Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Online kurz základů kybernetické bezpečnosti pro veřejnou správu

Bakalářská práce

Autor: Matěj Hubálek
Studijní obor: Informační managment

Vedoucí práce: doc. Mgr. Josef Horálek, Ph.D.

Hradec Králové Duben 2024

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 5.4.2024

Matěj Hubálek

Poděkování:

Děkuji vedoucímu bakalářské doc. Mgr. Josef Horálek, Ph.D. za metodické vedení práce, ochotu a pevné nervy při výběru tématu bakalářské práce.

Abstrakt

V éře digitalizace a rostoucí závislosti veřejné správy na informačních technologiích přichází stále nové výzvy v oblasti kybernetické bezpečnosti. Tato práce se zaměřuje na vytvoření online vzdělávacího kurzu, který reaguje na tyto výzvy. Kurz představuje různé typy kybernetických útoků a způsoby, jak se jim efektivně bránit. V praktické části je kurz prezentován prostřednictvím interaktivní webové stránky, doplněný o interaktivní testy, které slouží k ověření a upevnění získaných znalostí. Z výsledků testů vyplynulo, že ačkoliv většina zaměstnanců dokáže identifikovat podvodné e-maily a SMS zprávy, existuje stále významný podíl, který je náchylný k těmto hrozbám.

Práce poskytuje základ pro další rozvoj vzdělávacího kurzu, který se musí adaptovat na neustále se měnící požadavky a hrozby v digitálním světě.

Abstract

Title: Online cyber security fundamentals course for public administration

In the era of digitalization and the growing dependence of public administration on information technologies, there are continually emerging new challenges in the field of cybersecurity. This work focuses on the creation of an online educational course that responds to these challenges. The course introduces various types of cyberattacks and ways to effectively defend against them.

In the practical part, the course is presented through an interactive website, supplemented by interactive tests that serve to verify and reinforce the acquired knowledge. The results of the tests revealed that although most employees can identify fraudulent emails and text messages, there is still a significant portion of respondents who are vulnerable to these threats.

This work provides a foundation for the further development of the educational course, which must adapt to the ever-changing demands and threats in the digital world.

Obsah

Úvod

Dnešní éra je spíše ve znamení digitálních technologií, kdy se digitalizace stává neodmyslitelnou součástí, stojí veřejná správa stále před nově příchozími výzvami v oblasti kybernetické bezpečnosti. Její rostoucí závislost na informačních technologiích s sebou přináší vysoké riziko kybernetických útoků.

Hlavním cílem kybernetické bezpečnosti je ochrana osobních údajů, finančních informací a důvěrných dokumentů. Ztráta dat tohoto typu může mít závažné důsledky pro jednotlivce, úřad nebo i společnost jako celek.

Mnoho lidí se domnívá, že kybernetická bezpečnost spočívá v ochraně před hackery a kybernetickými útoky pomocí implementace robustních bezpečnostních protokolů a technologií. Avšak tento pojem má mnohem širší význam.

Mnoho kybernetických útoků bylo úspěšných právě kvůli lidské chybě. Proto jedním z klíčových aspektů je nekončící proces vzdělávání a seznamování s novými trendy mezi kybernetickými útoky. A zároveň dobře znát způsoby a aplikovat, jakými zabráníme jejich úspěšnému napadení.

Tento kurz se v první části zabývá analýzou bezpečnostních požadavků vyplívajících z platné legislativy České republiky, a to zejména Vyhlášky o kybernetické bezpečnosti 82/2013 Sb. [1] Analyzuje klíčové pojmy jako například řízení a evidenci aktiv, identifikaci a zvládání rizik, organizační bezpečnost aj. Přičemž poskytuje komplexní přehled o nutnosti správného nastavení interních procesů a procedur v rámci organizace. Tato analýza je stěžejní pro vytvoření online kurzu pro veřejnou správu.

Teoretická část se soustředí na aspekty kybernetické bezpečnosti, které jsou přímo zaměřené na koncové uživatele. V této části je kladen velký důraz na fyzickou bezpečnost, vysvětluje princip a důležitost politiky čistého stolu. Dále se věnuje identifikaci a prevenci před různými typy kybernetických útoků. Podstatnou částí jsou praktické návody, jak se v případě výskytu hrozby rychle a efektivně zachovat, včetně preventivních opatření, jako je vytváření záloh, správné nakládání s hesly nebo jak se bezpečně připojit k internetu i mimo kancelář.

Teoretická část je následně prezentována pomocí webové stránky, která zahrnuje interaktivní cvičné a ostré testy pro procvičování a ověření znalostí. Tato část kurzu je následně doplněna samostatnou kapitolou „Vyhodnocení kurzu“, která umožňuje hlubší pochopení a reflexi naučeného materiálu.

Cíl a metodika práce

Hlavním cílem práce je poskytnout komplexní a praktický průvodce pro zvyšování úrovně kybernetické bezpečnosti ve veřejné správě. Záměrem je nejen analyzovat aktuální bezpečnostní požadavky dle platné legislativy České republiky, ale také poskytnout efektivní vzdělávací nástroje a metody, jak se vypořádat s potenciálními kybernetickými hrozbami. Významná pozornost je věnována nejen technologickým aspektům bezpečnosti, ale také lidskému faktoru a preventivním opatřením, aby se snížila pravděpodobnost úspěšného kybernetického útoku kvůli lidské chybě.

Hlavním cílem kvantitativního výzkumu je zhodnotit účinnost a efektivitu online kurzu v oblasti kybernetické bezpečnosti zaměřeného na zaměstnance veřejné správy, konkrétně ve Finanční správě. Záměrem je zjistit, do jaké míry se zvýšily znalosti účastníků v oblasti kybernetické bezpečnosti a jak jsou schopni aplikovat získané informace v praxi. Tuto metodu jsem využil z důvodu získání většího vzorku dat. Průzkumné otázky byly umístěny na webovou stránku ve formě vstupního a závěrečného testu. Tyto otázky se nachází v obou testech z důvodu ověření získaných znalostí během online kurzu. Vytvořená webová stránka byla následně nasdílena vybrané skupině zaměstnanců Finanční správy. Počet účastníků v dotazované skupině je 198 ve věku od 25 do 65 let. Návratnost z vyplněných testů je 27 % a vyhodnocení těchto testů je uvedeno v poslední kapitole „Vyhodnocení kurzu“.

Tento výzkum má kritický význam pro posouzení, zda kurz splnil své vzdělávací cíle a přispěl k zvýšení úrovně kybernetické bezpečnosti mezi zaměstnanci ve veřejné správě. Vyhodnocení také umožňuje identifikovat oblasti, které potřebují další zlepšení nebo detailnější zaměření v budoucích verzích kurzu.

1 Analýza bezpečnostních požadavků

V následující analýze se zaměříme na identifikaci klíčových bezpečnostních požadavků vyplývajících z platné vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění zákona č. 104/2017 Sb. Na základě požadavků vyplývajících z této analýzy bude sestaven Online kurz základů kybernetické bezpečnosti pro veřejnou správu. Shrnutí a diskuse výsledků
Obsahuje souhrn a kritickou diskusi vlastních výsledků, získaných v průběhu řešení problému (soulad výsledků s literaturou či předpoklady; výsledky a okolnosti, které zvláště ovlivnily předkládanou práci, nové poznatky včetně jejich odvození ze získaných výstupů atd.).

1.1 Řízení aktiv

První klíčový prvek v rámci kybernetické bezpečnosti a obecně v oblasti řízení rizik. Odvolává na procesy a postupy spojené s identifikací, hodnocením, monitorováním a řízením aktiv organizace s cílem minimalizovat rizika. Aktiva mohou zahrnovat informační technologie, datové soubory, infrastrukturu, zařízení, lidské zdroje a další. [2, s. 30-60] Prakticky se jedná o věci, které představují pro organizaci nějakou hodnotu.
Řízení aktiv krok za krokem:

1.1.1 Identifikace aktiva

Identifikace aktiv zahrnuje identifikaci a katalogizaci všech prvků, které mají pro organizaci hodnotu. Je primárně důležité identifikovat všechna aktiva. Pokud by došlo k opomenutí aktiva, mohlo by to vést v některých případech i k fatálním následkům pro celou organizaci. Aktiva je následně důležité rozdělit na primární a podpůrná aktiva.

a. Primární aktiva – informace a služby blízce související s hlavní činností organizace a v případě ztráty nebo narušení těchto aktiv by byl narušen chod a bezpečnost celé organizace.
b. Podpůrná aktiva – tato aktiva sama o sobě nepředstavují žádnou hodnotu, ale zároveň jsou důležitá pro správné fungování a zajištění bezpečnosti primárních aktiv. Obvykle se jedná o technické a programové vybavení, komunikační prostředky, lidské zdroje, dodavatele, aj.

1.1.2 Určení garantů

Pověření osoby s kompletní znalostí daného aktiva, který se následně zapojuje do procesu řízení aktiv a rizik. Garanti jsou vybíráni na základě jejich pracovního zařazení (obvykle ředitelé a vedoucí) a odborných znalostí daného aktiva.

1.1.3 Ohodnocení aktiva

Při hodnocení aktiv se posuzují všechny možné scénáře, bez ohledu na uplatňovaná bezpečnostní opatření organizace. Aktiva se hodnotí podle jejich důvěrnosti, případného dopadu při narušení integrity a dostupnosti. Pro vyhodnocování důležitosti aktiv je možné využít připravenou stupnici, viz. Tabulka 1.

Důvěrnost – Ochraně citlivých informací před neoprávněným přístupem nebo odhalením. Ochrana důvěrnosti zahrnuje šifrování, správu přístupů a politiky ochrany dat k zabránění zneužití citlivých informací. Pro bezpečné a snazší sdílení citlivých informací byl v roce 2000 vyvinut Trafic Light Protocol (TLP). Tento protokol efektivně zjednodušuje a urychluje způsob výměny informací mezi subjekty, zároveň minimalizuje riziko neoprávněného přístupu k informacím. TLP obsahuje čtyři hlavní úrovně: WHITE, GREEN, AMBER a RED, každá z těchto úrovní označuje odlišnou citlivost informací. TLP:WHITE se používá pro označení veřejně přístupných informací, pravým opakem je TLP:RED, označující přísně tajné informace.

Integrita – Správná konzistence informací. To znamená, že během sdílení by informace neměla být žádným způsobem narušena nebo pozměněna. Integrita u informačních systémů označuje nedotčenost a ochranu před neoprávněným přístupem. Ochrana integrity zahrnuje zavádění kontrolních součtů, monitorování aktivit a správy přístupových práv.

Dostupnost – Zajištění přístupu k informacím, datům a službám v případě potřeby. Jedná se o klíčový aspekt zejména v kritických odvětvích jako je zdravotnictví a veřejná správa, kde náhlý výpadek může mít závažné důsledky. Zajištění dostupnosti může zahrnovat zálohování, monitorování a řízení výkonu nebo implementace opatření na ochranu před DDoS útoky.

Při hodnocení důležitosti primárních aktiv je třeba posoudit alespoň následující body:

- rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství,
- rozsah dotčených právních povinností nebo jiných závazků,

- rozsah narušení vnitřních řídicích a kontrolních činností,
- poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty,
- dopady na poskytování důležitých služeb,
- rozsah narušení běžných činností,
- dopady na zachování dobrého jména nebo ochranu dobré pověsti,
- dopady na bezpečnost a zdraví osob,
- dopady na mezinárodní vztahy a
- dopady na uživatele informačního a komunikačního systému.

Na základě vyhodnocení aktiv lze stanovit přiměřený způsob zacházení s jednotlivými aktivy a případnou likvidaci podle příslušné úrovně.

Evidence aktiv

Následně každé aktivum musí být evidováno v Katalogu aktiv minimálně v tomto rozsahu: název, popis, gestor aktiva, garant aktiva, hodnocení důvěrnosti, integrity a dostupnosti.

V evidenci jsou zaznamenány vazby jak mezi primárními a podpůrnými aktivy, tak i mezi primárními aktivy navzájem.

Tabulka 1 – stupnice pro hodnocení důvěrnosti, integrity a dostupnosti aktiva [3, s. 49-55]

Úroveň dopadu	Důvěrnost	Integrita	Dostupnost
Nízká	Aktiva jsou veřejně přístupná a neomezeně šiřitelná. V případě narušení důvěrnosti aktiv, nedochází k žádnému ohrožení. V případě sdílení se používá kategorie TLP:WHITE, která povoluje sdílení bez omezení.	Není vyžadována žádá ochrana. Případné narušení integrity nedochází k žádnému ohrožení.	Narušení dostupnosti není nijak důležité pro chod organizace. Pokud dojde k výpadku aktiva, je zde tolerován i delší možný výpadek, např. v délce jednoho týdne.
Střední	Aktiva již nejsou dostupná veřejnosti a jsou výhradně určená pro interní sdílení, případně třetím stranám skrze neveřejné kanály. V případě sdílení je nutné označit předávané informace protokolem TLP. V této úrovni je doporučené označení TLP:GREEN nebo TLP:AMBER.	V případě narušení integrity aktiv může dojít k poškození zájmů, toto narušení může mít malé dopady na organizaci. K zabezpečení aktiv na této úrovni mohou být organizací zaváděny oprávněné přístupy k informacím, ta často zahrnují ověřování identity nebo omezení přístupu k fyzickým nosičům informací.	Výpadek dostupnosti aktiva by neměl překročit dobu pracovního dne, dlouhodobější výpadek by mohl vést k ohrožení chodu organizace. Pro zajištění dostupnosti jsou zřizovány zálohy dat a systému.
Vysoká	Aktiva s vysokým stupněm omezení přístupu, mohou sem spadat osobní údaje nebo nedostatky v ochraně systému. Aktiva na této úrovni nejsou určená veřejnosti a v případě sdílení se třetí stranou jsou ošetřeny právním předpisem nebo smluvním ujednáním. Při sdílení je opět používán TLP protokol, a to zejména TLP:AMBER	Narušení integrity může mít podstatné dopady na primární aktiva. Aktiva vyžadují jistou ochranu, z technického hlediska se zde objevuje pojem šifrování dat a sledování provedených změn.	Pokud by došlo k výpadku dostupnosti, výpadek by neměl překročit dobu několika hodin. Tyto výpadky se musí řešit neprodleně. Zajištění dostupnosti mohou zajišťovat záložní systémy.
Kritická	Aktiva spadají pod nejvyšší úroveň utajení, která vyžadují nadstandardní úroveň ochrany. Může se jednat o strategické rozhodování, obchodní tajemství aj. Přístup k těmto aktivům má pouze malý počet oprávněných osob, kteří splňují nejvyšší stupeň oprávnění. V rámci sdílení informací se používá klasifikace TLP:RED nebo TLP:AMBER.	Pro zajištění integrity se využívají prostředky k jednoznačné identifikaci osob (např. digitální podpis). Porušení integrity zpravidla vede k velmi vážným dopadům na primární aktiva.	Výpadek dostupnosti není nijak přípustný.

1.2 Řízení rizik

U každého identifikovaného aktiva v přechozí kapitole je primárně důležité identifikovat jejich možné hrozby a zranitelnosti a analyzovat jejich pravděpodobné dopady na organizaci. Samotná analýza rizik se zabývá zhodnocením pravděpodobností, že dané riziko se stane skutečností a hodnotí jeho potenciální dopady.

1.2.1 Dopad

rozsah a závažnost následků, které mohou nastat v případě bezpečnostního incidentu

1.2.2 Hrozba

potenciální nebezpečí nebo nebezpečné události, které by mohly ohrozit bezpečnost a způsobit škodu. Veškeré hrozby je opět nejprve potřeba identifikovat a zapsat do katalogu hrozeb. Jako příklad hrozeb si můžeme uvést zneužití identity, škodlivý kód, pochybení zaměstnanců nebo i požár.

1.2.3 Zranitelnost

slabá místa nebo nedostatky aktiva, případně nedostatky jiných aktiv, které by mohly představovat hrozbu. Veškeré zranitelnosti je třeba předem identifikovat a zapsat do katalogu zranitelností. Může se jednat například o zastaralost IS, nevhodně nastavená bezpečnostní oprávnění, nedostatečné bezpečnostní povědomí zaměstnanců, aj. [2, s. 62-73]

Každá z těchto tří kategorií je následně ohodnocena a umístěna do příslušné úrovně stupnice, viz. Tabulka 2.

Tabulka 2 – stupnice pro hodnocení rizik a zranitelností [3, s. 262-263]

Úroveň	Hrozba	Zranitelnost
Nízká	Žádná nebo jen málo pravděpodobná. Výskyt hrozby se předpokládá nanejvýše jednou za 5 let.	Neexistuje nebo je její zneužití málo pravděpodobné. Jsou implementována bezpečnostní zařízení, která umí včas detekovat zranitelnost a její případné zneužití.
Střední	Málo pravděpodobná až pravděpodobná. Předpoklad výskytu je v intervalu od 1 roku do 5let.	Málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, avšak jejich účinnost je v jisté míře omezená. Nejsou známy žádné úspěšné pokusy o překonání těchto opatření.
Vysoká	Pravděpodobná až velmi pravděpodobná. Předpoklad výskytu je v intervalu od 1 měsíce do 1 roku.	Pravděpodobné až velmi pravděpodobné. Jsou zavedena bezpečnostní opatření, tyto opatření nepokrývají všechny potřebné aspekty. Jsou známy dílčí úspěšné pokusy o překonání.
Kritická	Velmi pravděpodobná až jistá. Předpoklad výskytu je častější než jednou za měsíc	Velmi pravděpodobné až víceméně jisté. Není zavedené bezpečnostní opatření nebo jejich účinnost je značně omezena. Jsou známé úspěšné pokusy o překonání.

Rizika jsou následně vyhodnocována podle vzorce:

riziko = dopad x hrozba x zranitelnost

výslednou hodnotu v intervalu 1–64 si následně můžeme dosadit do následující tabulky, Tabulka 3, která podle stupnice hodnocení rizik vypovídá o míře a vážnosti hrozby pro organizaci.

Tabulka 3 – stupnice pro hodnocení rizik [2, s. 16]

Stupnice pro hodnocení rizik		
1–16	nízká	Riziko je považováno za přijatelné – akceptovatelné. Riziko se dále monitoruje.
17–31	Střední	V případě vysoké náročnosti opatření je možné riziko akceptovat. V opačném, případě může být riziko sníženo.
32–47	Vysoká	Riziko je dlouhodobě nepřípustné, a proto musí být zahájeny systematické kroky pro jeho odstranění.
48–64	Kritická	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

Hodnocení rizik je dynamický proces, který by měl být pravidelně aktualizován v souladu s měnícími se podmínkami organizace a jejím prostředím. Za významnou změnu může být považováno: změna primárních aktiv, nová hrozba nebo zranitelnost, modernizace aktiv, aj. Avšak doba od posledního hodnocení rizik by neměla přesáhnout dobu jednoho roku. Při vyhodnocování rizik je také potřeba zohledňovat dosud proběhlé bezpečnostní incidenty a audity kybernetické bezpečnosti.

1.2.4 Zvládání rizik

V návaznosti na hodnocení rizik je potřeba určit způsob, případně postup jejich zvládnutí. Z důvodu neustále měnícím se skutečnostem je potřeba všechna rizika monitorovat a přezkoumávat postupy pro jejich zvládnutí. Méně závažná rizika je vhodné periodicky monitorovat, ty závažnější je potřeba nepřetržitě sledovat a přezkoumávat. [2, s. 74-79], [3, s. 279-230]

Akceptace rizika – Každé riziko představující hrozbu můžeme akceptovat i bez přijmutí bezpečnostních opatření. Většinou se tak stává v případech, kdy riziko nepředstavuje příliš vysokou hrozbu. Uvedeme si příklad. V našem internetovém obchodě jsme právě vyhodnotili všechna rizika. Jedno z rizik v seznamu hodnocení, které jsme ochotni akceptovat je napadení zákaznického účtu. Přes dosud přijatá bezpečnostní opatření existuje malá pravděpodobnost vniknutí k zákaznickému účtu, a i kdyby se tak stalo, pro internetový obchod by byl dopad minimální.

Můžeme si uvést druhý příklad. Platba online nám v našem internetovém obchůdku přináší mnoho benefitů, platby máme předem a následné účetnictví je také snazší. I v tomto případě existuje riziko podvodu při platbě online a jisté ztráty v řádu tisíců korun, možná desetitisíců. Přesto jsme ochotni riziko přijmout, protože jistá opatření by byla daleko dražší než tento ojedinělý podvod, případně zodpovědnost za plnění můžeme převést na třetí stranu ve formě pojištění.

Z pohledu akceptace rizik můžeme dělit rizika následujícím způsobem:

- Pasivní – nezavádí se žádné opatření. Obvykle tak bývá u malých a středních rizik, u kterých neexistují smysluplná opatření.
- Aktivní – u středních rizik se vytvoří malá rezerva finančních a lidských zdrojů, aby v případě výskytu rizika zmírnila nebo úplně redukovala dopad. U vysokých rizik je nutné alokovat potřebný množství zdrojů na zavedení bezpečnostního opatření.

Redukce rizika – Cílem redukce rizika je, aby úroveň rizika byla snížena, nejlépe na akceptovatelnou úroveň, pomocí aplikování vhodného bezpečnostního opatření. Jedná se o nejčastěji používanou metodu při zvládání rizik pro rizika střední až kritické úrovně.

Vyhnutí se riziku – Metoda spočívá v utlumení nebo úplném vypnutí aktiva. Využívá se v případech, kdy následky bezpečnostního incidentu jsou kritické a pravděpodobnost výskytu téměř jistý.

Přenesení nebo sdílení rizika: používá se v případech, kdy organizace nemá dostačující kapacity na zavedení bezpečnostního opatření. V tomto případě se přenáší odpovědnost na organizaci třetí strany. Může jít o dodavatele, který svou službou bude zajišťovat snížení rizika nebo o pojištění organizace.

1.2.5 Plán zvládání rizik

Plán zvládání rizik je dokument, který obsahuje strategie, opatření a postupy pro identifikaci, hodnocení a řízení rizik v rámci organizace. Tento plán je klíčovým nástrojem pro dosažení efektivního řízení rizik a minimalizaci negativních dopadů na organizaci. Zde jsou obecné kroky, které by mohl obsahovat plán zvládání rizik:

- cíle a přínosy bezpečnostních opatření pro zvládání rizik,
- určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik,
- potřebné finanční, technické, lidské a informační zdroje,
- termíny zavedení opatření,
- popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními,
- způsob realizace bezpečnostních opatření,
- způsob hodnocení úspěšnosti zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.

1.3 Organizační bezpečnost

Důležitým krokem je stanovení bezpečnostních politik a odpovědností v rámci bezpečnosti řízení informací. Vrcholové vedení by mělo vymezit dostačující zdroje pro zavedení, udržování a zvyšování bezpečnostních opatření a tím zvýšit celkovou kybernetickou bezpečnost organizace. Součástí je pověření odpovědných osob, které zodpovídají za kybernetickou bezpečnost, včetně stanovení jejich povinností, odpovědností a pravomocí. Osoba s tímto postavením je odpovědná za řízení, rozvoj a kontrolu stavu kybernetické bezpečnosti. Aktivně se podílí na zavádění bezpečnostních opatření. Vrcholový managment náležitě podporuje zavádění kybernetických opatření,

prosazované pověřenou osobou v kybernetické bezpečnosti. Pověřená osoba nesmí vykonávat roli běžného správce informačního systému. Toto opatření je vyžadováno z důvodu možné špatné politiky prosazování a dodržování bezpečnostních opatření. Osoby zajišťující bezpečnost informací by měli mít podepsanou dohodu o mlčenlivosti a náležitě ji dodržovat. [4, s. 4-7]

Dále je nutné vytvořit úměrné bezpečnostní politiky a dokumentaci, tyto dokumenty nesmí obsahovat složitosti a musí být dostatečně návodné, aby bylo zajištěno náležité pochopení dané problematiky a snadné aplikování uvedených postupů v praxi. Dokumentace by měla vystihovat aktuální stav, z tohoto důvodu je nutné v pravidelných intervalech vyhodnocovat situaci a aktualizovat dokumentaci. Součástí organizační bezpečnosti je i školení podřízených zaměstnanců, kteří by měli být v pravidelných intervalech seznámeni s bezpečnostními opatřeními a měnícími se riziky. [5, s. 12]

1.3.1 Plán zavádění bezpečnostních opatření

Jedná se o soupis všech aplikovatelných opatření, které je nutné v nejbližší době zavést. Dokument může být i použitý jako podklad pro plánování zdrojů. Obsah dokumentu by opět měl reflektovat aktuální dění v oblasti kybernetické bezpečnosti a možná rizika. V samotném plánu se vždy uvádí popis bezpečnostního opatření, odpovědné osoby a případné zdroje potřebné pro realizaci. Každý plán má také pevně stanovený termín realizace, je důležité, aby zvolený termín byl realistický a dosažitelný vzhledem k požadavkům opatření a dostupným zdrojům. [5, s. 6-7]

1.3.2 Řízení lidských zdrojů a bezpečnostní role

Lidskými zdroji se rozumí veškerý personál, který má přístup k informačnímu systému nebo na jeho funkčnost může mít jistý vliv. Do této kategorie spadá vedení organizace, správce informačního systému i řadový pracovník. Pokud vyhodnotíme, že pracovník úklidové služby, údržby, aj. může nějakým způsobem ovlivnit chod informačního systému, řadíme jej také do této kategorie. Všichni zaměstnanci musí být náležitě proškoleni ve vstupním školení a v pravidelných intervalech minimálně jednou ročně, kde budou seznámeni s jejich povinnostmi a bezpečnostní politice. Součástí školení jsou i postupy chování zaměstnanců při výskytu nestandardní situace. Zaměstnanci zastávající

bezpečnostní role a správci informačního systému by měli také absolvovat odborná a specializovaná školení.

Bezpečnostní role:

- Výbor pro řízení kybernetické bezpečnosti – nese odpovědnost za celkové řízení a rozvoj kybernetické bezpečnosti, definují strategické cíle a zbylé bezpečnostní role.
- Manažer kybernetické bezpečnosti – odpovídá za strategické vedení, plánování a provádění opatření v oblasti kybernetické bezpečnosti v organizaci. Pravidelně informuje vrcholový managment o činnostech vyplívajících z rozsahu jeho odpovědnosti a stavu řízení bezpečnosti informací. Také spolupracuje s ostatními vedoucími pracovníky a odděleními na zajištění komplexní bezpečnostní strategie.
- Architekt kybernetické bezpečnosti – odborník na návrh, implementaci a správu bezpečnostních opatření v informačních systémech.
- Auditor kybernetické bezpečnosti – provádí nezávislé posouzení bezpečnostních postupů, systémů a infrastruktury v organizaci.
- Garant aktiva – zajišťuje rozvoj, použití a udržování bezpečného stavu přiřazených aktiv.

Odpovědné osoby, případně správci informačního systému nemohou vykonávat více jak jednu funkci jim přidělenou. [4, s. 5-6]

1.4 Řízení dodavatelů

Řízení dodavatelů je proces, který organizace používá k řízení vztahů s externími dodavateli s cílem zajištění efektivního a bezpečného získávání produktů nebo služeb.

Již při průběhu výběrového řízení, ještě před podepsání smlouvy je nutné, zejména u významných dodavatelů, kteří mohou pro organizaci představovat potenciální bezpečnostní rizika, vyhodnotit rizika související s poskytovanou službou dodavatele. Poté, v rámci smluvních vztahů, se stanovují způsoby a úrovně bezpečnostních opatření, společně s odpovědnostmi za vedení a kontrolu bezpečnostních opatření. Po podepsání smlouvy je nadále nutné pravidelně hodnotit rizika a kontrolovat zavedenou úroveň bezpečnostního opatření. V případě nalezených nedostatků najít jejich řešení.

Významní dodavatelé jsou vedeni v evidenci a o jejich zařazení do evidence jsou dodavatelé informování. Obvykle tak dochází prostřednictvím uzavírané smlouvy. Každý dodavatel by měl být náležitě a prokazatelným způsobem poučený o jeho povinnostech, nastavené bezpečnostní politice a způsobu podávání hlášení nestandardních situacích. [6, s. 4-11]

1.5 Řízení provozu, přístupu a komunikací

Pro bezpečný a bezproblémový chod systému je hned na začátku nutné definovat jasná pravidla a postupy. Zejména jsou důležité tyto postupy:

- Postup pro rozdělování, evidenci, přidělování a schvalování přístupových rolí:
    - V rámci tohoto postupu je nutné definovat pravidla pro omezení a kontrolu používaných aktiv z důvodu případného narušení bezpečnosti. Toho se dosahuje pomocí uživatelských účtů, kterým je umožněn přístup k aktivu na základě jim přidělených skupin obsahující potřebná oprávnění.
    - Každý uživatel přistupující do systému by měl mít přidělený jednoznačný přístupový identifikátor na který se vážou jemu přidělená přístupová práva. Každý uživatelský účet by také měl mít přidělená pouze ta oprávnění, která odpovídá jeho pracovní náplni. V přiřazování nadstandardních práv by se neměli dělat výjimky. Samotná oprávnění by měla být evidována a průběh přidělování práv postupně dokumentován.
    - Pro přihlašování do systému by měla být dodržená politika bezpečných hesel. Dále se doporučuje používání dvoufázového ověřování, pokud je dostupné.
    - Přidělená oprávnění a jejich rozsah je nutné pravidelně kontrolovat.
- Postupy a pravidla pro ochranu před škodlivým kódem:
    - Ochrana před škodlivým kódem se uplatňuje zejména na koncových stanicích, mobilních zařízeních, serverech, datových nosičích a komunikační sítě. Součástí ochrany je monitoring používaných výměnných zařízení, přidělování oprávnění, aktualizování nástrojů pro ochranu před škodlivým kódem a segmentace sítě a její kryptografie při vzdálených přístupech.

- Postupy řízení a schvalování provozních změn,
- pravidla a postupy pro ochranu informací a dat. [5, s. 19-22]

1.6 Řízení změn

Řízení změn je proces, který organizace používají k systematickému řízení a kontrole změn v rámci svých systémů, procesů, projektů nebo obecně celkové organizační struktury. Cílem tohoto procesu je zajistit, že změny jsou řádně plánovány, implementovány a sledovány, aby minimalizovaly negativní dopady na organizaci.

Proces zahrnuje evidenci změn, jejich systematické vyhodnocování možných dopadů, implementaci a koordinaci schválených změn. Podstatným krokem u řízení změn je určení výrazných změn, u kterých se zajišťuje analýza rizik, přijímá se opatření pro minimalizaci dopadů. Na základě vyhodnocené analýzy rizik je možné provádět průběžné testování zranitelností, případně penetrační testy. Jestliže neúspěšné implementace změny, je nutné zajistit návrat do původního stavu. [5, s. 13]

1.7 Zvládání kybernetických bezpečnostních opatření

Opatření zahrnuje řadu strategií a praktik, které se používají k ochraně informačních aktiv a infrastruktury před kybernetickými hrozbami. Výchozím krokem, jak předejít obdobným hrozbám je zavedení procesu detekce a vyhodnocování incidentů.

Kvůli možnému opakování incidentu je nutné evidovat jednotlivé incidenty, zejména pro následnou analýzu a poučení se z chybně zavedených opatření. Pro kvalitní analýzu bezpečnostního incidentu je nezbytné disponovat provozními záznamy. Tyto záznamy můžeme získat například z koncových zařízení ve formě systémových událostí, antivirů, firewallu, aplikací, aj.

Jednotlivá zařízení v síti je nutné mít jednoznačně identifikovaná. Každé zařízení by za jeho chodu mělo pořizovat a uchovávat auditní záznamy, především tyto:

- datum a čas,
- identifikace přihlášených účtů, včetně neúspěšných pokusů o přihlášení,
- spouštění, ukončování a typy činností,
- změny v konfiguraci a oprávnění,
- neprovedení činnosti z důvodu neoprávněného přístupu,

- varovná, kritická i chybová hlášení,
- přístupu k záznamům o událostech, pokusy změny záznamů a příslušných nástrojů pro zaznamenávání události. [5, s. 23-26]

1.8 Audit kybernetické bezpečnosti

Audit kybernetické bezpečnosti je proces, během kterého jsou hodnoceny a ověřovány bezpečnostní postupy, politiky a technická opatření organizace s cílem identifikovat a řídit kybernetická rizika. Výsledky auditu je možné použít pro průběžné porovnání míry zabezpečení a zohledňovat je při vyhodnocování rizik. Pokud z vykonaného auditu vyplynuly nějaké nedostatky, je případně nutné určit daná opatření pro nápravu a ty zařadit do plánu zavádění bezpečnostních opatření.

Audit by měl být vykonáván v pravidelných intervalech, minimálně jednou za dva roky nebo při provedení významných změn, a to v rámci jejich rozsahu. Pokud by nastal incident se závažným dopadem na organizaci, managment organizace by měl posoudit, zda v rámci přijímání bezpečnostních opatření neprovést mimořádný audit.

K zajištění nezávislého auditu a její nestrannosti je vždy lepší využít službu třetí strany.

1.9 Fyzická bezpečnost

Ačkoliv to možná na první pohled nevypadá, tak i fyzická bezpečnost aktiv hraje významnou roli v bezpečnosti organizace a zahrnuje taková opatření a postupy, které jsou navrženy tak, aby chránily fyzické prostředí organizace před neoprávněným přístupem, krádeží, špionáží nebo i přírodními katastrofami. Zejména se může jednat o kontrolu přístupu, monitorování prostor, zabezpečení budovy aj.

Výchozím krokem pro stanovení bezpečnostních opatření je vymezení bezpečnostní oblasti, ve které budou zpracovávány a uchovávány informace, případně důležitá technická aktiva, jako jsou například servery. Tato oblast by měla být náležitě oddělena od prostor pro veřejnost. Vstup do oblasti by měl být umožněn pouze po předchozí identifikaci. Jedním možným opatřením může být využívání turniketů a elektronických zámků s čtečkou čipových karet, který na základě platných zaměstnaneckých certifikátů nahraných na kartě umožní vstup do oblasti. Zároveň je nutné nastavit pravidla i pro návštěvy organizace, například identifikace návštěvy hned při vstupu do budovy a umožnění vstupu pouze při doprovodu zaměstnancem organizace. Zabezpečení oblasti

mimo pracovní dobu může být zajištěno pomocí zamykání dveří, alarmu nebo i využitím služby třetí strany poskytující nepřetržitý dozor. [5, s.18]

2 Teoretická část

Teoretická část vychází z předchozí kapitoly Analýzy bezpečnostních požadavků a zpracovává jednotlivá témata se zaměřením na koncové uživatele, resp. zaměstnance. Zároveň je tato část doplněná o formy možných útoků a hrozeb, se kterými se mohou zaměstnanci během výkonu své práce a mimo ni setkat.

Na základě teoretické části bude následně vypracován obsah praktické části bakalářské práce, obohacený znalostními testy z jednotlivých podkapitol.

2.1 Fyzická bezpečnost

První a zároveň nejstarší oblastí zabezpečení je fyzická bezpečnost. Ačkoliv je tato oblast zabezpečení stejně důležitá, jako ta zbylá, kterou si uvedeme níže, tak ve světě 21. století je často opomíjena. Obzvlášť díky velké konektivitě k internetové síti a vzdálenému přístupu jsou organizace napadány v drtivých případech zvenčí, provedením hackerského útoku. Detailnější zpracování požadovaných technických opatření fyzické bezpečnosti jsou uvedena ve Vyhlášce č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků [7]

Fyzická bezpečnost podle vyhlášky 82/2018 Sb.:

„Povinná osoba v rámci fyzické bezpečnosti

a) předchází poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního a komunikačního systému,

b) stanoví fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému, a

c) u fyzického bezpečnostního perimetru stanoveného podle písmene b) přijme nezbytná opatření a uplatňuje prostředky fyzické bezpečnosti

1. k zamezení neoprávněnému vstupu,

2. k zamezení poškození a neoprávněným zásahům a

3. pro zajištění ochrany na úrovni objektů a v rámci objektů.“ [1]

2.1.1 Technická opatření

Do této kategorie spadají mechanické a elektronické prostředky, zabraňující vniknutí nepovolaným osobám a monitorující prostor budovy nebo jednotlivých oblastí a při výskytu mimořádné situace slouží i jako poplachové zařízení.

Vybrané technické prostředky:

- mechanické zábranné prostředky,
- elektrické zámky a systém kontroly vstupu,
- monitorovací systémy,
- elektronická zabezpečovací signalizace (EZS),
- elektrická požární signalizace (EPS),
- zařízení proti aktivnímu a pasivnímu odposlechu.

2.1.2 Režimová opatření

Režimová opatření spojují bezpečnostní opatření a jednotlivé osoby pohybující se v prostorách organizace. Často se jedná o soupis interních, přesně definovaných příkazů, omezení a postupů, pomocí nichž se dají aplikovat jednotlivá bezpečnostní opatření a tím docílit bezpečný chod organizace.

Jako režimová opatření si můžeme představit například oprávnění pro vstup a následný pohyb v objektu, pokud do práce dojíždíme, tak se nás může týkat oprávnění vjezdu na soukromé parkoviště organizace. Režim vstupu můžeme dál rozdělit na pracovníky, externí pracovníky a návštěvy, každá osoba z těchto kategorií bude potom mít jiná přístupová oprávnění v rámci objektu. Z hlediska bezpečnosti není žádoucí, aby návštěvy měli přístup do všech částí budovy. Proto je také nutné rozdělit objekt na příslušné oblasti ohraničené např. dveřmi s elektronickými zámky a do těchto oblastí vpouštět návštěvy pouze za doprovodu zaměstnance organizace. Samotné pracovníky můžeme dál dělit podle jim přidělených oprávnění k citlivým informacím a jednotlivým režimovým pracovištím.

Dalším režimovým opatřením je přidělování a manipulace s klíči a identifikačními prostředky. Veškeré klíče, čipy a identifikační karty by měli být jednoznačně evidovány. Předávání/ přebírání klíčů, karet a čipů je nutné stvrdit podpisem přebírajícího zaměstnance, aby bylo zabránění jejich zneužití. Každý zaměstnanec následně po převzetí

zodpovídá sám za jemu svěřený majetek a manipulaci s ním. V případě ztráty je povinen ihned tuto skutečnost ohlásit zaměstnavateli, aby předešel zneužití ztraceného předmětu (vniknutí do objektu jeho klíči, aj.)
Do režimových opatření náleží také opatření a postupy v případě výskytu mimořádných událostí, jako je požár, zemětřesení nebo teroristický útok. V tomto případě jsou opatření řízena například o požárním evakuačním plánem nebo příručku o postupu chování při ozbrojeném útoku. [8, s. 164-167]

2.1.3 Ostraha

Ostrahou se rozumí osoba pověřená dohledem nad děním v objektu. Úkolem této osoby je zpozorovat nežádoucí výskyt události, jako jsou například pokusy o krádež, špionáž nebo třeba i požár, prasklý vodovod aj., obzvlášť v noci, kdy se v objektu nenachází žádný ze zaměstnanců. Dohled nad objektem je vykonáván v přítomnosti strážných přímo v objektu nebo vzdáleně pomocí monitorovacích zařízení a zařízení EZS.
Bližší požadavky na technická a režimová opatření jsou uvedeny v příloze č. 1 k vyhlášce č. 528/2005 Sb.

2.1.4 Politika tzv. „čistého stolu“

Politika čistého stolu se zabývá problematikou ztráty a případného zneužití citlivých informací či zamezení rizika využití koncového zařízení zaměstnance při cíleném útoku na infrastrukturu organizace v nepřítomnosti zaměstnance na pracovišti. Nežádoucímu nakládání s citlivými informacemi se dá jednoduše předejít dodržováním následujících bezpečnostních zásad:

- v okamžiku nepřítomnosti zaměstnance na svém pracovním místě, jeho pracovní stanice musí být uzamčena a na konci pracovní směny vypnuta,
- dokumenty obsahující citlivé a důvěrné informace, s nimiž se nepracuje, musí být umístěny v uzamykatelné skříni a při odchodu z pracoviště musí být tato skříň zavřená a zamknutá,
- klíče k těmto skříním a jiným uložištím s citlivými nebo důvěrnými informacemi, by měly být pod neustálým dohledem,

- pracovní dokumenty, při jejich likvidaci, je vždy nutné stanoveným způsobem skartovat nebo zlikvidovat,
- hesla a jiné přístupové údaje se nesmí nacházet bezprostředně na očích v podobě papírků nebo jiných poznámek. [9]

2.2 Správa a ověřování identit

Jak v tom pracovním, tak i soukromém životě, přistupujeme do virtuálního světa pomocí identit. Naše identita je v tomto virtuálním světě prezentována mnoha způsoby, a to například jménem a příjmením, našimi iniciály, přezdívkou, smyšleným jménem nebo i v obrázkové podobě ve formě avatara. Ovšem všechny tyto prezentace virtuální identity mají v našem případě jedno společné. Ke všem účtům se musíme nějakým způsobem přihlásit a tím ověřit svoji identitu. Pro přihlašování se využívají metody jako jsou uživatelská jména a hesla, vystavené kryptografické klíče, PIN kódy nebo v případě mobilních zařízení gesta, otisky prstu nebo skenování obličeje. [8, s. 171-174]

2.2.1 Tvorba hesel

Jedním z nejrozšířenějších způsobů přihlašování k virtuálním účtům je za pomocí uživatelského jména a hesla. Tato metoda přihlašování je v mnohých případech často podceňována. Uživatelé si při zakládání účtů volí snadno zapamatovatelná hesla a příliš nehledí na jejich sílu a odolnost proti prolomení. Při tvorbě samotného hesla je důležité dodržovat jistá pravidla a zásady, které při správném použití útočníkům velmi znesnadní prolomení a případné zneužití hesla. A tím i zamezení odcizení Vašeho účtu. [3, s. 464]

Požadavky na bezpečné heslo podle České společnosti Avast software:

Délka – dostatečně silné heslo by mělo obsahovat alespoň 10 znaků, avšak vyhláška o kybernetické bezpečnosti uvádí minimální délku o 12 znacích. Dle mých zkušeností, jak bude vidět v následující ukázce, je dobré řídit se pravidlem více je lépe. V první řadě je důležité nepřizpůsobovat délku hesla minimálnímu požadavku a vždy se snažit vymyslet něco navíc.

Složitost – při tvorbě hesel bychom se měli vyvarovat používání celých slov, výhradně pak jmen členů rodiny, mazlíčků, bydliště apod. a důležitých čísel, jako jsou data narození, výročí aj. Typy hesel tvořené tímto způsobem jsou obvykle mezi prvními pokusy o prolomení hesla. Současně bychom si měli dát pozor na používání předvídatelných

pozic. To si můžeme vyložit jako používání velkých písmen, čísel a speciálních znaků pouze na začátku a konci hesla, například „Matej10“.

Pro zajištění bezpečného hesla by se heslo mělo skládat z náhodně uspořádaných velkých a malých písmen, čísel a speciálních znaků. Bezpečné heslo by mělo vypadat nějak takto: „Dzu8u460~kEC;MR“. Složitá hesla nemusíme vždy vymýšlet sami. K tomuto účelu existují generátory náhodných znaků, které „vymyslí“ heslo za nás. Při generování hesla je potřeba brát zřetel na důvěryhodnost stránky a vygenerované heslo případně ještě nějakým způsobem modifikovat, aby nedošlo k jeho zneužití již na počátku. Pro vygenerování bezpečného hesla jsem využil generátor od společnosti Avast software. [10] Následně můžeme porovnat, jak dlouho by přibližně mohlo trvat prolomení uvedených hesel. Heslo „Matej10“ je extrémní příklad, kdy heslo nesplňuje žádnou z uvedených podmínek pro bezpečné heslo (heslo je příliš krátké a nevyužívá speciální znaky) a jak je vidět, dalo by se prolomit zhruba během jedné minuty. K prolomení druhého, vygenerovaného hesla, splňující všechny zásady bezpečného hesla, by bylo potřeba zhruba 33 milionů let. [11]

Obměna hesla – *„f) pro povinnou změnu hesla v intervalu maximálně po 18 měsících…“*.[1] Ačkoliv můžeme mít sebevíc silné heslo, nikdy si nemůžeme být jistí, že jsme jediní, kdo naše heslo zná. Proto je potřeba jednou za čas si heslo obměnit, a to v nejlepším případě za heslo úplně jiné. Vyšší četnost změny hesel minimalizuje možnost odhalení aktuální podoby hesla. Není od věci měnit heslo i několikrát ročně.

Jedinečnost – Pokud by došlo k odcizení hesla, útočník s největší pravděpodobností vyzkouší všechny možné účty, které vlastníte, jak ty pracovní, tak i soukromé jako jsou bankovní účty, sociální média, online hry nebo i emailová schránka. Aby se tomu zamezilo je potřeba, aby všechny uživatelské účty měly vlastní jedinečné heslo.

Ukládání hesel – v tuto chvíli máme odpovídající délku hesel i složitost a ke každému účtu unikátní heslo, které se u žádných účtů nikde neopakuje. Jenže co s takovým množstvím hesel? V ideálním případě by bylo si všechna hesla zapamatovat. Ale to i za použití slovních hříček a pomůcek může být velmi náročné. Lidé si často svá hesla poznamenávají na papír, který mají k dispozici poblíž svého zařízení, v těch lepších případech si je ukládají přímo do webového prohlížeče. Tyto způsoby ukládání často lákají svojí jednoduchostí a snadnou použitelností při výpadku hesla z mysli. Díky lehké zneužitelnosti se tyto způsoby ukládání hesel výhradně nedoporučují. [12]

K zaznamenávání hesel můžeme využít správce hesel nebo šifrovanou jednotku USB s biometrickou čtečkou. Jedním známým a rozšířeným správcem hesel je KeePass. Pro přístup k heslům je potřeba jen jedno „superheslo“, kterým se zpřístupní všechna uložená hesla. Všechna hesla uložená v KeePass jsou šifrovaná a bez hesla je téměř nemožné dešifrovat obsah. KeePass nabízí funkci generování hesel, kde při výchozím nastavení generuje hesla o délce 20 znaků a hesla obsahují velká a malá písmena, číslovky i speciální znaky. [13] Z důvodu bezpečnosti se nedoporučuje důležitá hesla, například k bankovnictví, nikdy nikam neukládat.

Svá hesla nikdy nikomu nesdělujte.

2.2.2 Dvoufaktorové ověřování

Dvoufaktorové ověřování přidává účtu další stupeň zabezpečení. Může fungovat jako poslední záchrana při odcizení nebo prolomení hesla. Ověřování obvykle spočívá v zasílání SMS nebo emailu s časově omezeným kódem, případně odkazem, který je vyžadován v posledním kroku přihlašování. Další způsob ověření identity je za pomoci důvěryhodného zařízení, přiřazenému k účtu nebo skrz aplikaci.

Mobilní zařízení

Přenosná zařízení jako jsou mobilní telefony, notebooky jsou velmi náchylná ke krádežím, s tím je třeba počítat už při prvním spuštěním, kdy nám sám výrobce nabízí způsob, jakým svá zařízení zabezpečit v případě krádeže. Jako prevence proti vniknutí do zařízení slouží zámek obrazovky. Zámek může být zajištěn jedním z následujících způsobů:

Heslo – posloupnost velkých a malých písmen, čísel a speciálních znaků. Využití u mobilních telefonů je velmi nepraktické, obzvlášť, pokud se zařízení často používá. Odemykání telefonu se může velmi rychle stát otravným. Zabezpečení samo o sobě je velmi dobré. Avšak, pokud si dá někdo záležet může heslo okoukat nebo si kamerou ve svém zařízení nahrát způsob odemykání Vašeho zařízení a pak jej pouze zopakovat.

PIN – čtyř nebo šestimístná číselná řada číslic. Využití pouze číselné řady k odemykání mobilního zařízení vede ke zrychlení procesu odemykání. Rychlost bohužel s sebou nese vetší riziko prolomení zámku. Nejen, že je snazší si zapamatovat těch pár zadaných číslic, ale i pomocí kamery lze lépe zachytit pohyb prstů po monitoru a odhadnou jejich pozici při dopadu prstu na displeji.

Gesto – gesto si můžeme představit jako souvislý pohyb po mřížce o rozměru 3x3. Souvislým pohybem dojde ke spojení určitých bodů na obrazovce a tím dojde k odemčení mobilního zařízení. Jednoduchost a snadné okoukání tohoto principu řadí použití gesta mezi méně bezpečné způsoby zabezpečení mobilního zařízení.

Otisk prstu – velmi praktický a bezpečný způsob odemykání mobilního zařízení. I tato metoda má pár drobných nevýhod, například při odemykání telefonu se špinavými prsty, popraskanou, popř. vysušenou kůží na konečcích prstů je třeba více pokusů. Je potřeba upozornit, že během spánku nebo bezvědomí může dojít k zneužití otisků a odemknutí zařízení. I přesto se jedná mezi běžnými uživateli o nejbezpečnější způsob zabezpečení mobilního zařízení.

Sken obličeje – v porovnání s otiskem prstu se při skenování porovnává více bodů. U starších zařízení hrozí nebezpečí oklamání za použití fotografií, a to samé hrozí i během spánku a bezvědomí, díky absenci rozpoznání otevřených očí.

Pokud by při odemykání zařízení pomocí skenu obličeje nebo otisku prstu došlo k absenci snímače, se jako alternativa odemykání volí PIN kód, popř. heslo.

2.3 Ochrana před škodlivým kódem

2.3.1 Firewall

Dříve měl pojem Firewall v anglickém jazyce význam pouze pro stěnu oddělující dvě budovy, aby zabránila rychlému šíření požáru. [14] Od 80. let 20. století tento pojem označuje fyzické zařízení nebo programové vybavení určené pro filtrování komunikace v rámci sítě a tvoří bariéru mezi privátní sítí a veřejným internetem. Softwarové Firewally jsou součástí programového vybavení všech zařízení podporující připojení k síti. Skrze tuto pomyslnou zeď proudí veškerá komunikace. Tato komunikace je nepřetržitě monitorována. Na základě nastavených pravidel a politik Firewall vyhodnocuje důvěryhodnost komunikace a zabraňuje neoprávněnému přístupu k síti. V okamžiku stažení škodlivého kódu do zařízení, Firewall dokáže zabránit rozšíření viru z infikovaného zařízení směrem do soukromé sítě. [15]

2.3.2 Antivir

Od roku 1971, se s objevením prvního viru začal vyvíjet i první antivirový program. Za uběhlé roky se současné verze antivirových programů staly velmi sofistikovanými nástroji pro odhalování přítomnosti škodlivých programů. Aby antiviry udržely krok s neustále se vyvíjejícími hrozbami, zavedla se spolupráce na globální úrovni. Za pomoci výměny informací jsou vzájemně doplňovány virové databáze jednotlivých antivirových programů. [16] V důsledku rychlého výskytu nových virů, je zapotřebí aktualizovat virovou databázi i několikrát za den.

Antivirus sám o sobě dokáže odhalit nebezpečný kód, zamezit jeho spuštění a bezpečným způsobem odstranit ze zařízení. [17] Toto platí pouze za předpokladu, že máme na zařízení nainstalovanou nejnovější verzi antivirového programu.

Jestliže chcete udržet své zařízení v bezpečí, nikdy nevypínejte Firewall, ani antivirus. Některé programy během instalace vyžadují vypnutí obou bezpečnostních prvků. Takové požadavky samy o sobě ukazují na možnost výskytu nebezpečného kódu a v žádném případě byste neměli pokračovat v instalaci.

Dalším významným způsobem, jak se chránit před nebezpečným kódem, je aktuálnost softwarového vybavení. Aktualizace obvykle reagují na výskyt zranitelností v předchozích verzích. Proto je nutné tyto aktualizace nainstalovat co nejrychleji a tím zamezit zneužití zranitelnosti na Vašem zařízení. [18]

2.3.3 Zálohování dat

Záloha dat Vás nijak neochrání proti útoku na Vaše zařízení, ale je dobrým nástrojem pro obnovu a zotavení při ztrátě nebo zašifrování dat v následku úspěšného prolomení zabezpečení zařízení.

Prvním krokem při zálohování je uvědomění si, jaká data je potřeba zálohovat. Zálohovat se můžou jednotlivé soubory, programy a aplikace, jednotlivá nastavení nebo i samotný operační systém. Takže když se stanete obětí útoku, můžete jednoduše obnovit poslední zálohu. Jediná data, která budou chybět budou ty, co se od posledního cyklu zálohování pozměnily.

Zálohu můžeme provádět různými způsoby. Vždy jako první je nutné udělat plnou zálohu všech klíčových dat. **Úplná záloha** vždy zabere určitý čas, vše se odvíjí na objemu

zálohovaných dat. Určitě nechceme provádět úplnou zálohu denně, od toho existují další dva způsoby přírůstkového zálohování:

Diferenciální zálohování – zálohovány jsou pouze ty data, která byla pozměněna od poslední úplné zálohy.

Inkrementální zálohování – u tohoto způsobu se zálohují pouze pozměněná data od poslední zálohy. Díky tomu jsou zálohovaná data menší a průběh zálohy časově úspornější.

V závislosti na objemu ukládaných dat je nutné zvolit i vhodnou strategii při plánování intervalů záloh. Čím více změn, tím častější záloha. Přírůstkové zálohy není od věci jednou za čas proložit úplnou zálohou například jednou týdně/měsíčně/ročně. [19]

2.3.4 Škodlivý kód

Malware – Slovo malware vzniklo spojením dvou anglických slov „malicious software“, což můžeme volně přeložit jako škodlivý program. Pod pojem malware řadíme veškerý škodlivý kód, přičemž nezáleží, jakým způsobem napadá zařízení a ani způsob jeho chování. Mezi druhy malwaru patři například Trojské koně, Spyware, Ransomware, aj. [20]

Trojský kůň – každý už určitě slyšel o slavném dobytí Trójy, kdy řečtí vojáci předali jako dar obřího dřevěného koně plných vojáků.

Stejným způsobem v moderní době fungují i ty virové Trojské koně. Ačkoliv se stažený soubor do počítače může zdát na první pohled v pořádku, vše je funkční, jak má a žádným způsobem nevzbuzuje pozornost, že by šlo o virovou hrozbu, skutečnost může být vždy jiná. Škodlivý kód může být skrytý za funkčností jiných souborů, programů, filmů nebo digitální pohlednicí a vyčkávat na spuštění libovolné události na zařízení. Spouštěčem může být prakticky cokoliv, například x-té spuštění zařízení nebo systémový čas. Po nastání této spouštěcí události může dojít k převzetí kontroly nad napadeným zařízením, odcizení uživatelských dat nebo spuštění jiného zákeřnějšího škodlivého kódu.

Nejznámějším případem použití Trojského koně byl zdokumentován už v roce 1989 pod názvem AIDS Trojan. Vir se šířil za využití disket, které byly rozesílány poštou. Na těchto disketách měly být údajně interaktivní databáze o nemoci AIDS. Po jejím nainstalování Trojský kůň následně vyčkal 90 cyklů zapnutí počítače. Za využití Ransomware

škodlivého kódu se následně zašifrovala velká část souborů. Za odšifrování těchto souborů bylo požadováno výkupné ve výši 189 dolarů. [21]

Ransomware – *„Ransomware je typ malwaru, který blokuje přístup k souborům a počítačovým systémům a zároveň požaduje výkupné výměnou za opětovný přístup. Ransomware používá šifrování k blokování přístupu k infikovaným souborům, takže jsou nepoužitelné a nepřístupné obětem.“* [22]

Po zasáhnutí Ransomwarem se obvykle objevuje uživateli hláška o zaplacení tzv. výkupného za dešifrování dat. Ani v tomto se nedá útočníkům věřit a často po zaplacení požadované částky zašifrované soubory nedešifrují zpět, takže oběť zůstává se zašifrovanými daty a bez peněz. Napravení škod ve většině případech ani není možná.

Po zjištění útoku je potřeba neprodleně odpojit nejlépe všechna zařízení od sítě, případně je vypnout přímo od zdroje napájení a kontaktovat zkušeného odborníka, který dokáže poradit.

Spyware – Odhalení samotného Spywaru je pro lajka velmi obtížné. V případě podezření infikace zařízení Spywarem je potřeba dávat pozor na běžící procesy na pozadí. Během běžného používání zařízení si můžete povšimnout otevírajících se programů v liště a značného zpomalení zařízení. Spyware pro komunikaci využívá připojení do sítě, zpomalení připojení k internetu může být také výrazně zpomaleno, to může být dalším vodítkem k odhalení nechtěného kódu.

Slovo „spy“, odvozené od anglického slova „špión“ nebo „špionáž“ dokonale popisuje princip fungování škodlivého kódu. Aniž bychom o něčem věděli, Spyware postupně sbírá veškeré informace o historii navštívených stránek, přístupové údaje, bankovní údaje, používané soubory a programy nebo i stisk jednotlivých kláves. Takový sběr informací většinou vedou k pokusu o krádeže identity. [23]

Počítačový červ – tímto termínem se označuje typ Malwarovského kódu, jenž je schopný svévolného rozmnožování prostřednictvím sítě nebo přenosných médií. [24]

Počítačový virus – počítačový virus má za cíl získat kontrolu nad celým zařízením a tím získat citlivá data. Při úspěšném převzetí kontroly nad zařízením může útočník sledovat váš obraz na monitoru nebo ovládat webkameru a ostatní periferie zařízení. [25]

Zavirování zařízení se nedá vždy úplně zabránit, ale můžeme tomu v mnoha případech předcházet. První zásadou, jak zamezit stáhnutí škodlivého kódu je se řádně ujistit, co přesně stahujeme. Aplikace a programy stahovat vždy a pouze z oficiálních zdrojů. Při

používání webového prohlížeče postupovat obezřetně, zaměřit se na používání stránek umožňující bezpečnou komunikaci prostřednictvím protokolu HTTPS, samotný protokol si představíme později. V žádném případě neklikejte na vyskakovací okna.

2.4 Důvěryhodná komunikace

Email, hojně využívaný pracovní nástroj umožňující snadnou komunikaci v rámci organizací, ale i s vnějším světem nebo pro soukromé účely. Díky své rozšířenosti a obecnému nevědomí o možných hrozbách, patří emailová komunikace mezi oblíbené způsoby útoků.

Kdybych tvrdil, že se každý z nás během života setkal s jednou z forem internetového podvodu, určitě bych měl z 99 % pravdu. Možná by někteří jedinci zpočátku tvrdili pravý opak, ale po přečtení následujícího tématu by svoji odpověď přehodnotili.

V následující části si probereme nejčastěji používaný druh útoků, a to internetové podvody, primárně mířené na uživatele zařízení, u kterých záleží jen na rozhodnutí, jak se v dané chvíli uživatel zachová.

2.4.1 Phishing

Phishing je nejběžnějším typem sociálního inženýrství. Aktéři posílají zprávy, ve kterých se vydávají za důvěryhodnou osobu s cílem získat citlivé údaje nebo na Vaše zařízení nahrát škodlivý kód. [26] Předem připraveném scénářem se útočníci snaží donutit oběť, aby otevřela přiložený odkaz nebo soubor. Pod odkazem se ukrývá stránka, naprosto totožná s oficiální verzí, rozdílem však je podvrhnutý přihlašovací formulář. Na takové stránce by vyplnění přihlašovacích údajů a jiných citlivých údajů nevedlo k přihlášení k Vašemu účtu, nýbrž k odeslání všech údajů útočníkovi. Scénář obvykle doprovází časová tíseň. [27]

Připravené scénáře můžou odkazovat na napadení Vašeho bankovního účtu, neplatnou platbu, [28] vzniklé dluhy, probíhající exekuce [29, s. 250] nebo zjištěná bezpečnostní hrozba ve Vašem zařízení.

Další formy phishingu:

Spear phishing – neboli cílený phishing. Označuje cílený útok adresovaný na konkrétní cíle. Útočník si dopředu zjišťuje veškeré dostupné informace o oběti, aby docílil co nejdůvěryhodněji, a tím zvýšil efektivitu svého útoku. [26]

Whaling – v překladu lov velryb, alias lov velkých ryb. Útočníci se zaměřují na vyšší managment a další vysoce postavené osoby v organizacích. Cílené útoky jsou daleko sofistikovanější než obyčejný phishing. Útočníci se často vydávají za jednoho znadřízených čímž způsobí psychický nátlak na svoji oběť. Ty následně podlehnou požadavku v obavách o neuposlechnutí rozkazu nadřízeného. [30]

Vishing a Smishing – jedná se o podvody mířené na mobilní zařízení. Útoky jsou často mířeny na lidi s nižším povědomí o zacházení s telefony. Vishing využívá hlasových hovorů. Útočníci v roli vyšetřovatele banky nebo jiné instituce informuje oběť o krádeži účtu a pro identifikaci vyžadují citlivé informace pro ověření identity. [26] Smishing je založen na posílání SMS zpráv, založených obvykle na stejném principu krádeže účtu nebo náhlé výhry. Součástí zprávy je odkaz, jako u běžného phishingu.

Jak efektivně rozpoznat phishing a jak se správně zachovat, při jeho obdržení:

Pokud obdržíte neočekávanou zprávu od neznámého odesilatele obsahující přiliž mnoho podrobností nebo vytvářející nátlak na rychlé jednání, měli byste zbystřit. V prvním kroku je nutné zkontrolovat adresu odesilatele, přiložené odkazy a soubory a použitou gramatiku.

2.4.2 Spam

„Spam je jakákoliv forma nevyžádané hromadné digitální komunikace. Jde o nevyžádaná reklamní sdělení ve formě e-mailů, SMS nebo zpráv v komunikačních aplikacích, na sociálních sítích nebo diskuzních fórech, zasílané velkému počtu příjemců nebo publikované na velkém počtu míst na internetu.“ [31] Obsahem sdělení můžou být různé formy obchodních nabídek (např. slevy, produkty, služby, aj.) nebo propagace. Obdržené zprávy jsou samy o sobě často neškodné, ale i tak se může přihodit, že jsou doprovázeny škodlivým virem. Spam obsahující kriminální či jiný podvodný obsah je označován jako scam. [29, s. 231-235]

2.4.3 Scam

Útok často využívá principy phishingu, krádeží identity aj. a cílí na získání finančních prostředků oběti. Nejčastější typy scamu, se kterými se můžete setkat jsou:

Romance scam – útočníci zpravidla využívají falešnou identitu. Za využití seznamovacích aplikací navážou kontakt s obětí, ke které předstírá silné city. Pomocí důvěryhodného

příběhu, kde popisují svojí práci v zahraničí, často se jedná o bojovou misi nebo práci na lodi. Po nějakém čase pod záminkou brzkého setkání lákají peníze na pokrytí finanční tísně spojenou s přicestováním do země. [32]

Nigerijské dopisy – podvod starý jako Jeruzalém, tento druh útoku se už před rozšířením počítačů šířil faxy. Nabídka dědictví po zemřelém, kterého ani neznáte zní dobře, obzvlášť, když jde o obří dům a nepředstavitelnou sumu na účtu. Takový je dost často příběh útočníka, ten žádá jen malý obnos za „zprostředkování". [29, s. 237]

Scam na internetových bazarech – při prodeji starého krámu, jenž nikdo nechce se náhle ozve zájemce, který je úplně nadšený z nabízeného produktu a co nejrychleji by ho chtěl mít doma, zařídí kurýrní službu a pošle odkaz s platební bránou, přes kterou Vám dopředu pošle peníze. Po kliknutí na zaslaný odkaz jste zpravidla přesměrováni na neznámou stránku, kde chtějí vyplnit údaje o kreditní kartě. Avšak po vyplnění místo připsání slíbené částky dochází k pravému opaku.

2.4.4 Hoax

Poplašná zpráva, anglicky hoax, označuje šíření nepravdivých, občas až těžko uvěřitelných informací. Typický hoax nám důvěryhodným způsobem předkládá fakta o vzniklých nebezpečích, naléhavé pomoci nebo šokujících odhalení. Jako příklad si uvedeme jeden z hoaxů z portálu hoax.cz, kolující u nás už od roku 2007.

„Oficiálně z banky:
Jakmile se ocitnete v situacii a musíte pod nátlakem vybrat peníze z bankovního automatu na požádáni/přinuceni nasilnikem, zadejte svůj PIN opačně:
to je od konce - např. máte-li 1234, tak zadáte 4321, automat vám peníze přesto vydá, ale též současně přivolá policií, která vám přijde na pomoc. Tato zpráva byla před nedávnem vysílaná v TV, protože málo lidí využívalo tuto skutečnost, protože o tom nevěděli." [33]

2.4.5 Na co si dávat pozor

Adresy a hypertextové odkazy – při útocích využívající hypertextových odkazů útočníci často spoléhají na nedbalost uživatele. Útočníci obvykle zasílají odkaz se změněným pořadí jednotlivých písmen. Na první pohled může odkaz vypadat stejně, jako ten, který dobře známe. Například youtube.com může útočník transformovat na yuotube.com, kliknutím na odkaz se dostaneme na útočníkovu stránku, totožnou s její oficiální verzí.

Tato stránka při vstupu může vyžadovat zadání přihlašovacích údajů, po jejichž zadání útočník získá naše přihlašovací údaje. Taková stránka může i sama o sobě obsahovat malware.

Skeptismus je na místě. Důkladně si prohlédněte adresu, na kterou Vás přiložený odkaz chce přesměrovat. V počítači můžete zkontrolovat adresu najetím myší na odkaz, v dolním rohu prohlížeče se objeví přesná podoba odkazu. Na mobilním zařízení je pro kontrolu nutné na odkazu podržet prst. Hledejte překlepy, přesmyčky nebo výskyt podobných znaků, je snadné zaměnit „I“ za „l“, tedy velké Íčko za malé Lko nebo „O“ za „0“. [34]

Přetrvávající pochyby můžete ověřit nástrojem skenování adres URL od společnosti Google pod názvem Stav webu. [35] Vložený podezřelý odkaz se během několika sekund otestuje výskyt hrozeb schované pod odkazem. Pokud máte podezření o podvrhu, nikdy neklikejte na přiložené odkazy a připnuté přílohy.

Přílohy – Jak jsme si už řekli, každá neočekávána zpráva by ve Vás měla vzbudit jisté podezření, obzvlášť, pokud obsahuje podivný odkaz nebo přílohu. V těchto případech je nutné, zda je příloha skutečně tou, za kterou se vydává. Existuje mnoho způsobů, jak zamaskovat pravou podobu přiložených souborů. Proto byste měli vědět, jak takový soubor ověřit.

První, co by Vás mělo u podezřelých souborů zajímat je přípona samotného souboru. V prostředí Windows doporučuji zapnou náhled přípon souborů. Volbu pro zapnutí přípon nalezneme v Průzkumníku Windows v záložce Zobrazení a tam zaškrtneme okénko s volbou Přípony názvů souborů.

Ovšem ne každý soubor s koncovkou .docx nemusí nutně být textovým souborem. Vždy se zajímejte o písmena příloh za poslední tečkou v názvu souboru. Pokud obdržíte soubor s názvem „Faktura.docx.exe“ nejedná se o textový dokument, nýbrž o spustitelný soubor.

Nebezpečné přílohy, u kterých byste se měli vyvarovat jejich stažení:

.iso – soubory se obecně používají pro vytváření kopií fyzického disku a pro šíření operačních systémů. Útočníci tento typ souborů využívají pro šíření malwaru a jiných virů.

.exe – spustitelné soubory

Neexistuje žádný rozumný důvod, proč by někdo posílal tyto dva typy souborů emailem. Takže pokud obdržíte zprávu s takovým souborem, můžete si být jistí, že se jedná o podvrh.

Komprimované soubory – používají se ke zmenšování velikosti příloh, aby je bylo možné poslat v jedné zprávě. Proto je mnohdy těžké na první pohled odhalit možný problém. Opět buďte skeptičtí, zkontrolujte adresu odesilatele, jestliže si nebudete jistí o původu samotné zprávy, neotvírejte žádnou přílohu. Komprimované soubory mohou mí přípony ve tvaru .zip, .rar, .arc, aj. [36]

Makra – používání maker nám dokáže zjednodušit a urychlit práci s dokumenty. Prakticky to samé platí i pro útočníky, kteří používají makra, aby do našich zařízení dostali škodlivý obsah.

docx vs. docm – přípona .docx označuje textové dokumenty. Pokud textový dokument obsahuje makra, jeho název obsahuje příponu .docm. [37] Na soubory obsahující makra je nutné si dávat obzvlášť pozor. Samotné makro, aniž bychom to tušili, do našeho zařízení stáhne a spustí škodlivý kód. [38]

Textové programy mají ve výchozím nastavení v rámci bezpečnosti spouštění maker zakázané. Spuštění maker je tedy výhradně na vás. Takže pokud si nejste jistí původem souboru nebo funkčností maker, nikdy povolujte tento obsah.

Abyste si nemysleli, že riziko se skrývá pouze v makrech, přikládám úryvek článku ze stránky antivirovecentrum.cz, který varuje na výskyt malwaru i v obyčejných dokumentech s příponou .docx.

„Možná si říkáte, že útoky, kde musí uživatel odklikat tolik varovných hlášek, nemohou být úspěšné. Omyl! Třeba úspěšné odrůdy havěti ransomware se šířily podobnou cestou. Skrze nevinně vypadající dokument Wordu (přípona .docx / .doc) taktéž s nutností odsouhlasit ze strany uživatele několik varování. Ke spuštění havěti se v takovém případě využívají makra." [39]

2.4.6 Zachování důvěryhodnosti komunikace

Elektronický podpis – *„Elektronický podpis podle nařízení eIDAS slouží k projevu vůle (souhlasu) podepisující osoby s dokumentem – čili obdobně jako v „listinném světě". Stejně jako podpis na listinném dokumentu, je elektronický podpis vyhrazen pouze fyzickým osobám."* [40]

Pojem elektronický podpis označuje libovolný podpis v digitální, který z právního hlediska dokáže zastoupit vlastnoruční podpis, sloužící k rychlému podepsání

elektronických dokumentů. Sofistikovanější elektronické podpisy dokážou zaručit integritu dokumentů a pravost podpisu. [41]

- **Prostý elektronický podpis** – jedná se o nejnižší formu elektronických podpisů, nevyužívající žádný bezpečnostní prvek. Jako prostý el. podpis si můžeme představit naskenovanou verzi vlastnoručního podpisu nebo automaticky doplňovaný podpis v patičce emailové zprávy. [42]
- **Zaručený elektronický podpis** – vyšší a bezpečnější forma elektronických podpisů založený na certifikačních službách. Při podepisování se využívá vlastní privátní klíč, který zajišťuje integritu dat a jejich původ. Jako nosič privátního klíče se obvykle využívá karta nebo USB zařízení s nahranými certifikáty, umožňující ověření platnosti. [43]
- **Kvalifikovaný elektronický podpis**– nejvyšší možná forma elektronického podpisu využitelná při komunikaci se státními orgány v rámci ČR a EU. [44] Kvalifikované certifikáty jsou vydávány certifikačními autoritami. U nás v ČR jsou tyto certifikační autority: První certifikační autorita, a.s., Česká pošta, s.p. (PostSignum), EIdentity a.s. [45] Kvalifikační certifikát je během registrace jednoznačně spojen s žadatelem prostřednictvím průkazu totožnosti. Pro zachování důvěrnosti je možné certifikát ukládat pouze na certifikované čipové karty nebo USB zařízení. [40]

2.5 Konektivita

Občas se každému vyskytne situace, kdy je nutné se vzdáleně připojit do pracovního prostředí, aby se uhasil požár v podobě těsných termínů nebo něčeho, co se zapomnělo udělat při zbrklém úprku z práce. V posledním okruhu se podíváme na připojování skrze veřejné sítě, řekneme si jaké výhody poskytuje osobní hotspot a vysvětlíme si zkratky VPN a HTTPS.

2.5.1 Veřejné sítě

Určitě to znáte, sedíte v kavárně a potřebujete nutně použít svůj přenosný počítač, abyste něco dodělali. Ale k tomu potřebujete internet, takže otevřete seznam dostupných sítí

a hned mezi prvníma vidíte nezaheslovanou wifi síť s názvem kavárny. Jenže je tato možnost připojení bezpečná?

Otevřená síť – pokud se budete chtít na veřejnosti přihlásit k otevřené wifi síti, nejprve tento krok vážně zvažte. Stejně tak snadno, jak se můžete připojit Vy, má tuto možnost každý v okolí, dokonce i neznámý útočník. Útočník v takové síti může jednoduše odposlouchávat veškeré dění na síti a tím získat citlivé informace. [46] Na takové sítě není rozumné se nikdy připojovat, ovšem pro rychlé vyhledání informací jsou poměrně ideální. Na otevřených sítích zvažte vyplňování přihlašovacích údajů a už vůbec nevstupujte ke svým bankovním účtům. Pro vyšší bezpečnost využívejte stránky zabezpečené protokolem HTTPS. [47]

HTTPS – protokol HTTPS je bezpečnou verzí http a využívá se k šifrování spojení mezi serverem a koncovým zařízením a tím zajišťuje soukromí dat. V prohlížeči se pozná podle visacího zámku zobrazeného v poli url adresy. některé starší stránky visací zámek neukazují, v takovém případě samotná url adresa začíná znaky https:// [48]

Nenechte se oklamat, pokud budete na veřejném místě a připojíte se k síti pomocí hesla napsaném na tabuli u baru nebo na konci meníčka, nikdy to neznamená zcela bezpečné připojení. Pokud na internetu najdeme vše, co jsme potřebovali, síť opojíme a vypneme wifi v zařízení, abychom předešli nechtěnému připojení k jiné síti. [3, s. 448]

2.5.2 Mobilní síť a hotspot

Mobilní sítě jsou tou nejlepší možností pro připojení k internetu. Díky šifrování a vysokému zabezpečení je možné přistupovat téměř kamkoliv. Stále tu platí zásada nenavštěvovat pochybné weby a nestahovat soubory, o nichž nic nevíme. A zároveň upřednostňovat weby poskytující bezpečnou komunikaci pomocí HTTPS. Pokud dodržíme tyto zásady, můžeme se bezstarostně přihlašovat na sociální sítě, email i bankovní účet. [49]

Jestliže potřebujete sdílet data z jednoho zařízení na druhé za využití hotspotu, nikdy nezapomeňte pro připojení k Vašemu zařízení nastavit dostatečně silné heslo. Častou chybou se stává, že sdílená data nejsou zabezpečeny a v tom momentu se stávají lehce napadnutelné. Pokud máte při vytváření hesla na výběr způsobu zabezpečení, vždy vyberte protokol WPA2 nebo jeho novější variantu WPA3.

- WPA2(AES) – díky svým pokročilým šifrovacím metodám se jedná o současně nejvyužívanější způsob zabezpečení sítě už od roku 2004. [3] WPA2 je šifrovaný bezpečnostní protokol, chránící komunikaci v bezdrátových sítích. Díky důmyslnému dynamickému šifrování dat je pro útočníky velmi složité a téměř nemožné rozluštit komunikaci v rámci sítě. [50]
- WPA3 – protokol vycházející ze standardů WPA2. WPA3 využívá vylepšené zabezpečení, díky kterým je daleko složitější narušení sítě. WPA3 byl představen v roce 2018, z toho důvodu na něj u starších zařízení nenarazíme.[51]

2.5.3 Virtuální privátní síť (VPN)

VPN, často používaný způsob v organizacích a firmách pro bezpečné vzdálené připojení zaměstnanců na pracovní plochu napříč veřejným internetem. [52]

VPN poskytuje soukromé a zabezpečené připojení mezi dvěma body přes veřejnou síť. Po odeslání žádosti o připojení na druhé koncové zařízení se díky autentizaci ověří uživatelské údaje a k nim navázaná oprávnění. Když se uživatel ztotožní, mezi oběma koncovými body se vytvoří pomyslný tunel, skrz který proudí veškerá zašifrovaná komunikace. To zamezuje odposlechu sítě a poskytuje bezpečné připojení v nedůvěryhodných a nezabezpečených sítích. [53] Během nastavovací fáze obě komunikující strany vytvoří sdílený tajný klíč, který následně využívají po dobu trvání relace pro šifrování a dešifrování dat proudící tunelem. VPN dokáže zajistit důvěrnost a integritu dat, v případě pokusu o čtení nebo změnu dat je útočník neprodleně detekován. [54]

VPN skýtá mnoha způsoby využití. Mohli bychom ji využít i v naší oblíbené kavárně s otevřenou sítí. Pomocí jejich „nebezpečné“ sítě se můžeme jednoduše připojit například na vlastní domácí privátní síť a tam si bezpečně brouzdat internetem, platit faktury a další. Ovšem za splnění základních bezpečnostních zásad, které jsme si již dříve uváděli.

3 Praktická část

Cílem praktické části projektu bylo navrhnout a implementovat vzdělávací webovou stránku zaměřenou na oblast kybernetické bezpečnosti. Hlavním úkolem bylo nejen poskytnout užitečné informace o tomto tématu, ale také zároveň zjistit dosavadní úroveň znalostí uživatelů v této oblasti. Webová stránka je dostupná na internetové adrese https://lide.uhk.cz/fim/student/hubalma3/

Již na vstupní stránce se uživatelům nabízí možnost k absolvování vstupního testu. Tento test je zásadní k posouzení jejich úrovně znalostí ještě před zahájením samotného kurzu. Test obsahuje řadu otázek, mezi nimiž se nachází vybraná sada otázek, která se opět opakují i v závěrečném testu. Po vyhodnocení testu dochází k ukládání odpovědí uživatelů u vybraných otázek. Tento proces umožňuje efektivně porovnat počáteční a závěrečnou úroveň znalostí všech účastníků. Takové srovnání poskytuje přehled o celkovém rozsahu zlepšení, kterého uživatelé jako skupina dosáhli v průběhu absolvování kurzu.

Během kurzu je uživatelům poskytnuto pět studijních témat, z nichž každé je zakončeno cvičným testem. Tyto testy jsou navrženy tak, aby poskytly uživatelům příležitost k procvičení a upevnění získaných znalostí.

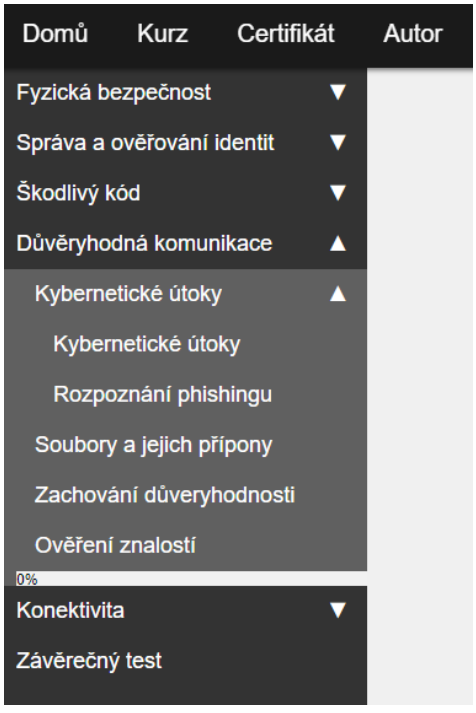
Jedinečnou vlastností tohoto kurzu je možnost získání certifikátu za úspěšné absolvování testů. Aby uživatelé tento certifikát získali, musí u cvičných testů dosáhnout průměru 70 % nebo vyšší a také úspěšně splnit cvičný test s výsledkem alespoň 70 %.

3.1 Webová stránka

3.1.1 Navigace

Pro zjednodušení pohybu mezi základními bloky webové stránky bylo zvoleno navigační menu umístěné v záhlaví stránky. Návštěvník webu by měl být schopen jednoduchým způsobem přepínat jednotlivé sekce, které jsou:

- Úvod: slouží jako první kontakt uživatele s webem, kde je při vstupu nabízena možnost absolvování vstupního testu.
- Kurz: V této sekci uživatelé naleznou veškerý vzdělávací obsah kurzu společně s průběžnými a závěrečným testem.
- Certifikát: zde má každý uživatel možnost zkontrolovat jeho dosavadní úspěšnost ve cvičných testech. Dále na stránce je vysvětlen proces pro získání certifikátu a kritéria, která musí být splněna pro jeho obdržení.
- Autor: poslední sekce poskytuje informace o tvůrci webu.



Obrázek 1 – navigační menu. Zdroj: vlastní tvorba

V sekci věnované kurzu se objevuje druhý navigační prvek, v podobě rozbalovací horizontální navigace. V této druhé navigaci jsou vypsaná jednotlivá témata kurzu. Po kliknutí na některé z témat dojde k rozbalení rodičovského prvku vybraného tématu, tato možnost je naznačena šipkou směřující směrem dolů. Kliknutím jsou zobrazeny podkapitoly daného tématu společně s cvičným, průběžným testem. Kliknutím na vybrané podkapitoly, případně testy dochází k přesměrování na vybranou stránku.

Na obrázku 1 je zachycena finální podoba rozbalovacího navigačního panelu. V rámci snadnější orientace během procházení kurzu, je aktuálně zobrazovaná kapitola stále zobrazena v navigačním menu. Pod každým cvičným testem, který je označen jako „Ověření znalostí“ je navíc uvedena procentuální úroveň úspěšnosti ve cvičném testu.

3.1.2 Testy

Cvičné testy v rámci kurzu jsou navržený tak, aby zpravidla obsahovaly 9 otázek s výběrem jedné správné odpovědi a 1 otázku, kde je možné zvolit více možných odpovědí. Jedinou výjimkou je první cvičný test spadající pod téma Fyzické bezpečnosti. Tento test se skládá z celkem 6 otázek. Zde podobně jako u ostatních testů, poslední otázka umožnuje výběr více správných odpovědí.

Vstupní a závěrečný test obsahují kromě standartních otázek zaměřené na ověření znalostí také speciální otázky, které nejsou součástí hodnocení. Tyto otázky mají charakter dotazníkového šetření a jsou navrženy tak, aby zjistili předchozí zkušenosti účastníků s různými aspekty kybernetické bezpečnosti. Cílem těchto doplňkových otázek je získat informace o tom, jaké mají účastníci zkušenosti s podvody v kybernetickém prostoru a jakým způsobem přistupují k ochraně svých účtů. Tento přístup poskytuje užitečná data, která mohou být využita pro další rozvoj kurzu a aby lépe reflektoval potřebám a znalostní úrovně účastníků.

3.1.2.1 Vyhodnocování testů

Kód uvedený na obrázku 2 demonstruje, jakým způsobem probíhá vyhodnocování testů s otázkami, kde je možné zvolit pouze jednu možnou odpověď.

Na začátku kódu je definována proměnná „body“, která slouží k počítání celkového počtu bodů. Tato proměnná se před započetí vyhodnocování inicializuje na nulovou hodnotu. Následně je vytvořeno pole „spravneVysledky“. Toto pole je naplněné jednotlivými identifikátory správných odpovědí z formuláře testu. Samotné vyhodnocování začíná cyklem „for“, který postupně prochází jednu zvolenou odpověď za druhou s předpokladem, že je test složený ze stejného počtu otázek, jako je délka pole „spravneVysledky“. V prvním kroku při ověřování správnosti zvolených odpovědí se z formuláře načte odpověď, kterou uživatel zvolil. Ta se v dalším kroku otestuje, zda odpověď byla vůbec vybrána. V poslední fázi se zvolená odpověď porovnává se správnou odpovědí z pole. Pokud se vybraná odpověď shoduje se správným výsledkem, odpověď se na uživatelově obrazovce zezelená a bude mu přičten bod. V opačném případě zčervená a bodové ohodnocení se nezmění.

```
var body = 0;
spravneVysledky = ["spam", "zamer", "vypnout", "oficialni", "18", "12", "nakladani"];
for (let i = 1; i <= spravneVysledky.length; i++) {
    let selectedAnswer = document.querySelector(`input[name="question${i}"]:checked`);
    if (selectedAnswer != null) {
        if (selectedAnswer.id == spravneVysledky[i - 1]) {
            document.getElementById(selectedAnswer.id + "1").style.color = "green";
            body++;
        } else {
            document.getElementById(selectedAnswer.id + "1").style.color = "red";
        }
    }
}
```

Obrázek 2 – vyhodnocování otázek s jednou možnou odpovědí. Zdroj: vlastní tvorba

V tento moment máme vyhodnocené všechny testy s jednou možnou odpovědí a zbývá vyhodnotit správnost odpovědí u otázek s více možnými správnými odpověďmi. Na následujícím obrázku 3 je uveden kód, jehož pomocí jsou testy vyhodnocovány.

Kód začíná definicí dvou klíčových hodnot. První proměnná „checkedValue“, je nastavena na prázdnou hodnotu „null“. Druhá proměnná „pocetCheckboxu“ je nastavena na hodnotu 1, což slouží jako počítadlo. Ve třetím řádku začíná samotný proces vyhodnocování zaškrtnutých odpovědí. V tomto bodě pomocí cyklu „while“ je postupně přistupováno ke každé otázce s vícenásobnou odpovědí vyskytující se v testu, až do momentu, kdy již nejsou další otázky k vyhodnocení. Při vyhodnocování testů je v prvním kroku nutné získání dat z formuláře a uložení do pomocného pole „inputElements“. Následně je toto pole postupně procházeno a s využitím podmínky jsou vybrány pouze ty odpovědi, které uživatel označil. V posledním kroku se porovnávají označené odpovědi s polem správných odpovědí. Toto porovnání probíhá obdobným způsobem, jako u otázek s jednou možnou odpovědí.

```
var checkedValue = null;
var pocetCheckboxu = 1;
while (document.getElementsByName(`check${pocetCheckoxu}[]`).length != 0) {
    var inputElements = document.getElementsByName(`check${pocetCheckboxu}[]`);
    for (var i = 0; inputElements[i]; ++i) {
        if (inputElements[i].checked) {
            checkedValue = inputElements[i].id;
            document.getElementById(inputElements[i].id + "1").style.color = "red";
            for (var j = 0; j < spravneVysledkyCheck[pocetCheckboxu - 1].length; j++) {
                if (inputElements[i].id == spravneVysledkyCheck[pocetCheckboxu - 1][j]) {
                    document.getElementById(spravneVysledkyCheck[pocetCheckboxu - 1][j] + "1")
                        .style.color = "green";
                    body++;
                    break;
                } else if (j == spravneVysledkyCheck[pocetCheckboxu - 1].length - 1) {
                    body--;
                }
            }
        }
    }
    pocetCheckoxu++;
}
```

Obrázek 3 – vyhodnocování otázek s výběrem více možných odpovědí. Zdroj: vlastní tvorba

3.1.3 Ukládání označených odpovědí do souboru

```
if (isset($_POST["submit-btn"])) {
    $pocet = 7;
    $dataCh = array($_POST["question1"], $_POST["question2"], $_POST["question3"], $_POST["question4"],
    $check = 1;
    while (isset($_POST["check{$check}"])) {
        foreach ($_POST["check{$check}"] as $checkbox) {
            $dataCh[$pocet] = $checkbox;
            $pocet++;
        }
        $check++;
    }
    $dataCh = implode(";", $dataCh,);
    $dataCh = PHP_EOL . $dataCh;
    file_put_contents("./testy/vstupniTest.csv", $dataCh, FILE_APPEND);
```

Obrázek 4 – ukládání do soboru formátu CSV. Zdroj: vlastní tvorba

Celý proces ukládání začíná v okamžiku, kdy je odeslán formulář, který je předem ošetřen pomocí JavaScriptu, aby se zabránilo odeslání v případě, že nejsou nezodpovězeny všechny testovací otázky. Prvním krokem v procesu ukládání uživatelem vybraných odpovědí je inicializace pole „$dataCh“, do kterého jsou uloženy odpovědi na otázky s jednou možnou odpovědí. K těmto otázkám se přistupuje prostřednictvím jejich identifikátorů „question“. V další fázi procesu je použit cyklus „while“, jehož cílem je postupně projít všechny otázky obsahující více možných odpovědí. Uvnitř samotného cyklu jsou postupně z každé otázky vybírány uživatelem zaškrtnuté odpovědi a ty se následně přidávají na konec pole „dataCh“.

Jakmile jsou všechny odpovědi zaznamenány v poli, využívá se metoda „implode“, která převádí obsah pole na řetězec hodnot, oddělených středníky. Pro finální uložení je použita

funkce „file_put_contents“ s příznakem „FILE_APPEND“, díky čemuž jsou shromážděné odpovědi z formuláře uloží do existujícího souboru typu CSV, a to na nový řádek.

3.1.4 Použité technologie

- HTML: pro vytvoření základní struktury webové stránky byl vybrán značkovací jazyk HTML.
- CSS: využitím kaskádových stylů se podařilo vytvořit plně responzivní a uživatelsky přívětivý web.
- JavaScript: tento jazyk je využíván pro automatické rozbalování obsahu v horizontální navigaci během přesunu mezi jednotlivými tématy. JavaScript je dále využíván k ověření, zda byly zodpovězeny všechny otázky v testu. A následně provádí vyhodnocování všech testů.
- PHP: v porovnání s ostatními jazyky je PHP použito jen v malém rozsahu. Pomocí PHP dochází k ukládání odpovědí uživatelů do souborů ve formátu CSV.

3.1.5 Obrázky a grafika

Při vytváření webové stránky bylo třeba se vypořádat s otázkou užití obrázků a jiných grafických prvků. Jako řešení tohoto problému bylo převážně zvoleno využití volně dostupných obrázků ze serveru pixabay.com, kde jsou obrázky nabízeny pod jejich vlastní autorskoprávní licencí, která umožňuje jejich užití pro nekomerční účely bez uvedení autora.
Seznam těchto obrázků je uveden v závěru práce. Výjimku tvoří několik obrázků z jiných zdrojů, které jsou na webové stránce řádně citovány.

4 Vyhodnocení kurzu

Cílem tohoto výzkumu je vyhodnotit znalosti a efektivitu online vzdělávacího kurzu v oblasti kybernetické bezpečnosti pro zaměstnance veřejné správy.

4.1 Příprava dotazníku

Dotazník, ve formě kybernetického testu, je navržen tak, aby poskytl údaje o znalostech účastníků před zahájením a po dokončení vzdělávacího kurzu. Test zahrnuje několik vybraných otázek, které se zaměřují jak na teorii obsaženou v kurzu, tak i na průzkumné aspekty kybernetické bezpečnosti, pokrývající široké spektrum témat.

Struktura testu je záměrně konzistentní – stejná sada otázek je požita ve vstupním i závěrečném testu. Tento přístup je přesné srovnání výsledků účastníků na začátku a na konci.

4.2 Distribuce a sběr dat

Testy, které tvoří integrální součást kurzu kybernetické bezpečnosti určeného pro veřejnou správu, byly poskytnuty celému pracovišti Finančního úřadu, čítajícího 198 zaměstnanců. Zaměstnanecká struktura tohoto úřadu je charakteristická většinovým zastoupením žen, přičemž věkové rozmezí zaměstnanců se pohybuje od 25 do 65 let.

Z údajů o návratnosti vyplněných testů vyplývá, že vstupní test byl vyplněn celkem 62krát, což představuje zhruba 31% účast. Závěrečný test pak vyplnilo 54 zaměstnanců, což odpovídá zhruba 27% účasti. Tento mírný pokles v počtu vyplněných testů mezi vstupním a závěrečným testem může odrážet různé faktory, včetně ztráty zájmu nebo časových omezení zaměstnanců.

4.3 Vyhodnocení

4.3.1 Dotazníkové šetření

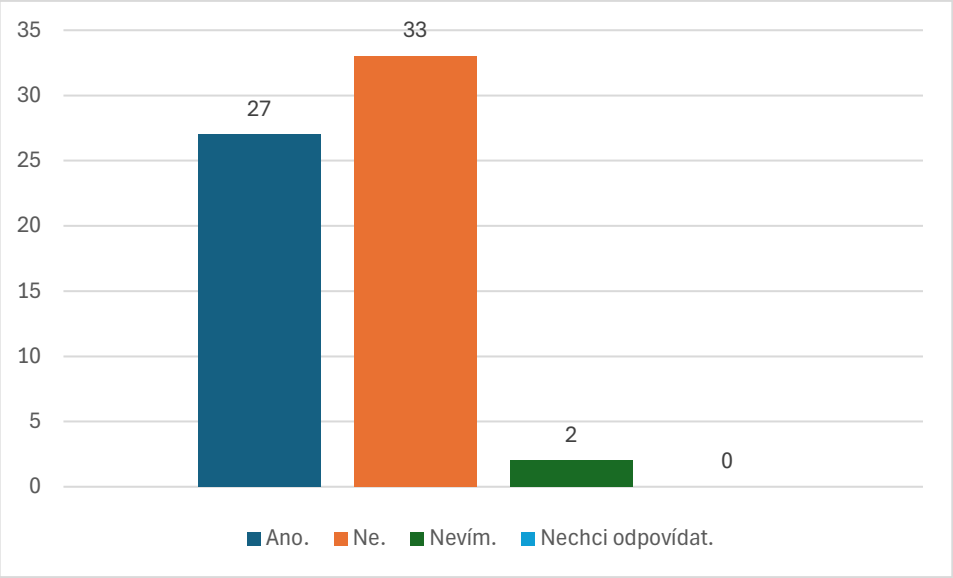
V rámci průzkumu byly shromažďovány informace o dosavadních zkušenostech uživatelů s podvody v kyberprostoru a o preventivních opatřeních, která uživatelé používají k ochraně před potenciálním napadením a ke zmírnění jeho dopadů.

Do testu byly umístěny následující otázky.

Stali jste se už někdy v minulosti obětí kybernetického útoku?

V první otázce byla uživatelům položena otázka, zda se někdy v minulosti stali obětí kybernetického útoku. Dle informací vyplývajících z Grafu 1 se 27 dotázaných již v minulosti stalo obětí nějaké formy kybernetického útoku. Dalších 33 uvedlo, že doposud odolávalo možným útokům a zbylí 2 nedokázali identifikovat, zda se už v minulosti stali obětmi kybernetického útoku.

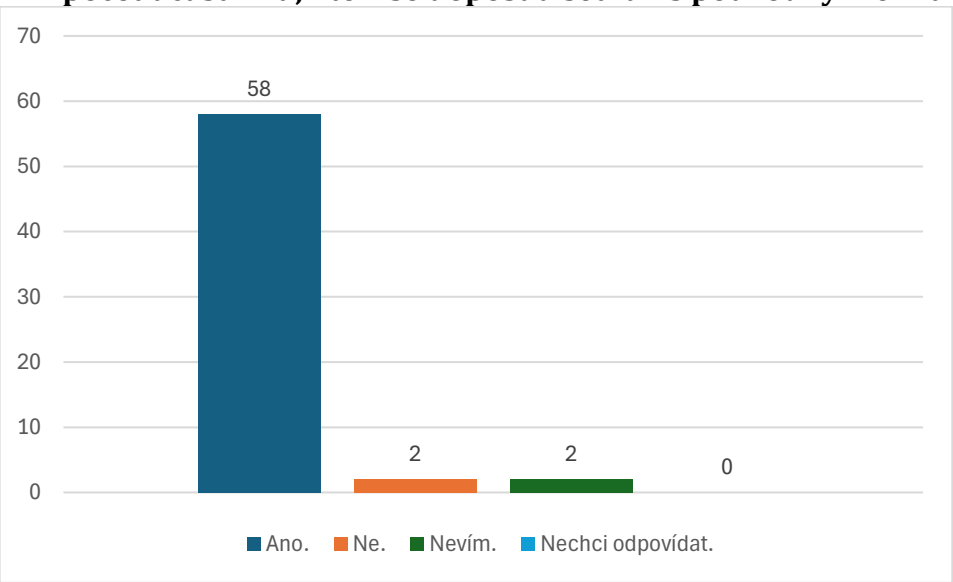
Graf 1 – počet účastníků napadených kybernetickým útokem



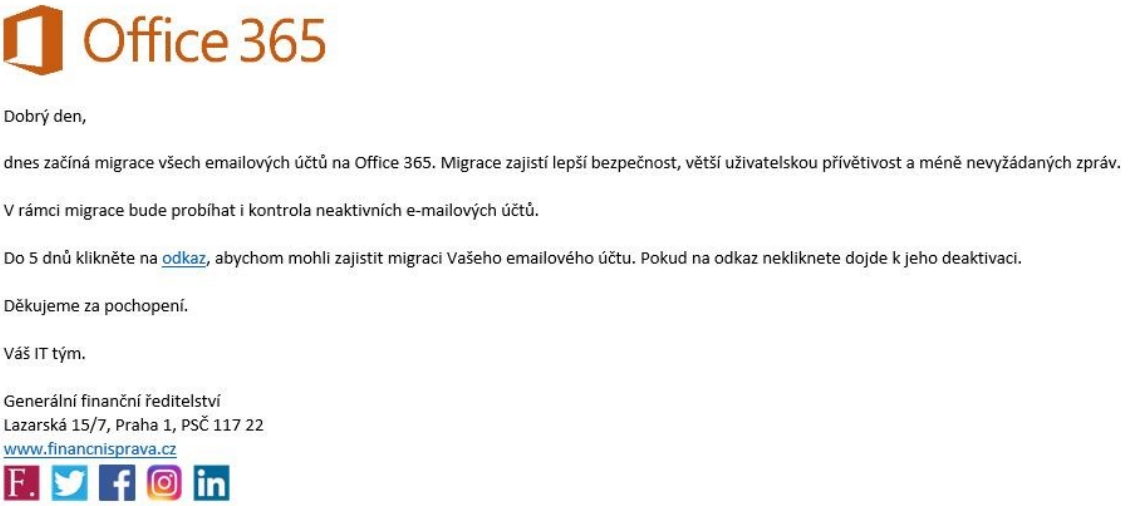
Obdrželi jste někdy podezřelý email?

Další otázka byla zaměřena na zjištění, kolik oslovených respondentů již mělo zkušenost s podvodnými e-maily. Dle výsledků, prezentovaných v grafu, zaznamenala drtivá většina respondentů, celkem 58 osob, v minulosti příjem podvodného e-mailu.

Graf 2 – počet účastníků, kteří se doposud setkali s podvodným e-mailem



Vyhodnotili byste následující email jakožto podvodný?



Office 365

Dobrý den,

dnes začíná migrace všech emailových účtů na Office 365. Migrace zajistí lepší bezpečnost, větší uživatelskou přívětivost a méně nevyžádaných zpráv.

V rámci migrace bude probíhat i kontrola neaktivních e-mailových účtů.

Do 5 dnů klikněte na odkaz, abychom mohli zajistit migraci Vašeho emailového účtu. Pokud na odkaz nekliknete dojde k jeho deaktivaci.

Děkujeme za pochopení.

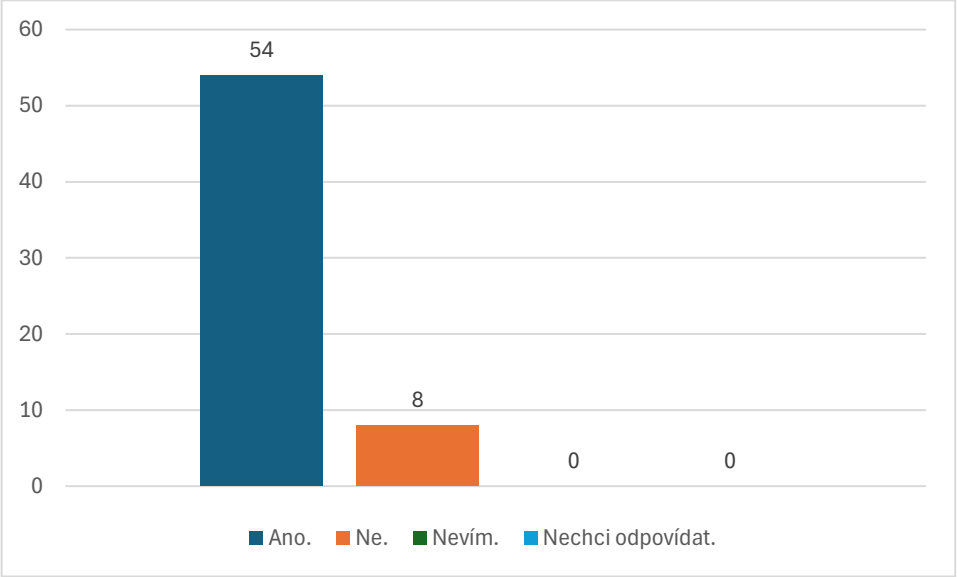
Váš IT tým.

Generální finanční ředitelství
Lazarská 15/7, Praha 1, PSČ 117 22
www.financnisprava.cz

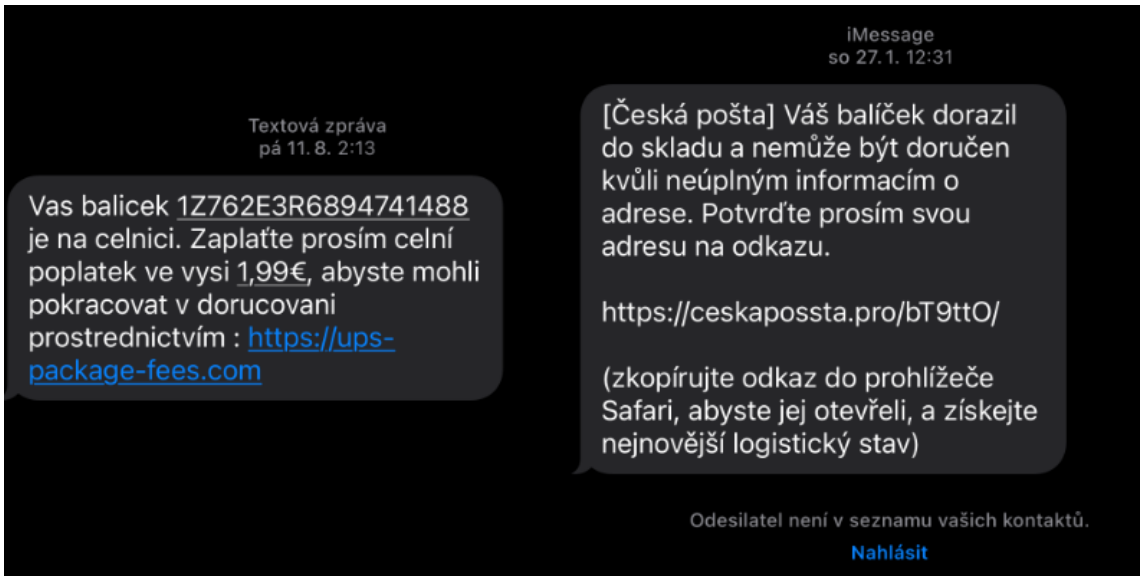
Obrázek 5 – podvodný e-mail.

Průzkum zahrnoval i otázku, zda jsou uživatelé schopni identifikovat podvodný e-mail. Jako referenční materiál pro tuto část průzkumu byl využit konkrétní podvodný e-mail, který se v minulosti šířil mezi zaměstnanci Finanční správy, předložený jako Obrázek 5. Z výsledků, prezentovaných v Grafu 3, je zřejmé, že ačkoli většina oslovených nepodlehla podvodu, existuje stále ta část, která by mohla v případě obdržení podobného e-mailu s potenciálně škodlivým obsahem, kliknout na vložený odkaz, což by mohlo vést k výrazným škodám.

Graf 3 -počet účastníků, kteří vyhodnotili e-mail jakožto podvodný



Vyhodnotili byste tyto SMS jako podvodné?

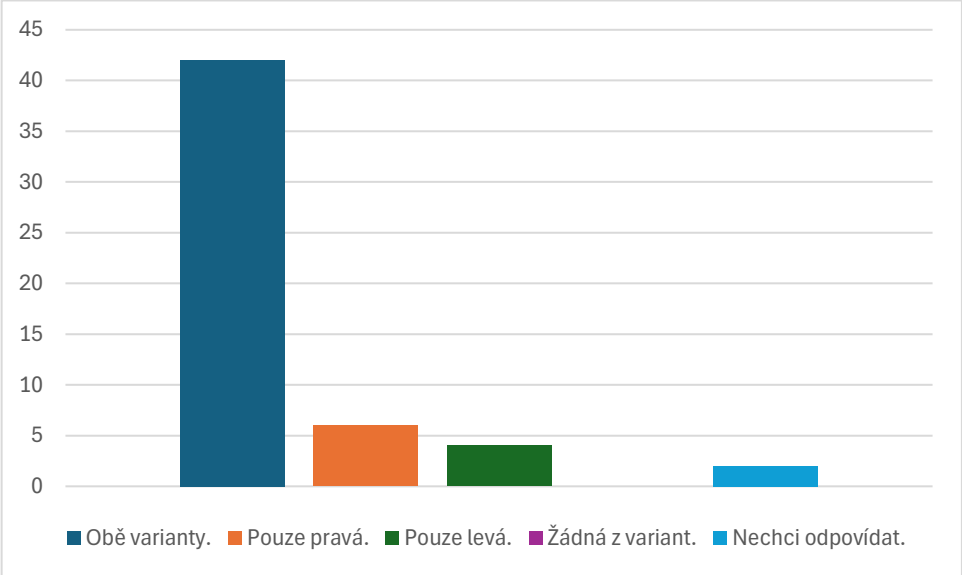


Obrázek 6 – podvodné SMS

Další otázka určená k identifikaci podvodu byla umístěna až na závěru kurzu. Cílem této otázky bylo zjištění, zda jsou respondenti obezřetní i při používání textových zpráv, a to jak na služebních, tak i na soukromých telefonech.

Podle výsledků zaznamenaných v grafu číslo 4 většina oslovených správně identifikovala obě SMS jako podvodné. V deseti případech se respondenti nechali zmást a vybrali pouze jednu z uvedených SMS. Povzbudivější je fakt, že žádný z respondentů nespadl do pasti obou podvodných zpráv, což svědčí o rostoucím povědomí o kybernetických hrozbách mezi účastníky kurzu.

Graf 4 – počet účastníků, kteří vyhodnotili SMS jako podvodné.

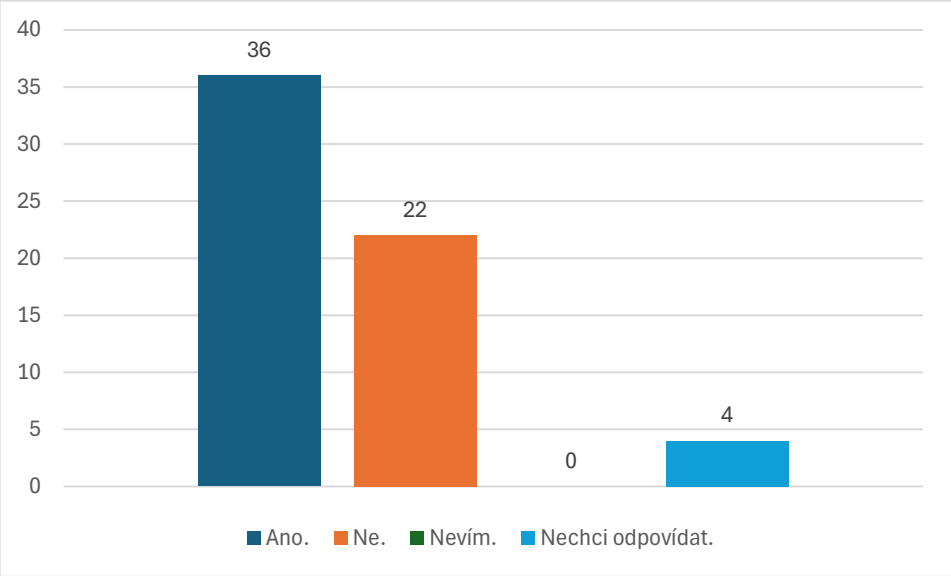


Používáte antivirový program ke skenování stažených souborů z neoficiálních zdrojů?

Jednou z položených otázek byla i ta, zda uživatelé využívají antivirový program k prohlížení souborů, které jsou z externích, potenciálně neznámých zdrojů.

Z přiloženého grafu je zřejmé, že většina účastníků, konkrétně 36 z nich, využívá antivirové programy pro bezpečnostní kontrolu souborů. Nicméně značný počet respondentů, 22 zaměstnanců, takové programy nepoužívá, což může představovat vysoké riziko, zejména pokud dojde ke stažení potenciálně škodlivého souboru. Zbylí 4 se zdrželi odpovědi.

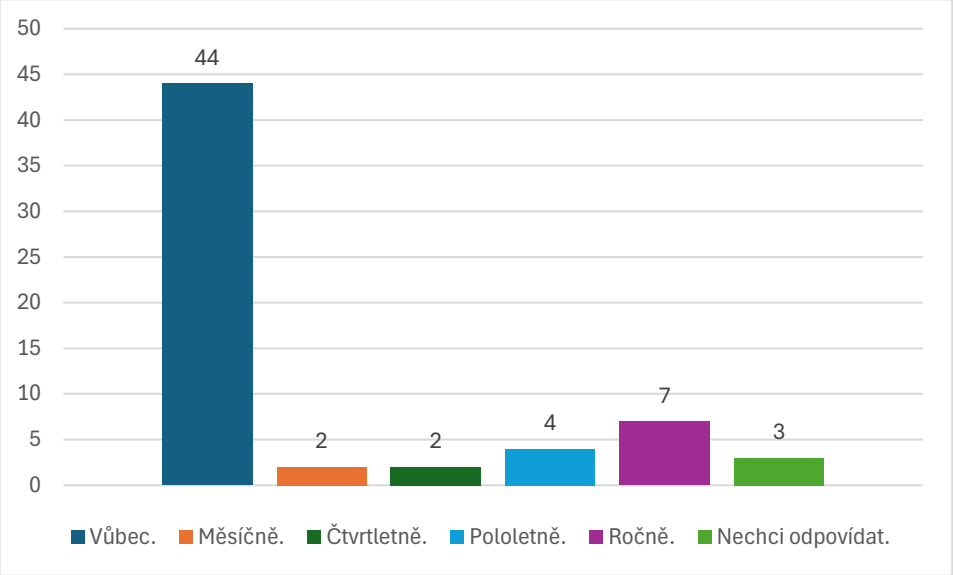
Graf 5 – počet účastníků používající antivirový program ke skenování stažených cizích souborů



Jak často obměňujete svá hesla?

V rámci poslední otázky byli respondenti dotazováni na to, jak často mění svá hesla.
Z grafu je zřejmé, že z dotázaných 44 respondentů si svá hesla vůbec nemění. Z ostatních respondentů si hesla mění: 2 respondenti v intervalu 1–3 měsíců, další dva každé čtvrtletí, čtyři jednou za půl roku a zbývajících 7 alespoň jednou za rok. Tři respondenti na tuto otázku neodpověděli.

Graf 6 – přehled četnosti obměny hesel jednotlivých účastníků



4.3.2 Výsledky vstupního testu

Jak již bylo naznačeno, součástí vstupního a závěrečného testu je skupina vybraných otázek u které je sledována míra zlepšení znalostí po nastudování témat kybernetického kurzu.

Vstupní test a úvodní dotazník vyplnilo celkem 62 respondentů. Odpovídali na základní úvodní otázky a také na specifickou sadu vybraných otázek, které zahrnovaly:

Otázka 1. Jaký termín označuje reklamní e-maily rozesílané ve velkém rozsahu?

Správná odpověď: Spam.

Otázka 2. Z jakého důvodu bychom měli být obezřetní při obdržení podezřelého e-mailu?

Správná odpověď: U neznámých odesilatelů nemůžeme jasně říct, s jakým záměrem byl e-mail odeslán.

Otázka 3. Jak se správně zachovat, pokud je počítač zasažen virem?

Správná odpověď: Vypnout počítač a vyhledat odbornou pomoc.

Otázka 4. Vyberte správné tvrzení:

Správná odpověď: Je doporučeno stahovat aplikace pouze z oficiálních obchodů.

Otázka 5. Jaký je doporučený interval pro obměnu hesel?

Správná odpověď: Nejdéle každých 18 měsíců.

Otázka 6. Víte, jaká je minimální délka hesla, aby splňovala zásady bezpečného hesla?

Správná odpověď: 12

Otázka 7. Víte, co označuje tzv. Politika čistého stolu?

Správná odpověď: Bezpečnostní zásady ohledně nakládání s citlivými informacemi.

Otázky číslo 8 až 10 jsou koncipovány jako otázky s více správnými odpověďmi, kde účastníci mají možnost zvolit více než jednu odpověď.

Otázka 8. Které osvědčené postupy mohou pomoci proti útokům sociálního inženýrství?

Správné odpovědi:

- Používání dvoufázové ochrany.
- Vzdělávání a informování zaměstnanců o aktuálních dění v kybernetickém prostoru.
- Neklikat na podezřele vypadající odkazy.

Otázka 9. Jaké zásady je třeba dodržet pro ochranu počítače?

Správné odpovědi:

- Neodkládat aktualizace.

Otázka 10. Víte, jaké postupy pomáhají snížit riziko úspěšného kybernetického útoku na veřejnosti?

Správné odpovědi:

- Používání mobilních dat.
- Zapínat wifi pouze pokud je potřeba internetové připojení.
- Udržovat software vždy aktualizovaný.

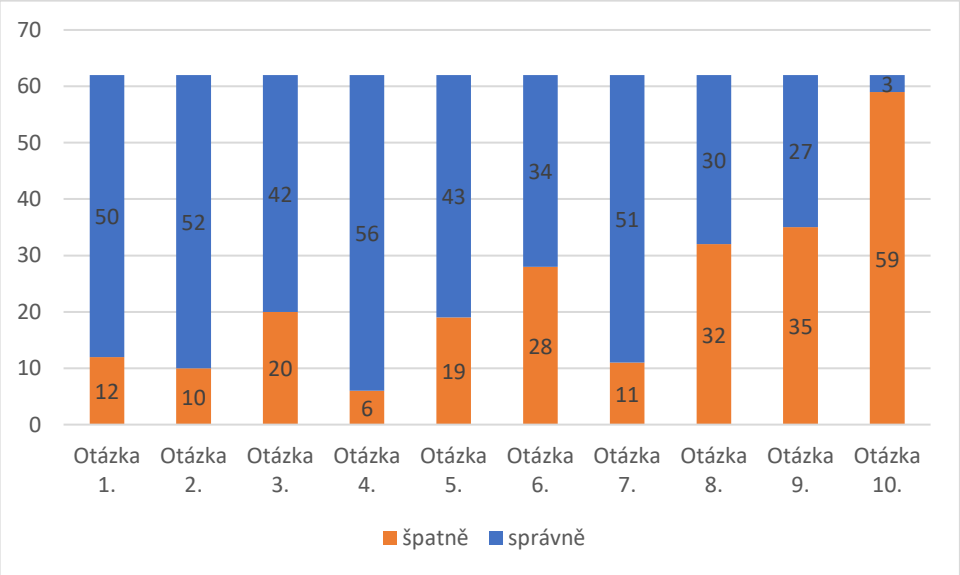
V následujícím grafu je zpracovaný poměr správnosti odpovědí všech respondentů na výše uvedené otázky.

Z Grafu 6 je patrné, že chybovost odpovědí v úvodních otázkách je nízká. Výrazný pokles v počtu správných odpovědí je zaznamenán u otázek číslo 3 a 6. Z 20 respondentů, kteří chybně odpověděli na otázku č. 3, by se 19 z nich v případě nákazy pokusilo samostatně identifikovat a odstranit zdroj infekce za použití antivirového programu, což v organizačním prostředí není vhodný postup. U otázky č. 6, která se týká minimální délky

hesla, je znepokojivé, že z 28 respondentů, kteří odpověděli chybně na otázku č. 6, si 9 z nich myslí, že délka hesla nemá význam v prevenci proti prolomení hesel.

Další výrazný pokles ve správných odpovědích je patrný u otázek s více možnostmi výběru.

Graf 7 – vyhodnocení správnosti odpovědí ze vstupního testu

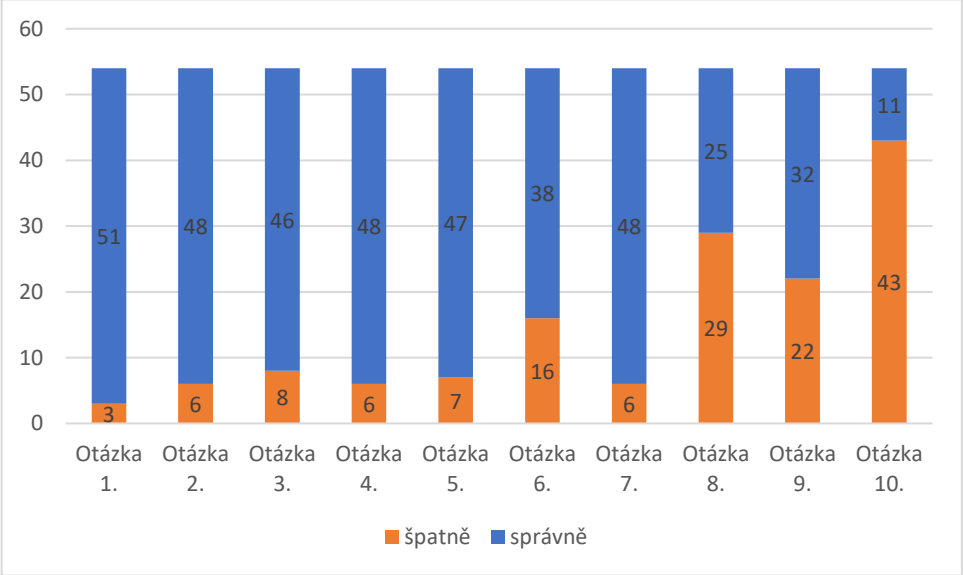


4.3.3 Výsledky závěrečného testu

Jak je na první pohled patrné, díky nastudování materiálů umístěných v kurzu kyber došlo ke snížení chybných odpovědí u vytypované sady otázek určené ke sledování progresu uživatelských znalostí.

Otázka číslo 9 zaznamenala největší zlepšení ve výsledcích, s 13 respondenty navíc, kteří na ni odpověděli správně ve srovnání se vstupním testem.

Graf 8 – vyhodnocení správnosti odpovědí ze závěrečného testu

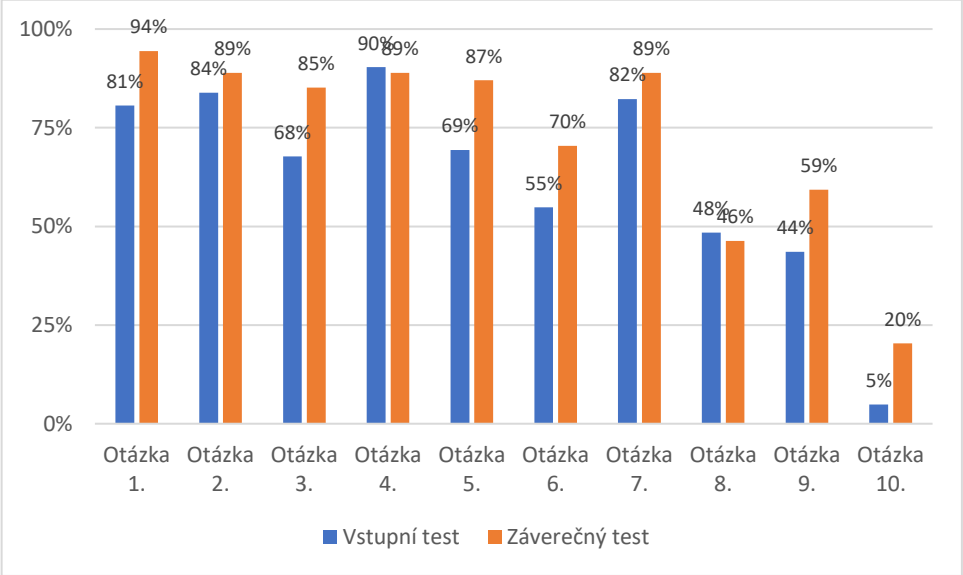


4.3.4 Porovnání úspěšnosti

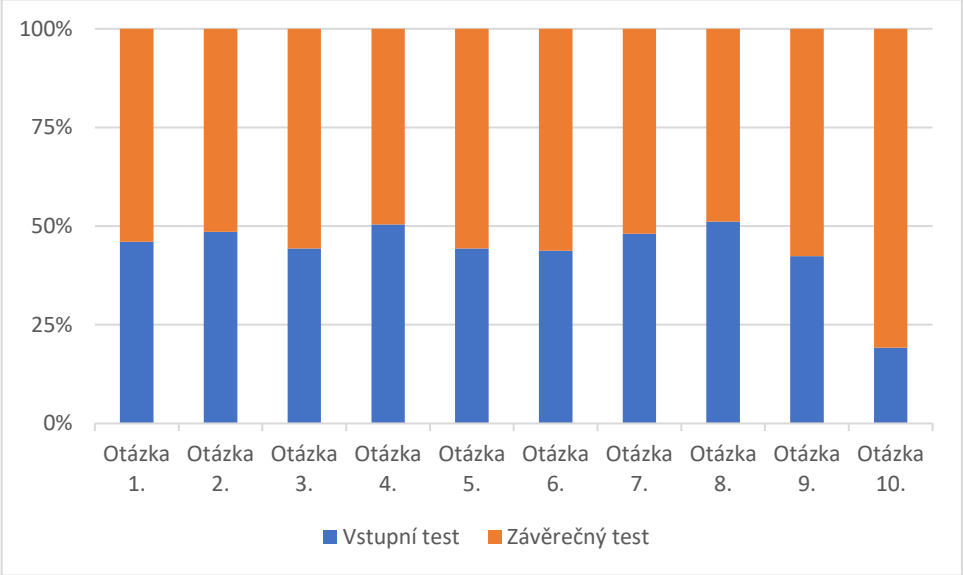
Ve závěrečné části se detailně věnujeme hodnocení zlepšení skupiny respondentů mezi vstupním a závěrečným testem. Pro vyhodnocení efektivity kurzu jsou sledovány procentuální míry správných odpovědí u jednotlivých sledovaných otázek.

Po absolvování kurzu došlo k pozoruhodnému zlepšení ve většině sledovaných otázek. Výjimku představují otázky 4 a 8, kde jsme zaznamenali mírný pokles ve správných odpovědích.

Graf 9 – porovnání správnosti odpovědí vstupního a závěrečného testu



Graf 10 – procentuální poměr zlepšení mezi jednotlivými testy



5 Závěry a doporučení

Z výsledků kvantitativního výzkumu prostřednictvím dotazníků vyplněných zaměstnanci Finančního úřadu vyplynulo, že přestože se většina dotázaných již setkala s nějakou formou kybernetického útoku, existuje stále významný prostor pro zlepšení v oblasti osobní kybernetické bezpečnosti. Překvapivě vysoký počet zaměstnanců nevyužívá antivirové programy a velká část z nich si také pravidelně nemění hesla, což naznačuje značné riziko v oblasti ochrany citlivých dat a osobních údajů. Zároveň je více než povzbudivé, že většina zaměstnanců v případě obdržení podvodného e-mailu či SMS, dokáže na první pohled identifikovat podvod.

Závěrečné vyhodnocení kurzu odhalilo zlepšení ve vědomostech zaměstnanců ve veřejné správě, přičemž výrazný pokrok byl patrný v lepším rozpoznání kybernetických hrozeb a lepší aplikaci bezpečnostních opatření. Z toho plyne, že kontinuální vzdělávání a zvyšování povědomí o kybernetické bezpečnosti je klíčové pro ochranu osobních a institucionálních dat v digitálním světě.

Závěrem je nutné zdůraznit, že v dynamicky se vyvíjejícím kybernetickém prostředí je neustálé vzdělávání a aktualizace znalostí v oblasti kybernetické bezpečnosti klíčové.

Tato práce položila základy pro další rozvoj a adaptaci vzdělávacího kurzu, jenž by měl odrážet nejnovější trendy v kybernetické bezpečnosti a pružně reagovat na měnící se potřeby a výzvy digitálního světa.

Seznam použité literatury

1. ČESKO. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: Zákony pro lidi.cz [online]. © AION CS 2010–2024 [cit. 15. 1. 2024]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82
2. *Průvodce řízením aktiv a rizik dle VKB* [online]. 1. NÚKIB, 2022 [cit. 2023-12-17]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/
3. KOLOUCH, Jan, Pavel BAŠTA, Andrea KROPÁČOVÁ a Martin KUNC. *CYBERSECURITY*. Praha: CZ.NIC, z. s. p. o., 2019. ISBN 978-80-88168-34-8.
4. *Bezpečnostní role a jejich začlenění v organizaci*. Online. V3.1. NÚKIB, 2023. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/. [cit. 2023-12-19].
5. *Minimální bezpečnostní standard*. Online. V1.2. NÚKIB, 2023. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/. [cit. 2023-12-19].
6. *Řízení dodavatelů*. Online. 2.0. NÚKIB, 2023. Dostupné z: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/. [cit. 2023-12-20].
7. ČESKO. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In: Zákony pro lidi.cz [online]. © AION CS 2010–2024 [cit. 15. 1. 2024]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528
8. SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8
9. *5 Benefits to Having a Clean Desk Policy*. Online. 2023, 2023-01-29. Dostupné z: https://www.privacysense.net/clean-desk-policy/. [cit. 2024-01-24].
10. *Generátor náhodných hesel* [online]. 2024 [cit. 2024-01-16]. Dostupné z: https://www.avast.com/cs-cz/random-password-generator#pc

11. *How Secure Is My Password?* Online. 2024. Dostupné z: https://www.security.org/how-secure-is-my-password/. [cit. 2024-03-30].
12. MCCLURE, Stuart; SCAMBRAY, Joel a KURTZ, George. *Hacking bez záhad*. Praha: Grada, 2007. ISBN 978-80-247-1502-5.
13. *KeePass Password Safe*. Online. 2024. Dostupné z: https://keepass.info/. [cit. 2024-03-30].
14. Wikipedia contributors*:* Firewall (computing) [online]. c2023 [citováno 17. 01. 2024]. Dostupný z WWW: <https://en.wikipedia.org/w/index.php?title=Firewall_(computing)&oldid=1191613587>
15. *What is Firewall?* Online. 2024. Dostupné z: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/. [cit. 2024-01-17].
16. *What is Antivirus*. Online. 2024. Dostupné z: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-antivirus/. [cit. 2024-01-17].
17. *Co je to antivirus*. Online. 2024. Dostupné z: https://www.eset.com/cz/antivirus-software/. [cit. 2024-01-17].
18. *What is Patch Managment?* Online. 2024. Dostupné z: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-patch-management/. [cit. 2024-01-17].
19. *What is Backup? (Data Backup) Comprehensive Guide*. Online. 2023, 2023-07-17. Dostupné z: https://www.acronis.com/en-us/blog/posts/data-backup/. [cit. 2024-01-17].
20. Co je to malware? Online. 2024. Dostupné z: https://www.avast.com/cs-cz/c-malware. [cit. 2024-01-17].
21. Trojský kůň. Online. 2024. Dostupné z: https://www.eset.com/cz/trojsky-kun/. [cit. 2024-01-17].
22. *The Essential Guide to Ransomware*. Online. 2023, 2023.10.11. Dostupné z: https://www.avast.com/c-what-is-ransomware. [cit. 2024-01-17].
23. *Co je Spyware a jak ho spolehlivě odstranit?* Online. 2024. Dostupné z: https://www.eset.com/cz/spyware/. [cit. 2024-01-17].
24. *Počítačový červ*. Online. 2024. Dostupné z: https://www.avast.com/cs-cz/c-computer-worm. [cit. 2024-01-17].

25. *Co je počítačový virus?* Online. 2024. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus. [cit. 2024-01-17].
26. *What is Phishing?* Online. 2024. Dostupné z: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/. [cit. 2024-01-18].
27. *Počítačová kriminalita*. Online. 2024. Dostupné z: https://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx. [cit. 2024-01-18].
28. *Podvody, které zrovna letí*. Online. 2024. Dostupné z: https://www.airbank.cz/co-vas-nejvic-zajima/podvody-ktere-zrovna-leti/. [cit. 2024-01-18].
29. *CyberCrime*. CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8.
30. *Whaling ve 3 bodech*. Online. 2021, 2021-11-11. Dostupné z: https://www.whalebone.io/post/whaling-ve-3-bodech-co-to-je-proc-to-funguje-a-jak-se-uchranit. [cit. 2024-01-18].
31. *Co je to spam? Jak se zbavit spamu?* Online. 2024. Dostupné z: https://www.eset.com/cz/spam/. [cit. 2024-01-18].
32. *Co je scam?* Online. 2024. Dostupné z: https://www.eset.com/cz/scam/. [cit. 2024-01-18].
33. *Hoax*. Online. 2024. Dostupné z: https://www.hoax.cz/hoax/. [cit. 2024-01-18].
34. *What Are the Risks of Clicking on Malicious Links?* Online. 2023, 2023-11-3. Dostupné z: https://www.mcafee.com/blogs/internet-security/what-are-the-risks-of-clicking-on-malicious-links/. [cit. 2024-01-18].
35. *Stav webu*. Online. 2024. Dostupné z: https://transparencyreport.google.com/safe-browsing/search. [cit. 2024-01-18].
36. *Don't Click On These 5 Dangerous Email Attachments*. Online. 2021, 2021-1-16. Dostupné z: https://www.forbes.com/sites/barrycollins/2021/01/16/dont-click-on-these-5-dangerous-email-attachments/. [cit. 2024-01-19].
37. *Ochrana před viry v makrech*. Online. 2024. Dostupné z: https://support.microsoft.com/cs-cz/office/ochrana-p%C5%99ed-viry-v-makrech-a3f3576a-bfef-4d25-84dc-70d18bde5903. [cit. 2024-01-19].

38. *What is Fileless Malware?* Online. 2024. Dostupné z: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/what-is-fileless-malware/. [cit. 2024-01-19].
39. *Nové nebezpečné přípony souborů*. Online. 2018, 2801-07-19. Dostupné z: https://www.antivirovecentrum.cz/aktuality/nove-nebezpecne-pripony-souboru.aspx. [cit. 2024-01-19].
40. *Metodický pokyn k elektronickým podpisům a pečetím pro VP*. Online. V2. Ing. Roman Vrba, 2019. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/informace-pro-uzivatele/metodicky-pokyn-k-elektronickym-podpisum-a-pecetim-pro-verejnopravni-puvodce/. [cit. 2024-01-24].
41. *What is an e-signature*. Online. 2023. Dostupné z: https://www.techtarget.com/searchcontentmanagement/definition/e-signature. [cit. 2024-01-24].
42. NAVARA, David. *Elektronický podpis prostý*. Online. 2021, 2021.03.10. Dostupné z: https://www.elektronicky-podpis.info/pojmy/elektronicky-podpis-prosty.dot. [cit. 2024-01-24].
43. *Požadavky na zaručený a uznávaný elektronický podpis*. Online. 2024. Dostupné z: https://www.ica.cz/zaruceny-a-uznavany-ep. [cit. 2024-01-24].
44. *Kvalifikované certifikáty*. Online. 2024. Dostupné z: https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/kvalifikovane-certifikaty. [cit. 2024-01-24].
45. *Seznam důvěryhodných certifikační autorit ke komunikaci s CS OTE*. Online. 2023, 2023-06. Dostupné z: https://www.ote-cr.cz/cs/registrace-a-smlouvy/pristup-do-cs-ote/seznam-povolenych-certifikacnich-autorit-ke-komunikaci-s-cs-ote. [cit. 2024-01-24].
46. *Cyber Security Wi-Fi Attacks* [online]. 2024 [cit. 2024-01-24]. Dostupné z: https://www.w3schools.com/cybersecurity/cybersecurity_wifi_attacks.php
47. *Jak bezpečně používat veřejné Wi-Fi sítě*. Online. 2022, 2022-06-09. Dostupné z: https://nordictelecom.cz/novinky/32/. [cit. 2024-01-24].

48. *What is SSL Inspection?* Online. 2024. Dostupné z: https://www.checkpoint.com/cyber-hub/network-security/what-is-ssl-inspection/. [cit. 2024-01-24].
49. *Comparing Cellular and Wi-Fi*. Online. 2023, 2023-07-14. Dostupné z: https://www.boltontechnical.co.za/blogs/news/comparing-cellular-and-wi-fi-assessing-the-security-of-cellular-data. [cit. 2024-01-24].
50. *What is WPA2?* Online. 2022, 2022-05-10. Dostupné z: https://www.avg.com/en/signal/what-is-wpa2. [cit. 2024-01-24].
51. *Co je to WPA3?* Online. 2021, 2021-21-30. Dostupné z: https://www.asus.com/cz/support/FAQ/1042478/. [cit. 2024-01-24].
52. *Jak (a proč) nastavit VPN ještě dnes - 1. díl*. Online. 2023, 2023-03-22. Dostupné z: https://www.pcworld.cz/clanky/jak-a-proc-nastavit-vpn-jeste-dnes-1-dil/. [cit. 2024-01-24].
53. *Benefits of a Virtual Private Network (VPN)*. Online. 2024. Dostupné z: https://www.checkpoint.com/cyber-hub/network-security/what-is-vpn/benefits-of-a-virtual-private-network-vpn/. [cit. 2024-01-24].
54. *VPN Security - How Secure is a VPN?* Online. 2024. Dostupné z: https://www.checkpoint.com/cyber-hub/network-security/what-is-vpn/how-does-a-vpn-work/vpn-security-how-secure-is-a-vpn/. [cit. 2024-01-24].

Seznam obrázků

Seznam obrázků použitých ve webové stránce

- Word-document-document-text. Online. 2024. Dostupné z: https://pixabay.com/vectors/word-document-document-text-150594/. [cit. 2024-03-29].
- Mobile-phone-pin-lock-transparent. Online. 2024. Dostupné z: https://pixabay.com/illustrations/mobile-phone-pin-lock-transparent-3647803/. [cit. 2024-03-29].
- To-hack-fraud-map-code-computer. Online. 2024. Dostupné z: https://pixabay.com/vectors/to-hack-fraud-map-code-computer-7109362/. [cit. 2024-03-29].
- Cyber-security-word-computer-cloud. Online. 2024. Dostupné z: https://pixabay.com/vectors/cyber-security-word-computer-cloud-2120014/. [cit. 2024-03-29].
- Mask-anonymous-face-disguise. Online. 2024. Dostupné z: https://pixabay.com/vectors/mask-anonymous-face-disguise-1587566/. [cit. 2024-03-29].
- Key-lock-icon-set-. Online. 2024. Dostupné z: https://www.freevector.com/key-lock-icon-set-19822. [cit. 2024-03-29].
- Security-surveillance-camera. Online. 2024. Dostupné z: https://pixabay.com/vectors/security-surveillance-camera-3800514/. [cit. 2024-03-29].

- Avatar-flat-modern-minimal. Online. 2024. Dostupné z: https://pixabay.com/vectors/avatar-flat-modern-minimal-5261902/. [cit. 2024-03-29].
- Phone-security-mobile-smartphone. Online. 2024. Dostupné z: https://pixabay.com/vectors/phone-security-mobile-smartphone-1537387/. [cit. 2024-03-29].
- Warning-alert-detected-malware. Online. 2024. Dostupné z: https://pixabay.com/vectors/warning-alert-detected-malware-2168379/. [cit. 2024-03-29].
- Phishing e-mail. Online. In: Phishing: Jak jej včas rozpoznat a „nenaletět“. 2015, 2015-09-05. Dostupné z: https://csirt.cz/public/media/1576047273/80/. [cit. 2024-01-18].
- Phishing: Jak jej včas rozpoznat a „nenaletět“. Online. 2015. Dostupné z: https://csirt.cz/cs/kyberbezpecnost/pro-uzivatele/phishing-jak-jej-vcas-rozpoznat-a-nenaletet/. [cit. 2024-03-30].
- Smishing. Online. In: Podvody, které zrovna letí. 2024. Dostupné z: https://www.airbank.cz/data/wysiwyg/poradna/sms-phishing-01.png. [cit. 2024-01-18].
- Wifi-internet-technology-coffee. Online. 2024. Dostupné z: https://pixabay.com/vectors/wifi-internet-technology-coffee-8401111/. [cit. 2024-03-29].
- Certifikát kurzu Kybernetického zabezpečení. Pro vytvoření byla použita AI ChatGPT 4.
- Podoba zobrazení aktivního HTTPS v prohlížeči Safari. Zdroj: vlastní tvorba
- Pravděpodobný podvod. Zdroj: vlastní tvorba
- Podezřelý e-mail. Zdroj: vlastní tvorba
- Zobrazení skrytých přípon u souborů. Zdroj: vlastní tvorba
- Ověření podezřelého odkazu podle google.com. Zdroj: vlastní tvorba

Seznam tabulek

Seznam grafů

Přílohy

U každé přílohy musí být v pravém horním rohu uvedeno číslo přílohy (např. Příloha č. 4). Přílohou bakalářské/diplomové může být i datové médium (CD, DVD, …), které je nutné vložit do vhodné obálky připevněné k zadní desce práce a popsat také jako přílohu v textu. Také v přílohách musí být korektně citovány použité zdroje informací. Digitální přílohy v podobě softwarových projektů mohou být také přiloženy formou odkazu na příslušný cloudový repositář projektu (Github, Gitlab apod.).

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2022/2023

Studijní program: Informační management
Forma studia: Kombinovaná

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení:	**Matěj Hubálek**
Osobní číslo:	**I2100127**
Adresa:	Kostěnice 123, Kostěnice, 53002 Pardubice 2, Česká republika
Téma práce:	Online kurz základů kybernetické bezpečnosti pro veřejnou správu
Téma práce anglicky:	Online cyber security fundamentals course for public administration
Jazyk práce:	Čeština
Vedoucí práce:	doc. Mgr. Josef Horálek, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

Cílem práce je vytvořit webový kurz základů kybernetické bezpečnosti pro zaměstnance veřejné správy. V teoretické části práce autor provede výzkum v oblasti znalosti kybernetické bezpečnosti ve veřejném sektoru, na jehož základě stanoví obsah kurzu s přihlédnutím k aktuálně platné legislativě. V praktické části pak autor vytvoří webový portál s kurzem základů kybernetické bezpečnosti zaměřenou a potřeby veřejné správy.

Seznam doporučené literatury:

STEINBERG, Joseph. Cybersecurity for dummies. 2nd Edition. Hoboken, NJ : For Dummies [2022]. ©2022. xix, 386 stran. ISBN 978-1-119-86718-0.
MCCLURE, Stuart – SCAMBRAY, Joel – KURTZ, George. Hacking bez záhad. 1. vyd. Praha : Grada, 2007. 520 s. ISBN 978-80-247-1502-5.
JIROVSKÝ, Václav. Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha : Grada, 2007. 284 s. Dostupné na internetu: <http://toc.nkp.cz/NKC/200801/contents/nkc20071751477_1.pdf> ISBN 978-80-247-1561-2.
SMEJKAL, Vladimír – SOKOL, Tomáš – KODL, Jindřich. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2019. 378 stran. ISBN 978-80-7380-765-8.

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: