylo provedeno nasazení v rámci šestého jednání se zákazníkem [107].

Dále bylo nutné do tabulky o uživatelích přidat uživatele, kteří budou aplikaci využívat. Pro testování aplikace firma KPCS přidala pět uživatelů [77].

Společnost KPCS importovala data o kurzech do tabulky „tab_Couses" ze souboru tabulkového procesoru, který byl společnosti předán. Dále v tabulce „tab_CompletionTimes" definovala časy, do kterého mají být jednotlivé kurzy pro tento rok splněny. [107]

7.2.3 Přiřazení oprávnění uživatelům

Microsoft Dataverse používá model zabezpečení založený na rolích, které pomáhají zabezpečit přístup k databázi. Role zabezpečení (neboli security roles) lze použít ke konfiguraci přístupu ke všem prostředkům prostředí nebo ke konfiguraci přístupu ke konkrétním aplikacím a datům v prostředí. Role zabezpečení řídí přístup uživatele ke zdrojům prostředí prostřednictvím sady úrovní přístupu a oprávnění. Kombinace úrovní přístupu a oprávnění, které jsou součástí konkrétní role zabezpečení, řídí omezení uživatelského pohledu na aplikace,data a na interakce uživatele s těmito daty. (Přel. Petrtýlová Markéta) [108]

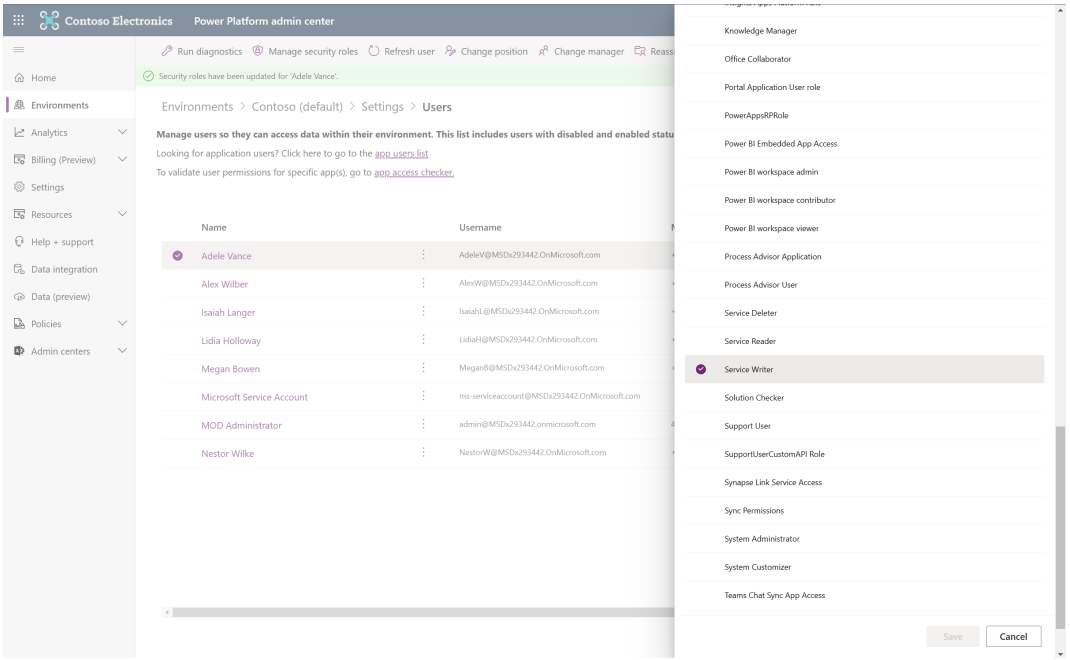
Pro možnost práce s daty uloženými v Dataverse v rámci používání aplikace jako běžný uživatel musí mít daný uživatel přiřazenou roli nazvanou Service Writer. Ta má plné oprávnění k vytváření, čtení a zápisu pro všechny entity včetně vlastních entit (Přel. Petrtýlová Markéta) [108]. Tato role byla již zmíněným uživatelům přiřazena v portálu Power Platform Admin Center. Proces přiřazení role je zobrazen na obrázku 7.10.

7.2.4 Přehled dat

V nástroji Power BI musela společnost KPCS změnit prostředí (environmet) ze kterého se čerpají data pro přehled. Zvoleno zde bylo prostředí v jejich tenantu, kde byla již nasazena aplikace. Dále už bylo potřeba přehled pouze publikovat pomocí tlačítka Publikovat.

7.3 Testování

Testování je důležitou součástí SDLC jelikož pomáhá zajistit kvalitu aplikace dodávané zákazníkům. Dokáže identifikovat problémy a závady a poskytuje příležitost tyto problémy opravit, aby byla aplikace spolehlivější. (Přel. Petrtýlová Markéta) [104]



Obrázek 7.10 Přiřazení oprávnění uživatelům

7.3.1 Testování v rámci implementace

Před nasazením byla aplikace testovaná, kromě již zmíněných regresních testů, také pomocí uživatelského testování. A to jednak v průběhu samotného vývoje, kdy byla aplikace testována dodavatelem i zadavatelem, kterému před každým jednáním byla zaslána aplikace v aktuálně rozpracovaném stavu, ale také před nasazením aplikace zákazníkovy v rámci příprav na nasazení.

7.3.2 Testování po nasazení a podpora zadavatele

Poté, co je kód vyvinut, je testován podle požadavků shromážděných od společnosti na začátku projektu. Během této fáze se provádějí všechny typy funkčního testování, jako je testování jednotek, testování integrace, testování systému, akceptační testování, jakož i nefunkční testování. (Přel. Petrtýlová Markéta) [51]

Po nasazení aplikace do produkčního prostředí společnosti KPCS pět zaměstnanců této společnosti aplikaci testovalo. [77] Následující část popisuje poznatky z testovací aplikace, které zaměstnanci zadavatele předali dodavateli.

Zadavatel aplikaci akceptoval. Velice kladně vyzdvihli zaměstnanci KPCS grafiku, která je intuitivní, dobře ovladatelná, srozumitelná a líbivá. Aplikace obsahuje dle počáteční domluvy dva vzdělávací kurzy na téma Phishing a Sociální inženýrství. Obsah vyhovuje potřebám společnosti

KPCS a firma věří, že napomůže jí, i případným jejím zákazníkům, rozšířit znalosti zaměstnanců, a tak lépe ochránit firmu před útoky sociálního inženýrství. [107]

Společnost přidala také několik poznatků, o které by do budoucna mohla být aplikace rozšířena. Prvním podnětem bylo, že by se do tabulky uživatelů automaticky uložil uživatel, když prvně navštíví aplikaci. Zde by však nastával problém u přehledu, kde by nebylo jasné, kolik je celkem zaměstnanců, co mají kurz splnit, jelikož by nebyli v tabulce uživatelů přidáni ti, kdo aplikaci zatím vůbec nenavštívili. [107]

Druhým podnětem bylo vytvořit přehled dat z aplikace přímo v aplikaci a zobrazovat tam zaměstnancům přehled o osobních výsledcích. Dále by bylo možné ještě přidat přehled pro manažery, kde by viděli všechny členy jejich týmu. [107]

Společnost aplikaci vytkla pár gramatických chyb a překlepů v textech kurzů. Tyto nedostatky byly opraveny a společnosti byly zaslány podklady pro upgrade aplikace na novou verzi. [107]

7.4 Podpora

Podpora probíhala v rámci nasazení aplikace a přehledu dat. Zde dodavatel asistoval na on-line hovoru během celého procesu nasazení, včetně přiřazení práv uživatelům, kteří aplikaci budou testovat pro možnost plného používání aplikace. Zároveň proběhlo také představení aplikace i přehledu dat. Drobné nedostatky nalezené během testování aplikace již v prostředí zadavatele byly opraveny a zákazníkovi byla zaslána nová verze aplikace, jak již bylo zmíněno v předešlé sekci. [77]

7.5 Vize dalšího rozvoje

Pro další možný rozvoj aplikace, nad rámec této práce, jsou navržené tyto funkcionality a rozšíření:

- Přidat vzdělávací kurz pro technické týmy, kde bude na základě páté kapitoly sepsán podrobný postup toho, jak postupovat v případě, že jim někdo nahlásí pokus o útok.
- V e-mailové zprávě s potvrzením zasílat uživatelům také podepsaný certifikát o splnění kurzu, který si budou moci vytisknout či sdílet.
- Vytvořit přehled dat z aplikace přímo v aplikaci a zobrazovat tam zaměstnancům přehled o osobních výsledcích. Dále by bylo možné ještě přidat přehled pro manažery, kde by viděli všechny členy jejich týmu.

Kapitola 8

Ekonomicko-manažerské zhodnocení

Následující kapitola shrnuje nejdůležitější informace o projektu z pohledu manažera, který se rozhoduje pro finanční podpoření vývoje aplikace pro rozvoj znalostí zaměstnanců jeho firmy v oblasti sociálního inženýrství. Případně by chtěl vzdělávací aplikaci také dále prodávat.

8.1 Zadání

Společnost KPCS CZ, S.R.O. je česká společnost se sídlem v Praze založena v roce 2006. Firma je partnerskou společností společnosti Microsoft a primárně nabízí prémiové služby v oblasti IT, licence Microsoft CSP, podporu a spravované služby. [52]

Cílem KPCS je zlepšit znalosti zaměstnanců v oblasti útoků sociálního inženýrství, především se zaměřením na phishing. Tímto krokem chce společnost zlepšit svoji ochranu proti internetovým útokům. [52]

Cílem první schůzky se zástupci společnosti je definice přesného tématu a požadavků na aplikaci, která by měla pomoci v rozvoji znalostí zaměstnanců v oblasti sociálního inženýrství. [52]

8.2 Vize řešení

Vytvoření e-learningové aplikace s kurzy zaměřenými na oblast sociálního inženýrství a především na oblast útoků phishing. Součástí řešení bude také vytvoření databáze, ze které budeme schopni čerpat data pro zobrazení přehledu o plnění kurzů. [52]

Na základě požadavků získaných od zaměstnanců společnosti KPCS byla pro tento projekt navržena architektura zobrazená na obrázku 8.1.

Obrázek 8.1 Návrh architektury

8.2.1 Obsah prvního kurzu

Po konzultaci se společností KPCS byla odsouhlasena následující osnova pro první vzdělávací kurz. Podkladem pro vzdělávací texty v aplikaci jsou první až pátá kapitola této bakalářské práce, která analyzuje oblast sociálního inženýrství.

- Jak velký dopad mají útoky sociálního inženýrství?
- Příklad úspěšně provedeného útoku z posledních let.
- Představení jednotlivých typů sociálního, a na co si u nich dávat pozor:
  - E-mail Phishing.
  - Spear Phishing.
  - Whaling.
  - Smishing.
  - Vishing.
  - Baiting.
  - Scareware.

  - Pretexting
  - Honey Trap.
  - Spamming.
- Na koho jsou útoky mířeny?
- Jak postupovat v případě napadení.

Kurz bude proložen deseti otázkami na právě probraná témata, ze kterých uživatel bude muset osm správně zodpovědět pro splnění kurzu. [66]

8.2.2 Obsah druhého kurzu

Druhý vzdělávací kurz bude zaměřený na rozpoznávání phishingu v e-mailové komunikaci [66], což je dle analýzy z předešlých kapitol nejčastější forma útoku sociálního inženýrství.

8.2.3 Požadavky na projekt

Společnost má tři klíčové požadavky pro tento projekt. Přehled ostatních požadavků rozdělených na funkční a nefunkční se nachází v sekci 6.3.

1. Společnost KPCS požaduje řešení používat pro vzdělávání svých zaměstnanců, ale i jej prodávat, jak jsme si uvedli již v minulé sekci, Hlavním požadavkem je, aby řešení bylo postavené na produktech z balíčku aplikací Power Platform a platformě PowerBI od společnosti Microsoft. Tato řešení je totiž možné používat v rámci platformy pro firemní komunikaci Microsoft Teams i jako individuální webovou aplikaci. [52]

2. Jelikož se chce firma v následujícím období zaměřit na zlepšení vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti a především sociálního inženýrství, požaduje, aby vytvořené řešení obsahovalo kurzy, které budou tyto znalosti rozvíjet a testovat. [52]

3. Společnost chce mít přehled o pokrocích a učení zaměstnanců, a proto požaduje vytvořit také přehled, kde tyto informace může sledovat. [52]

8.2.4 SWOT analýza projektu

Popis této analýzy je k nalezení v sekci 6.6, v tabulce 8.1 se nachází analýza pro tento projekt.

Tabulka 8.1 SWOT analýza projektu

Silné stránky (Strengths)	▬ Snadná grafická úprava aplikace dle nároků zákazníka při prodeji tohoto řešení, i díky vyškoleným zaměstnancům KPCS v této oblasti. ▬ Možnost úpravy řešení do cizích jazyků. ▬ Možnost vytváření dalších kurzů v této aplikaci. ▬ Přístup k aplikaci skrze platformu Microsoft Teams. ▬ Přístup k aplikaci i analytikám z počítače i tabletu. ▬ KPCS má s technologiemi používanými při vývoji zkušenosti a plánuje se v této oblasti rozvíjet.
Slabé stránky (Weaknesses)	▬ Méně nabízených kurzů než nabízí jiné platformy. ▬ Společnost KPCS je v prodávání vzdělávacích aplikací o kybernetické bezpečnosti nováčkem.
Příležitosti (Opportunities)	▬ Příznivé podmínky na trhu, společnosti se zajímají o vzdělávání svých zaměstnanců a někdy poskytují kurzy zdarma jako benefit. ▬ Jen jeden konkurent, který se primárně zaměřuje na přidání vzdělávacího portálu přímo do platformy Microsoft Teams, avšak nenabízí kurzy v českém jazyce. ▬ Kurzy jsou v českém jazyce, což je preference mnoha českých firem.
Hrozby (Threats)	▬ Zvýšení konkurence, která bude také nabízet možnost začlenit svoji platformu přímo do Microsoft Teams. ▬ Pokud by KPCS aplikaci prodávala, může se stát, že konkurence dokáže díky delšímu působení na trhu jít níže s cenou a zatraktivnit tak svoje řešení.

8.3 Harmonogram projektu

V rámci přípravy na druhé jednání byla vytvořena tabulka 8.2 obsahující jednotlivé fáze projektu rozdělené dále do dvou etap. Harmonogram byl zákazníkovi představen v rámci druhé konzultace, jejíž příprava a zápis je součástí příloh této práce.

Tabulka 8.2 Harmonogram projektu

Fáze projektu	Délka trvání	Předběžné datum zahájení fáze
Definování a schválení zadání	5 MD	01.09.2022
Návrh designu	6 MD	19.09.2022
Definice a sepsání obsahu vzdělávacích kurzů	15 MD	31.10.2022
Návrh aplikace a vypracování aplikace	20 MD	15.12.2022
Testování řešení před nasazením	5 MD	03.03.2023
Implementace poznatků z testování	5 MD	15.03.2023
Akceptace řešení pro možnost nasazení aplikace	3 MD	27.03.2023
Nasazení finální verze aplikace	5 MD	10.04.2023
Testování nasazeného řešení	5 MD	21.04.2023
Představení aplikace uživatelům, podpora uživatelů	5 MD	01.05.2023
Celkem	**74 MD**	

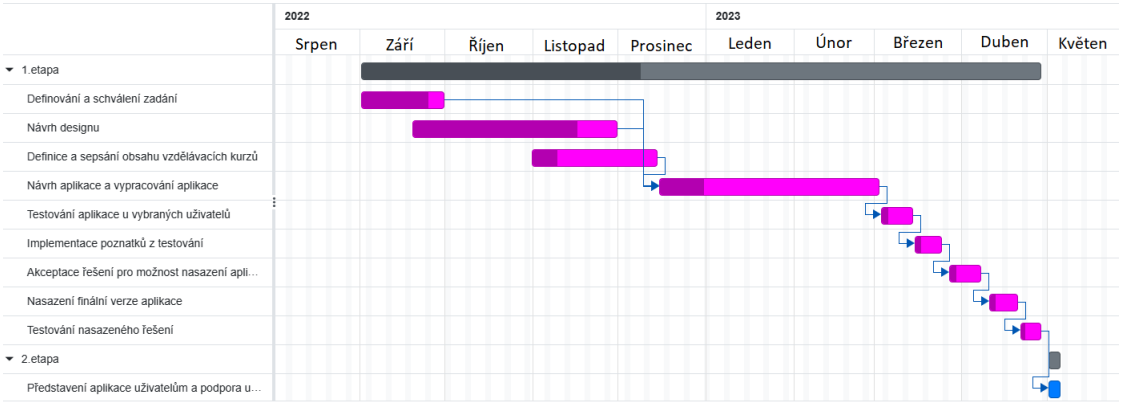
8.3.1 1. etapa (01.09.2022 až 30.04.2023)

Od počátku září 2022 začíná první etapa projektu. V této etapě bude provedena analýza konkurence i oblasti sociálního inženýrství. Dále bude navržena, implementována, nasazena a otestována aplikace.

8.3.2 2. etapa (01.05.2023 až 05.05.2023)

Od počátku května 2023 začíná druhá etapa projektu zaměřená na servisní podporu a podporu uživatelů.

Podrobnější časový harmonogram je zobrazen na obrázku 8.2 v Ganttově diagramu. Popis tohoto diagramu se nachází v sekci 6.7



Obrázek 8.2 Harmonogram v Ganttově diagramu

8.4 Cenová nabídka

Zde je uvedena konečná cenová nabídka, detailní výpočet a popis jednotlivých nákladů jsou uvedeny v kapitole 6.8.

$$\text{Celkové náklady} = \text{Náklady za mzdu} + \text{Náklady za licence} + \text{Náklady za hardware} + \text{Rezerva}$$

$$\text{Celkové náklady} = 449\ 195 + 0 + 4\ 284 + (449\ 195 + 0 + 4\ 284) * 0,2 \doteq 544\ 175\ \text{Kč}$$

V ceně nejsou zahrnuty případné change requesty, o které zákazník může projevit zájem. Ty budou řešeny vždy individuálně. Není zde také zahrnuté pořízení hardwaru, jelikož společnost již všechno potřebné vybavení obstarala. Maximální odchylka odhadu, s ohledem na definované požadavky a získané informace od společnosti KPCS, je ±20 %.

8.5 Součinnost

8.5.0.1 Součinnost dle etap a počtu člověkodní (1. etapa)

V tabulce 8.3 je představena požadovaná součinnost zadavatele práce. Zobrazen je zde přehled objemu součinnosti v jednotlivých fázích projektu. Tento přehled navazuje na časový harmonogram ze sekce 6.7. Minimální požadovaná součinnost pro první etapu je dle tabulky 24 MD.

Tabulka 8.3 Součinnost v 1. etapě

Fáze projektu	Délka součinnosti
Definování a schválení zadání	2 MD
Schválení návrhu designu	1 MD
Schválení obsahu vzdělávacích kurzů	2 MD
Schválení návrhu aplikace	3 MD
Testování řešení před nasazením	5 MD
Akceptace řešení pro možnost nasazení aplikace	3 MD
Nasazení finální verze aplikace	3 MD
Testování nasazeného řešení	5 MD
Celkem	**24 MD**

8.5.0.2 Součinnost dle etap a počtu člověkodní (2. etapa)

Dle harmonogramu projektu, který je detailně popsán v sekci 6.7, je v druhé etapě dodavatelem poskytnuto 5 MD na představení aplikace uživatelům a podporu. V rámci toho času bude dedikován minimálně jeden zaměstnanec společnosti KPCS pro školení o aplikaci a podporu systému

po nasazení. Minimální požadovaná součinnost pro druhou etapu je 5 MD při komunikaci s jedním zaměstnancem společnosti. Celkem pak minimální požadovaná součinnost činí za obě etapy 29 MD.

8.6 Přínosy

Z analýzy sociálního inženýrství v teoretické části této práce vyvstalo, že útoků sociální inženýrství každým rokem v posledních letech narůstá. Společnosti mají zájem ochránit svá data a data svých zaměstnanců. Chtějí vzdělávat své zaměstnance o sociálním inženýrství a především o nových trendech v této oblasti.

Navržená aplikace vzdělává zaměstnance v oblasti sociálního inženýrství a testuje jejich znalosti. Zaměřuje se z velké části na útoky phishing v e-mailové komunikaci, které jsou v dnešní době nejčastějším typem útoku sociálního inženýrství a jejichž útoku se chce společnost KPCS zejména naučit vyvarovat. Pokud bude KPCS prodávat toto řešení dalším firmám, je po takovéto aplikaci aktuálně zájem.

Aplikace bude postavena na produktech z balíčku Microsoft Power Platform, se kterým má již KPCS zkušenost. Vzdělávaní je s touto aplikací možné kromě webové stránky také přímo v platformě Microsoft Teams, kterou KPCS interně používá pro komunikaci. Je tedy velice rychle přístupná z počítače i tabletu. Velkým benefitem je, že na trhu je pouze jeden konkurent, který se primárně zaměřuje na přidání vzdělávací aplikace přímo do platformy Microsoft Teams, avšak nenabízí kurzy v českém jazyce.

Kurzy v aplikaci jsou aktuálně v českém jazyce a je zde možnost přidat do aplikace další jazyky. Lze také přidávat další vzdělávací kurzy.

8.7 Rizika

V této sekci jsou uvedena potenciální projektová rizika a potenciální rizika navrženého řešení.

8.7.1 Projektová rizika

Projektová rizika uvedená v této sekci odpovídají rizikům, která se mohou při realizaci aplikace s nejméně malou pravděpodobností výskytu objevit.

Tabulka 8.4 Riziko RZ01: Neposkytnutí součinnosti zákazníka

Popis rizika:	Neposkytnutí součinnosti zákazníka.
Pravděpodobnost výskytu:	Malá.
Dopad:	Dopad na kvalitu projektu a termín jeho dodání.
Plán pro eliminaci rizika:	Včasná eskalace problému na ostatní zaměstnance společnosti KPCS. Průběžné konzultace v rámci implementace projektu a reportování aktuálního stavu.
Krizový plán:	Dohoda se zákazníkem o posunutí termínu nebo změně rozsahu projektu. Zákazník uvedl, že nemá přesné časové požadavku na dodání projektu. [52]

Tabulka 8.5 Riziko RZ02: Zadrhávání komunikace mezi dodavatelem a zákazníkem

Popis rizika:	Zadrhávání komunikace mezi dodavatelem a zákazníkem.
Pravděpodobnost výskytu:	Malá.
Dopad:	Dopad na kvalitu projektu a termín jeho dodání.
Plán pro eliminaci rizika:	Jasné určení pravidel stylu a nástrojů komunikace. Komunikace se zákazníkem probíhá přes e-mailové zprávy a konzultace přes platformu Microsoft Teams.
Krizový plán:	Dohoda se zákazníkem o změně komunikačních nástrojů či změně zaměstnance společnosti KPCS, se kterým dodavatel komunikuje.

8.7.2 Potenciální rizika navrženého řešení

Potenciální rizika navrženého řešení odpovídají rizikům, která mohou být způsobena výběrem daného návrhu aplikace. Tato rizika se vykytují nejméně s malou pravděpodobností výskytu.

Tabulka 8.6 Riziko RZ03: Možnost získání znalostí z jiného zdroje

Popis rizika:	Možnost získání znalostí z jiného zdroje.
Pravděpodobnost výskytu:	Střední. Řešení je pro zaměstnance postavené přímo na míru, avšak další výukové zdroje na toto téma se především v cizích jazycích vyskytují.
Dopad:	Nižší počet zaměstnanců, kteří jsou uživateli aplikace.
Plán pro eliminaci rizika:	Seznámení zaměstnanců s možností vzdělávání a určení tohoto způsobu vzdělávání jako doporučeného jejich zaměstnavatelem. Komunikace ze zadavatelem projektu o potřebách a preferencích jeho zaměstnanců.
Krizový plán:	Upravení kurzů dle zpětné vazby zaměstnanců společnosti KPCS pro spokojené používání aplikace.

8.8 Vize dalšího rozvoje

Pro další možný rozvoj aplikace, nad rámec této práce, jsou navržené tyto funkcionality a rozšíření:

Tabulka 8.7 Riziko RZ04: Nesprávný cenový odhad implementace projektu

Popis rizika:	Nesprávný cenový odhad implementace projektu.
Pravděpodobnost výskytu:	Střední.
Dopad:	Nutnost dalších investic nebo omezení funkčností aplikace.
Plán pro eliminaci rizika:	Připravení detailního finančního plánu.
Krizový plán:	Do rozpočtu bude započítaná rezerva a zákazník bude obeznámen s možnými změnami konečné ceny od původního návrhu. Bude definována maximální odchylka odhadu ceny.

Tabulka 8.8 Riziko RZ05: Nasazení systému po plánovaném termínu

Popis rizika:	Nasazení systému po plánovaném termínu.
Pravděpodobnost výskytu:	Střední. Řešení je pro zaměstnance postavené přímo na míru, avšak další výukové zdroje na toto téma se především v cizích jazycích vyskytují.
Dopad:	Prodloužení aktuálního stavu plýtvání zdrojů. Další navýšení nákladů na implementaci řešení.
Plán pro eliminaci rizika:	Vytvoření úvodní studie. Rozdělení projektu do etap. Klauzule ve smlouvě o nasazení systému po plánovaném termínu.
Krizový plán:	Včasné upozornění zadavatele a domluvení změny harmonogramu. Případné sankce pro dodavatele.

- Přidat vzdělávací kurz pro technické týmy, kde bude na základě páté kapitoly sepsán podrobný postup toho, jak postupovat v případě, že jim někdo nahlásí pokus o útok.
- V e-mailové zprávě s potvrzením zasílat uživatelům také podepsaný certifikát o splnění kurzu, který si budou moci vytisknout či sdílet.
- Vytvořit přehled dat z aplikace přímo v aplikaci a zobrazovat tam zaměstnancům přehled o osobních výsledcích. Dále by bylo možné ještě přidat přehled pro manažery, kde by viděli všechny členy jejich týmu.

Závěr

Cílem teoretické části bakalářské práce bylo analyzovat oblast sociálního inženýrství a na základě této analýzy vytvořit osnovy pro obsah vzdělávacích kurzů pro společnost KPCS, později i texty kurzů. Dílčím cílem bylo analyzovat již existující školící řešení, požadavky společnosti KPCS a možné nástroje pro vytváření výukových aplikací. Na základě této analýzy bylo cílem navrhnout vlastní školící aplikaci.

Cílem praktické části bakalářské práce bylo vytvořit aplikaci, která bude zaměstnance společnosti KPCS formou kurzů vzdělávat v oblasti sociálního inženýrství a bude je testovat z nově nabytých znalostí. Následovalo testování a samotná implementace vzniklého řešení společně se získáním zpětné vazby na rozvoj znalostí uživatelů. Vytvořeno bylo také ekonomicko-manažerské vyhodnocení, kde byly popsány přínosy tohoto řešení pro společnost KPCS a přehled nákladů na vývoj aplikace.

Všechny stanovené cíle pro tuto práci byly naplněny. Analýzou sociálního inženýrství se zabývá druhá až pátá kapitola. Na jejím základě byly sepsány vzdělávací texty v aplikaci. Aplikace je aktuálně nasazená v produkčním prostředí zákazníka. Pomocí dvou kurzů vzdělává a testuje znalosti zaměstnanců společnosti KPCS. Tím pomáhá chránit společnost před napadením útokem sociálního inženýrství, jelikož jsou zaměstnanci připraveni na to, čemu se mají vyvarovat a jak s útoky zacházet.

V průběhu vývoje žádné nečekané problémy nenastaly a aplikace tak mohla být vytvořena přesně dle požadavků KPCS. V rámci návrhu, vývoje i testování aplikace jsem pravidelně dostávala od zaměstnanců KPCS zpětnou vazbu na aktuální verzi aplikace a směřování projektu. Společnost po závěrečném testování navrhla podněty na rozšíření aplikace do budoucna, které jsou nad rámec aktuálního vývoje. Zásadní podněty pro rozvoj od společnosti KPCS a od autorky této bakalářské práce jsou zmíněné na konci sedmé kapitoly.

Osobním přínosem bakalářské práce bylo prohloubení znalostí autorky bakalářské práce v oblasti sociálního inženýrství a v oblasti vývoje aplikací pomocí aplikací z balíčku Micorosft Power Platform. Práce jí pomohla v rozvoji komunikace, především pak komunikace se zákazníkem za účelem prodání nabízeného řešení.

Příloha A

Příprava na první jednání

Tabulka A.1 Přehled prvního jednání

Datum:	07.09.2022
Čas:	14:30 – 15:00
Místo konání:	on-line
Pozvaní účastníci:	Zdeněk Vinduška, Jiří Bečka, Martina Koutníková, Markéta Petrtýlová
Připravili:	Markéta Petrtýlová

A.1 Souhrn spolupracujících lidí na projektu

Tabulka A.2 Osoby podílející se na projektu

Kontaktní osoba	**Pozice, společnost, role v rámci tohoto projektu**
`Markéta Petrtýlová`	`Studentka, ČVUT FIT`
`Zdeněk Vinduška`	`Sharepoint Consultant, KPCS CZ, S. R. O.,` V rámci tohoto projektu má pozici projektového manažera, klíčového uživatele a testera.
`Martina Koutníková`	`IT Recruiting, KPCS CZ, S. R. O.,` V rámci tohoto projektu má pozici zadavatele projektu a běžného uživatele.
`Jiří Bečka`	`Senior IT Consultant, KPCS CZ, S. R. O.,` V rámci tohoto projektu má pozici běžného uživatele.

A.2 Zadání projektu

Společnost KPCS CZ, S.R.O. je česká společnost se sídlem v Praze založena v roce 2006. Firma je partnerskou společností společnosti Microsoft a primárně nabízí prémiové služby v oblasti IT, licence Microsoft CSP, podporu a spravované služby. [52]

Na základě předchozí především e-mailové komunikace byla společností KPCS CZ, S.R.O. sdílena poptávka po e-learningové aplikaci pro rozvoj zaměstnanců firmy především v oblasti sociálního inženýrství. Řešení má napomoci k lepší ochraně dat firmy i jejich zaměstnanců a má pomoci společnosti předejít nákladnému odstranění škod po internetových útocích.

Cílem první schůzky se zástupci společnosti je definice přesného tématu a požadavků na aplikaci, která by měla pomoci v rozvoji znalostí zaměstnanců v oblasti sociálního inženýrství.

A.3 Plán společnosti

Cílem firmy je zlepšit znalosti zaměstnanců v oblasti útoků sociálního inženýrství, především se zaměřením na phishing. Tímto krokem chce společnost zlepšit svoji ochranu proti internetovým útokům.

A.4 Navrhované řešení

Vytvoření e-learningové aplikace s kurzy zaměřenými na oblast sociálního inženýrství a především na oblast útoků phishing. Součástí řešení bude také vytvoření databáze, ze které budeme schopni čerpat data pro zobrazení přehledu o znalostech zaměstnanců a jejich učení.

A.5 Součinnost

Dodavatelem projektu je Markéta Petrtýlová. Zadavatelem projektu včetně požadavků je společnost KPCS CZ, S.R.O. za níž vystupují v tomto projektu zaměstnanci Zděněk Vinduška, Martina Koutníková a Jiří Bečka.

A.6 Ostatní, diskuze

- Jaké informace chce společnost svým zaměstnancům prostřednictvím kurzů předat?
- Jaká jsou technologická omezení?
- Jaké má společnost preference na použité technologie pro řešení?

- Poskytne zadavatelská společnost vlastní prostředí pro tvorbu aplikace?

Příloha B

Zápis z prvního jednání

Tabulka B.1 Přehled prvního jednání

Datum:	07.09.2022
Čas:	14:30 – 15:00
Místo konání:	on-line
Pozvaní účastníci:	Zdeněk Vinduška, Jiří Bečka, Martina Koutníková, Markéta Petrtýlová
Připravili:	Markéta Petrtýlová

B.1 Tým pracující na projektu

Tabulka B.2 Osoby podílející se na projektu

Kontaktní osoba	**Pozice, společnost**
Markéta Petrtýlová	Studentka, ČVUT FIT
Zdeněk Vinduška	Sharepoint Consultant, KPCS CZ, S. R. O.
Jiří Bečka	Senior IT Consultant, KPCS CZ, S. R. O.

B.2 Specifikace zadání

Na základě konzultace se obě strany shodly na následujícím:

E-lerningová aplikace pro rozvoj kybernetické bezpečnosti

Práci zadává společnost KPCS CZ, S.R.O., která vnímá potřebu vzdělávat své zaměstnance v oblasti kybernetické bezpečnosti. Zaměřit se chce především na rozvoj znalostí v oblasti útoků phishing a sociálního inženýrství.

Hlavním cílem bakalářské práce bude společnosti umožnit vzdělávat své zaměstnance efektivní metodou v předem zmíněných oblastech. Součástí práce bude sepsat edukativní materiál, který bude tvořit podklad pro obsah vzdělávacích kurzů. Dále také vytvořit aplikaci, která bude zaměstnance společnosti formou kurzů vzdělávat a bude je testovat z nově nabytých znalostí po dokončení vzdělávací části kurzu v aplikaci. Následovat bude samotná implementace a testování vzniklého řešení společně se získáním zpětné vazby na rozvoj znalostí uživatelů. Shrnuté bude také ekonomicko-manažerské vyhodnocení, kde budou popsány přínosy tohoto řešení pro společnost KPCS a přehled nákladů na vývoj.

B.3 Požadavky společnosti KPCS

- Zadavatel požaduje vytvoření e-lerningové aplikace, ke které budou mít přístup všichni zaměstnanci skrze svůj firemní počítač nebo tablet.
- Aplikace bude obsahovat dva kurzy. První kurz bude o sociálním inženýrství a druhý o phishingu. Každý kurz bude obsahovt kvíz, který bude testovat znalosti uživatelů.
- Pro řešení bude použita Microsoft Power Platform, pro aplikaci bude použita služba Microsft PowerApps. Tyto služby vyžaduje společnost použít, jelikož chce prodávat toto nebo podobné řešení zákazníkům a aplikace bude využívat již zakoupených licencí firmy. Firma má se službami zkušenosti a stále se v této oblasti plánují zlepšovat. Jednoduchá adaptace aplikace do mnoha jazyků, rychlá úprava dle přesných požadavků společnosti a snadné analytiky nad uloženými daty napomáhají tomuto rozhodnutí. Takto vytvořené řešení je zároveň na rozdíl od klasické webové aplikace možné používat i přímo v platformě Microsoft Teams, kterou firma používá pro komunikaci. Tím tedy firma urychlí a ulehčí přístup ke vzdělávání svým zaměstnancům.
- Data z aplikace se mají ukládat v Microsoft Dataverse, jelikož společnost se chce rozvíjet v tomto způsobu ukládání dat. Z této databáze se také dají čerpat data pro vytvoření přehledu dat v PowerBI.
- Je vyžadováno vytvořit přehled dat z aplikace pomocí platformy PowerBI.
- Společnost KPCS CZ, S.R.O. nemá konkrétní časové požadavky pro vytvoření tohoto řešení.
- Aplikace i přehled dat budou zhotoveny v českém jazyce.

B.4 Ostatní, diskuze

- Společnost má pro všechny své zaměstnance požadované licence a hardware (počítače či tablety) pro plné používání aplikace.
- Společnost KPCS CZ, S.R.O. poskytne po dobu práce na projektu prostředí pro tvorbu aplikace.
- Společnost KPCS požaduje řešení používat pro vzdělávání svých zaměstnanců, ale i jej prodávat dalším firmám.
- Finální definice zadání práce a tedy téma samotné práce musí být nyní schváleno konzultantem a garantem oboru z ČVUT FIT.
- Ve společnosti KPCS v současné době neprobíhá žádný souběžný projekt, který by výrazným způsobem mohl ovlivnit implementaci vzdělávací aplikace.

B.5 Zápis plynoucí z jednání

Na schůzce byly prodiskutovány požadavky společnosti na aplikaci i samotné kurzy. Dále bylo určeno vývojové prostředí a byl prodiskutován očekávaný harmonogram implementace, jehož finální návrh bude předmětem dalšího jednání.

Příloha C

Příprava na druhé jednání

Tabulka C.1 Přehled druhého jednání

Datum:	21.09.2022
Čas:	14:30 – 15:00
Místo konání:	on-line
Pozvaní účastníci:	Zdeněk Vinduška, Markéta Petrtýlová
Připravili:	Markéta Petrtýlová

C.1 Harmonogram projektu

C.1.1 1. etapa (01.09.2022 až 30.04.2023)

Od počátku září 2022 začíná první etapa projekt projektu. V této etapě bude navržena, implementována, nasazena a otestována aplikace.

C.1.2 2. etapa (01.05.2023 až 05.05.2023)

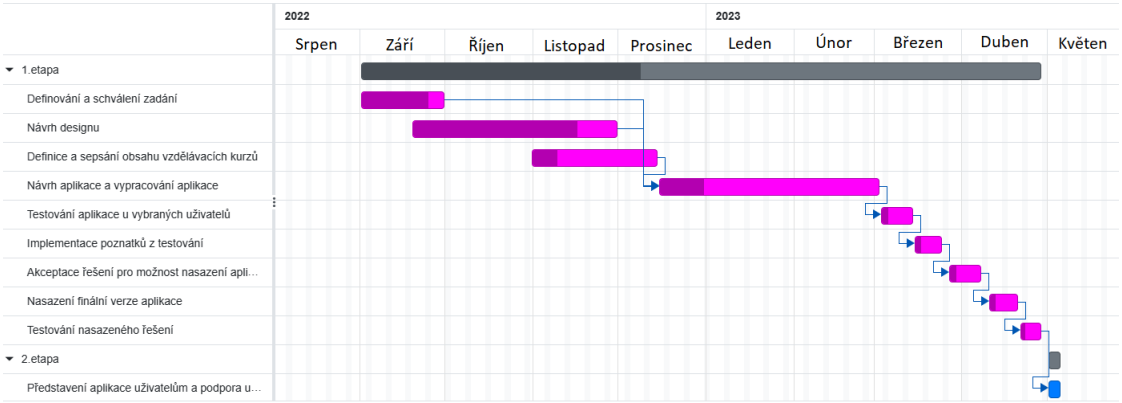
Od počátku května 2023 začíná druhá etapa projektu zaměřená na servisní podporu a podporu uživatelů.

C.2 Vize řešení

Na základě předchozí konzultace se společností KPCS CZ, S.R.O. je navrhovaným řešením pro společnost vytvořit e-learningovou aplikaci s kurzy zaměřenými na sociální inženýrství a přede-

Tabulka C.2 Harmonogram projektu

Fáze projektu	Délka trvání	Předběžné datum zahájení fáze
Definování a schválení zadání	5 MD	01.09.2022
Návrh designu	6 MD	19.09.2022
Definice a sepsání obsahu vzdělávacích kurzů	15 MD	31.10.2022
Návrh aplikace a vypracování aplikace	20 MD	15.12.2022
Testování aplikace vybranými uživateli	5 MD	03.03.2023
Implementace poznatků z testování	5 MD	15.03.2023
Akceptace řešení pro možnost nasazení aplikace	3 MD	27.03.2023
Nasazení finální verze aplikace	5 MD	10.04.2023
Testování nasazeného řešení	5 MD	21.04.2023
Představení aplikace uživatelům a podpora uživatelů	5 MD	01.05.2023



Obrázek C.1 Přehled harmonogramu [10]

vším phishing apolečně s přehledem dat o dokončených kurzech. Celé řešení společnost vyžaduje vytvořit pomocí Microsoft Power Platform a PowerBI.

C.3 Klíčové benefity navrženého řešení

- Společnost KPCS požaduje řešení používat pro vzdělávání svých zaměstnanců, ale i jej prodávat. Hlavním požadavkem je, aby řešení bylo postavené na produktech z balíčku aplikací Power Platform a platformě PowerBI od společnosti Microsoft. Tato řešení je totiž možné používat v rámci platformy pro firemní komunikaci Microsoft Teams i jako individuální webovou aplikaci a společnost se plánuje v této oblasti dále rozvíjet. Umožnění zaměstnancům společnosti zadavatele vzdělávání v žádaných oblastech.

- Jelikož se chce firma v následujícím období zaměřit na zlepšení vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti a především sociálního inženýrství, požaduje, aby vytvořené řešení obsahovalo kurzy, které budou tyto znalosti rozvíjet a testovat.
- Společnost chce mít přehled o pokrocích a učení zaměstnanců, a proto požaduje vytvořit také přehled, kde tyto informace může sledovat.

C.4 Rizika navrženého řešení i projektová rizika

- Možnost získání znalostí z jiného zdroje.
- Neposkytnutí součinnosti zákazníka. Nemá však žádné projekty, které by měli ovlivňovat harmonogram tohoto projektu.

C.5 Cenová nabídka

C.5.1 Mzdové náklady

Dle povahy projektu by se na jeho vypracování podílely především osoby na následujících pracovnách pozicích.

- Projektový manažer: Řídí projekt, projektový tým, školení a komunikaci se zákazníkem. K 08.04.2023 je průměrný měsíční plat osob na této pozici v České republice 51 478 Kč[83].
- UX/UI designér: Podílí se na návrhu grafického designu aplikace a přehledu dat. K 08.04.2023 je průměrný měsíční plat osob na této pozici v České republice 59 676 Kč[84].
- Programátor: Pracuje na implementaci projektu, implementaci databáze a zhotovuje přehled dat. K 08.04.2023 je průměrný měsíční plat osob na této pozici v České republice 58 469 Kč[85].
- Quality Engineer (Tester): Testuje řešení v rámci vývoje aplikace i po nasazení aplikace k zákazníkovi. K 08.04.2023 je průměrný měsíční plat osob na této pozici v České republice 47 873 Kč [86].

Jelikož na tomto projektu tyto role zastává jedna osoba, vypočteme její měsíční platové ohodnocení jako průměr měsíčních platových ohodnocení lidí na čtyřech zmíněných pracovních pozicích:

$$\text{Měsíční plat} = \frac{51\ 478 + 59\ 676 + 58\ 469 + 47\ 873}{4} = 54\ 365\ \text{Kč/měsíc}$$

V roce 2023 je 250 pracovních dní [87]. Vydělením tohoto čísla 12 dle počtu měsíců dostanu, že v jednom měsíci je necelých 21 dní. MD neboli man-day je jednotka která odpovídá jednomu pracovnímu dni jednoho člověka, tedy 8 odpracovaných hodin.

Plat osoby pracující na tomto projektu za jeden den je poté měsíční plat vydělený průměrným počtem dní v měsíci neboli:

$$\text{Denní plat} = \frac{54\ 365}{21} \doteq 4\ 530\ \text{Kč/MD}$$

Jelikož nám vyšlo, že na projekt nutné dedikovat 74 MD, vypočteme plat na celý projekt vynásobením denního platu počtem MD:

$$\text{Plat za celé období práce na projektu} = 4\ 530 * 74 = 335\ 220\ \text{Kč}$$

Zaměstnavatelé však kromě platu za zaměstnance platí také sociální a zdravotní pojištění. Zdravotní pojištění je celkem 13,5 % ze mzdy, z toho jednu třetinu platí zaměstnanec a zbytek zaměstnavatel, zaměstnavatel tedy platí 9 % ze mzdy. Sociální pojištění je celkem 31,5 % ze mzdy, z toho 6,5 % platí zaměstnanec, zbylých 25 % zaměstnavatel. [88] Výsledné mzdové náklady zaměstnavatele na jednoho zaměstnance se tedy skládají ze mzdy, ke které je připočteno 9 % ze mzdy na zdravotní pojištění a 25 % ze mzdy na sociální pojištění:

$$\text{Celkové náklady za mzdu} = 335\ 220 + 335\ 220 * 0,09 + 335\ 220 * 0,25 \doteq 449\ 195\ \text{Kč}$$

C.5.2 Licence a prostory

Zákazník poskytl bezplatné prostředí pro vývoj aplikace, a tedy cena za licence v rámci vývoje je pro dodavatele nulová. Stejně tomu tak je i s prostory pro vývoj aplikace. Zákazník již vlastní všechny potřebné licence pro následné umožnění plného využívání aplikace pro všechny své zaměstnance.

C.5.3 Hardware

Společnost již obstarala všechen potřebný hardware pro provoz aplikace, nikoliv však pro vývoj a podporu. Vývoj a podpora probíhala v rámci 9 měsíců (září 2022 až květen 2023). Pro vývoj aplikace je lze využít například notebook Lenovo Yoga Slim 7 Pro 14IHU5 Slate, který je jeden z nejlevnějších notebooků v nabídce zařízení k zapůjčení na stránkách internetového obchodu Alza, cena za měsíc je k 08.04.2023 476 Kč [89] . Za devět měsíců tedy pak 4 284 Kč.

C.5.4 Rezerva

K součtu cen za předchozí položky bude přičteno 20 % jako rezerva.

C.5.5 Celková cena

Celkové náklady = Celkové náklady za mzdu+Náklady za licence+Náklady za hardware+Rezerva

$$\text{Celkové náklady} = 449\ 195 + 0 + 4\ 284 + (449\ 195 + 0 + 4\ 284) * 0,2 \doteq \mathbf{544\ 175\ Kč}$$

V ceně nejsou zahrnuty případné change requesty, o které zákazník může projevit zájem, ty budou řešeny vždy individuálně. Není zde také zahrnuté pořízení hardwaru, jelikož společnost již všechno potřebné vybavení obstarala. Maximální odchylka odhadu, s ohledem na definované požadavky a získané informace od společnosti KPCS je ±20 %.

C.6 Obsah kurzů

Se zákazníkem bude projednán návrh na osnovu vzdělávacích kurzů:

C.6.1 První kurz: Sociální inženýrství

Návrh na obsah prvního vzdělávacího kurzu:

1. Upoutávka z výzkumu (proč je dobré se o těchto tématech učit).
2. Co je to sociální inženýrství.
3. Jak funguje sociální inženýrství.
4. Příklady známých útoků.
5. Phishing.
6. Spear Phishing.
7. Vishing (voice phishing).
8. Smishing.
9. Whaling.
10. Baiting.

11. Scareware.
12. Pretexting.
13. Honey trap.
14. Email spamming.
15. Proč jsou útoky tak nebezpečné a na koho jsou primárně cíleny?
16. Jak předejít sociálnímu inženýrství?

Kurz bude obohacen o kvíz 10 otázek, na 8 z nich bude muset uživatel správně odpovědět pro splnění testu. Tyto kvízy budou testovat právě nabyté znalosti z kurzu.

C.6.2 Druhý kurz: Phishing

Druhý kurz bude interaktivní formou uživatele vybízet k rozeznaní phishingových zpráv od legitimních. Uživateli se zobrazí 10 příkladů zpráv, mezi kterými bude muset rozeznat zprávy, které jsou součástí phishingového útoku a alespoň 8 z 10 zpráv správně označit za legitimní či s phishingem.

C.7 Grafický návrh aplikace

Se zákazníkem bude prodiskutován návrh grafického rozhraní a bude požádáno o grafické požadavky a předpisy společnosti.

C.8 Ostatní, diskuze

- Jaké zdroje informaci chce společnost pro tvorbu kurzů použít?
- Jaké je kritérium pro úspěšné splnění obou kurzů?
- Jaké grafické požadavky a předpisy má společnost?
- Jaké má zákazník licence, především v oblasti služeb, které požaduje využít pro tvorbu aplikace?

Obrázek C.2 Příklad první verze grafického návrhu [10]

Příloha D

Zápis z druhého jednání

Tabulka D.1 Přehled druhého jednání

Datum:	21.09.2022
Čas:	14:30 – 15:00
Místo konání:	on-line
Pozvaní účastníci:	Zdeněk Vinduška, Markéta Petrtýlová
Připravili:	Markéta Petrtýlová

D.1 Harmonogram projektu

Zaměstnanci společnosti KPCS CZ, S.R.O. schválili navržený harmonogram v původním znění.

D.2 Navrhované řešení

Zákazník nenavrhl žádné změny v dosavadním navrhovaném řešení ani v popisu tohoto řešení. Zákazník má pro všechny své zaměstnance již zakoupené licence a hardware umožnující používání aplikace všem zaměstnancům, zaměstnanců je aktuálně 50. Při případném navýšení počtu zaměstnanců společnosti KPCS bude na zákazníkovy obstarat potřebné licence a zařízení pro nové zaměstnance.

D.3 Obsah kurzů

Zákazník souhlasil s osnovou obou kurzů a doporučil čerpat především ze zdrojů oficiálních dokumentací a podkladů od společnosti Microsoft. Dále také stanoví hranici bodového minima

u kurzů pro jejich úspěšné splnění, a to osmdesát procent pro úspěšné splnění kurzu. V aplikaci chce zákazník signalizovat splnění kurzu pomocí získaného odznaku. Zákazník požaduje přidaní možnosti opustit kurz v průběhu jeho plnění

D.4 Cenová nabídka

Zákazníkovi byla přestavena cenová nabídka.

D.5 Grafický návrh aplikace

Zákazník poskytl podklady a pravidla pro grafické zpracování a požaduje úpravu pozadí aplikace z grafického návrhu. Zákazník kromě pozadí schválil grafický návrh aplikace.

D.6 Zápis plynoucí z jednání

V rámci schůzky byly prodiskutovány požadavky společnosti na navrhované řešení a na obsah kurzů. Dále také byl prodiskutován grafický návrh, cenový návrh a detailní harmonogram projektu.

Příloha E

Příprava na třetí jednání

Tabulka E.1 Přehled třetího jednání

Datum:	07.12.2022
Čas:	14:30 – 15:00
Místo konání:	on-line
Pozvaní účastníci:	Zdeněk Vinduška, Markéta Petrtýlová
Připravili:	Markéta Petrtýlová

E.1 Body k diskuzi

Zákazníkovi byla před konzultací poskytnuta rozpracovaná aplikace pro možnost testování doposud implementovaných funkcí a možnost schválení grafického zpracování aplikace. Na základě e-mailové komunikace vyvstalo několik bodů, které budou pro-komunikovány na následujícím meetingu:

- Formulace odpovědí na otázky v kurzu zaměřeném na phishing.
- Způsob náhodného generování otázek v kurzu o phishingu.
- Umístění loga společnosti.
- Přidání možnosti opuštění kurzu v průběhu.
- Schválení grafického zpracování aplikace.

Příloha F

Zápis z třetího jednání

Tabulka F.1 Přehled třetího jednání

Datum:	07.12.2022
Čas:	14:30 – 15:00
Místo konání:	on-line
Pozvaní účastníci:	Zdeněk Vinduška, Markéta Petrtýlová
Připravili:	Markéta Petrtýlová

F.1 Grafické zpracování aplikace

Zákazník schválil grafický zpracování aplikace s jediným požadavkem na změnu a tím je změna pozice loga společnosti KPCS na levou polovinu strany v menu aplikace.

F.2 Kurz Phishing

Generovat otázky kurzu v tomto kurzu chce zadavatel zcela náhodně nehledě na procento zpráv, které jsou legitimní či obsahují phishing. Požaduje také detailnější popis odůvodnění správné možnosti otázek.

F.3 Všechny kurzy v aplikaci

Zákazník požaduje ukončit kurz automaticky vždy, jakmile uživatel nasbírá tři špatné odpovědi a možnost ukončení kurzu v rámci jeho plnění přechodem do menu aplikace. Každý kurz lze také možné opakovat i po jeho úspěšném či neúspěšném splnění.

F.4 Change request (požadavky na změnu vůči původnímu zadání).

Oproti původnímu zadání se do aplikace požadují přidat emaily s potvrzením o úspěšném dokončení kurzu. Kvůli nízké časové náročnosti neovlivní tento požadavek finanční část projektu a bude implementován jako součást aplikace.

Příloha G

Příprava na čtvrté jednání

Tabulka G.1 Přehled čtvrtého jednání

Datum:	21.02.2023
Čas:	13:00 – 13:30
Místo konání:	on-line
Pozvaní účastníci:	Zdeněk Vinduška, Markéta Petrtýlová
Připravili:	Markéta Petrtýlová

Zákazníkovi byla před konzultací poskytnuta rozpracovaná aplikace pro možnost testování doposud implementovaných funkcí.

G.1 Návrh databáze

Diskuze nad ukládání dat v Microsoft Dataverse, jaká všechny data ukládat a zda vyhovuje navrhovaný způsob ukládání dat zákazníkovi.

G.2 Ostatní body k diskuzi

V rámci testování si všimli zaměstnanci KPCS chyby u phishingového kurzu s názvem kurzu, který problikával při najetí na něj myší. Tato chyba bude do konzultace opravena.

Příloha H

Zápis z čtvrtého jednání

Tabulka H.1 Přehled čtvrtého jednání

Datum:	21.02.2023
Čas:	13:00 – 13:30
Místo konání:	on-line
Pozvaní účastníci:	Zdeněk Vinduška, Markéta Petrtýlová
Připravili:	Markéta Petrtýlová

H.1 Návrh databáze

V Dataverse budou ukládána data o všech ukončených kurzech, a to dokončených úspěšně či neúspěšně. Součástí ukládaných dat budou u kurzu o phishingu ukládán seznam čísel otázek, které byly uživateli vygenerovány. Dále bude uloženo, zda uživatel kurz splnil, email uživatele a datum dokončení kurzu. Zadavatel požaduje také ukládání seznamu náhodně vygenerovaných otázek v kurzu o phishingu.

H.2 Ostatní body k diskuzi

- V aplikaci má být zobrazen konečný termín dokončení jednotlivých kurzů.
- Chyba u phishingového kurzy byla opravena.

Příloha I

Přírava na páté jednání

Tabulka I.1 Přehled pátého jednání

Datum:	06.04.2023
Čas:	14:00 – 14:30
Místo konání:	on-line
Pozvaní účastníci:	Zdeněk Vinduška, Markéta Petrtýlová
Připravili:	Markéta Petrtýlová

I.1 Aplikace a databáze

Před konzultací byly jednomu ze zaměstnanců ze společnosti KPCS zaslány přístupové údaje, pomocí kterých mu bylo umožněno testovat aplikaci a databázi. Na následující schůzce prodiskutujeme případné požadavky na změnu, popřípadě necháme od zákazníka schválit aktuální verzi aplikace jako konečnou a připravenou k nasazení.

I.2 Přehled dat

Se zákazníkem budou prodiskutovány změnové požadavky k první verzi přehledu dat. Přehled byl také zaslán zákazníkovi před konzultací pro testování jeho spokojenosti.

I.3 Nasazení, podpora a testování

Se zákazníkem bude detailně prodiskutován plán nasazení, testování a podpory.

- Do jakého prostředí zákazníka se bude aplikace nasazovat? Zákazník na minulých konzultacích zmínil, že má produkční a testovací prostředí.
- Kolik firma přesně poskytne testerů, kteří následně zašlou zákazníkovi zpětnou vazbu?
- Přesnou formu podpory jakou firma v rámci nasazení, testování a první interakce s aplikací a přehledem firma požaduje?

Příloha J

Zápis z pátého jednání

Tabulka J.1 Přehled pátého jednání

Datum:	06.04.2023
Čas:	14:00 – 14:30
Místo konání:	on-line
Pozvaní účastníci:	Zdeněk Vinduška, Markéta Petrtýlová
Připravili:	Markéta Petrtýlová

J.1 Aplikace a databáze

Aplikace a databáze schváleny bez změnových požadavků.

J.2 Přehled dat

Zákazník požaduje možnost filtrovat dle uživatele, času a splnění konkretního kurzu. Vždy má jít zvolit pouze jedna či více možností u každého typu filtru. Přehled bude upraven do následující konzultace.

J.3 Nasazení, podpora a testování

- Zákazník požaduje nasadit aplikaci do svého produkčního prostředí. Zákazník chce vlastnoručně aplikaci do prostředí nasadit. Chce tak provést v rámci hovoru, kde bude asistovat dodavatel s nasazením aplikace.

- Společnost KPCS poskytne 5 testerů, kteří budou zároveň lidmi pro zaučení při práci s aplikací.
- Společnost KPCS požaduje podporu dodavatele v rámci celého procesu nasazování aplikace a přehledu dat do svého prostředí. Tato podpora bude probíhat v rámci hovoru přes platformu Teams. Firma požaduje v rámci nasazení asistenci i při přidělování práv uživatelům. Dále společnost bude testovat nasazené řešení, nejméně se na testování bude podílet 5 zaměstnanců z různých týmů a různého služebního věku. Dále bude vedena diskuze nad úpravami aplikace.

Příloha K

Přírava na šesté jednání

Tabulka K.1 Přehled šestého jednání

Datum:	20.04.2023
Čas:	8:30 – 9:30
Místo konání:	on-line
Pozvaní účastníci:	Zdeněk Vinduška, Markéta Petrtýlová
Připravili:	Markéta Petrtýlová

Pro nasazení byla aplikace, jejíž součástí jsou v tomto případě datové toky a regresní testy, společně s tabulkami v Dataverse vložena do Solutions. Solutions (v překladu Řešení) se používají k přenosu aplikací a komponent z jednoho prostředí do druhého. Solutions může obsahovat jednu nebo více aplikací a také další komponenty, jako jsou mapy webu, tabulky, procesy, webové zdroje, volby, toky a další. [105] Výhodou vložení komponent do tohoto balíčku je následný možný export celého balíčku jako celku a tedy toto řešení umožňuje jednodušší přenos aplikací. Balíček se exportuje jako jedna zazipovaná složka s koncovkou .zip.

Jelikož tabulky se exportují bez dat, tak data tabulky, kde jsou nadefinované kurzy byly exportovány zvlášť do souboru tabulkového procesoru.

Samostatně byl také exportován přehled dat aplikace v souboru s koncovkou .pbix, což je soubor nástroje Power BI.

Příloha L

Zápis z šestého jednání

Tabulka L.1 Přehled šestého jednání

Datum:	20.04.2023
Čas:	8:30 – 9:30
Místo konání:	on-line
Pozvaní účastníci:	Zdeněk Vinduška, Markéta Petrtýlová
Připravili:	Markéta Petrtýlová

Během šestého jednání probíhalo nasazení aplikace a přehledu dat. V prostředí Solutions v aplikaci Power Apps se provádí import pomocí tlačítka „Import solution" a následném zvolení zazipované složky.

Dále bylo nutné do tabulky o uživatelích přidat uživatele, kteří budou aplikaci využívat. Pro testování aplikace firma KPCS přidala pět uživatelů [77].

Společnost KPCS importovala data o kurzech do tabulky „tab_Couses" ze souboru tabulkového procesoru. Déle v tabulce „tab_CompletionTimes" definovala časy, do kterého mají být jednotlivé kurzy pro tento rok splněny. [107]

Pro možnost práce s daty uloženými v Dataverse v rámci používání aplikace jako běžný uživatel, musí mít daný uživatel přiřazenou roli nazvanou Service Writer. Ta má plné oprávnění k vytváření, čtení a zápisu pro všechny entity včetně vlastních entit [108]. Tato role byla již zmíněným uživatelům přiřazena v portálu Power Platform Admin Center.

Co se týče přehledu dat, tak v nástroji PowerBI, díky kterému je přehled vytvořen, musela společnost změnit prostředí (environmet) z kterého se čerpají data pro přehled a tedy ve kterém je e-lerningová aplikace v jejich prostředí. Dále už bylo potřeba přehled pouze publikovat pomocí tlačítka „Publikovat".

L.1 Komunikace spojená s testováním aplikace po nasazení

Po nasazení aplikace do produkčního prostředí společnosti KPCS pět zaměstnanců této společnosti aplikaci testovalo. Následující část popisuje poznatky z testovací aplikace, které zaměstnanci zadavatele předali dodavateli.

Velice kladně vyzdvihli zaměstnanci KPCS grafiku, která je intuitivní, dobře ovladatelná, srozumitelná a líbí se jim i z grafického pohledu.

Aplikace obsahuje dle počáteční domluvy dva vzdělávací kurzy na téma phishing a sociální inženýrství. Obsah vyhovuje potřebám společnosti KPCS a firma věří, že napomůže jí i případným jejím zákazníkům rozšířit znalosti zaměstnanců, a tak lépe ochránit firmu před útoky sociálního inženýrství.

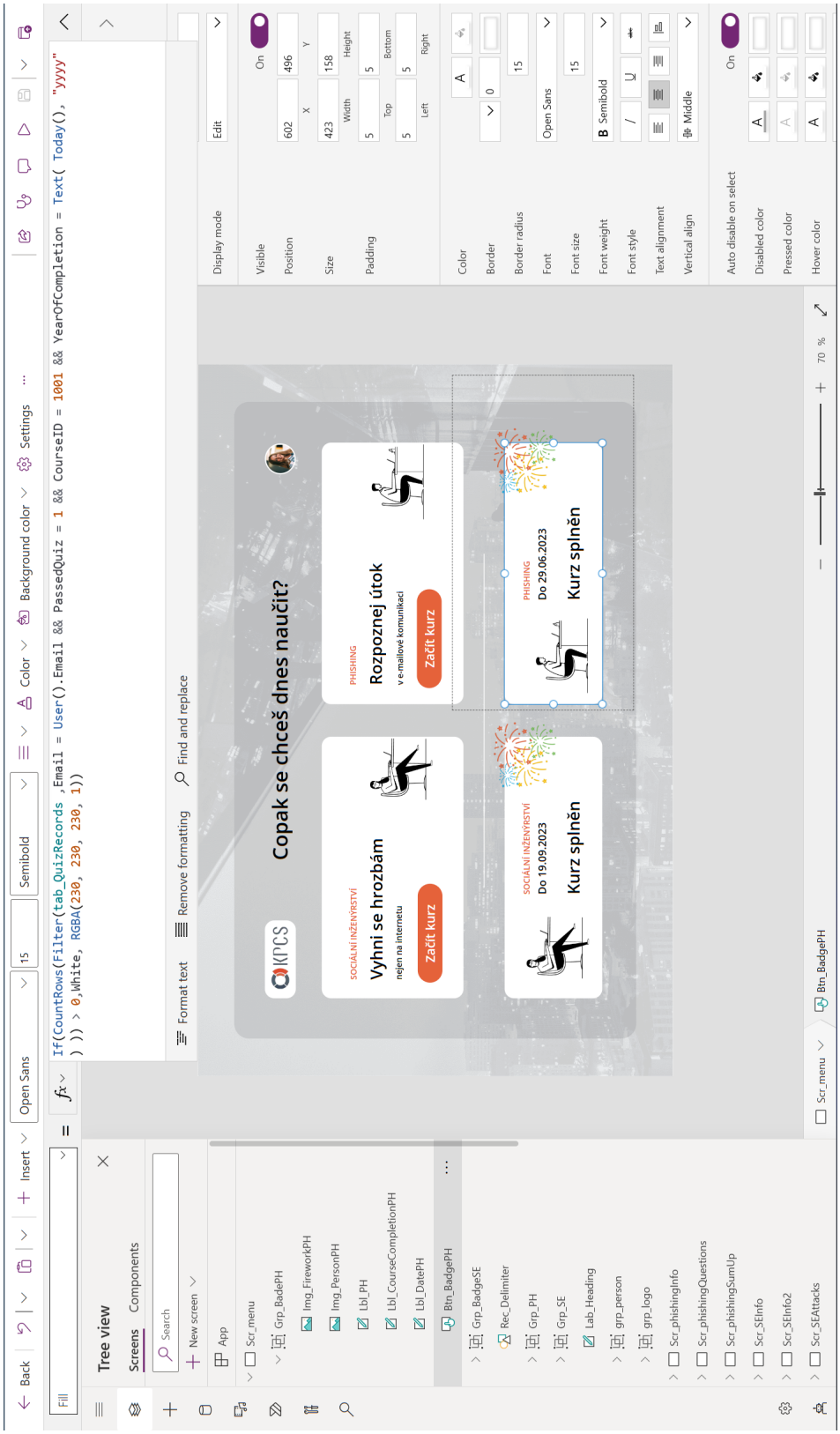
Společnost přidala také několik poznatků, o které by do budoucna mohla být aplikace rozšířena. Prvním podnětem bylo, že by se do tabulky uživatelů automaticky uložil uživatel, když prvně navštíví aplikaci. Zde by však nastával problém u přehledu, kde by nebylo jasné, kolik je celkem zaměstnanců, co mají kurz splnit, jelikož by nebyli v tabulce uživatelů přidáni ti, kdo aplikaci zatím vůbec nenavštívili.

Druhým podnětem bylo vytvořit přehled dat z aplikace přímo v aplikaci a zobrazovat tam zaměstnancům přehled o osobních výsledcích. Dále by bylo možné ještě přidat přehled pro manažery, kde by viděli všechny členy jejich týmu.

Společnost aplikaci vytkla pár gramatických chyb a překlepů v textech kurzů. Tyto nedostatky byly opraveny a společnosti byly zaslány podklady pro upgrade aplikace na novou verzi.

Příloha M

Ukázka vývojového prostředí



Obrázek M.1 Ukázka vývojového prostředí

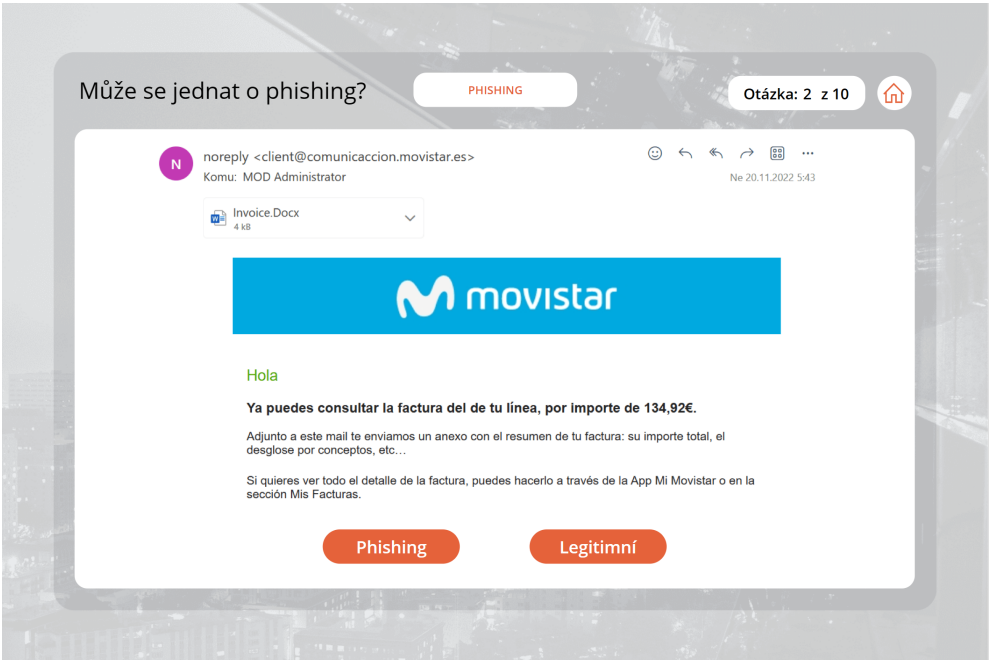
Příloha N

Uživatelské rozhraní

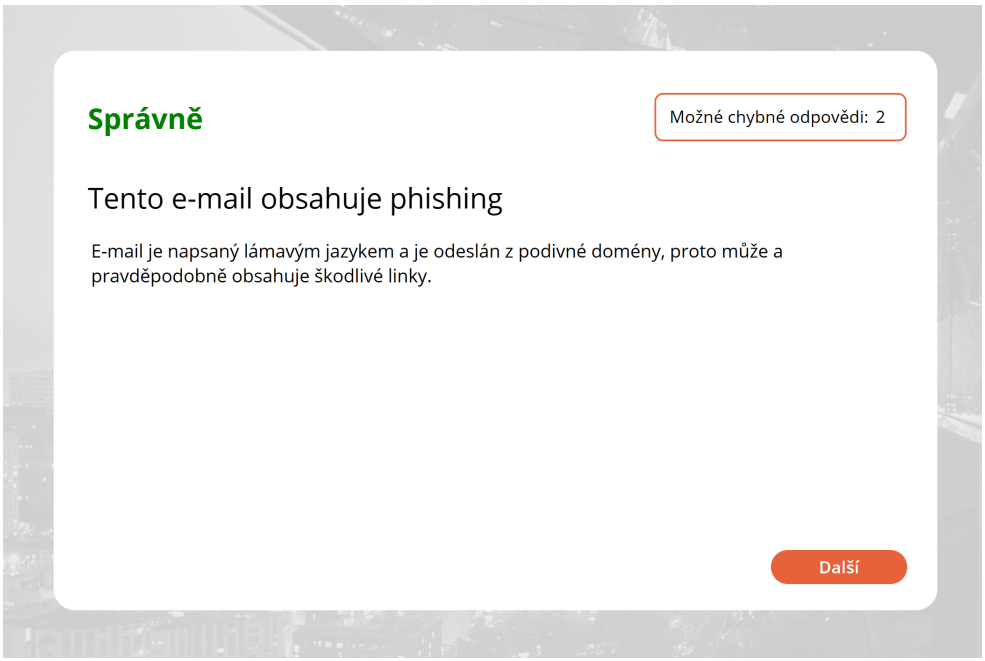
N.1 Menu

Obrázek N.1 Menu v aplikaci

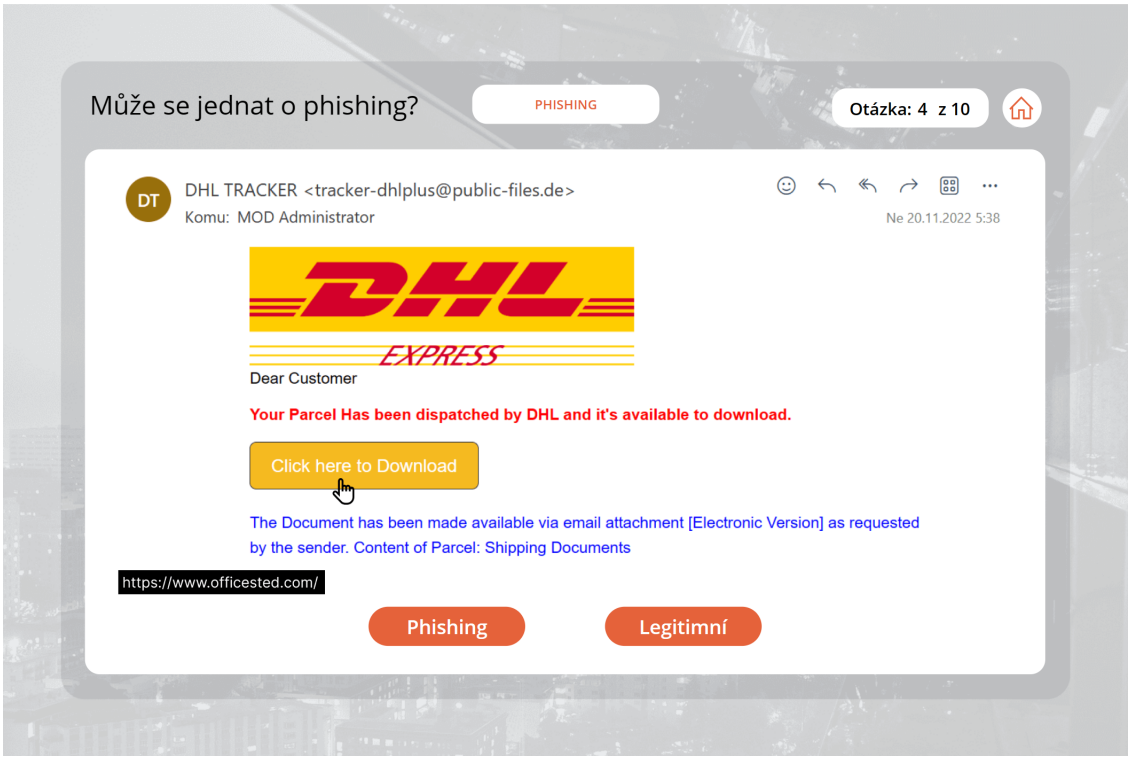
N.2 Kurz o phishingu



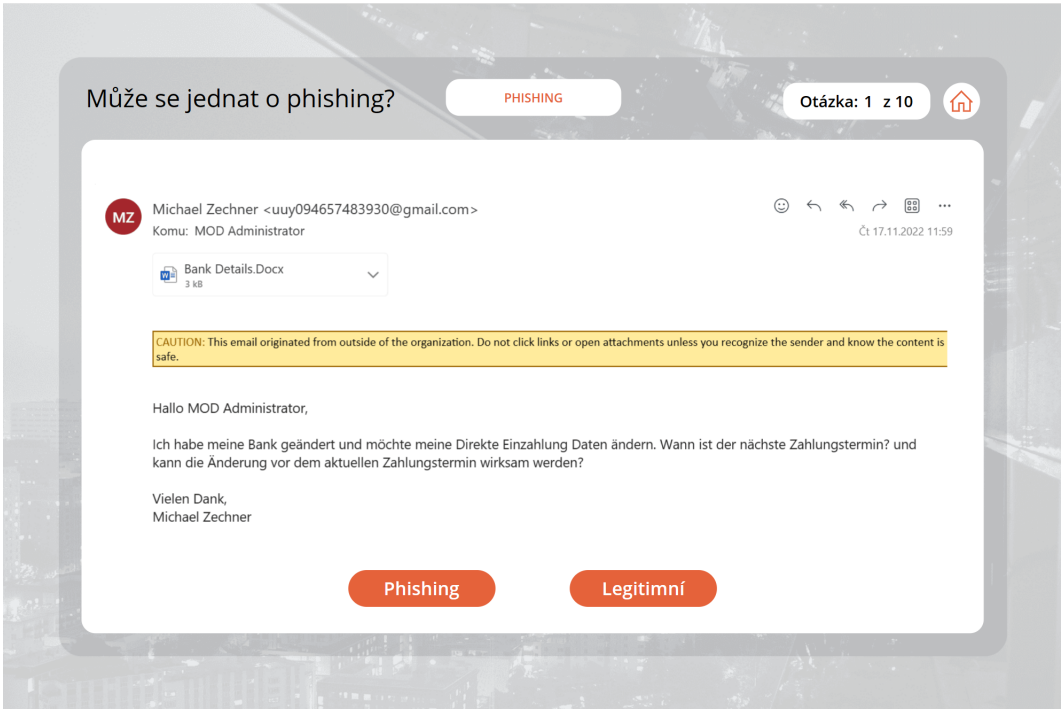
Obrázek N.2 Ukázka kurzu Phishing 1



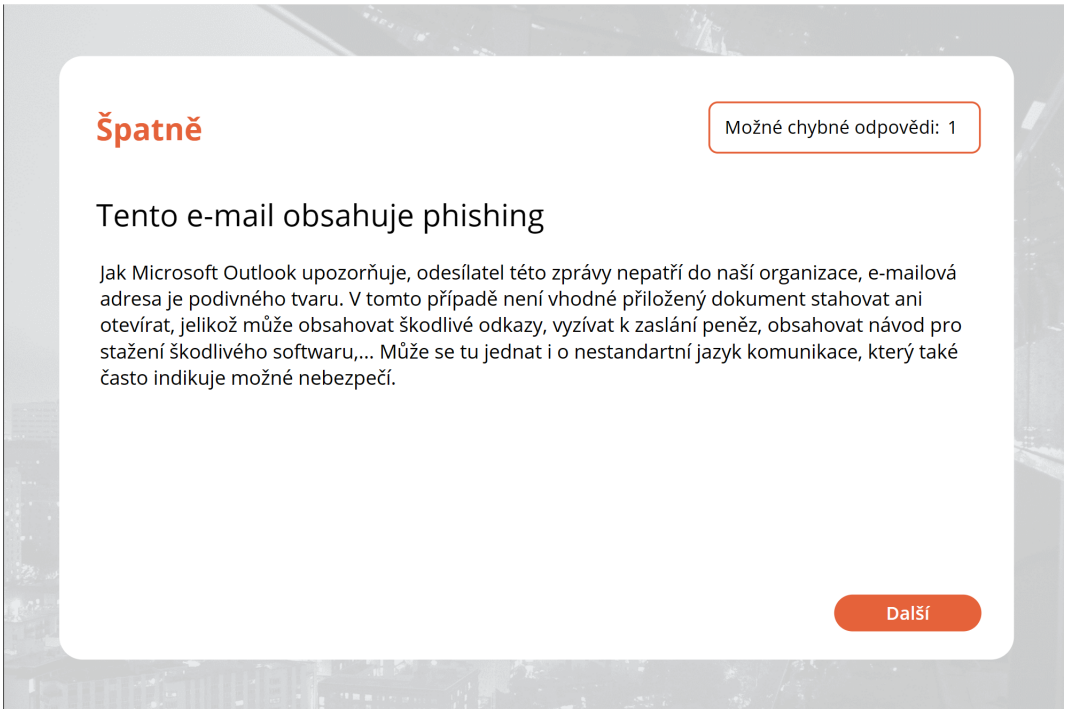
Obrázek N.3 Ukázka kurzu Phishing 2



Obrázek N.4 Ukázka kurzu Phishing 3

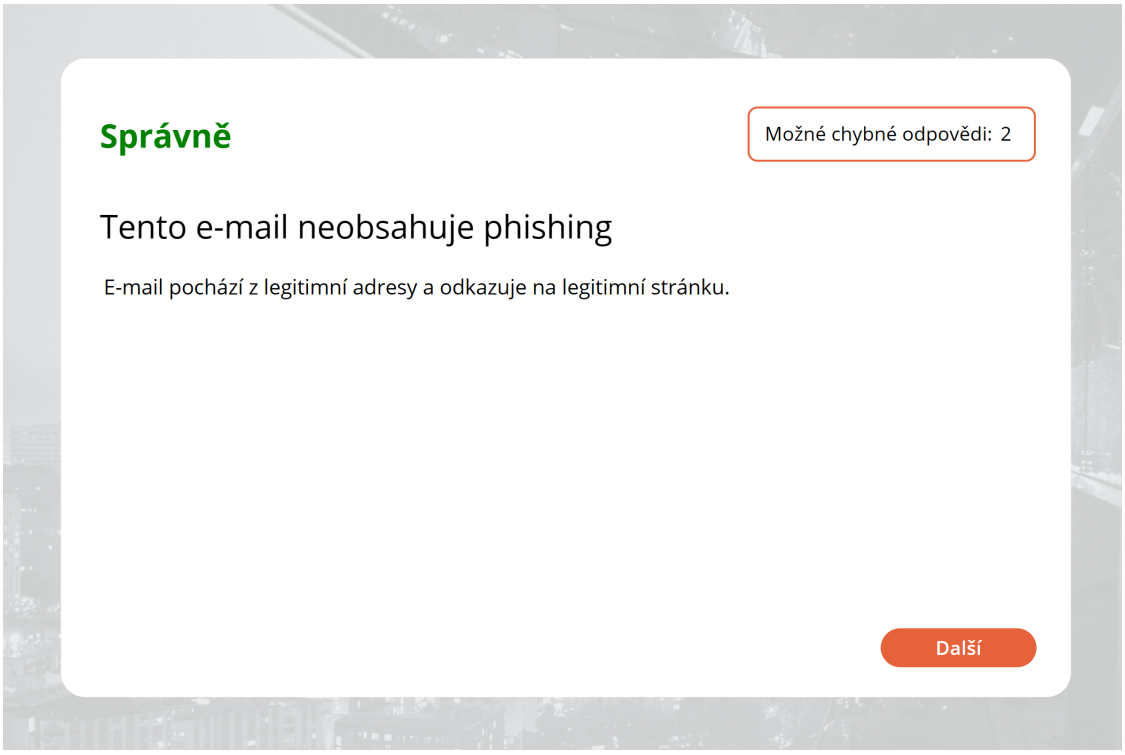


Obrázek N.5 Ukázka kurzu Phishing 4



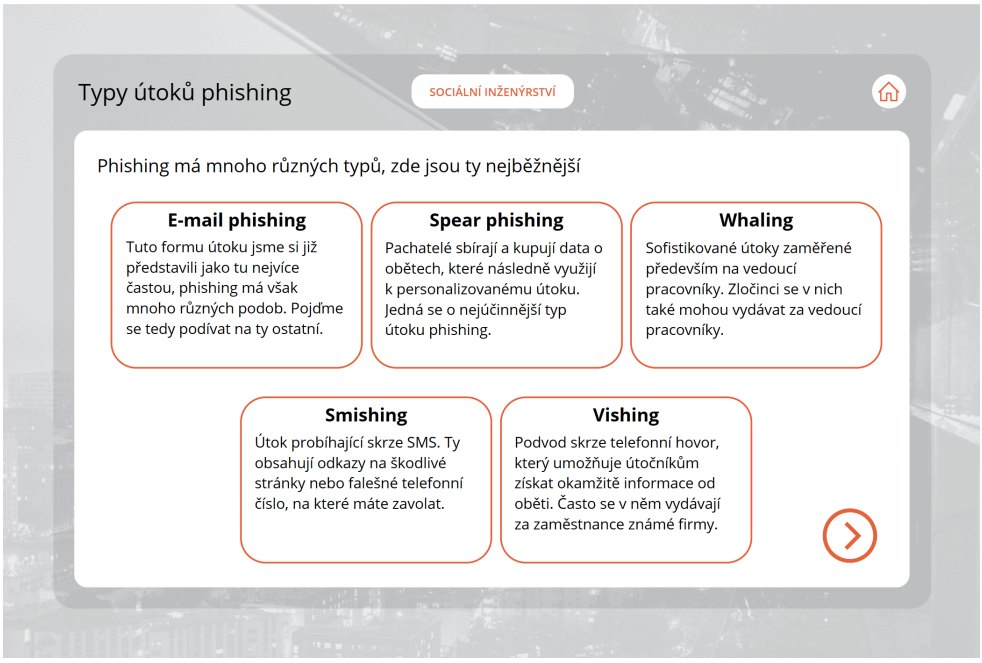
Obrázek N.6 Ukázka kurzu Phishing 5

Obrázek N.7 Ukázka kurzu Phishing 6

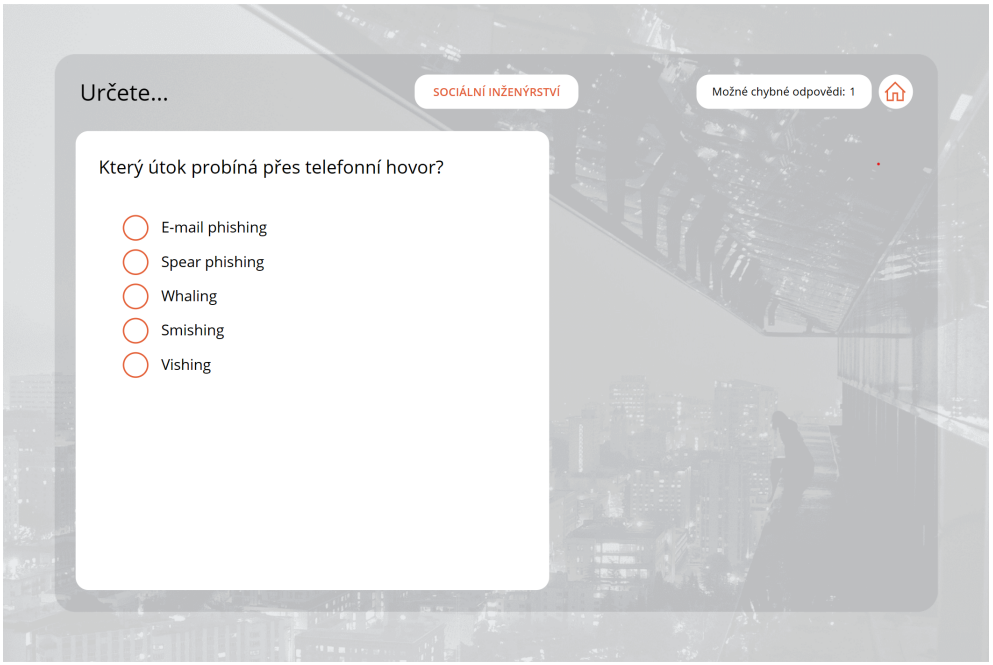


Obrázek N.8 Ukázka kurzu Phishing 7

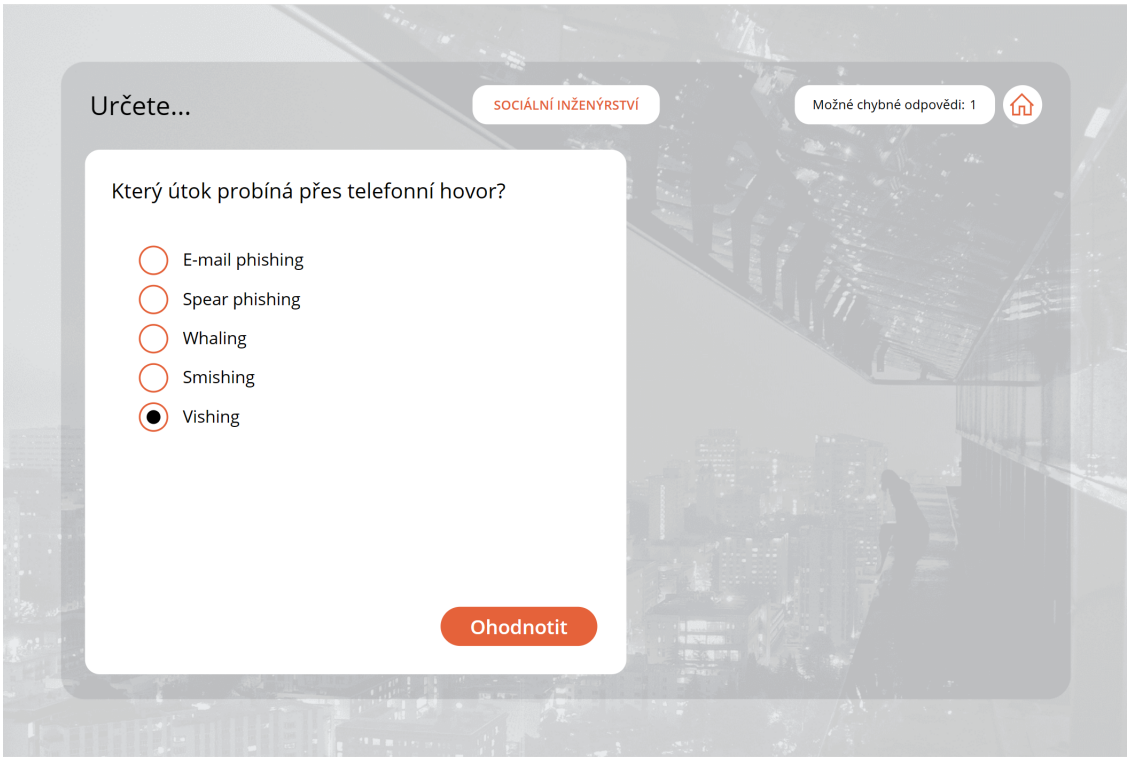
N.3 Kurz o sociálním inženýrství



Obrázek N.9 Ukázka kurzu Sociální inženýrství 1

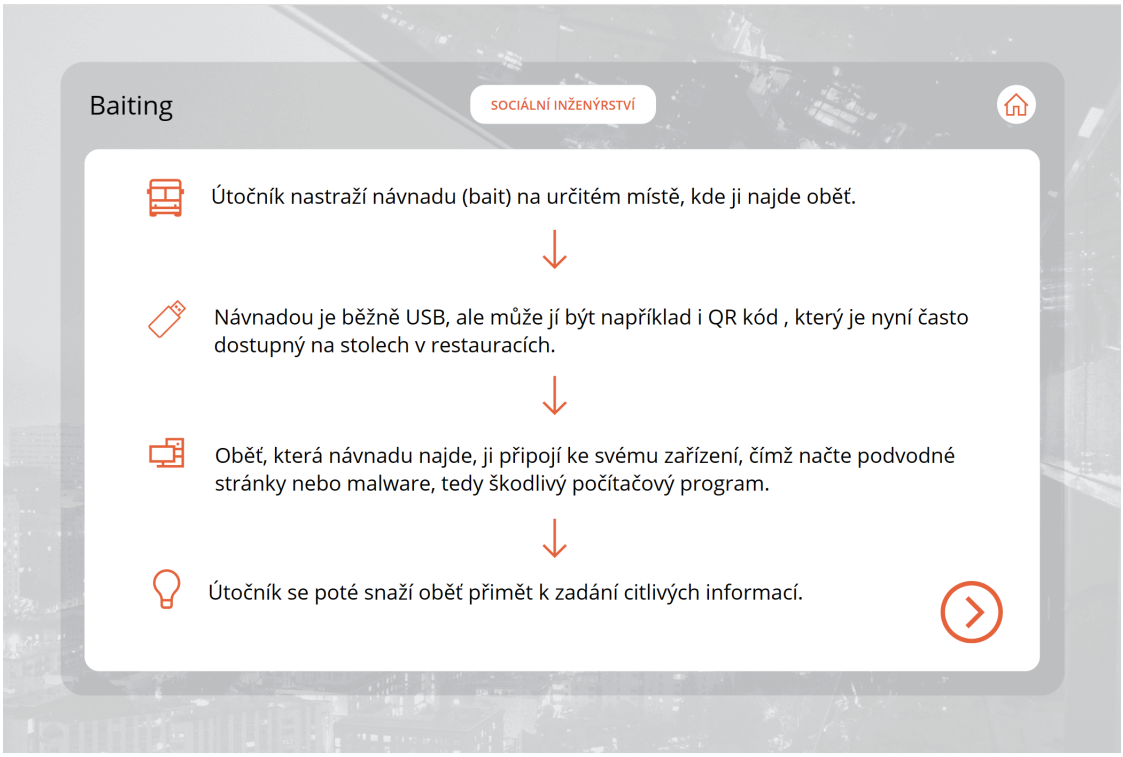


Obrázek N.10 Ukázka kurzu Sociální inženýrství 2



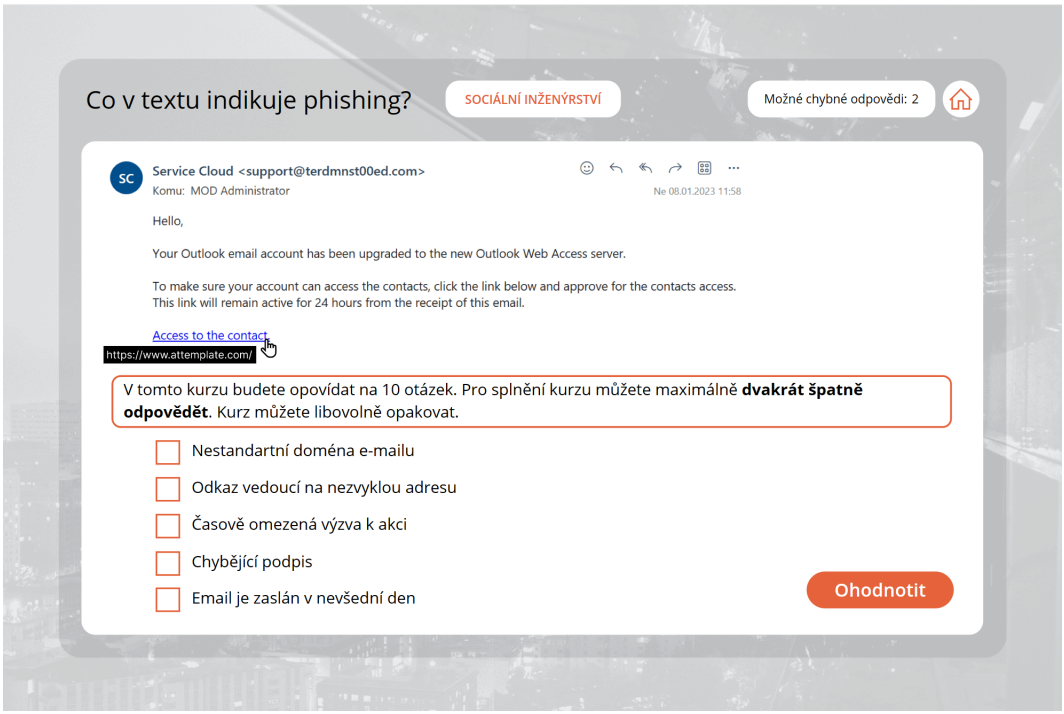
Obrázek N.11 Ukázka kurzu Sociální inženýrství 3

Obrázek N.12 Ukázka kurzu Sociální inženýrství 4



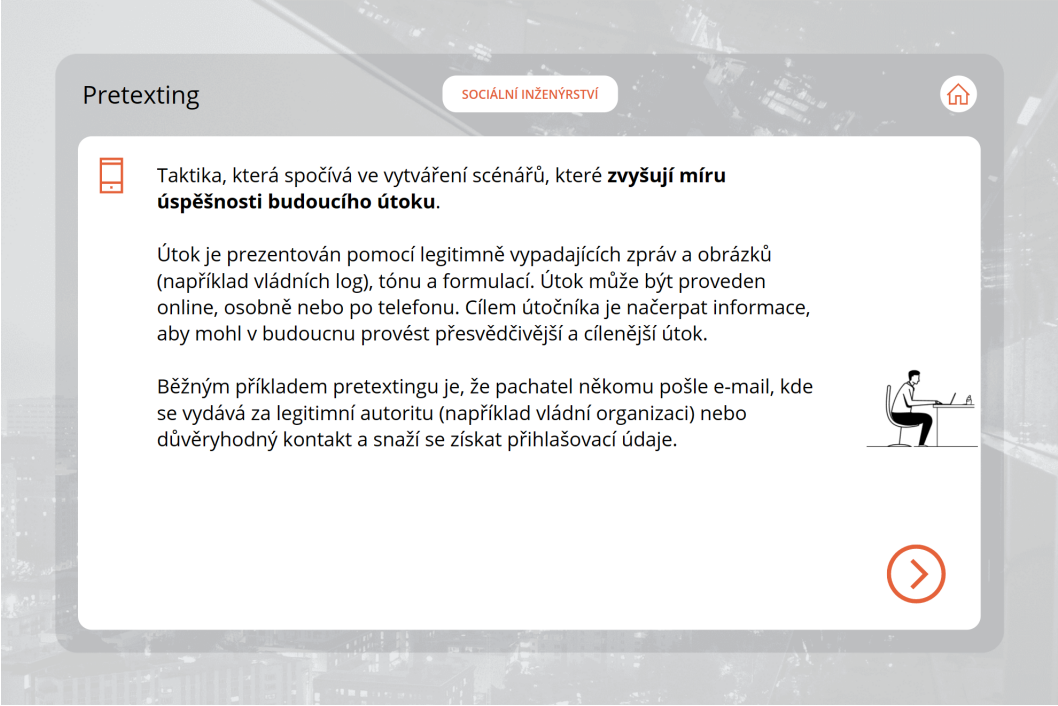
Obrázek N.13 Ukázka kurzu Sociální inženýrství 5

Obrázek N.14 Ukázka kurzu Sociální inženýrství 6

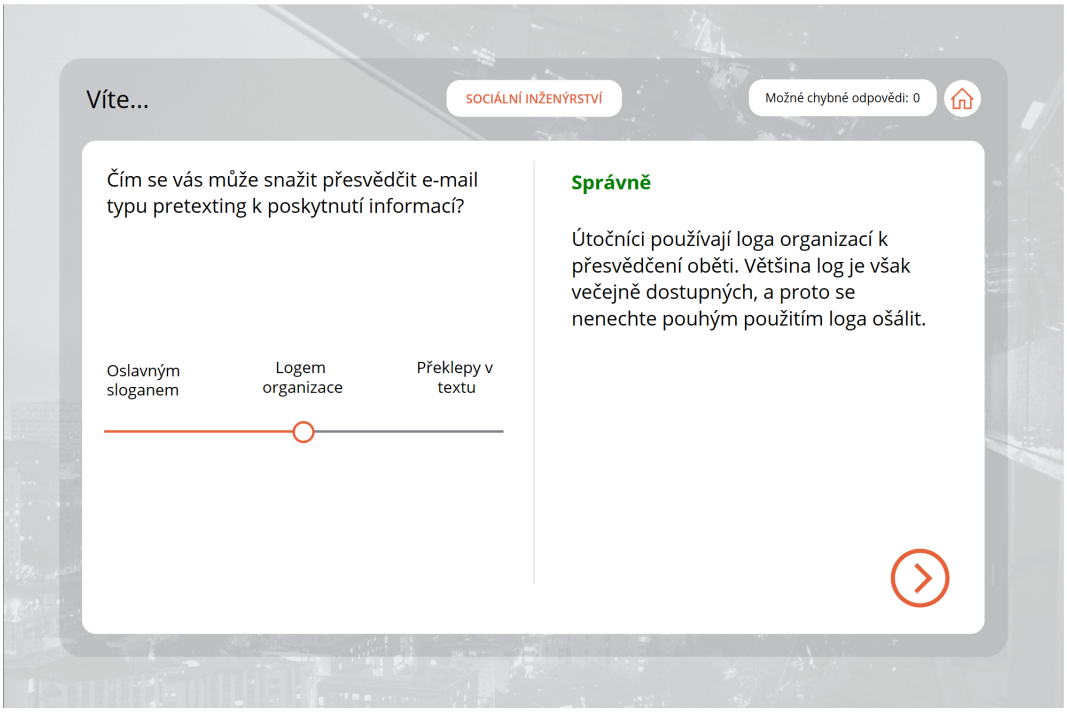


Obrázek N.15 Ukázka kurzu Sociální inženýrství 7

Obrázek N.16 Ukázka kurzu Sociální inženýrství 8

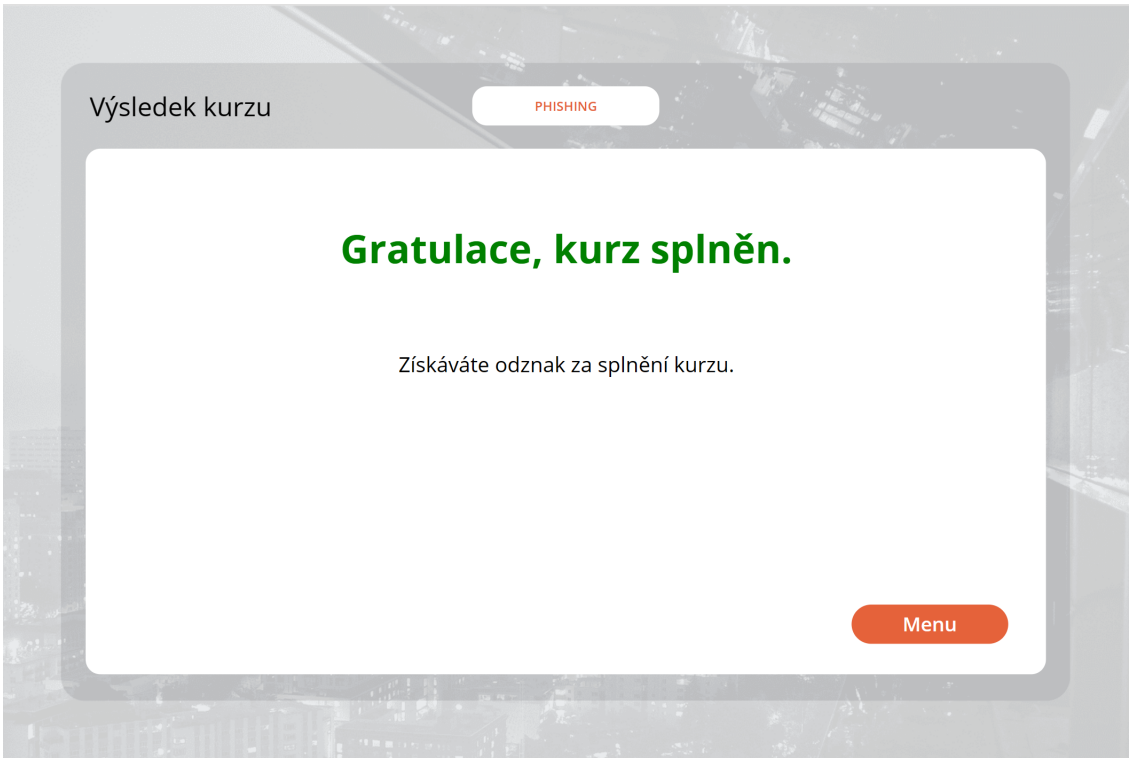


Obrázek N.17 Ukázka kurzu Sociální inženýrství 9

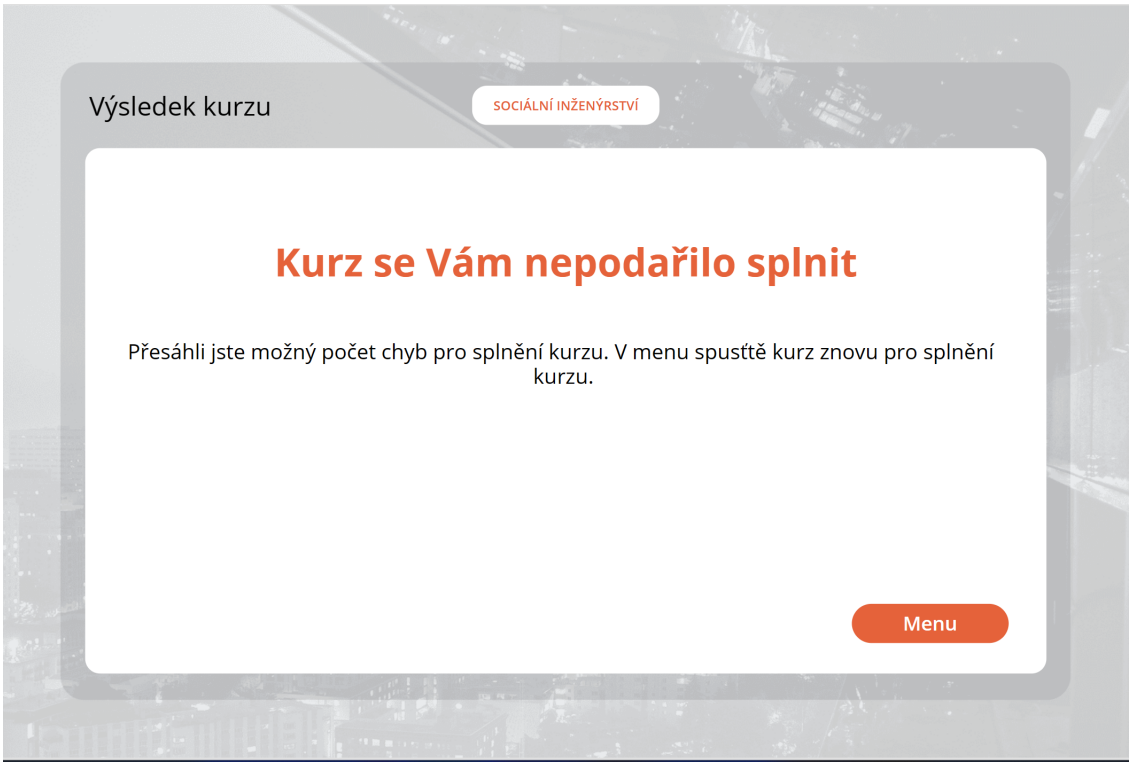


Obrázek N.18 Ukázka kurzu Sociální inženýrství 10

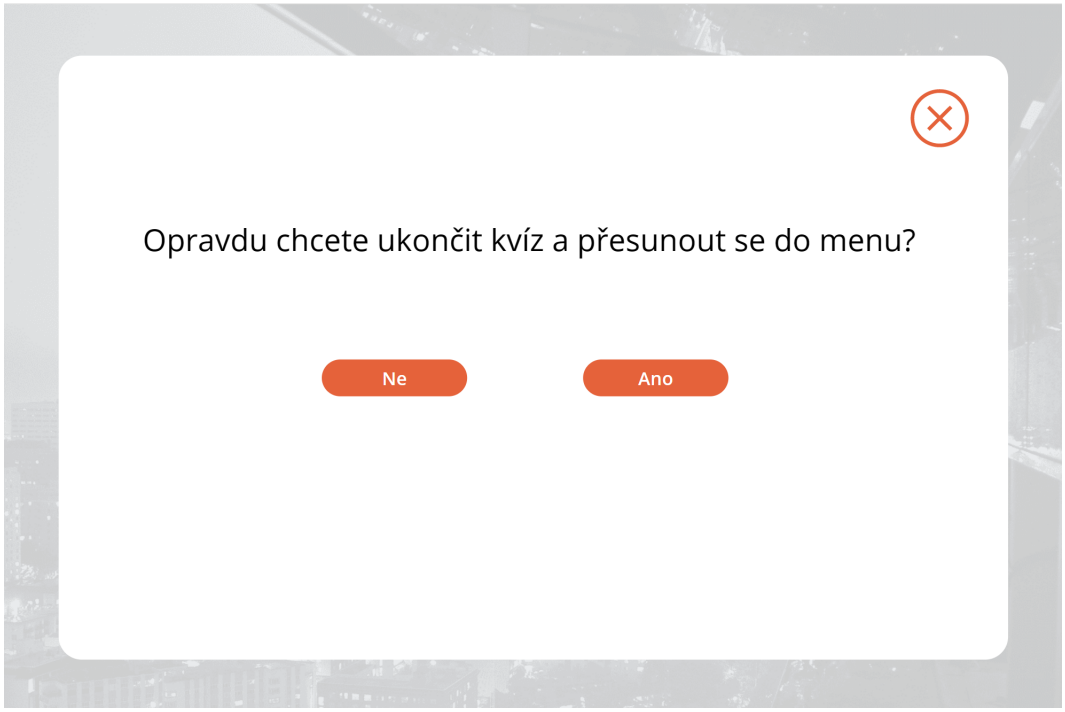
N.4 Ukončení kurzu



Obrázek N.19 Úspěšného ukončení kurzu



Obrázek N.20 Neúspěšné ukončení kurzu



Obrázek N.21 Předčasné ukončení kurzu přechodem do menu díky symbolu domu

Bibliografie

1. EGRESS. *Insider Data Breach Survey 2021* [online]. Anglie, 2022 [cit. 2022-03-12]. Tech. zpr. Egress. Dostupné z: `https://www.egress.com/media/4kqhlafh/egress-insider-data-breach-survey-2021.pdf`.
2. ABBATE, Paul. *Internet Crime Report 2021* [online]. Spojené státy americké, 2022 [cit. 2022-12-03]. Tech. zpr. FEDERAL BUREAU of INVESTIGATION. Dostupné z: `https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf`.
3. KPCS CZ, S.R.O. *KPCS ve zkratce* [online]. 2018. [cit. 2023-03-14]. Tech. zpr. Společnost KPCS CZ, s.r.o. Dostupné z: `https://www.kpcs.cz/cs/kpcs/kpcs-ve-zkratce.html`.
4. POLICIE ČESKÉ REPUBLIKY. *Kyberkr-iminalita* [online]. Česká republika, 2022 [cit. 2023-01-16]. Tech. zpr. Policie České republiky. Dostupné z: `https://www.policie.cz/clanek/kyberkriminalita.aspx`.
5. MITNICK, Kevin D.; SIMON, William L. *The Art of Deception: Controling the Human Element of Security Helion*. Polsko: Helion S.A, 2003. ISBN 83-7361-210-6.
6. MANN, Ian. *Hacking the Human: Social Engineering Techniques and Security Countermeasures*. Hampshire, Anglie: Gower Publishing Limited, 2008. ISBN 0566087731.
7. IMPERVA. *Social Engineering* [online]. Spojené státy americké, 2022 [cit. 2023-02-12]. Tech. zpr. Imperva. Dostupné z: `https://www.imperva.com/learn/application-security/social-engineering-attack/`.
8. ESET SOFTWARE SPOL. S R.O. *Phishing* [online]. Česká republika, 2022 [cit. 2022-12-04]. Tech. zpr. ESET software spol. s r.o. Dostupné z: `https://www.eset.com/cz/phishing/#co-je-phishing-utok`.

9. AARON, Greg. *Unifying the Global Response To Cybercrime* [online]. Spojené státy americké, 2020 [cit. 2022-12-04]. Tech. zpr. APWG. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf.

10. *What is Phishing Attack? Definition, Types and How to Prevent it* [online]. 2022. [cit. 2022-12-04]. Dostupné z: https://images.app.goo.gl/8bQoKBYVmnKKcEcd7.

11. CISCO. *Cyber security threat trends: phishing, crypto top the list* [online]. Spojené státy americké, 2021 [cit. 2022-12-04]. Tech. zpr. CISCO. Dostupné z: https://learn-cloudsecurity.cisco.com/umbrella-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list.

12. PANDA. *11 Types of Phishing + Real-Life Examples* [online]. Španělsko, 2021 [cit. 2023-01-24]. Tech. zpr. Panda. Dostupné z: https://www.pandasecurity.com/en/mediacenter/tips/types-of-phishing/.

13. CLOUDFLARE. *What is a phishing attack?* [online]. Spojené státy americké, 2022 [cit. 2022-12-04]. Tech. zpr. Cloudflare. Dostupné z: https://www.cloudflare.com/learning/access-management/phishing-attack/.

14. HADNAGY, Christopher; FINCHER, Michele. *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails*. Spojené státy americké: John Wiley a Sons, Inc, 2015. ISBN 9781119183624.

15. CHIN, Kyle. *19 Most Common Types of Phishing Attacks in 2023* [online]. Spojené státy americké, 2023 [cit. 2023-01-21]. Tech. zpr. UpGuard. Dostupné z: https://www.computerworld.cz/clanky/osint-aneb-co-je-mozne-zjistit-o-organizaci-z-otevrenych-zdroju/.

16. AXIANS. *OSINT aneb co je možné zjistit o organizaci z otevřených zdrojů* [online]. Česká republika, 2022 [cit. 2023-01-21]. Tech. zpr. Internet Info DG, a.s. Dostupné z: https://www.computerworld.cz/clanky/osint-aneb-co-je-mozne-zjistit-o-organizaci-z-otevrenych-zdroju/.

17. BODNAR, Danielle. *Insider Data Breach Survey 2021* [online]. Česká republika, 2022 [cit. 2023-01-21]. Tech. zpr. Avast. Dostupné z: https://www.avast.com/c-social-engineering.

18. GRAY, Joe. *Practical social engineering*. Spojené státy americké: William Pollock, 2022. ISBN 978-1-7185-0098-3.

19. KASPERSKY. *What is scareware? Definition and explanation* [online]. Spojené státy americké, 2023 [cit. 2023-01-21]. Tech. zpr. Rusko. Dostupné z: https://usa.kaspersky.com/resource-center/definitions/scareware.

20. FORTINET. *What Is Pretexting?* [online]. Spojené státy americké, 2023 [cit. 2023-01-21]. Tech. zpr. Fortinet. Dostupné z: https://www.fortinet.com/resources/cyberglossary/pretexting.

21. INNEFU. *InnSight* [online]. Indie, 2014 [cit. 2023-01-21]. Tech. zpr. Innefu. Dostupné z: https://www.innefu.com/blog/honey-trap-the-new-espionage-outfit/.

22. IRWIN, Luke. *The 5 Biggest Phishing Scams of All Time* [online]. Evropa, 2022 [cit. 2023-02-02]. Tech. zpr. IT Governance. Dostupné z: https://www.itgovernance.eu/blog/en/the-5-biggest-phishing-scams-of-all-time.

23. ŠPAČKOVÁ, Iva. *Zcela nový podvod ve světě peněz. Na vaše úspory útočí „živý člověk“* [online]. česká republika, 2023 [cit. 2023-02-02]. Tech. zpr. Seznam Zprávy. Dostupné z: https://www.seznamzpravy.cz/clanek/ekonomika-finance-osobni-zcela-novy-podvod-ve-svete-penez-na-vase-uspory-utoci-zivy-clovek-224764.

24. BULLÉE, Jan-Willem H.; JUNGER, Marianne. *Social Engineering* [online]. Švédsko a Nizozemsko, 2020 [cit. 2023-01-22]. Tech. zpr. University of Twente a Linköping University. Dostupné z: https://www.researchgate.net/publication/339676784_Social_Engineering.

25. FEDERAL BUREAU OF INVESTIGATION. *2013 Internet Crime Report* [online]. Spojené státy americké, 2013 [cit. 2023-01-22]. Tech. zpr. Federal Bureau of investigation. Dostupné z: https://www.ic3.gov/Media/PDF/AnnualReport/2013_IC3Report.pdf.

26. OLIVEIRA, Daniela; ROCHA, Harold; YANG, Huizi; ELLIS, Donovan; DOMMARAJU, Sandeep; MURADOGLU, Melis; WEIR, Devon; SOLIMAN, Adam; LIN, Tian; EBNER, Natalie. *Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing* [online]. Spojené státy americké, 2017 [cit. 2023-01-22]. Tech. zpr. University of Florida a York University. Dostupné z: http://library.usc.edu.ph/ACM/CHI%5C%202017/1proc/p6412.pdf.

27. SHENG, Steve; HOLBROOK, Mandy; KUMARAGURU, Ponnurangam; CRANOR, Lorrie; DOWNS, Julie. *Who Falls for Phish? ADemographic Analysis of Phishing Susceptibility and Effectiveness of Interventions* [online]. Spojené státy americké, 2010 [cit. 2023-01-22]. Tech. zpr. Carnegie Mellon University, Indraprastha Institute of Information Technology. Dostupné z: https://www.securityadvisor.io/risky-behavior-report.

28. SECURITYADVISOR. *Support the Human Firewall by Identifying the Riskiest Users and Their Most Dangerous Online Behaviors* [online]. Spojené státy americké, 2023 [cit. 2023-01-22]. Tech. zpr. SecurityAdvisor. Dostupné z: https://www.securityadvisor.io/risky-behavior-report.

29. LABS, Keepnet. *Phishing trends report* [online]. cambridge, Anglie, 2020 [cit. 2023-01-22]. Tech. zpr. Keepnet LABS. Dostupné z: https://keepnetlabs.com/wp-content/uploads/2022/05/2020-Phishing-Trends-Report-1.pdf.

30. BENENSON, Zinaida; GASSMANN, Freya; LANDWIRTH, Robert. *Unpacking Spear Phishing Susceptibility* [online]. Německo, 2017 [cit. 2023-02-02]. Tech. zpr. Friedrich-Alexander-Universität Erlangen-Nürnberg a Universität des Saarlandes. Dostupné z: https://www.cl.cam.ac.uk/~rja14/shb17/benenson.pdf.

31. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *The Five Functions* [online]. Spojené státy amercké, 2023 [cit. 2023-04-15]. Tech. zpr. National Institute of Standards a Technology. Dostupné z: https://www.nist.gov/cyberframework/online-learning/five-functions.

32. SECURITY METRICS. *5 Tips to Train Workforce on Social Engineering* [online]. Spojené státy americké, 2023 [cit. 2023-02-05]. Tech. zpr. Security Metrics. Dostupné z: https://www.securitymetrics.com/learn/5-tips-train-workforce-social-engineering.

33. AVAST. *Návod pro firmy i zaměstnance, jak poznat phishingový e-mail* [online]. Česká republika, 2019 [cit. 2023-01-19]. Tech. zpr. Avast. Dostupné z: https://blog.avast.com/cs/how-to-detect-phishing-emails-sent-to-your-business.

34. WHOIS. *Every Great Idea Starts with a Great Domain Name* [online]. Spojené státy americké, 2023 [cit. 2023-04-15]. Tech. zpr. Whois.com. Dostupné z: https://www.whois.com/.

35. VIRUSTOTAL. *Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.* [online]. Španělsko, 2023 [cit. 2023-04-15]. Tech. zpr. Hispasec Sistemas. Dostupné z: https://www.virustotal.com/gui/home/url.

36. DOBROZENSKÝ, Dominik. *Není povolání jako povolání: základy hackingu aneb kdo je etický hacker a jak se jím stát?* [online]. Česká republika, 2022 [cit. 2023-02-04]. Tech. zpr. cnews.cz. Dostupné z: https://www.cnews.cz/zaklady-hackingu-jak-se-stat-etickym-hackerem.

37. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *PENETRAČNÍ TESTOVÁNÍ – ÚVOD DO PROBLEMATIKY* [online]. Česká republika, 2022 [cit. 2023-02-04]. Tech. zpr. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/2022-03-07_Penetracni-testovani_v1.0.pdf.

38. GONZALEZ, Cynthia. *Top 8 Social Engineering Techniques and How to Prevent Them [2022]* [online]. Spojené státy americké, 2022 [cit. 2023-02-03]. Tech. zpr. Exabeam. Dostupné z: https://www.exabeam.com/information-security/top-8-social-engineering-techniques-and-how-to-prevent-them-2022/.

39. LAIN, Daniele; KOSTIAINEN, Kari; CAPKUN, Srdjan. *Phishing in Organizations: Findings from a Large-Scale and Long-Term Study* [online]. Švýcarsko, 2021 [cit. 2023-02-04]. Tech. zpr. ETH Zurich. Dostupné z: https://arxiv.org/pdf/2112.07498.pdf.

40. IDEALAB. *Crowdsourcing* [online]. Česká republika, 2022 [cit. 2023-02-04]. Tech. zpr. Idealab. Dostupné z: https://idealab.cz/slovnik/crowdsourcing/.

41. BBC. *West Midlands Railway sent staff fake bonus email in cyber-security test* [online]. Anglie, 2021 [cit. 2023-02-04]. Tech. zpr. BBC. Dostupné z: https://www.bbc.com/news/uk-england-birmingham-57065311.

42. HARFORD, Isabella. *Do phishing simulations work? Sometimes* [online]. Spojené státy americké, 2022 [cit. 2023-02-04]. Tech. zpr. TechTarget. Dostupné z: //https_www.techtarget.com/?url=https%5C%3A%5C%2F%5C%2Fwww.techtarget.com%5C%2Fsearchsecurity%5C%2Ffeature%5C%2FDo-phishing-simulations-work-Sometimes.

43. AO KASPERSKY LAB. *Ways to avoid social engineering attacks* [online]. Rusko, 2023 [cit. 2023-02-04]. Tech. zpr. AO Kaspersky Lab. Dostupné z: https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks.

44. ČSOB. *Všechna hesla si zapamatovat nejde, používejte správce hesel* [online]. Česká republika, 2020 [cit. 2023-02-05]. Tech. zpr. ČSOB. Dostupné z: https://www.csob.cz/portal/v-obraze/blog/clanky/vsechna-hesla-si-zapamatovat-nejde-pouzivejte-spravce-hesel.

45. ONELOGIN. *The Truth about Passwordless Authentication* [online]. Spojené státy americké, 2023 [cit. 2023-02-05]. Tech. zpr. onelogin. Dostupné z: https://www.onelogin.com/learn/passwordless-authentication.

46. ONELOGIN. *How Does Single Sign-On Work?* [online]. Spojené státy americké, 2023 [cit. 2023-02-05]. Tech. zpr. onelogin. Dostupné z: https://www.onelogin.com/learn/how-single-sign-on-works.

47. BLEEPING COMPUTER. *MFA Fatigue attacks are putting your organization at risk* [online]. 2022. [cit. 2023-02-05]. Tech. zpr. Bleeping Computer. Dostupné z: https://www.bleepingcomputer.com/news/security/mfa-fatigue-attacks-are-putting-your-organization-at-risk/.

48. ZSCALER. *What Is Zero Trust?* [online]. Spojené státy americké, 2023 [cit. 2023-02-05]. Tech. zpr. Zscaler. Dostupné z: https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust.

49. AMAZON WEB SERVICES, INC. *7 Steps to Take During a Cyber Attack* [online]. Spojené státy americké, 2021 [cit. 2023-02-05]. Tech. zpr. Amazon Web Services, Inc. Dostupné z: https://wickr.com/7-steps-to-take-during-a-cyber-attack/.

50. COURSEA. *What Is the Software Development Life Cycle? SDLC Explained* [online]. Spojené státy americké, 2022 [cit. 2023-03-10]. Tech. zpr. Coursea. Dostupné z: https://www.coursera.org/articles/software-development-life-cycle.

51. JILVANPINHEIRO. *Software Development Life Cycle (SDLC) phases* [online]. 2018. [cit. 2023-03-10]. Tech. zpr. Medium. Dostupné z: https://medium.com/@jilvanpinheiro/software-development-life-cycle-sdlc-phases-40d46afbe384.

52. VINDUŠKA, Zdeněk; BEČKA, Jiří; KOUTNÍKOVÁ, Martina; PETRTÝLOVÁ, Markéta. *První rozhovor: Definice zadání* [online]. [B.r.]. [cit. 2022-09-07].

53. PREVENT, S.R.O. *FAQ* [online]. Česká republika, 2023 [cit. 2023-02-23]. Tech. zpr. Prevent, s.r.o. Dostupné z: https://www.instructor.cz/otazky-odpovedi-k-bozp-po.

54. LINKEDIN. *A learning experience built for skill builders.* [online]. Spojené státy americké, 2023 [cit. 2023-02-24]. Tech. zpr. LinkedIn. Dostupné z: https://learning.linkedin.com/.

55. LINKEDIN. *Start your 1-month free trial. Cancel anytime.* [online]. vSpojené státy americké, 2023 [cit. 2023-02-24]. Tech. zpr. LinkedIn. Dostupné z: https://www.linkedin.com/learning/subscription/products.

56. MICROSOFT. *Overview of Microsoft Viva Learning* [online]. Spojené státy americké, 2022 [cit. 2023-02-24]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/viva/learning/overview-viva-learning.

57. MICROSOFT. *Microsoft Viva Learning* [online]. Spojené státy americké, 2023 [cit. 2023-02-24]. Tech. zpr. Microsoft. Dostupné z: https://www.microsoft.com/en-us/microsoft-viva/learning.

58. LMC S.R.O. *Nejdostupnější firemní vzdělávání. Online.* [online]. Česká republika, 2023 [cit. 2023-03-05]. Tech. zpr. LMC s.r.o. Dostupné z: https://www.seduo.cz/pro-zamestnavatele.

59. SKILLSHARE. *Set Your Team Up For Success* [online]. Spojené státy americké, 2023 [cit. 2023-03-05]. Tech. zpr. Skillshare. Dostupné z: https://teams.skillshare.com/.

60. COURSERA INC. *Accelerate business transformation* [online]. Spojené státy americké, 2023 [cit. 2023-03-05]. Tech. zpr. Coursera Inc. Dostupné z: https://www.coursera.org/business?utm_campaign=website&utm_content=corp-to-home-for-enterprise&utm_medium=coursera&utm_source=header.

61. COURSERA INC. *Choose a learning plan that fits your business goals* [online]. Spojené státy americké, 2023 [cit. 2023-03-05]. Tech. zpr. Coursera Inc. Dostupné z: https://www.coursera.org/business/compare-plans?utm_campaign=website&utm_content=corp-to-home-for-enterprise&utm_medium=coursera&utm_source=header.

62. SEYFOR. *Co Knowee nabízí* [online]. Česká republika, 2023 [cit. 2023-03-05]. Tech. zpr. Seyfor. Dostupné z: https://knowee.com/cs-cz/proc-knowee.

63. SEYFOR. *Co Knowee nabízí* [online]. Česká republika, 2023 [cit. 2023-03-05]. Tech. zpr. Seyfor. Dostupné z: https://knowee.com/cs-cz/caste-otazky.

64. JAMA SOFTWARE. *Functional vs Nonfunctional Requirements: What's the difference?* [online]. Spojené státy americké, 2021 [cit. 2023-03-05]. Tech. zpr. Jama Software. Dostupné z: https://www.jamasoftware.com/blog/requirements-management-functional-requirement-vs-non-functional-requirements/.

65. VINDUŠKA, Zdeněk; PETRTÝLOVÁ, Markéta. *Čtvrtý rozhovor: Poznatky z uživatelského testování* [online]. [B.r.]. [cit. 2023-02-21].

66. VINDUŠKA, Zdeněk; PETRTÝLOVÁ, Markéta. *Druhý rozhovor: Schválení harmonogramu projektu* [online]. [B.r.]. [cit. 2022-09-21].

67. VINDUŠKA, Zdeněk; PETRTÝLOVÁ, Markéta. *Třetí rozhovor: Schválení grafických podkladů a podkladů pro vzdělávací kurzy* [online]. [B.r.]. [cit. 2022-07-12].

68. MICROSOFT. *Do more with less by using low-code tools to adapt* [online]. Spojené státy americké, 2023 [cit. 2023-03-11]. Tech. zpr. Microsoft. Dostupné z: https://powerplatform.microsoft.com/en-gb/?ef_id=fb09286e41b91f6272ba4c5b2f0a3a52:G:s&OCID=AIDcmmgly95xrd_SEM_fb09286e41b91f6272ba4c5b2f0a3a52:G:s&msclkid=fb09286e41b91f6272ba4c5b

69. DAVIS, Chris; SIMPSON, Daniel; ROBINS, Rebecca; RATULCH. *Simulate a phishing attack with Attack simulation training in Defender for Office 365* [online]. Spojené státy americké, 2023 [cit. 2023-02-26]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-simulations?view=o365-worldwide.

70. DAVIS, Chris; SIMPSON, Daniel; ROBINS, Rebecca; RATULCH; TRAN, James; VANGEL, Denise; ATHAVALE, Maghana; CHAKRABARTI, Ratula; KRISHNAN, Gopalakrishnan; KASARMA; CLARK, Stuart. *Get started using Attack simulation training in Defender for Office 365* [online]. Spojené státy americké, 2023 [cit. 2023-02-26]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?source=recommendations&view=o365-worldwide.

71. ANDERSON, Bill; KULKARNI, Venkat; SANTIAGO, David. *Manage tenants in your Microsoft Customer Agreement billing account* [online]. Spojené státy americké, 2022 [cit. 2023-02-26]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/azure/cost-management-billing/microsoft-customer-agreement/manage-tenants.

72. FLECK, Renee. *10 Fundamental UI Design Principles You Need to Know* [online]. Spojené státy americké, 2021 [cit. 2023-04-30]. Tech. zpr. Dribbble. Dostupné z: https://dribbble.com/resources/ui-design-principles.

73. MICROSOFT. *Co je cloud?* [online]. Spojené státy americké, 2023 [cit. 2023-02-24]. Tech. zpr. Microsoft. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-the-cloud.

74. JUN, Simon. *Proč je Figma dar z nebes?* [online]. 2022. [cit. 2023-02-24]. Tech. zpr. Dostupné z: https://www.simonjun.cz/blog/proc-je-figma-dar-z-nebes.

75. TECHTERMS.COM. *PowerPoint* [online]. 2023. [cit. 2023-03-04]. Tech. zpr. TechTerms.com. Dostupné z: https://techterms.com/definition/powerpoint.

76. GECKOBOARD. *12 Dashboard design tips for better data visualizatio* [online]. 2022. [cit. 2023-03-11]. Dostupné z: https://www.youtube.com/watch?v=t3cAUt7sOQg.

77. VINDUŠKA, Zdeněk; PETRTÝLOVÁ, Markéta. *Pátý rozhovor: Konzultace k datovému přehledu a nasazení aplikace* [online]. [B.r.]. [cit. 2023-04-06].

78. UDN APPS. *SWOT analýza: Co to je a jak jej používat (s příklady)* [online]. Česká republika, 2023 [cit. 2023-03-05]. Tech. zpr. UDN Apps. Dostupné z: https://udnapps.com/cs-czk/resource/swot-analysis-what-it-is-and-how-to-use-it-with-examples.

79. GANTT.COM. *What is a Gantt Chart?* [online]. 2023. [cit. 2023-03-27]. Tech. zpr. Gantt.com. Dostupné z: https://www.gantt.com/.

80. TUREK, Ludvík. *Cenová nabídka* [online]. 2022. [cit. 2023-04-08]. Tech. zpr. Czech Wealth. Dostupné z: https://www.czechwealth.cz/slovnik-pojmu/cenova-nabidka.

81. TESTY Z ÚČETNICTVÍ. *Slovníček účetních pojmů* [online]. 2023. [cit. 2023-04-08]. Tech. zpr. Testy z účetnictví. Dostupné z: http://www.testyzucetnictvi.cz/slovnicek-ucetnich-pojmu.php?pojem=naklad.

82. ECONOMY-PEDIA.COM. *Cena práce* [online]. 2023. [cit. 2023-04-08]. Tech. zpr. Economy-Pedia.com. Dostupné z: https://cs.economy-pedia.com/11032274-labor-cost.

83. INDEED. *Budujte si kariéru, kterou si zamilujete* [online]. 2023. [cit. 2023-04-08]. Tech. zpr. Indeed. Dostupné z: https://cz.indeed.com/career/projektov%5C%C3%5C%BD-mana%5C%C5%5C%BEer/salaries.

84. INDEED. *Budujte si kariéru, kterou si zamilujete* [online]. 2023. [cit. 2023-04-08]. Tech. zpr. Indeed. Dostupné z: https://cz.indeed.com/career/ux-designer/salaries?from=top_sb.

85. INDEED. *Budujte si kariéru, kterou si zamilujete* [online]. 2023. [cit. 2023-04-08]. Tech. zpr. Indeed. Dostupné z: https://cz.indeed.com/career/program%5C%C3%5C%A1tor/salaries.

86. INDEED. *Budujte si kariéru, kterou si zamilujete* [online]. 2023. [cit. 2023-04-08]. Tech. zpr. Indeed. Dostupné z: https://cz.indeed.com/career/quality-engineer/salaries?from=top_sb.

87. KALENDAR.BEDA.CZ. *Plánovací kalendář 2023, 8 hodinová pracovní doba* [online]. 2023. [cit. 2023-04-08]. Tech. zpr. kalendar.beda.cz. Dostupné z: https://kalendar.beda.cz/rocni-planovaci?year=2023&type=s1.

88. FINANCE.CZ. *Jak vysoké je sociální a zdravotní pojištění?* [online]. 2023. [cit. 2023-04-08]. Tech. zpr. finance.cz. Dostupné z: https://www.finance.cz/dane-a-mzda/mzda/odvody-socialniho-a-zdravotniho-pojisteni/.

89. ALZA. *NEO pronájem - Notebooky* [online]. 2023. [cit. 2023-04-08]. Tech. zpr. Alza. Dostupné z: https://www.alza.cz/notebooky/produkty-k-pronajmu/18842920-e15.htm#f&limit=8589--104990&cst=1&cud=1&pg=1&pn=1&prod=&sc=2264.631103515625.

90. THINKEASY. *Kolik stojí vývoj mobilní aplikace?* [online]. 2022. [cit. 2023-04-08]. Tech. zpr. ThinkEasy. Dostupné z: https://thinkeasy.cz/kolik-stoji-vyvoj-mobilni-aplikace/.

91. THINKEASY. *Kolik stojí vývoj webové aplikace?* [online]. 2022. [cit. 2023-04-08]. Tech. zpr. ThinkEasy. Dostupné z: https://thinkeasy.cz/vyvoj-webove-aplikace-cena/.

92. WEBFUSION. *Kolik stojí vývoj mobilní aplikace v roce 2023* [online]. 2023. [cit. 2023-04-08]. Tech. zpr. Webfusion. Dostupné z: https://webfusion.cz/kolik-stoji-vyvoj-mobilni-aplikace-v-roce-2023/.

93. VIVEK, Kurmar; MANIAR, Tapan; MINTS, Manjinder; LAUGESEN, Austin; WEATHERBY, Jager; HOLTZMAN, Jim; KARAFILOV, Tomislav; JAISWAL, Shubham; OWEN, Anne Frances. *What is Power Apps?* [online]. Spojené státy americké, 2022 [cit. 2023-03-06]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/power-apps/powerapps-overview.

94. DALY, Jim; VIVEK, Kuman; LINDHORST, Greg; MANIA, Tapan; BUTHUKURI, Nava Kiran; COULTER, David. *Microsoft Power Fx overview* [online]. 2023. [cit. 2023-03-20]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/power-platform/power-fx/overview.

95. TECHTARGET. *strongly typed programming language* [online]. 2023. [cit. 2023-03-22]. Tech. zpr. TechTarget. Dostupné z: https://www.techtarget.com/whatis/definition/strongly-typed.

96. HAWTHORNE, Mel. *Declarative Programming Language* [online]. 2019. [cit. 2023-03-22]. Tech. zpr. TechTarget. Dostupné z: https://www.technipages.com/definition/declarative-programming-language.

97. MITCHELL, Brad. *What Is Functional Programming and Why Use It?* [online]. 2022. [cit. 2023-03-22]. Tech. zpr. CodingDojo. Dostupné z: https://www.codingdojo.com/blog/what-is-functional-programming.

98. PEART, Matt; ATIKMAPARI; COULTER, David. *What is Microsoft Dataverse?* [online]. Spojené státy americké, 2022 [cit. 2023-03-06]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/power-apps/maker/data-platform/data-platform-intro.

99. MICROSOFT. *Microsoft Power Automate documentation* [online]. 2023. [cit. 2023-03-21]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/power-automate/.

100. BALLEW, Joli. *What Is Microsoft Outlook?* [online]. 2021. [cit. 2023-03-21]. Tech. zpr. LifeWire. Dostupné z: https://www.lifewire.com/microsoft-outlook-4164620.

101. BUCK, Alex; HART, Michele; SHERER, Tim; BLYTHE, Michael; BERDUGO, Mona; SHARABI, Kesem; SPARKMAN, Maggie; SHARKEY, Kent. *What is Power BI?* [online]. 2023. [cit. 2023-03-21]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/power-bi/fundamentals/power-bi-overview.

102. DUNCAN, Owen; BUCK, Alex; HOWELL, Jason. *DAX overview* [online]. 2023. [cit. 2023-03-21]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/dax/dax-overview.

103. HLAVA, Tomáš. *Regresní a procesná testy* [online]. 2011. [cit. 2023-04-05]. Tech. zpr. Testování softwaru. Dostupné z: http://testovanisoftwaru.cz/tag/regresni-testy/.

104. BAL, Chris; MANIAR, Tapan; AENGUSHEANEY; VIVEK, Kumar. *Test Studio* [online]. 2023. [cit. 2023-03-21]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/power-apps/maker/canvas-apps/test-studio.

105. JEFFRIES, Thomas; GARTY, Chris; YACK, David; VIVEK, Kumar; BURKE, Casey; TOWNSEND, Matt; MENON, Harysh; LAUGESEN, Austin; DEORE, Amol; PEART, Matt. *Solutions overview* [online]. Spojené státy americké, 2023 [cit. 2023-04-15]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/power-apps/maker/data-platform/solutions-overview.

106. MICROSOFT. *Zazipování a rozzipování souborů* [online]. Spojené státy americké, 2023 [cit. 2023-04-15]. Tech. zpr. Microsoft. Dostupné z: https://support.microsoft.com/cs-cz/windows/zazipov%5C%C3%5C%A1n%5C%C3%5C%AD-a-rozzipov%5C%C3%5C%A1n%5C%C3%5C%AD-soubor%5C%C5%5C%AF-8d28fa72-f2f9-712f-67df-f80cf89fd4e5.

107. VINDUŠKA, Zdeněk; PETRTÝLOVÁ, Markéta. *Šestý rozhovor: Nasazení aplikace a datového přehledu* [online]. [B.r.]. [cit. 2023-04-20].

108. ERICKSON, Sally; LIEW, Paul; PICHLER, Manuela; VIVEK, Kurman; COULTER, David; PEART, Matt; HOLTZMAN, Jim; DEORE, Amol. *Configure user security to resources in an environment* [online]. Spojené státy amercké, 2023 [cit. 2023-04-15]. Tech. zpr. Microsoft. Dostupné z: https://learn.microsoft.com/en-us/power-platform/admin/database-security#predefined-security-roles.

Obsah přiloženého média

- `readme.txt` ..... stručný popis obsahu média
- `video` ..... video-ukázka práce s aplikací
- `aplikace`
  - `eleariningApp.zip` ..... zdrojové kódy aplikace
  - `tab_Courses.xlsx` ..... data z tabulky tab_Courses
- `přehled dat`
  - `overview.pbix` ..... zdrojový kód pro přehled dat z aplikace
- `text`
  - `thesis.pdf` ..... text práce ve formátu PDF
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX