ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ
KATEDRA VÝPOČETNÍ A DIDAKTICKÉ TECHNIKY

PROBLEMATIKA POČÍTAČOVÉ BEZPEČNOSTI VE ZVOLENÉ JEDNOTCE INTEGROVANÉHO ZÁCHRANNÉHO SYSTÉMU

BAKALÁŘSKÁ PRÁCE

Jaroslav Jílek, DiS.
Přírodovědná studia, obor Informatika se zaměřením na vzdělávání

Vedoucí práce: Mgr. Jan Bezděka

Plzeň 2022

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, 27. dubna 2022

.....

vlastnoruční podpis

PODĚKOVÁNÍ.

Rád bych poděkoval vedoucímu práce, panu Mgr. Janu Bezděkovi, za rady, podnětné připomínky a vedení při zpracování této práce. Dále děkuji celému oddělení KIS HZS Pk za pomoc a cenné rady při volbě tématu zadání práce a při jeho realizaci. V neposlední řadě jsem vděčný své rodině a přátelům za jejich podporu.

OBSAH

SEZNAM ZKRATEK 5
ÚVOD 7
1 TEORETICKÁ ČÁST 9
1.1 DEFINICE KYBERNETICKÉHO ÚTOKU 9
1.2 POTŘEBA KYBERNETICKÉ BEZPEČNOSTI 9
1.3 HASIČSKÝ ZÁCHRANNÝ SBOR 10
1.3.1 Postavení a úkoly hasičského záchranného sboru 10
1.3.2 Stručná historie a vznik HZS ČR 10
1.3.3 Příslušník hasičského záchranného sboru a zaměstnanec 11
1.4 LEGISLATIVA KYBERNETICKÉ BEZPEČNOSTI 12
1.4.1 Zákon č. 181/2014 Sb. 12
1.4.2 Vyhláška č. 316/2014 Sb. 13
1.4.3 Vyhláška č. 82/2018 Sb. 13
1.4.4 Vyhláška č. 317/2014 Sb. 14
1.4.5 Legislativa o kybernetické bezpečnosti vztahující se k hzs čr 14
1.5 NEJČASTĚJŠÍ KYBERNETICKÉ HROZBY 14
1.5.1 Botnet 14
1.5.2 Malware 15
1.5.3 Spam 17
1.6 VŠEOBECNÉ BEZPEČNOSTNÍ ZÁSADY 18
2 PRAKTICKÁ ČÁST 21
2.1 PODMÍNKY PRO UŽÍVÁNÍ ICT U SLOŽKY HZS ČR 21
2.2 ZÁSADY KYBERNETICKÉ BEZPEČNOSTI U SLOŽKY HZS PK 21
2.3 DEFINICE CÍLOVÉ SKUPINY 24
2.4 VSTUPNÍ OVĚŘENÍ 25
2.5 ZHODNOCENÍ VSTUPNÍHO OVĚŘENÍ 25
2.5.1 Písemný test ze základů digitální gramotnosti a bezpečnosti 25
2.5.2 Analýza a vyhodnocení výsledků písemného testu 36
2.5.3 Druhá část vstupního ověření 37
2.5.4 Analýza a vyhodnocení výsledků rozeslaného e-mailu 41
2.6 TVORBA A REALIZACE ŠKOLÍCÍHO VÝUKOVÉHO MATERIÁLU 43
2.7 APLIKACE VYTVOŘENÉHO ŠKOLÍCÍHO A VÝUKOVÉHO MATERIÁLU 45
2.8 VYHODNOCENÍ APLIKACE A DOPADU VÝUKOVÉHO MATERIÁLU NA CÍLOVOU SKUPINU 46
2.8.1 Zhodnocení úspěšnosti otázek zkušebního písemného testu při jeho prvotním a opakovaném zadání 47
ZÁVĚR 49
RESUMÉ 51
RESUME 52
SEZNAM LITERATURY 54
SEZNAM OBRÁZKŮ 55
PŘÍLOHY I
OTÁZKY PÍSEMNÉHO TESTU I
VÝSLEDKY OPĚTOVNÉHO ZADÁNÍ PÍSEMNÉHO TESTU VII

SEZNAM ZKRATEK

ICT	Informační a komunikační technologie, z anglického Information and Communication Technologies
IZS	Integrovaný záchranný systém[1]
ČR	Česká republika
HZS ČR	Hasičský záchranný sbor ČR[2]
HZS Pk	Hasičský záchranný sbor Plzeňského kraje
KOPIS Pk	Krajské operační a informační středisko HZS ČR, Plzeňského kraje
KIS HZS Pk	Komunikační a informační systémy HZS Pk
SaP	Síly a prostředky
Shareware	software, který je možno za určitých podmínek stanovených v licenčním ujednání užívat bezúplatně
Peer to peer	doslovný překlad rovný s rovným, P2P nebo klient-klient je označení typu počítačových sítí, ve které spolu komunikují přímo jednotliví klienti (uživatelé)
ActiveX	technologie, kterou vyvinula společnost Microsoft pro sdílení informací mezi různými aplikacemi
CVC kód	z anglických slov Card Verification Code, bezpečnostní kód používaný u debetních platebních karet pro ověření online plateb
HTTPS	zkratka anglických slov Hypertext Transfer Protocol Secure, je to protokol umožňující zabezpečenou komunikaci v počítačové síti
MV ČR	Ministerstvo vnitra České republiky
PIN	zkratka anglických slov personal identification number, tedy osobní identifikační číslo, jde o unikátní číselný kód, kterým se ověřuje a autorizuje osoba

[1] Zákon č. 239/2000 Sb.
[2] Zákon č. 320/2015 Sb.

ID	překlad anglického slova identification, česky znamenající identifikace, označuje identitu, kterou si každý uživatel vytváří v různých zařízeních
E-podpis	elektronický podpis, nástroj pro identifikaci a autentizaci v prostředí internetu
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
End-to-end	koncové šifrování, při kterém je přenos dat zajištěn proti odposlechu správcem komunikačního kanálu i správcem serveru
VPN	virtuální soukromá síť, z anglického překladu Virtual Private Network, je zabezpečené šifrované připojení mezi dvěma sítěmi nebo mezi konkrétním uživatelem a sítí

ÚVOD

Žijeme v době a v takové společnosti, kde se moderní technologie staly nedílnou součástí našeho života. S používáním a rozšířením počítačů, internetu, či chytrých domácností rostou i počty jejich zneužití. Tyto technologie využíváme ke každodenní potřebě, ať je to v zaměstnání, pro komunikaci nebo např. online nákupy. Proto musí být na bezpečnost a ochranu dat na všech úrovních kladen velký důraz.

Vynalézavost útočníků se neustále vyvíjí a vzrůstá, objevují se nové druhy útoků a infiltrací. Ve světle tohoto se o zabezpečení dat a počítačů nemohou starat jen ICT oddělení firem a organizací, ale základní odpovědnost a povědomí musí mít i běžní uživatelé. Ti by měli znát a dodržovat byť i základní pravidla kybernetické bezpečnosti.

Dílčím cílem této bakalářské práce je vymezit oblast a cílovou skupinu běžných uživatelů v základní složce IZS ČR, konkrétně u HZS Pk, kterým se v rámci počítačové bezpečnosti bude dále věnovat. Zadáním vstupního testu bude zjištěna úroveň digitální gramotnosti a její následné zhodnocení. Na základě výsledků bude zpracována analýza, ze které vzejde v jaké formě a rozsahu je potřeba vypracovat školící materiál pro zlepšení znalostí cílové skupiny. Tímto bude dosaženo hlavního cíle této bakalářské práce, kterým je vytvoření konkretizovaného výukového materiálu, určeného specificky pro složku HZS Pk. Po aplikaci konkrétně zpracovaného školícího materiálu bude znovu otestována úroveň digitální gramotnosti, a tím zhodnocen dopad výukového materiálu na cílovou skupinu.

V teoretické části bude vymezen pojem kybernetického útoku, potřeba kybernetické bezpečnosti a popsána vybraná základní složka IZS ČR s cílovou skupinou uživatelů. Dále zde bude uveden základní právní rámec počítačové bezpečnosti, nejčastější kybernetické útoky a všeobecné bezpečnostní zásady.

V praktické části budou upřesněny zásady a podmínky používání ICT prostředků u složky HZS Pk. Pomocí dvojúrovňového ověření, skládajícího se z písemného testu a rozeslaného e-mailu s nedůvěryhodným odkazem, bude analyzována a popsaná vstupní úroveň ve zvolené oblasti počítačové bezpečnosti uživatelů z cílové skupiny. Dále bude zpracován školící materiál, kladoucí zvýšený důraz na slabé oblasti uživatelských znalostí a specifické podmínky ve složce HZS Pk. Motivací pro vznik výukového materiálu je zlepšení úrovně znalostí ve zmíněných oblastech.

Na závěr bude pomocí opětovného zadání dvojúrovňového ověření otestován dopad aplikace vytvořeného školícího materiálu na cílovou skupinu a vyhodnoceny dosažené výsledky.

Bakalářská práce bude vznikat v přislíbené a úzké spolupráci s oddělením KIS HZS Pk. Vzniklý výukový materiál bude proto autorem práce bezplatně poskytnut pro další potřeby HZS Pk a bude součástí pravidelné odborné přípravy v oblasti digitální gramotnosti a bezpečnosti.

1 TEORETICKÁ ČÁST

1.1 DEFINICE KYBERNETICKÉHO ÚTOKU

Kybernetický útok můžeme definovat jako jednání s úmyslem a cílem poškodit nebo získat informace ze systémů firem a organizací. Je veden jak jednotlivými útočníky, tak organizovanými skupinami.

Některé kybernetické útoky mohou být například motivované jen zvědavostí mladých hackerů, zda se dokáží dostat do zabezpečených systémů.

Důvody kybernetických útoků mohou být:

- získání důvěrných informací,
- prolomení nastaveného zabezpečení,
- zanesení chaosu a rozkladu do informací v systémech organizací,
- zcizení obchodních tajemství a know-how firem,
- poškození důvěryhodnosti a reputace organizace,
- přetížení a následné zničení serverů s nevratnou ztrátou dat,
- a další.

1.2 POTŘEBA KYBERNETICKÉ BEZPEČNOSTI

Všechny organizace a společnosti, ale i jakékoliv firmy potřebují informace pro své fungování. Bez informací nemůže řídící management rozhodovat, nemůžou se rozjet výrobní linky, nemocnice nezajistí správné diagnózy a například HZS Pk v rámci svého KOPIS, nemůže rozhodovat o nasazení SaP v operačním řízení (1), apod. Tok a správa informací v rámci společnosti jsou naprosto zásadní záležitostí. Proto jejich ztráta, poškození nebo zveřejnění může pro organizace znamenat fatální konce.

Kybernetická bezpečnost je soubor a systém bezpečnostních opatření, jež zabraňují zneužití informací a infrastruktury, které umožňují sdílení dat. Ochrana všech zařízení v organizaci, která jsou online připojena do sítě, je proto hlavní potřebou a cílem kybernetické bezpečnosti. V podstatě je nedůležité, jestli dané zařízení obsahuje citlivá data nebo ne, protože je potřeba se na všechna zařízení v případě kybernetické bezpečnosti dívat ve spojitosti se všemi ostatními zařízeními a celou organizací. Příkladem může být obyčejná tiskárna, která je připojena k interní síti. Tato tiskárna sice neobsahuje žádná citlivá data, ale v případě poškození kybernetickým útokem, zastoupeném

například připojením neznámého rizikového externího zařízení, může dojít k velkým ztrátám a úniku dat.

Potřeba a zvýšený důraz na kybernetickou bezpečnost je ve větší míře vnímán až s rozmachem a rozvojem internetu, informačních technologií a propojování informačních systémů. Proto také vznikl a byl v této době zaveden zcela nový pojem kyberprostor.

Kyberprostorem rozumíme vzájemně propojené informační systémy a elektronická zařízení ve virtuálním prostředí s vlastností předávání a sdílení dat. Například se může jednat o stolní počítače, notebooky, chytré televize, automobily, zařízení s virtuální realitou a další. Tato zařízení jsou schopna sbírat data a informace, přenášet je ke zpracování a sdílet s jinými zařízeními nebo úložišti dat.

Jak již bylo uvedeno v úvodu, kybernetická bezpečnost není jen otázkou pro ICT specialisty, ale je záležitostí každého uživatele. Téměř všichni tráví čas na sociálních sítích, přihlašují se do internetového bankovnictví a používají internet. Zde mají velkou řadu citlivých osobních dat a informací. Všichni by tedy proto měli pociťovat nutnost zavedení silnějšího hesla do systému a jeho pravidelnou aktualizaci, dvou-faktorové ověření identity, šifrování disků apod.

1.3 HASIČSKÝ ZÁCHRANNÝ SBOR

1.3.1 POSTAVENÍ A ÚKOLY HASIČSKÉHO ZÁCHRANNÉHO SBORU

„HZS ČR je jednotný bezpečnostní sbor, jehož základním úkolem je chránit životy a zdraví obyvatel, životní prostředí, zvířata a majetek před požáry a jinými mimořádnými událostmi a krizovými situacemi.“ (2)

„Hasičský záchranný sbor se podílí na zajišťování bezpečnosti České republiky plněním a organizováním úkolů na úseku požární ochrany, ochrany obyvatelstva, civilního nouzového plánování, integrovaného záchranného systému, krizového řízení a dalších úkolů v rozsahu a za podmínek stanovených zákonem a jinými právními předpisy.“ (2)

1.3.2 STRUČNÁ HISTORIE A VZNIK HZS ČR

V období 80. let dvacátého století začíná profesionální požární ochrana procházet významnějšími změnami, začíná se měnit počet a podíl zásahové činnosti jednotek požární ochrany. Do té doby převažovaly zásahy u požárů, později se ve větší míře začínají objevovat a prosazovat technické zásahy. Převážně ve formě činnosti u dopravních nehod,

zásazích u živelných pohrom a pandemií, vyhledávání osob a zvířat, odstraňování překážek apod.

Svojí všestrannou akceschopností profesionální jednotky požární ochrany začínají postupně nahrazovat některé vybrané technické služby a získávají stále větší pravomoci v oblasti přípravy státu a jeho výkonných orgánů na mimořádné události a krizové stavy, a to zejména v podobě provádění záchranných a likvidačních prací. Ve světle těchto změn je proto nutné změnit a upravit i stávající legislativu. Celkově je třeba přepracovat celou organizaci a koncepci jednotek požární ochrany. V roce 1985 dochází k vydání zákona o požární ochraně, který je několikrát novelizován a je dodnes platný. Zákon především vytváří podmínky pro účinnou ochranu života, zdraví a majetku občanů před všemi druhy živelných pohrom a jinými mimořádnými událostmi. Dále stanoví povinnosti ministerstev, právnických a fyzických osob a všech orgánů státní správy a samosprávy na úseku požární ochrany.

HZS ČR procházelo a prochází neustálými změnami a procesem vývoje, například v roce 1995 získává svůj současný název. Na přelomu tisíciletí Ministerstvo vnitra rozšiřuje svoji působnost o oblast krizového řízení, ochrany obyvatelstva, civilního nouzového plánování a integrovaného záchranného systému. Ve sbírce zákonů s účinností od 1. ledna 2001 jsou k tomuto rozšíření Parlamentem ČR vydány zákony 238/2000 Sb. o HZS ČR, 239/2000 Sb. o IZS a 240/2000 Sb. Krizový zákon. Těmito právními úpravami je mimo jiné sloučeno HZS ČR s úřadem civilní ochrany a tato široká oblast spadla výhradně do kompetence Ministerstva vnitra. HZS ČR získává stěžejní roli v přípravě státu na mimořádné události, od hrozeb terorismu, průmyslových havárií, až po živelné katastrofy. Stává se páteřní složkou a koordinátorem systému IZS, který v případě krize slučuje všechny záchranné složky a začíná se převažující měrou podílet na provádění záchranných a likvidačních prací. (3)

1.3.3 PŘÍSLUŠNÍK HASIČSKÉHO ZÁCHRANNÉHO SBORU A ZAMĚSTNANEC

„Úkoly hasičského záchranného sboru plní

a) příslušník hasičského záchranného sboru ve služebním poměru podle zákona o služebním poměru příslušníků bezpečnostních sborů,

b) zaměstnanec České republiky zařazený v hasičském záchranném sboru v pracovním poměru podle zákoníku práce.“ (2)

Z výše uvedené citace zákona o HZS ČR (2) vyplývá, že u tohoto bezpečnostního sboru jsou dva druhy pracovně právních poměrů. Pro využívání informačních technologií a pohybu v kyberprostoru však toto dělení nemá většího významu, protože uživatelem ICT může být jakýkoliv příslušník nebo zaměstnanec.

1.4 LEGISLATIVA KYBERNETICKÉ BEZPEČNOSTI

1.4.1 ZÁKON Č. 181/2014 SB.

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI A O ZMĚNÁCH SOUVISEJÍCÍCH ZÁKONŮ

Dne 13. srpna 2014 prezident České republiky podepsal zákon o kybernetické bezpečnosti a o změně souvisejících zákonů. Zákon o kybernetické bezpečnosti je účinný od 1. ledna 2015.

Zákon o kybernetické bezpečnosti upravuje povinnosti a práva osob, ale také i působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Jsou v něm zapracovány nadřazené předpisy Evropské unie a sjednocuje zajišťování bezpečnosti sítí, elektronických komunikací a informačních systémů. (4)

Nejdůležitějším rámcem zákona je stanovení základní úrovně bezpečnostních opatření, zlepšení detekce kybernetických bezpečnostních incidentů, zavedení hlášení kybernetických bezpečnostních incidentů, zavedení systému opatření k reakci na kybernetické bezpečnostní incidenty a upravení činnosti dohledových pracovišť.

V roce 2017 byly provedeny dvě významnější novely zákona o kybernetické bezpečnosti, a to zákonem č. 104/2017 Sb. s účinností od 1. července 2017 a zákonem č. 205/2017 Sb. s účinností od 1. srpna 2017. K dnešnímu datu jsou v platnosti novelizace vycházející z tohoto zákona, a to zákonem č. 183/2017 Sb., zákonem 35/2018 Sb., zákonem č. 111/2019 Sb., zákonem č. 12/2020 Sb. a aktuálně poslední novelizace zákonem č. 261/2021 Sb.

Zároveň se zákonem č. 181/2014 Sb. byly v témže roce vydány dvě jeho prováděcí vyhlášky.

1.4.2 VYHLÁŠKA Č. 316/2014 SB.

VYHLÁŠKA O BEZPEČNOSTNÍCH OPATŘENÍCH, KYBERNETICKÝCH BEZPEČNOSTNÍCH INCIDENTECH, REAKTIVNÍCH OPATŘENÍCH A O STANOVENÍ NÁLEŽITOSTÍ PODÁNÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI (VYHLÁŠKA O KYBERNETICKÉ BEZPEČNOSTI)

„Touto vyhláškou se stanoví obsah a struktura bezpečnostní dokumentace pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém, obsah bezpečnostních opatření, rozsah jejich zavedení, typy a kategorie kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivního opatření a jeho výsledku a vzor oznámení kontaktních údajů a jeho formu.“ (5)

Tato původní vyhláška z roku 2014 byla již zrušena a nahrazena vyhláškou č. 82/2018 Sb.

1.4.3 VYHLÁŠKA Č. 82/2018 SB.

VYHLÁŠKA O BEZPEČNOSTNÍCH OPATŘENÍCH, KYBERNETICKÝCH BEZPEČNOSTNÍCH INCIDENTECH, REAKTIVNÍCH OPATŘENÍCH, NÁLEŽITOSTECH PODÁNÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI A LIKVIDACI DAT (VYHLÁŠKA O KYBERNETICKÉ BEZPEČNOSTI)

Vyhláška nahrazuje vyhlášku 316/2014 Sb., se zabudovaným příslušným předpisem Evropské unie[3]. Pro informační a komunikační systém kritické informační infrastruktury, významný informační systém, informační systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb a pro informační systém základní služby tato vyhláška upravuje:

a) obsah a strukturu bezpečnostní dokumentace,

b) obsah a rozsah bezpečnostních opatření,

c) typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,

d) náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,

e) náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,

f) vzor oznámení kontaktních údajů a jeho formu,

[3] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

g) způsob likvidace dat, provozních údajů, informací a jejich kopií.

1.4.4 VYHLÁŠKA Č. 317/2014 SB.

VYHLÁŠKA O VÝZNAMNÝCH INFORMAČNÍCH SYSTÉMECH A JEJICH URČUJÍCÍCH KRITÉRIÍCH

Touto vyhláškou jsou stanoveny významné informační systémy a jejich určující kritéria podle § 6 písm. d) zákona č. 181/2014 Sb. (6)

1.4.5 LEGISLATIVA O KYBERNETICKÉ BEZPEČNOSTI VZTAHUJÍCÍ SE K HZS ČR

V zákoně č. 181/2014 Sb. a v jeho prováděcích vyhláškách je vymezen a definován pojem kritická informační infrastruktura, proto v této práci musí být zmíněn zákon č. 240/2000 Sb. (Krizový zákon), který vymezuje pojem kritická infrastruktura. Kritická informační infrastruktura je z velké části spojená s již určenými prvky kritické infrastruktury, identifikovanými zejména v oblastech energetiky, veřejné správy, elektronických komunikací a finančního trhu a měny. Nastane-li krizová situace v oblasti kybernetické bezpečnosti, může mít dopad na funkčnost subjektu kritické infrastruktury a mít tak dopad na jeho fungování a služby. Nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvků kritické infrastruktury, ve znění novely č. 315/2014 Sb., se v odvětvovém kritériu *„VIII. NOUZOVÉ SLUŽBY“* určuje jako prvek kritické infrastruktury v bodě A. - Integrovaný záchranný systém, konkrétně operační a informační středisko generálního ředitelství Hasičského záchranného sboru České republiky.

Posledním významnějším zákonem vztahující se ke kybernetické bezpečnosti a činnosti HZS ČR, je zákon č. 365/2000 Sb. o informačních systémech veřejné správy, kterým jsou stanovena práva a povinnosti související s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy, spravovaných státními orgány nebo orgány územních samosprávných celků. (7)

1.5 NEJČASTĚJŠÍ KYBERNETICKÉ HROZBY

1.5.1 BOTNET

Botnet lze v informatice definovat jako síť softwarových zařízení nebo internetových účtů a robotů, provádějících činnost automaticky nebo na základě příkazu samostatně. V současnosti je tento termín ponejvíce spojen s malware, například spamem. Síť zařízení označována jako Botnet, je síť infikovaná speciálním softwarem, která je útočníkem ovládaná centrálně z jednoho místa. Má k dispozici až stovky tisíc počítačů, z nichž každý

odešle část zprávy (spamu) a tím je takovýto provoz považován za bezproblémový a není zastaven. (8)

1.5.2 MALWARE

Malware (škodlivý software) je software určený ke vniknutí, narušení nebo poškození počítačového systému. Tímto způsobem získané informace dále využívá. Malware může mít celou řadu podob, toto souhrnné označení zahrnuje adware, spyware, počítačové viry, počítačové červy, trojské koně, backdoor, rootkit, keylogger a ransomware.

1. Adware

   lze volně přeložit jako software podporující reklamu. Většinou se jedná o méně nebezpečnou, ale výnosnou variantu malware. Počítačový systém zobrazuje obtěžující, vyskakující reklamu. Ve spojení se spyware, však může sledovat činnost a odcizit informace. (8)

2. Spyware

   je špehovací software, využívající bez vědomí uživatele internet a internetové stránky k odesílání dat ze zařízení, mobilního prostředku nebo jiných zařízení. Součástí odeslaných dat a programů mohou být pouze jednoduchá data o přehledu navštívených stránek či nainstalovaných programů. Účelem je zmapování zájmů nebo potřeb uživatele a využití těchto získaných informací pro zacílení reklamy. Spyware však existuje i ve formě, která dokáže odesílat čísla a hesla kreditních karet nebo funguje jako tzv. zadní vrátka. Spyware je často šířen bez vědomí uživatele, ale se souhlasem autora programu jako adware, který je součástí sharewaru. Týká se to často peer to peer programů a jejich klientských programů, umožňujících vzájemné stahování videí a hudby přes ostatní uživatele. (8)

3. Phishing

   je podvodný software používaný na internetu při elektronické komunikaci bez vědomí a souhlasu uživatele, sloužící k získávání citlivých a statistických údajů, jako jsou data o navštívených webových stránkách, čísla a hesla kreditních karet apod. Získaná data odesílá do datové schránky útočníka. Předstíráním, že přichází od ITC pracovníků nebo z úřadů státní správy, z platebních on-line portálů, z aukčních webů nebo sociálních sítí, se software snaží působit na důvěřivost veřejnosti a nalákat ji. Typickým projevem phishingu je rozesílání e-mailových sdělení,

většinou vyzývají uživatele k uvedení osobních údajů na smyšlenou webovou stránku, která má takřka identickou formu a podobu s oficiální. Stránka nebo okno se tváří například jako přihlašovací pole do internetového bankovnictví. Zadáním přihlašovacích jmen a hesel uživatel okamžitě své údaje automaticky vyzradí útočníkům, kterým prakticky již nic nebrání k vykradení peněz z jeho účtu. (8)

4. Viry,

   jedná se o program či závadný kód, který je schopen sám vytvářet své kopie, které mohou počítač poškodit, anebo sám sebe připojit k již existujícímu jinému souboru či dokumentu. K nakažení zařízení virem nebo k začátku jeho šíření je potřeba obvykle zahájit nějakou činnost. Kupříkladu přejít a otevřít přiloženou nakaženou e-mailovou přílohu nebo sdílet a přeposlat software mezi počítačovými sítěmi a systémy. (8)

5. Červi

   jsou na rozdíl od virů autonomní programy schopné vytvářet své vlastní kopie, které se pomocí síťové komunikace rozesílají do dalších počítačových sítí nebo systémů. Zde vyvíjejí další činnost, pro kterou byly naprogramovány. Šíření je velice rychlé a tím dochází k masivnímu zahlcení počítačové sítě nebo celé infrastruktury. Programy jsou schopny analyzovat bezpečnostní slabiny, a proto bývají využívány k vyhledávání bezpečnostních mezer. (8)

6. Trojský kůň a backdoor

   je označení pro software obsahující skryté funkce, o kterých uživatel neví nebo s nimi nesouhlasí a jsou potencionálně nebezpečné pro další fungování systému. Na rozdíl od klasických virů nemají schopnost se replikovat a šířit bez pomoci uživatele. Při aktivaci mohou být využity k blokování, mazání, kopírování dat, modifikaci či narušení běhu počítačových sítí a systémů. (8)

7. Rootkit

   je pojem nejen pro jednotlivý software, ale i pro celé technologie sloužící k zamaskování přítomnosti malware. Nepříliš objemný počítačový program mění chování celého operačního systému tak, aby se uživatel nedozvěděl o existenci nebezpečných programů ve svém počítači. (8)

8. Keylogger

   je software, který zaznamenává konkrétní stisky kláves na napadeném systému. Nejčastějším využitím je zaznamenání přihlašovacích údajů k účtům uživatele a jejich následné odeslání útočníkovi. (8)

9. Ransomware

   je druh tzv. vyděračského malwaru, který zabraňuje nebo omezuje přístup k jím infikovanému počítačovému systému. K znovu zpřístupnění počítače je zpravidla programem vyžadováno zaplacení výkupného. Ransomware a jeho některé formy šifrují a omezují soubory na pevném disku, tzn. funkčnost v celém systému. Jiné jen zamknou systém, který zůstává funkční. Pod výhrůžkou a zasláním zprávy, se program uživatele snaží přimět k zaplacení. (8)

1.5.3 SPAM

Spam je hromadné šíření nevyžádané reklamní pošty, sdělení či jiné zprávy, která je šířena internetem. Zprávy mohou obsahovat např. i viry, trojské koně apod.

1. Scam

   je podstatná část spamu, který obsahuje kriminální či jiný podvodný obsah. Většinou jde o e-mail nebo zprávu ze sociálních sítí, která například obsahuje lživé sdělení o výhře v loterii nebo žádost o peněžní podporu. (8)

2. Hoax

   je poplašná, zkreslená, řetězová nebo jinak zavádějící zpráva vykonstruovaná tak, aby budila dojem, že se opravdu jinak tak něco neuvěřitelného mohlo stát. Ve většině případů je to již obvykle zastaralé, emotivně nebo šokujíce působící sdělení, jen s výjimečnou pravdivostí. Jsou to e-maily, které typicky v obrovském množství rozesílají důvěřivější uživatelé internetu svým známým a přátelům. Obecně je šíření hoaxu považováno za velmi obtěžující nešvar. Při pochybnostech o případné pravdivosti sdělení, je možné tyto zprávy překontrolovat na adrese serveru *hoax.cz*. (8)

1.6 VŠEOBECNÉ BEZPEČNOSTNÍ ZÁSADY

Pro obecné povědomí uživatelů a omezení bezpečnostních incidentů, by měl být kladen co největší důraz na základní digitální bezpečnostní gramotnost. Je minimálně nutné v počítačových sítích organizací dodržovat následující zásady:

1. Nejprve pořádně přečíst, pak až klikat.
   Pro své fungování a chod potřebují některé internetové stránky další přídavné a podpůrné aplikace. Proto se při navštěvování webových stránek může stát, že načítaná stránka bude požadovat nainstalování chybějících programových komponentů pro korektní zobrazení. Internetový prohlížeč v novém okně vygeneruje otázku, zda si uživatel přeje stáhnout a nainstalovat chybějící součásti (např. ActiveX prvky). Tato a podobná hlášení je důležité nebrat na lehkou váhu a vždy si pečlivě přečíst a ověřit o jakou součást jde a teprve až pak dialogové okno potvrdit. V případě pochybností o původu programu kontaktovat technika ICT oddělení.

2. Používat bezpečná hesla.
   Bezpečné heslo by měla být co nejméně zjistitelná, uhodnutelná nebo jinak snadno zneužitelná posloupnost znaků, která je používaná jako identifikační a bezpečnostní prvek. Hesla v obecné rovině slouží pro ochranu přístupu k systémům a informacím, do kterých by se neměl dostat nikdo nepovolaný. Bezpečnost hesla je proto jeho základním a nejdůležitějším kritériem. Heslo by nemělo obsahovat například tyto údaje:

- název účtu, ke kterému slouží heslo jako ochranný prvek,
- vlastní jméno, příjmení nebo jméno člena rodiny, psa, apod.,
- rodné číslo či datum narození,
- popisné číslo domu, adresa, telefonní číslo,
- často užívané výrazy jako např. „12345“, „heslo“, „password“ nebo názvy,
- programů a to v jakýchkoliv kombinacích malých a velkých písmen,
- běžná slova, ani jejich obdobu.

Nejbezpečnější hesla by tedy měla být na první pohled „nesmyslné“ kombinace znaků. Takové heslo je ale těžko zapamatovatelné a v případě nepravidelného používání dochází často k jeho zapomenutí. Proto je dobré si k heslu vymyslet mnemotechnickou pomůcku, podle které bude snáze zapamatovatelné, ale i tato pomůcka ovšem musí zůstat stejně tajná jako heslo samotné.

3. Neposílat přes internet důvěrná data.
   Číslo kreditní karty, zejména CVC kód nebo osobní hesla, což jsou velice citlivá data, není přes internet vhodné vůbec posílat. Pokud je to ale opravdu nevyhnutelné a nutné, tak pouze ve výjimečných případech. Kdyby se takové údaje dostaly do nepovolaných rukou, mohlo by to mít za následek nejen finanční ztráty, ale i další problémy. Například zneužití kreditní karty pro nákup na internetu nebo uzavření smlouvy na zcizené osobní údaje apod. Proto by se důvěrné informace přes internet měli posílat pouze přes šifrované spojení, zastoupené např. protokolem HTTPS.

   Uživatelé internetu by však měli vědět, že opuštěním zabezpečené stránky budou data opět do sítě putovat nezabezpečená!

4. Nezanechávat na internetu stopy.
   Je zakázáno používat služební e-mail pro soukromé účely a registrace na serverech, které nesouvisí s pracovní náplní. Nikde neuvádět více informací než je nutné a potřebné. To platí hlavně u různých serverů vyžadující registraci. Pokud se již některá data musí uvést, vyplnit jen ta nezbytně nutná, tedy označená hvězdičkou. Pole bez hvězdičky raději nevyplňovat.

5. Důvěřovat, ale prověřovat.
   Při obdržení e-mailu od neznámého odesílatele musí být uživatel při jeho otevírání opatrný, hlavně při přechodu na přiložené odkazy a přílohy. Ve většině případů se jedná o reklamu a tím i spam, ale může jít i o počítačové viry nebo špionážní programy, jako je spyware. Přílohou e-maily většinou odkazují na nezaplacené faktury, exekuce, vysoké finanční výhry, levné zájezdy nebo další nabídky služeb. Dále je důležité mít na paměti, že žádné bankovní domy nerozesílají zprávy s žádostí o osobní údaje a odkazy na nové stránky internetového bankovnictví. Při výzvě k otevření spustitelných souborů z internetu je na místě zvýšená ostražitost.

Pokud je jeho původ neznámý, raději soubor neotevírat a už vůbec ne instalovat. Přílohy mohou obsahovat nebezpečný vir nebo jiný škodlivý obsah. Téměř všechny antivirové programy umožňují ještě před spuštěním daného souboru tento soubor zkontrolovat. Každý učiněný krok důkladně zvážit, být obezřetný a raději nedůvěřovat.

Při podezření na příchozí e-mail, kde není jistý jeho odesílatel, původ nebo pravdivost, raději kontaktovat ICT oddělení.

6. Certifikáty.
   Internet používá k ochraně identity různé certifikáty. Jde o prohlášení, zaručující identitu osoby nebo zabezpečení serveru, označované také jako digitální ID. Tyto certifikáty ve velké míře využívají služební e-maily a bezpečnostní systémy. Je tím zajištěno, že žádný jiný server nemůže převzít identitu původního zabezpečeného serveru. Při potvrzování podrobností uvedených v zabezpečení je nutné a důležité být obezřetný.

7. Ztrátu pracovního zařízení okamžitě hlásit.
   Ztrátu nebo odcizení přenosného pracovního zařízení, jako je mobilní telefon, notebook apod. bez zbytečného prodlení ohlásit ICT oddělení a svému nadřízenému.

8. Nevhodné internetové stránky a soubory.
   Mimo síť organizace a k internetu z pracovních počítačů přistupovat pouze za účelem plnění pracovních povinností a pro pracovní záležitosti. Datový tok a provoz je většinou monitorován a pravidelně vyhodnocován. Většina organizací má vnitřními předpisy nastaven zákaz navštěvovat webové stránky a stahovat soubory s rasistickým, násilným, sexuálním, vulgárním či zákonem nepovoleným obsahem.

9. Neznámé USB disky, SD karty apod.
   Nevkládat neznámá paměťová zařízení do služebních počítačů, mobilních telefonů či tabletů. Všechny soubory, i ty související s pracovními záležitostmi, které dříve mohly být použity mimo organizaci, před spuštěním překontrolovat antivirovým programem.

2 PRAKTICKÁ ČÁST

2.1 PODMÍNKY PRO UŽÍVÁNÍ ICT U SLOŽKY HZS ČR

Kybernetická bezpečnost je věcí a zodpovědností všech, nejen ICT pracovníků, ale i koncových uživatelů a řídících pracovníků. HZS ČR je součástí kritické informační infrastruktury, proto jsou interními akty a nařízeními upraveny další povinnosti a podmínky používání ICT:

- každý pracovník má nárok na přidělení pouze takových prostředků ICT (hardware, software a přístupová oprávnění k datům a ICT službám), které potřebuje pro zajištění výkonu činnosti zastávaného systemizovaného pracovního místa a funkce,
- jedinou osobou oprávněnou instalovat na stolní PC, notebook, tablet, chytrý telefon nebo jiné pracovní stanice jakýkoliv software a to i antivirový, nastavovat uživatelské účty, připojení do sítě včetně firewallu a k externím periferiím atd., je pověřený pracovník oddělení KIS HZS ČR.

2.2 ZÁSADY KYBERNETICKÉ BEZPEČNOSTI U SLOŽKY HZS PK

Pro bezpečné chování zaměstnance HZS Pk v kyberprostoru, jsou interními akty a nařízeními definovány zásady, kterými se každý uživatel ICT musí řídit a jsou závazná:

- podmínkou přístupu do kybernetického prostoru HZS Pk, tj. k prostředkům a službám ICT resortu MV ČR, např. pracovní stanice, počítačové sítě, informační systémy, komunikační služby je seznámení se s materiálem *„Základní materiály o dopadech zákona č. 181/2014 Sb. o kybernetické bezpečnosti na resort MV ČR – implementace systému řízení bezpečnosti informací v kybernetickém prostoru resortu MV ČR“* stanovené uvedeným zákonem a úpravami schválenými Ministrem vnitra,
- pro pracovní účely využívat primárně prostředky ICT přidělené a určené zaměstnavatelem. Vlastní soukromé pracovní stanice využívat pouze v souladu s licenčními podmínkami SW a se souhlasem zaměstnavatele při práci z domova,
- přidělené ICT prostředky využívat pouze pro pracovní účely a mobilní ICT prostředky zabezpečit proti zcizení, neoprávněnému použití a poškození,

- problém s prostředky ICT, jako i podezření na kybernetickou bezpečnostní událost (neoprávněný přístup k pracovním datům, nebo dokumentům resortu včetně dat uložených na mobilním zařízení, nedodržení bezpečnostních pravidel, selhání a poruchy, které by mohly způsobit ohrožení a dostupnost pracovních dat a informačních nebo komunikačních služeb, při obdržení spamu na pracovní e-mail adresu, apod.) bezodkladně nahlásit na organizačně příslušné oddělení KIS HZS ČR. Pokud k tomuto dojde mimo běžnou pracovní dobu, nahlásit službu konajícímu příslušníkovi oddělení KIS HZS Pk, cestou příslušného KOPIS Pk,
- ztrátu nebo odcizení pracovního mobilního zařízení, tj. pracovní stanice a paměťového nosiče bez zbytečného prodlení ohlásit oddělení KIS HZS Pk,
- osobním heslem nebo PIN zabezpečovat přístup k přiděleným prostředkům ICT a to jak do pracovní stanice stacionární, tak i mobilní,
- základní doporučená pravidla pro osobní hesla:
  - udržovat unikátní hesla, tj. různé pro jednotlivá zařízení i jednotlivé SW aplikace a systémy,
  - odlišné od uživatelského jména, jména či příjmení uživatele a od předchozího hesla (odlišnost min. ve třech znacích),
  - chránit a měnit při podezření na kompromitaci,
  - délka minimálně 12 znaků, z nich je nejméně jedno velké písmeno, jedno malé písmeno, jedna číslice a jeden speciální znak („.“; „,“; „@“; „#“; „%“; „!“;„$”; „&“; „+“; „-“; atd.),
  - nevyužívat bezpečnostní otázky pro „ztracené“ heslo, tj. v případě ztráty hesla kontaktovat organizačně příslušné oddělení KIS HZS Pk,
- zabránit, aby pod přihlášením jménem a heslem jednoho uživatele použil pracovní stanici, včetně mobilních nebo přístup k systémům organizace, neoprávněně jiný uživatel. Je-li pracovní stanice nebo systém určen pro více uživatelů, zajistit, aby každý musel přistupovat pouze pod svým jménem a heslem,
- pracovní stanici zamykat vhodným způsobem i při přerušení práce pokud je ponechána bez dozoru, např. z důvodu cesty k tiskárně mimo kancelář.

U operačních systémů Windows lze pro tuto operaci použít stisknutí kláves Windows + L,

- nespouštět žádné neověřené aplikace (soubory s příponou *.exe; *.bat; *.com; apod.),
- pracovní data a dokumenty je doporučeno ukládat výlučně na zaměstnavatelem určená úložiště nebo zaměstnavatelem přidělená a registrovaná přenosná paměťová média,
- pro pracovní elektronickou komunikaci využívat pouze pracovní adresy a schránky elektronické pošty a pracovní účty. Je zakázáno si pracovní komunikaci přeposílat na soukromé adresy a účty nebo ji z nich odesílat,
- v rámci komunikace neotevírat e-mail nebo jeho přílohu, jejichž odesílatel je neznámý, vybočuje ze standardní komunikace nebo jehož adresa odesílatele se neshoduje s odesílatelem uvedeným ve zprávě,
- z pracovních stanic ani pracovních adres či uživatelských účtů nerozesílat nevhodný, obtěžující nebo dokonce škodlivý (nevyžádané e-maily, řetězové zprávy apod.) obsah,
- ukládat soukromá data a dokumenty na mobilní pracovní stanice lze pouze s předchozím souhlasem nadřízeného, a je-li stanice schválena a nastavena i pro osobní použití, tj. má nastaveno takové zabezpečení, aby pracovní data byla od soukromých bezpečně oddělena,
- připojování cizích koncových stanic k síti složky HZS Pk je striktně řízeno a povoleno pouze v omezených případech. Podmínkou připojení pracovních stanic a uživatelů k počítačové a komunikační síti složky HZS Pk je jejich úspěšná autorizace a autentizace,
- nespouštět v intranetu žádné vložené hypertextové odkazy směřující na neznámé weby, mohou být zdrojem škodlivého kódu,
- do veřejného kyberprostoru, tj. na internet z pracovních stanic, přistupovat pouze za účelem splnění pracovních povinností,

- přistupovat na internetové stránky zjevně neodpovídající pracovní náplni je zakázáno,
- pracovní identitu (e-podpis) nikdy nevyužívat pro soukromé účely,
- služební data jiné kategorie než veřejná (HZS ČR používá klasifikaci dokumentů a dat) smějí být ukládána pouze na takové mobilní prostředky ICT, včetně paměťových úložišť a médií, která jsou registrovaná a šifrována,
- přistupovat k vnitřní síti složky HZS Pk přes veřejnou síť pouze prostřednictvím virtuální privátní sítě, kterou zřizuje ICT oddělení, a s využitím více faktorové autentizace (ne jen jméno a heslo, ale ještě další faktor),
- přistupovat přes veřejnou síť k systémům složky HZS Pk, a to i elektronické poště, pouze na základě vícefázové autentizace nebo certifikátu veřejného klíče nebo komerčního klíče a znalosti přístupového hesla ke klíči,
- osobním heslem nebo PIN zabezpečovat přístup do přidělených pracovních mobilních paměťových nosičů.

2.3 DEFINICE CÍLOVÉ SKUPINY

Pro zjištění úrovně digitální gramotnosti a dodržování bezpečnostních zásad budou jako cílová skupina vybrány dvě různé části koncových uživatelů.

Jako první část cílové skupiny osob byla vybrána dvě oddělení na krajském ředitelství HZS Pk, která jsou součástí ekonomického úseku, a to oddělení finanční a oddělení provozní a správy majetku. Tato oddělení zajišťují provoz a správu majetku, vedení účetnictví, tvorbu rozpočtů pro celé HZS Pk, dále zabezpečují výstrojní součástky, likvidaci a evidenci faktur atd. Většina uživatelů ICT zařízení na těchto odděleních jsou zaměstnanci v pracovním poměru, kteří ICT prostředky využívají každodenně ke své práci. V největší míře jsou využívané kancelářské programy a aplikace, zastoupené textovými a tabulkovými editory, e-mailovými klienty apod.

Druhou část cílové skupiny osob budou tvořit příslušníci ve služebním poměru. Budou to výjezdoví hasiči, sloužící na požární stanici ve 24 hodinových směnách. ICT prostředky jsou jimi využívány především pro přístup k programům, které jsou potřebné pro zajištění chodu

organizace, e-mailovému klientu, sdíleným diskům, sdílenému cloudovému prostředí a internetu.

2.4 VSTUPNÍ OVĚŘENÍ

Vstupní ověření digitální gramotnosti budou tvořit dvě části. V první části bude rozeslán test obsahující základní otázky kybernetické bezpečnosti. Hlavní kostra otázek bude z volně dostupné varianty testů na internetu a to od NÚKIB (9) a firmy AVAST (10), doplněna vlastními otázkami, směřujícími přímo do organizace HZS Pk. Kompletní text otázek a znění testu je vložen do příloh v závěru této bakalářské práce.

Druhou částí bude rozeslání e-mailu, který na první pohled bude součástí vnitřní komunikace v organizaci. Bude obsahovat rutinní sdělení a odkazovat na internetové stránky nebo složku. Po otevření odkazu bude vygenerována jednoduchá webová stránka s upozorněním na nedodržení a porušení stanovených zásad.

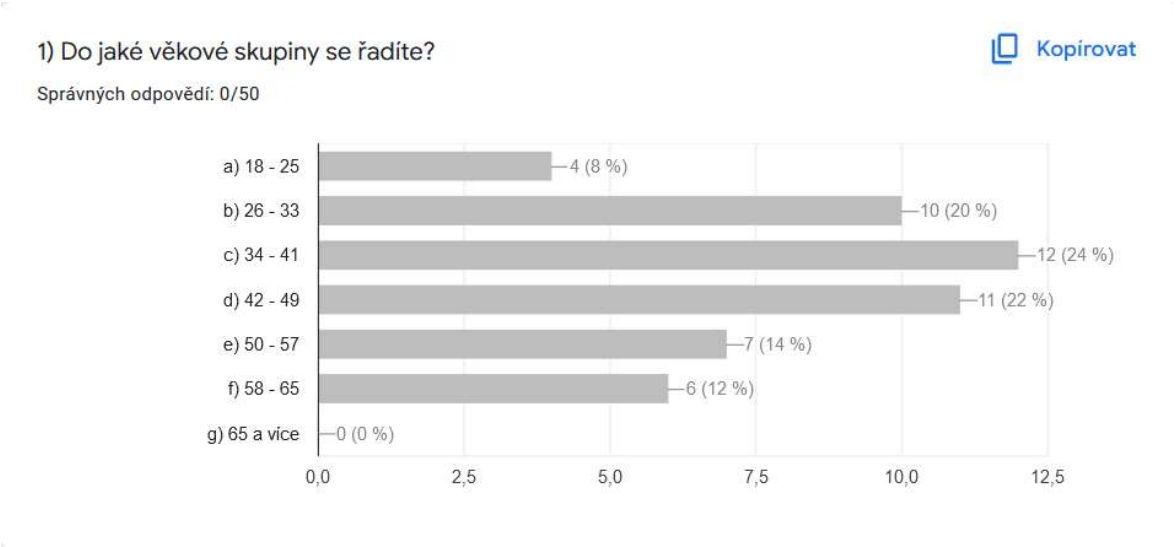
2.5 ZHODNOCENÍ VSTUPNÍHO OVĚŘENÍ

2.5.1 PÍSEMNÝ TEST ZE ZÁKLADŮ DIGITÁLNÍ GRAMOTNOSTI A BEZPEČNOSTI

Test obsahující otázky ze základních pravidel kybernetické bezpečnosti byl zpracován ve volně dostupné aplikaci Google Formuláře. Tyto formuláře umožňují základní souhrn a statistiku zodpovězených otázek, které jsou pro tento test více než dostačující. Formuláře jsou přes vygenerovaný odkaz každému účastníkovi testu přístupné bez dalšího dodatečného přihlašování, což je velice uživatelsky jednoduché a přívětivé.

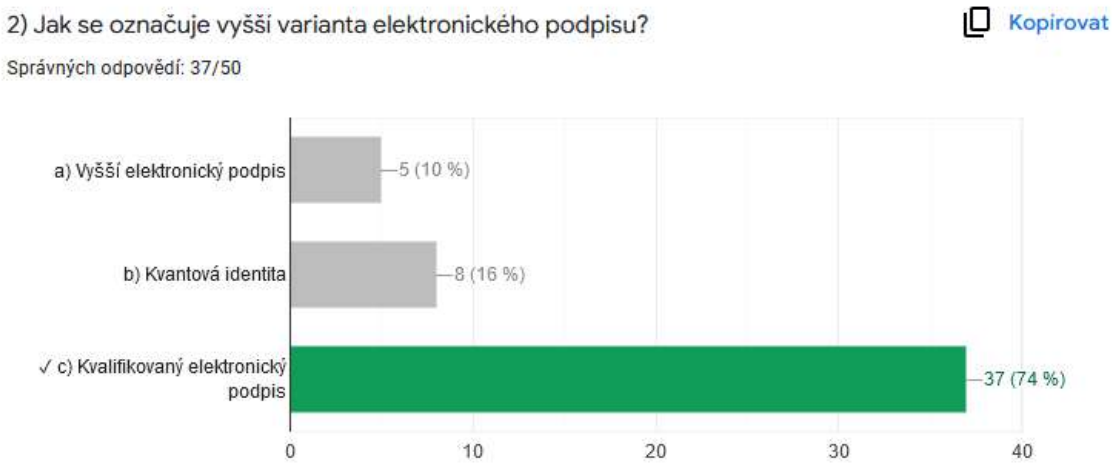
Test obsahuje dvacet jedna otázek, které jsou uvedeny v příloze této práce, včetně tučnou kurzívou označených správných odpovědí. Jako hranice uspokojivě zvládnuté otázky členy cílové skupiny byla stanovena 50% úspěšnost u všech odpovědí. V této části budou jednotlivě zhodnoceny všechny otázky. S tím, že u uspokojivě zodpovězených otázek bude pouze uvedena úspěšnost v procentech a krátký komentář. Neúspěšné otázky budou krátce slovně zhodnoceny. Na oblast otázek s nižší úspěšností bude posléze kladen větší důraz ve vypracovaném školícím a výukovém materiálu.

Otázka č. 1. - tato otázka (Obr. 1) byla jako jediná v testu povinná, proto aby mohl vzniknout rámcový přehled o věkovém složení cílové skupiny. Věk účastníku testu je v 60 % v rozmezí 25 – 50 let. Účastníci mladší 25 let jsou zastoupeny 8 %, ve věku 50 – 58 let je 14 % účastníků a 58 let a starší jsou zastoupeny 12 %.



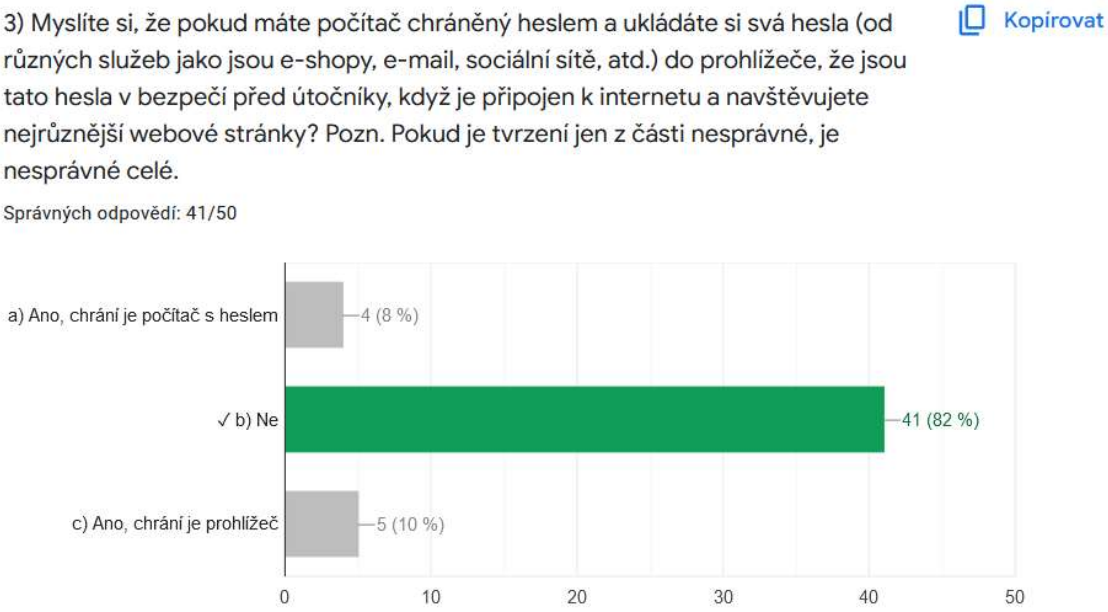
Obr. 1 – Otázka č. 1. vstupního ověření.

Otázka č. 2. – v této otázce (Obr. 2) bylo dosaženo celkové úspěšnosti 74 %, což je dobrá znalost nástroje pro identifikaci a autentizaci.



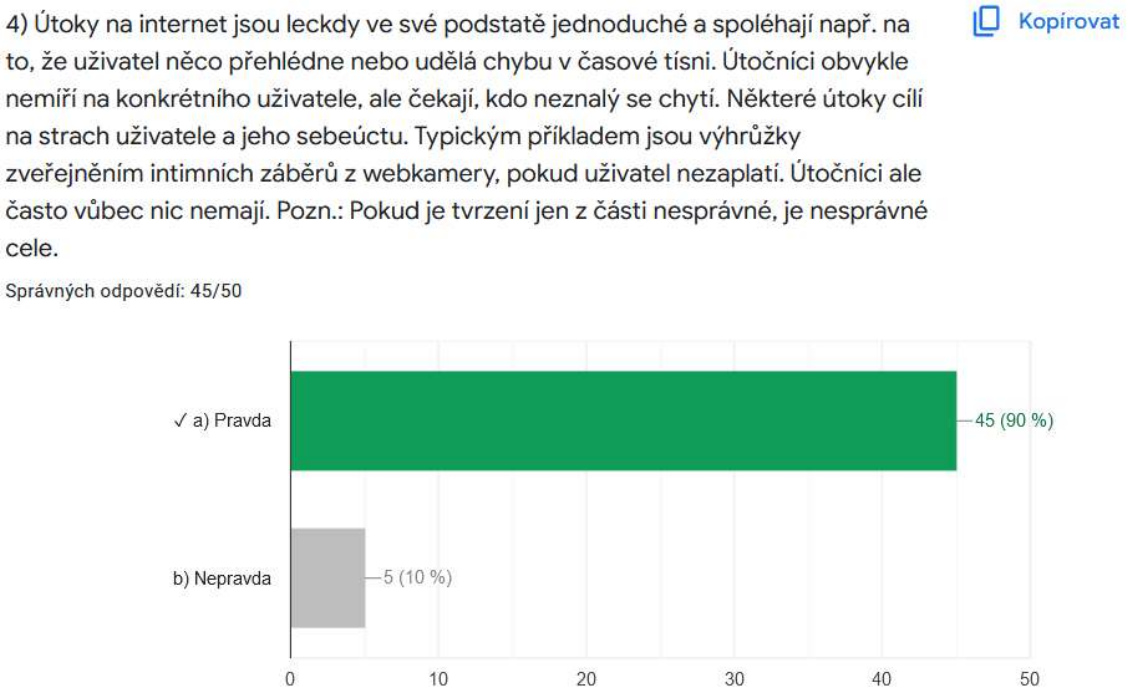
Obr. 2 – Otázka č. 2. vstupního ověření.

Otázka č. 3. - zde bylo (Obr. 3) dosaženo vysoké úspěšnosti, až do úrovně 82 % účastníci dobře znají riziko spojené s ukládáním hesel v internetovém prohlížeči.



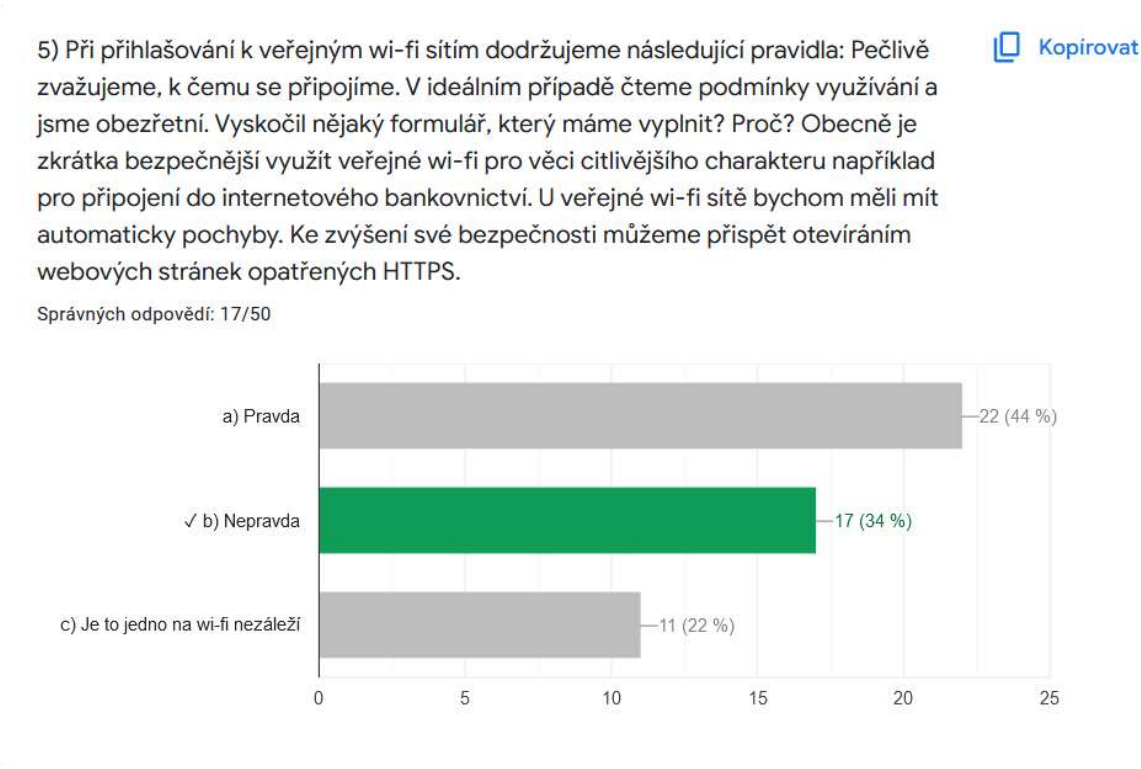
Obr. 3 – Otázka č. 3. vstupního ověření.

Otázka č. 4. – v této otázce (Obr. 4) bylo dosaženo velmi vysoké úspěšnosti, 90 % ve znalosti podstaty útoků na internetu.



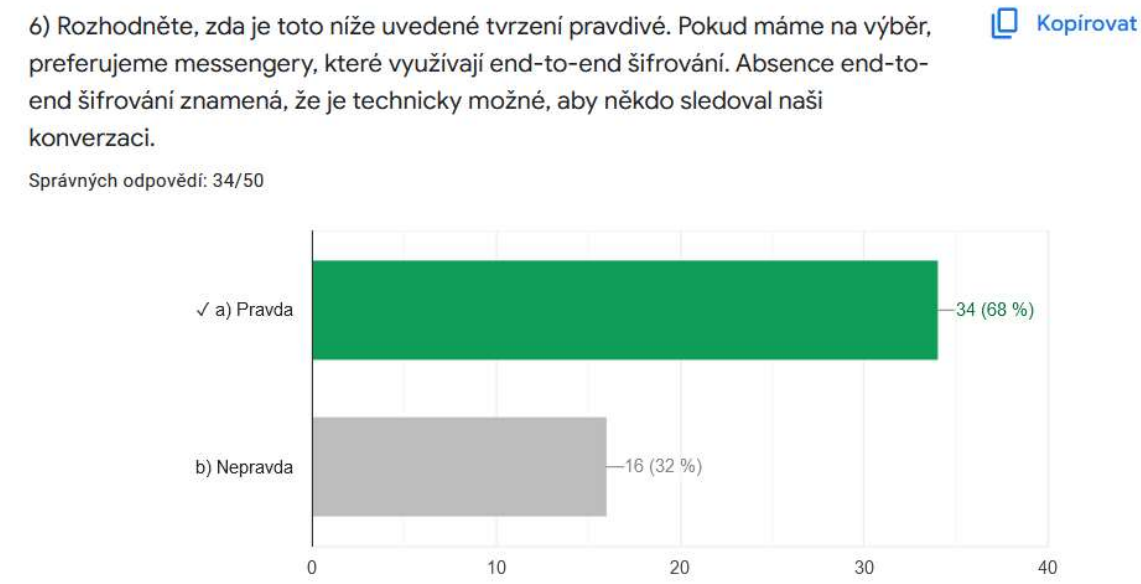
Obr. 4 – Otázka č. 4. vstupního ověření.

Otázka č. 5. – zde 2/3 účastníků (Obr. 5) dostatečně nevnímají všechna rizika veřejných Wi-Fi sítí a přihlašování k nim.



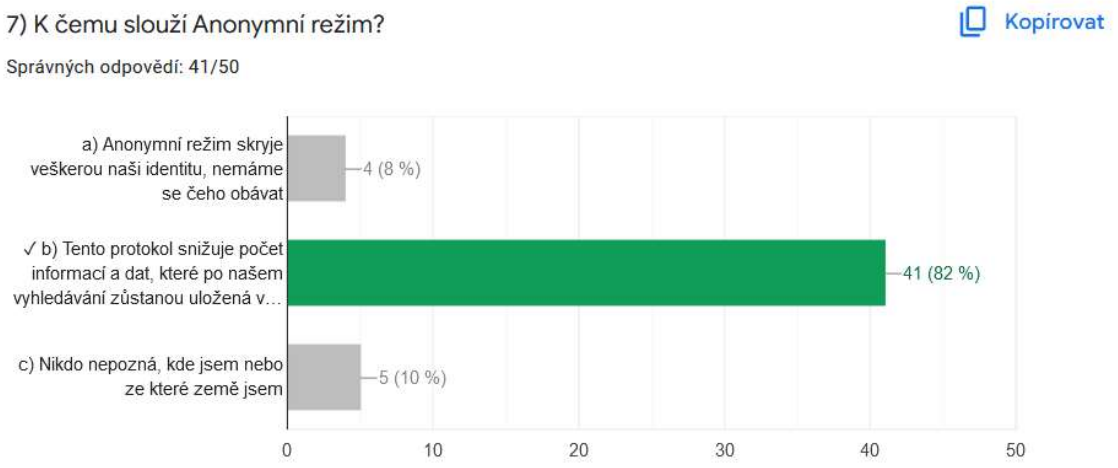
Obr. 5 – Otázka č. 5. vstupního ověření.

Otázka č. 6. – v této otázce (Obr. 6) bylo v 68 % správně rozhodnuto o potřebě preferování a používání end-to-end šifrování.



Obr. 6 – Otázka č. 6. vstupního ověření.

Otázka č. 7. – v této otázce (Obr. 7) 82 % účastníků vědělo, k čemu slouží a jak funguje anonymní režim.

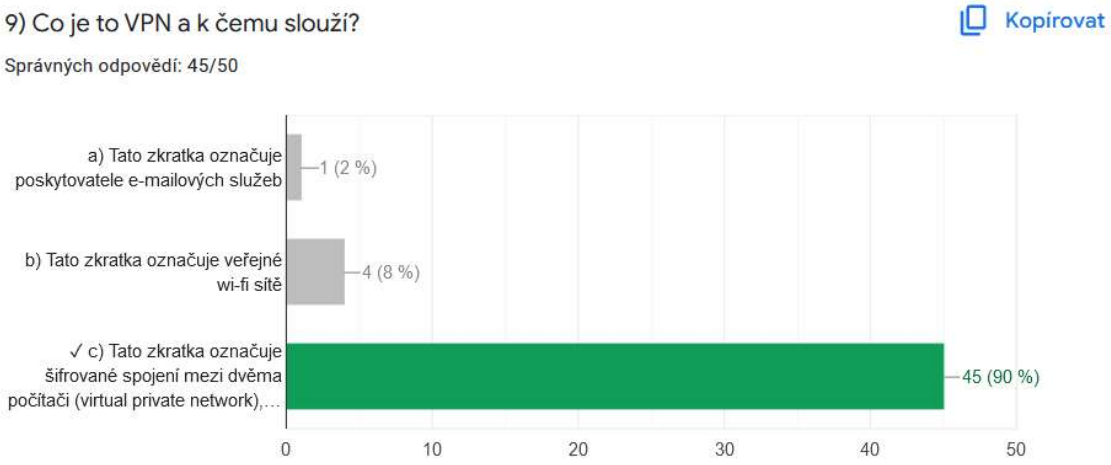


Obr. 7 – Otázka č. 7. vstupního ověření.

Otázka č. 8. – zde 69,4 % účastníků (Obr. 8) zná protokol HTTPS a jeho prospěch a využití při přihlašování k online službám.

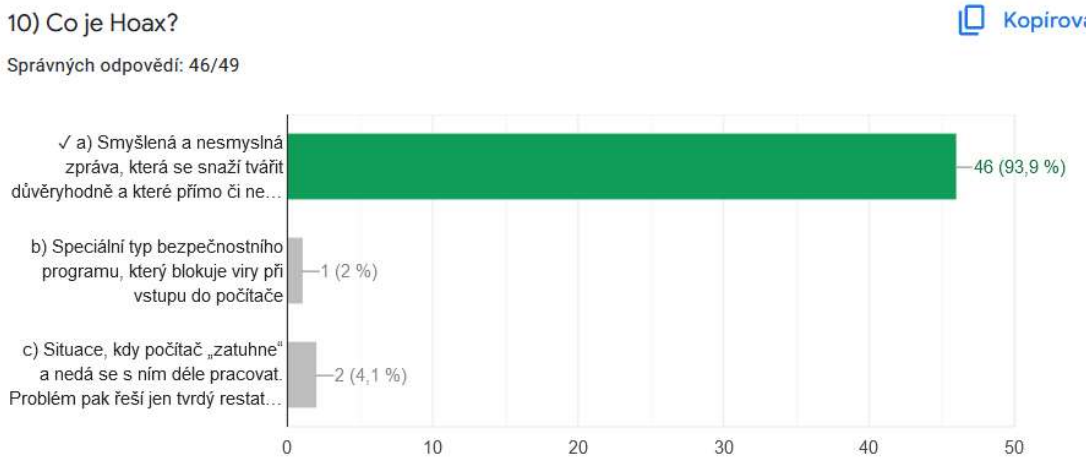
Obr. 8 – Otázka č. 8. vstupního ověření.

Otázka č. 9. – v této otázce (Obr. 9) 90 % účastníků vědělo, co znamená VPN a k čemu slouží.



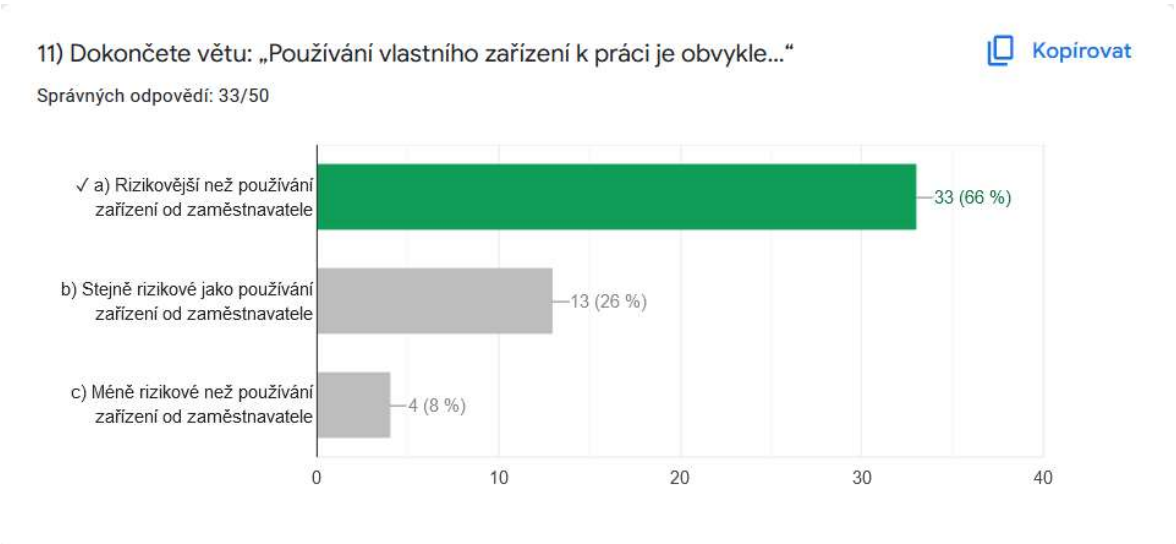
Obr. 9 – Otázka č. 9. vstupního ověření.

Otázka č. 10. – zde (Obr. 10), ve velmi vysokém procentu, skoro až v 94 %, účastníci znají Hoax a vědí, jaká jsou jeho nebezpečí.



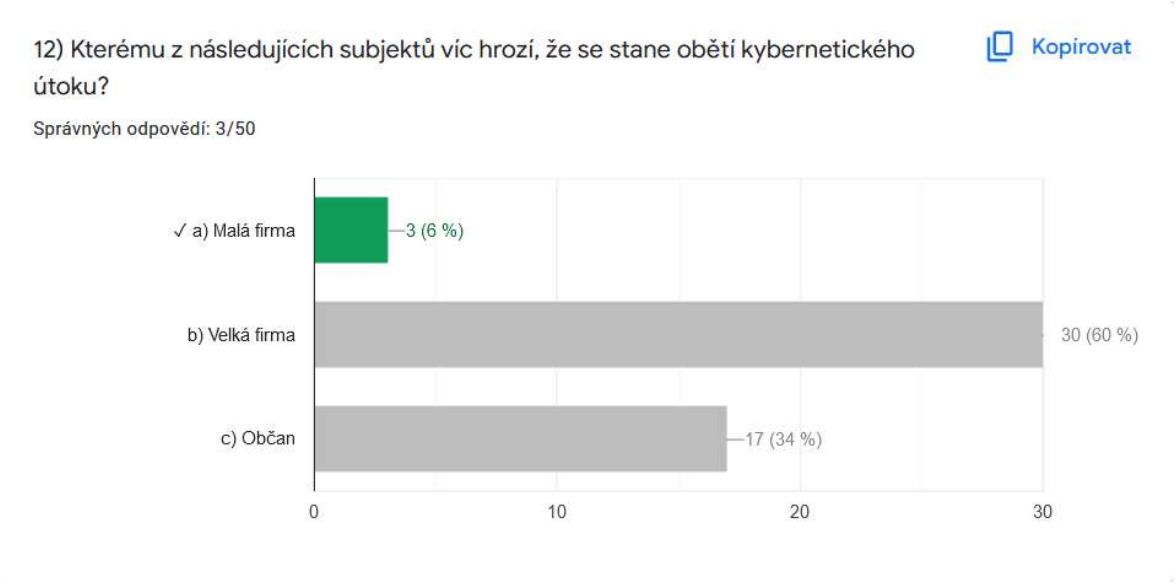
Obr. 10 – Otázka č. 10. vstupního ověření.

Otázka č. 11. – v této otázce (Obr. 11) si 66 % účastníků uvědomuje rizika spojená s používáním vlastního zařízení v zaměstnání.



Obr. 11 – Otázka č. 11. vstupního ověření.

Otázka č. 12. – zde si jenom 6 % účastníků (Obr. 12) uvědomuje, že zločinci sice útočí na firmy všech velikostí, ale že malé firmy jsou ohrožovány více, protože mají omezenější finanční možnosti a odborné znalosti v oblasti ochrany ICT prostředků a dat. Mnohdy nepoužívají odpovídající zabezpečení.

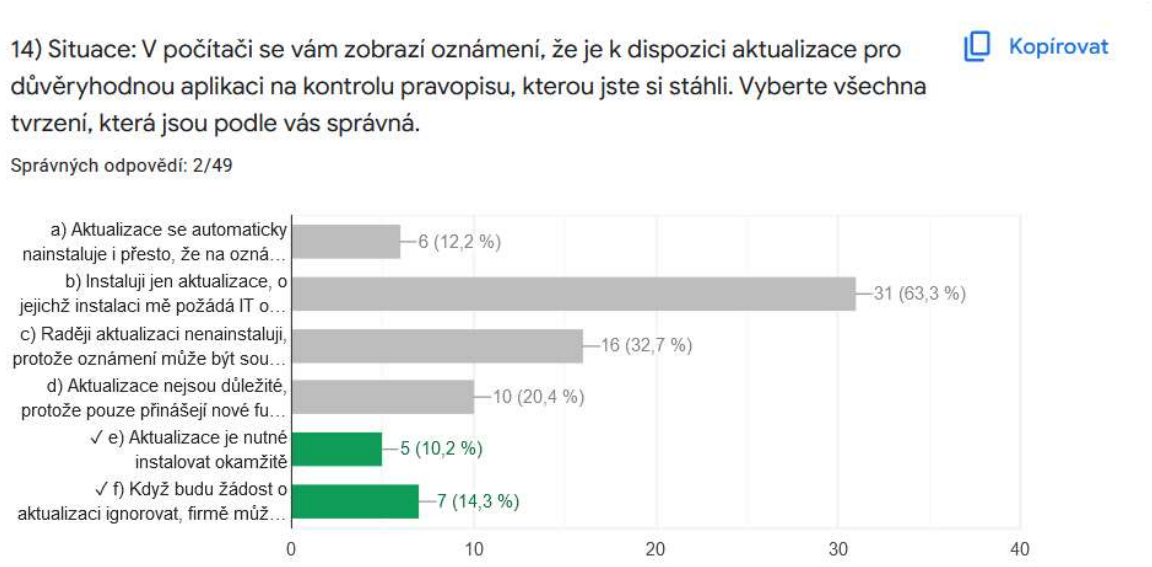


Obr. 12 – Otázka č. 12. vstupního ověření.

Otázka č. 13. – v této otázce (Obr. 13) 92 % účastníků zná pravidla používání bezpečných hesel.

Obr. 13 – Otázka č. 13. vstupního ověření.

Otázka č. 14. – zde si bohužel jen malé procento účastníků uvědomuje (Obr. 14), že když budou žádost o aktualizaci důvěryhodné aplikace ignorovat, organizaci může hrozit riziko kybernetického útoku. Takové aktualizace je nutné instalovat okamžitě, protože často obsahují opravy bezpečnostních nedostatků v původním kódu a uživatelé nemusí čekat na žádost nebo povolení aktualizace od ICT oddělení.

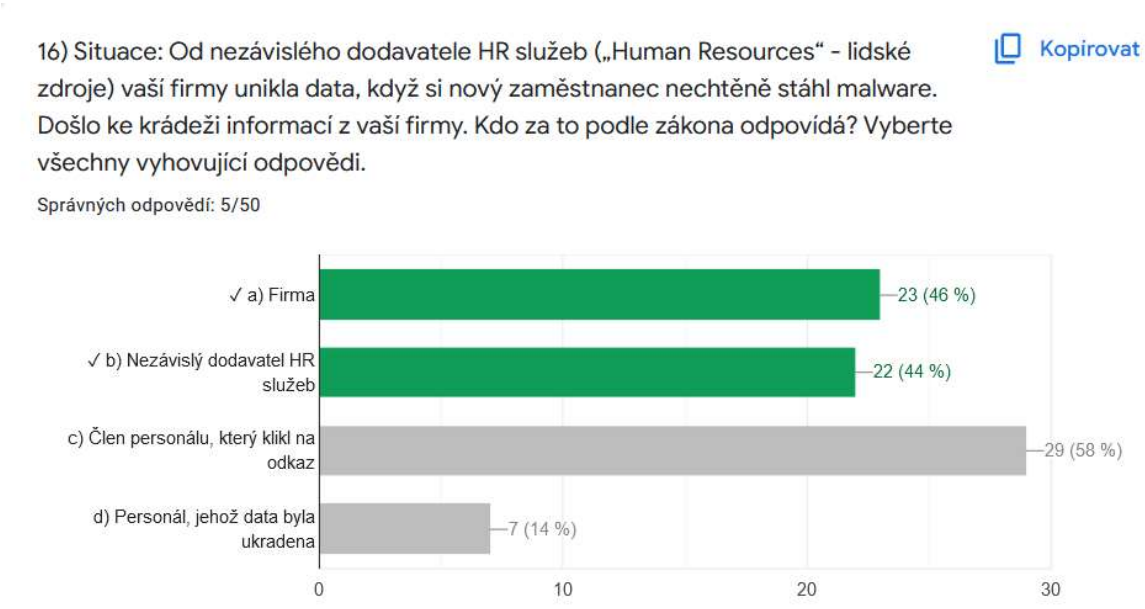


Obr. 14 – Otázka č. 14. vstupního ověření.

Otázka č. 15. – v této otázce (Obr. 15) si jenom 32 % účastníků připouští fakt, že úniky dat mohou být důsledkem útoků zevnitř organizace (například zkorumpovanými zaměstnanci nebo dodavateli), ale také mohou být způsobeny neúmyslnými chybami personálu.

Obr. 15 – Otázka č. 15. vstupního ověření.

Otázka č. 16. – zde účastníci zhruba v polovině případů vědí (Obr. 16), že se firma musí postarat o to, aby všechny služby, včetně nezávislých poskytovatelů, které nakládají s jejími daty, dodržovaly předpisy ohledně ochrany dat. Ale v 58 % mylně vnímají odpovědnost zaměstnance, protože podle zákona o kybernetické bezpečnosti (4) sice všichni zaměstnanci musí vědět, jak chránit data, ale většina personálu za úniky dat odpovědná není.

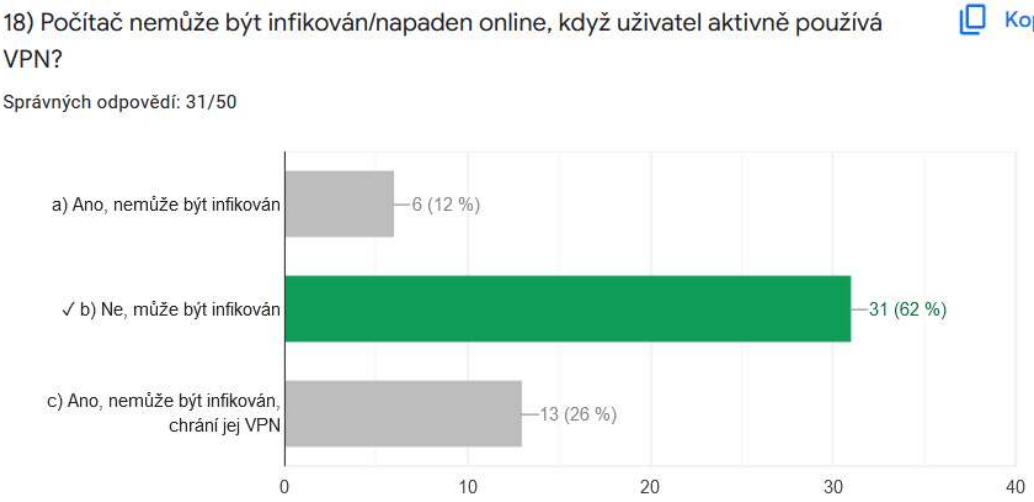


Obr. 16 – Otázka č. 16. vstupního ověření.

Otázka č. 17. – v této otázce (Obr. 17), podle dosažených procentuálních bodů, si účastníci dobře uvědomují potřebu používání komplexní bezpečnostní strategie, která zahrnuje všechny uvedené aspekty.

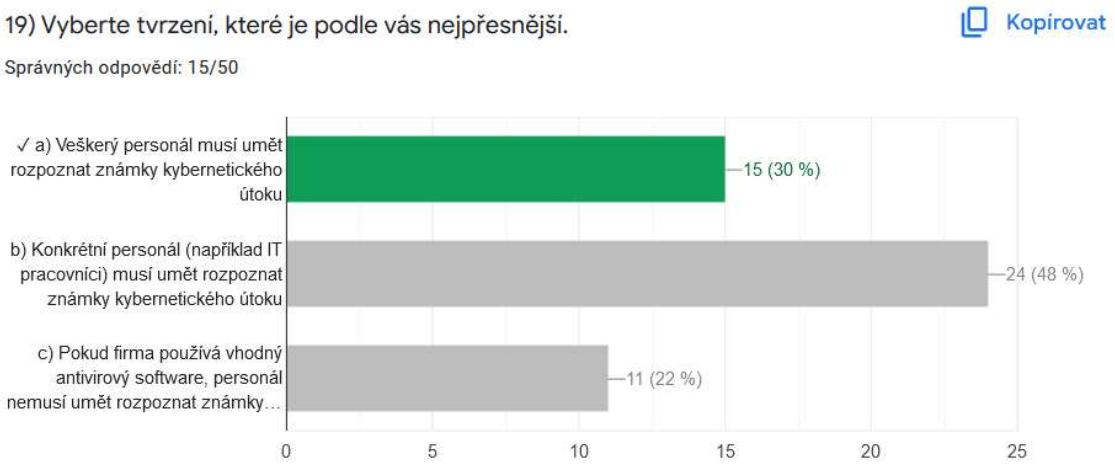
Obr. 17 – Otázka č. 17. vstupního ověření.

Otázka č. 18. – zde je částečně navázáno na předchozí otázku (Obr. 18), účastníci v 62 % vědí, že VPN sice může pomáhat s ochranou online soukromí, nelze ji však používat jako jediné bezpečnostní řešení.



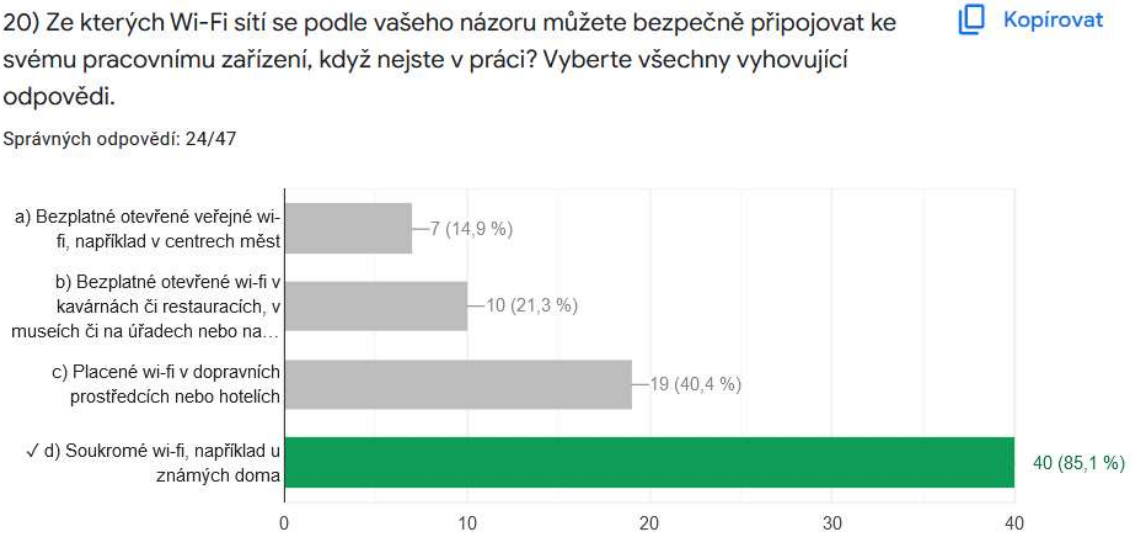
Obr. 18 – Otázka č. 18. vstupního ověření.

Otázka č. 19. – v této otázce (Obr. 19) si účastníci bohužel jen v 30 % uvědomují, že kybernetický zločin se neustále vyvíjí a šíří. Napadeno může být libovolné zařízení, škodlivý obsah občas dokáže proniknout i automatickou ochranou, a proto všichni zaměstnanci musí vědět, jak rozpoznat kybernetický útok.



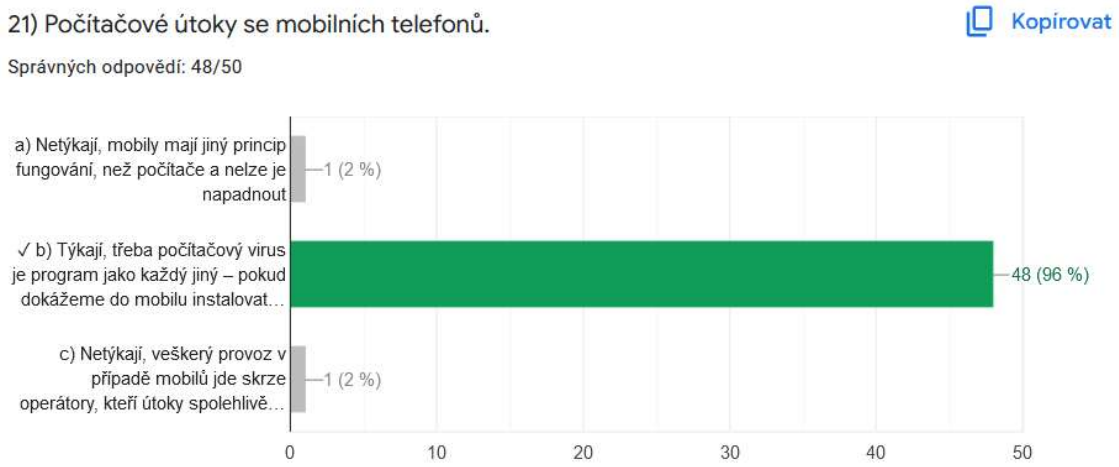
Obr. 19 – Otázka č. 19. vstupního ověření.

Otázka č. 20. – zde účastníci zhruba v 85 % vědí (Obr. 20), že používání soukromých Wi-Fi je nejbezpečnější, protože je známo, kdo sítě nastavil a kdo se k nim nejspíše připojuje a jaké má úmysly (kolegové, rodina či přátelé). Stále si ale v poměrně velkém procentu neuvědomují fakt, že placené sítě nejsou zárukou bezpečí.



Obr. 20 – Otázka č. 20. vstupního ověření.

Otázka č. 21. – v této otázce (Obr. 21) si v 96 % účastníci správně uvědomují, že mobilní telefon je zařízení stejné jako jakékoliv jiné a může být i stejným způsobem napadeno a infikováno.



Obr. 21 – Otázka č. 21. vstupního ověření.

2.5.2 ANALÝZA A VYHODNOCENÍ VÝSLEDKŮ PÍSEMNÉHO TESTU

Z vyhodnocení zadaného testu na základy digitální gramotnosti a bezpečnosti vyplývá, že v cílové skupině jsou pro naši potřebu znalosti na předpokládané úrovni. Povědomí o specifických prostředcích, nástrojích, funkcích a bezpečnostních prvcích, jako je elektronický podpis, end-to-end šifrování, anonymní režim a VPN, je celkově vysoké a rozšířené. Členové cílové skupiny vědí, co je a jak vypadá Hoax, že hesla uložená v internetovém prohlížeči nejsou v bezpečí před útočníky a zabezpečené připojení se musí provádět přes protokol HTTPS. Uvědomují si, že zabezpečení musí nést aspekty komplexního řešení, včetně používání antivirových programů, firewallů, dvojstupňového ověřování a používání silných hesel. Je potřeba organizovat školení všech zaměstnanců a to v rámci zákona o kybernetické bezpečnosti (4), protože útoky na internet mohou být ve své podstatě jednoduché a tím i nevyzpytatelné. Nemíří obvykle na konkrétního uživatele, ale čekají, kdo neznalý se chytí. Spoléhají například na to, že uživatel něco přehlédne nebo udělá chybu v časové tísni. Vědí, že používání vlastního zařízení k práci je obvykle rizikovější, než používání zařízení od zaměstnavatele, protože toto zařízení není chráněné firemním bezpečnostním řešením a tak se může připojovat i k nezabezpečeným a rizikovým Wi-Fi sítím nebo do něj mohou být staženy škodlivé aplikace. Znají fakt, že připojování

k soukromým Wi-Fi sítím je bezpečnější. U těchto sítí je známo, kdo a jak síť nastavil a kdo se k ní připojuje.

Bohužel dostatečně necítí nebezpečí v používání placených veřejných Wi-Fi sítí a přes ně odesílaných dat citlivějšího charakteru, protože placené neznamená bezpečné. Ve velmi vysokém procentu si neuvědomují, že sice útočníci cílí na firmy všech velikostí, ale malé firmy jsou jimi ohrožovány nejvíc. Většinou tyto společnosti mají jen omezené finanční možnosti a odborné znalosti v oblasti ochrany ICT prostředků a mnohdy nepoužívají odpovídající zabezpečení. Úniky dat mohou být často důsledkem útoků zevnitř organizace, ale také mohou být způsobeny neúmyslnými chybami personálu.

Zhruba v polovině případů vědí, že se firma nebo organizace ze zákona musí postarat o to, aby všechny služby, včetně nezávislých poskytovatelů, které nakládají s jejími daty, dodržovaly předpisy ohledně ochrany dat. Také si mylně vykládají odpovědnost zaměstnance podle zákona o kybernetické bezpečnosti. (4) Všichni zaměstnanci musí sice vědět, jak chránit data, ale většina personálu za úniky dat neodpovídá.

Jen v malém procentu si připouštějí fakt, že když bude žádost o aktualizaci důvěryhodné aplikace ignorována, organizaci může hrozit riziko kybernetického útoku. Takové aktualizace je nutné instalovat okamžitě, protože často obsahují opravy bezpečnostních nedostatků v původním kódu a nemusejí čekat na žádost nebo povolení aktualizace od ICT oddělení. S tím je spojeno nedostatečné si uvědomování faktu, že kybernetický zločin se neustále vyvíjí a rozšiřuje do více oblastí. Napadeno může být libovolné zařízení. Škodlivý obsah dokáže občas proniknout i automatickou, aktualizovanou ochranou, a proto všichni zaměstnanci musí umět rozpoznávat kybernetické útoky.

Zhodnocením výsledků testu byla shledána potřeba vypracování konkretizovaného školícího materiálu, který nejenže prohloubí a zopakuje všeobecné znalosti a informace o kybernetické bezpečnosti, ale zejména bude mířit na oblasti, ve kterých cílová skupina vykazovala nejslabší výsledky.

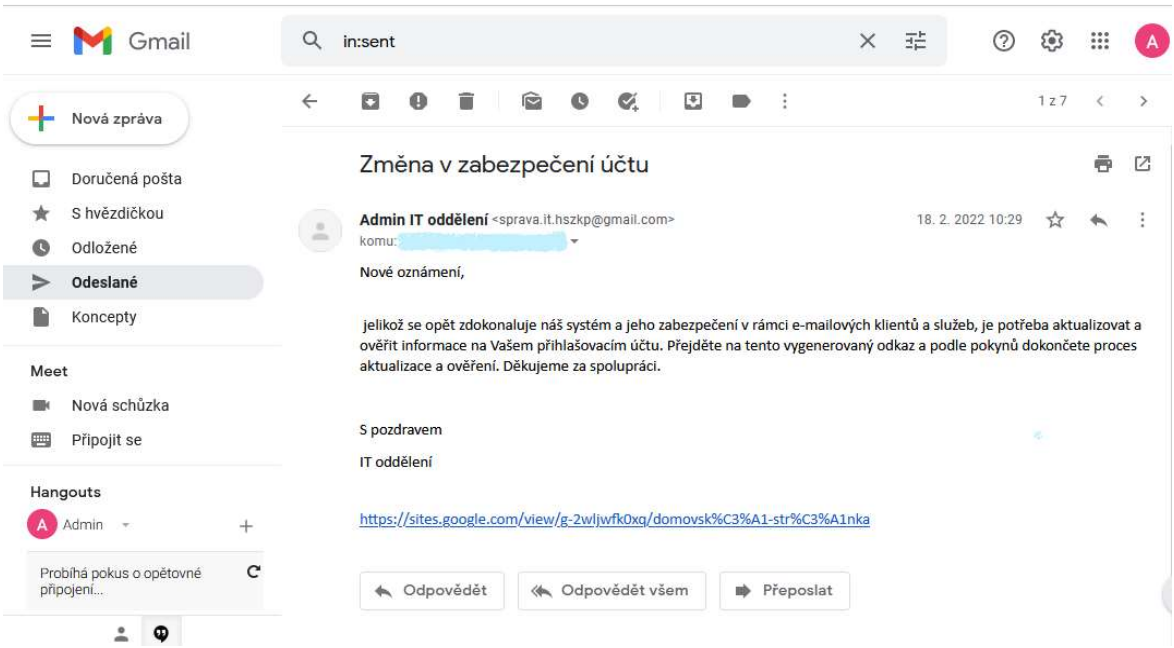
2.5.3 DRUHÁ ČÁST VSTUPNÍHO OVĚŘENÍ

Jako druhá část vstupního ověření byl rozeslán e-mail s externím odkazem. Text sdělení je záměrně napsán tak, aby na první pohled působil běžným a neškodným obsahem. Následně

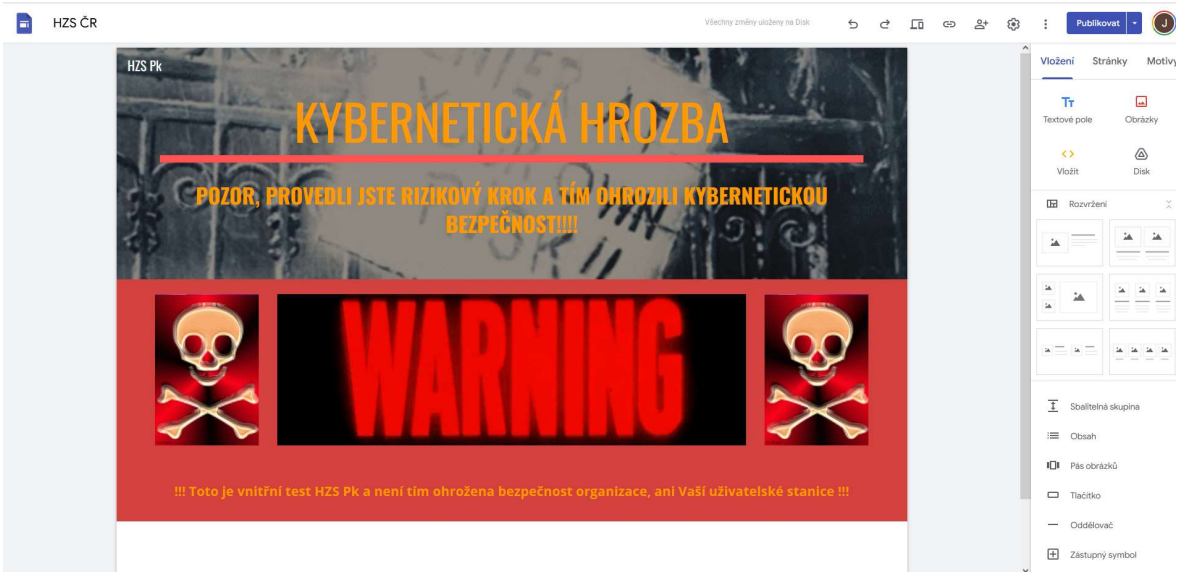
byla sledována reakce na tento e-mail a statistika přechodu uživatelů k otevření externího odkazu.

Pro účely rozeslání je založen bezplatný účet s e-mailem u společnosti Google. Rovněž jednoduchá webová prezentace pro externí odkaz byla vytvořena v nástroji Google Weby (Google Sites).

Text zkušebního emailu (Obr. 22) obsahuje sdělení o potřebě aktualizace uživatelského účtu a nabádá k otevření externího odkazu (Obr. 23) a tím ověření osobních údajů a informací.



Obr. 22 – Text zkušebního emailu.



Obr. 23 – Forma webové prezentace pro externí odkaz.

U HZS Pk je používáno několik druhů a úrovní uživatelských účtů s e-mailovými adresami. První úroveň je založena na popisném způsobu. V místní části adresy je uvedena funkce a dislokace, např. bozkov.dispecerka@hzspk.cz. Od této formy, která má do určité míry všeobecný charakter a může být potenciálním rizikem, se postupně upouští. Postupně se přechází na úrovně personalizovaných účtů a e-mailů, kde místní část adresy obsahuje osobní evidenční číslo. Každý zaměstnanec a příslušník HZS ČR vlastní specifické číslo, proto e-mailová adresa má tvar např. 700007@hzspk.cz. Tímto způsobem je zaručeno, že účty a e-maily jsou lépe chráněny, zlepšuje se kontrola a dohledatelnost konkrétních aktivit na nich. Delší dobu používanou, ale podobnou úrovní je forma, kde v místní části adresy je jméno a příjmení uživatele, např. jmeno.prijmeni@hzspk.cz.

Tato bakalářské práce vzniká v době, kdy jsou e-mailové útoky pravidelně stupňovány a v období ozbrojeného konfliktu na území Ukrajiny. V souvislosti s tímto stavem je dokonce NÚKIB podle § 12, odst. 1 zákona č. 181/2014 Sb. o kybernetické bezpečnosti vydáno varování s kritickou úrovní. Ve znění – *„Varování před hrozbou v oblasti kybernetické bezpečnosti, spočívající v realizaci kybernetických útoků na informační a komunikační systémy v České republice, zejména pak na systémy veřejné správy, ale i dalších strategických organizací.“*

Pro uvedenou zhoršenou situaci ve společnosti a po konzultaci s oddělení KIS HZS Pk, se kterým v úzké spolupráci tato bakalářská práce vzniká, a po poradě s jeho pověřeným příslušníkem za kybernetickou bezpečnost u složky HZS Pk, bude e-mail se zkušebním textem rozeslán pouze do jedné části cílové skupiny. Test se bude týkat úrovně e-mailových adres, ve kterých jsou v místní části uvedeny osobní evidenční čísla. Tato úroveň je u HZS Pk používaná nejkratší dobu, a proto nebyla doposud vystavena takovému množství rozesílaných škodlivých textů a sdělení. V rámci cílové skupiny tuto úroveň nejvíce zastupují příslušníci sloužící ve směnách, na hasičských stanicích, a ti ji využívají minimálně. Většinou jen pro komunikaci s personálním oddělením a příjem zpráv určených všem zaměstnancům a příslušníkům HZS Pk. Tím mají menší zkušenost s příchozími rizikovými e-maily do organizace. Úroveň, ve které je její součástí jméno a příjmení je využívá nejdéle a vlastníkem je přibližně polovina členů cílové skupiny. Tito uživatelé e-mailové adresy používají ke každodenní práci a komunikaci. Mají také nejvíce zkušeností s podobnými útoky a podvodnými e-maily. V drtivé většině okamžitě reagují na všechny nestandartní

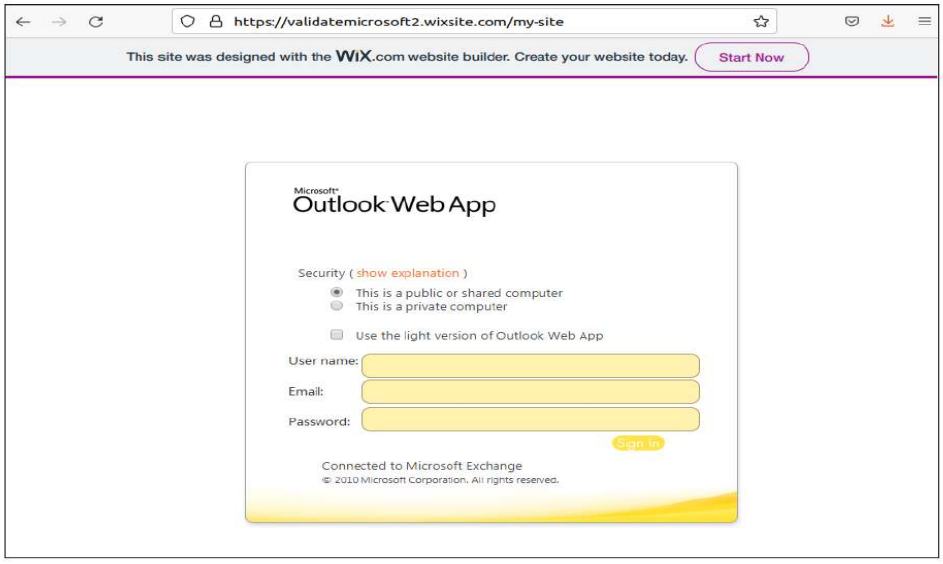
e-maily a kontaktují oddělení KIS HZS Pk. Tato reakce je podpořena dlouhodobou činností a prací pověřeného příslušníka za kybernetickou bezpečnost u složky HZS Pk, který pravidelně a okamžitě upozorňuje na všechny nové příchozí hrozby. Zároveň stále a systematicky, v každém rozeslaném e-mailu s upozorněním na novou hrozbu, připomíná tato základní pravidla práce s e-mailovou poštou:

- **věnovat zvýšenou pozornost přijímaným podezřelým e-mailovým zprávám** od nedůvěryhodných kontaktů, na podezřelé e-maily nereagovat, nenačítat externí obrázky, neotevírat soubory v příloze a neklikat na žádné odkazy,
- kontrolovat e-mailovou adresu odesílatele a **mít na paměti, že i důvěryhodný odesílatel může mít napadenou e-mailovou schránku nebo adresa může být podvržená,**
- být na pozoru v případě urgentních nebo neobvyklých požadavků (např. požadavek na aktualizaci přihlašovacích údajů do různých služeb – typicky e-mail),
- **nebezpečné jsou dokumenty kancelářské sady Office, které vyžadují povolení spuštění maker,**
- nepovolovat makra u dokumentů z nedůvěryhodného zdroje,
- **obzvláště nebezpečné jsou přílohy typu *.exe, *.com, *.vb, *.vbs, *.bat,**
- v případě nejistoty nebo podezření kontaktovat oddělení KIS HZS Pk.

Dále je jeho snahou pomocí grafiky a snímků obrazovky co nejlépe popsat a přiblížit příchozí nebezpečí všem běžným uživatelům. Zde je uvedena ukázka (Obr. 24, Obr. 25) z výše popsané činnosti pověřeného příslušníka za kybernetickou bezpečnost u složky HZS Pk.

Obrázek č. 1: Podvodný e-mail s výzvou k aktualizaci účtu. Nedůvěryhodný odesílatel z ruské domény.

Obr. 24 – Popsaná hrozba od manažera kybernetické bezpečnosti.



Obrázek č. 4: Podvodná webová stránka s formulářem pro zadání přihlašovacích údajů do Outlook webové aplikace. Z kontroly URL je patrné, že se jedná o nedůvěryhodný web provozovaný na doméně služby Wixsite.com.

Obr. 25 – Popsaná hrozba od manažera kybernetické bezpečnosti.

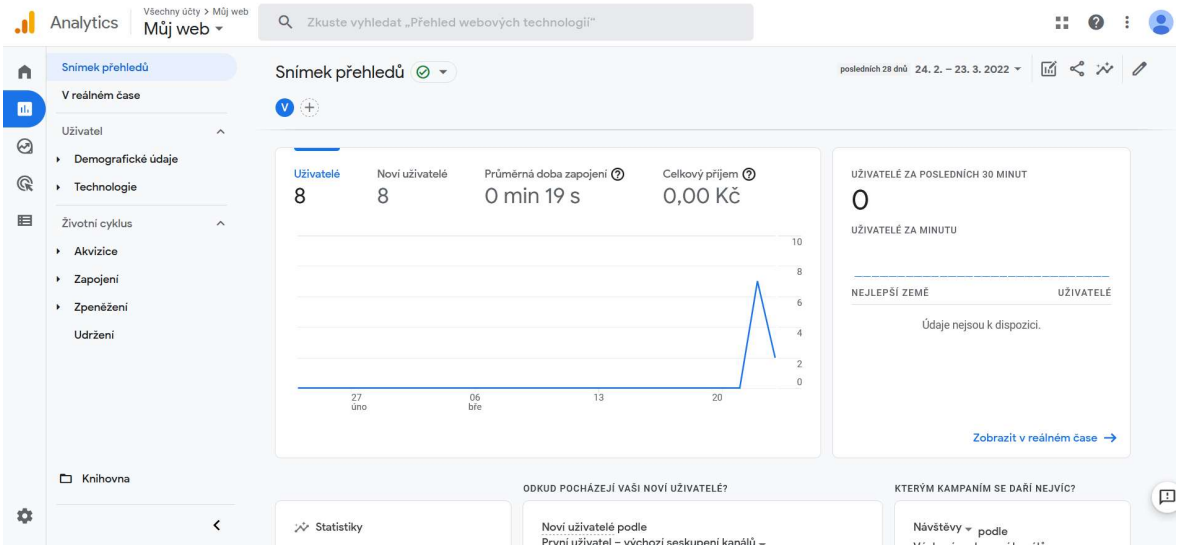
2.5.4 ANALÝZA A VYHODNOCENÍ VÝSLEDKŮ ROZESLANÉHO E-MAILU

Pro vyhodnocení počtu přechodů, a tím otevření externího odkazu v uvedeném zkušebním e-mailu v definované části cílové skupiny, je použit nástroj Google Analytics od společnosti Google. Umožňuje získávat statistická data o uživatelích webových stránek a díky této službě je možné sledovat aktuální i historickou návštěvnost.

Sdělení, které je zasláno od externího a soukromého poskytovatele e-mailových účtů, by již při přijetí e-mailu mělo být prvním signálem, že toto není standartní postup. V uživatelském

jméně účtu jsou jako další, v náhodném pořadí, použita klíčová slova a písmena připomínající adresu organizace HZS Pk, což by mělo být dalším podnět pro zamyšlení o pravosti zaslané zprávy. Již uvedené prvotní signály by měly vést při nejmenším k obezřetnosti a zamyšlení. Odkaz, který na první pohled převádí uživatele na soukromé externí webové stránky, je zlomový okamžik pro odrazení od další činnosti. Uživatel musí e-mail označit jako spam a nahlásit příslušnému oddělení KIS HZS Pk.

E-mail byl odeslán třiceti pěti členům cílové skupiny. S týdenní dobou odstupu od odeslání byla v uvedeném nástroji Google Analytics provedena analýza a statistika návštěvnosti webové stránky z přiloženého externího odkazu. Z této statistiky vyplývá, že přiložený externí odkaz otevřelo 8 osob (Obr. 26), což odpovídá 1/5 dotčených. Těchto 20 procent je již poměrně vyšší poměr záchytu, který pravděpodobně souvisí s malou vytížeností v používání e-mailové adresy. Příčina je v nedůsledném přijímání a čtení hromadných sdělení, a tím si neuvědomění hrozícího rizika.



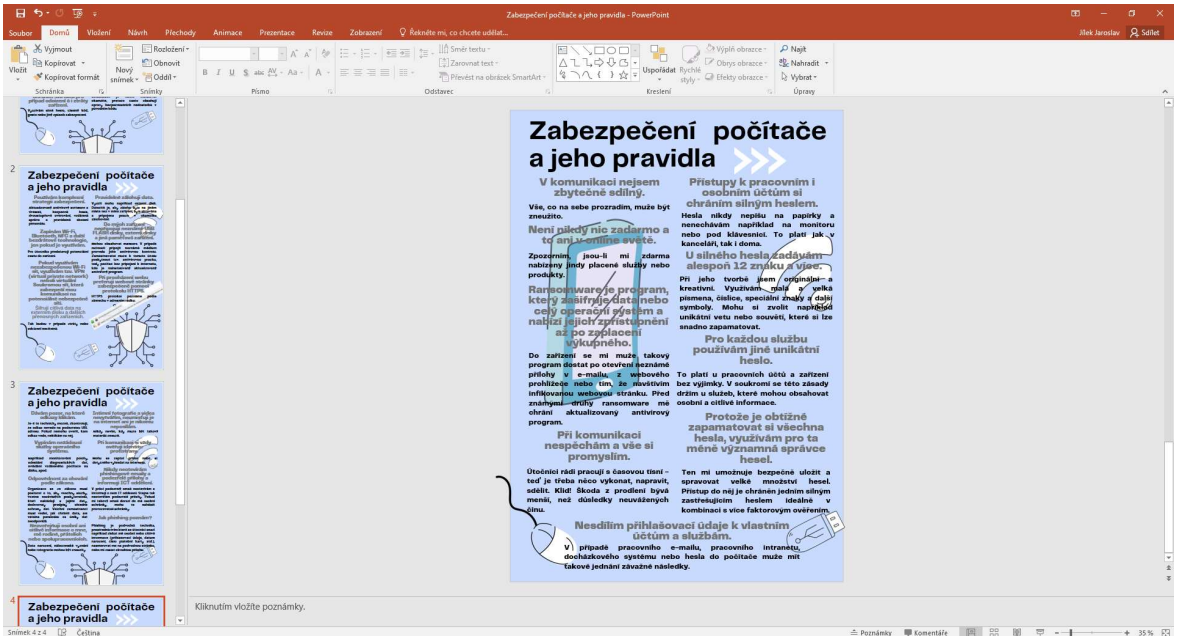
Obr. 26 – Statistika z Google Analytics.

Zbylé části členů cílové skupiny nebyl z výše uvedených pracovních a společenských důvodů zkušební e-mail rozeslán. Pro potřeby analýzy kybernetické bezpečnosti byla však oddělením KIS HZS Pk poskytnuta reálná data, která byla získána při zjištění a záchytu posledního rizikového e-mailu. Tato data mají velkou vypovídající hodnotu, protože jsou posbírána z mnohem širší základny, než je počet členů cílové skupiny. Z poskytnuté statistiky vyplývá, že z přibližně 250 přijatých potencionálně rizikových e-mailů byl externí odkaz otevřen jen ve čtyřech případech. Což je velmi dobrá úroveň znalostí o kybernetické

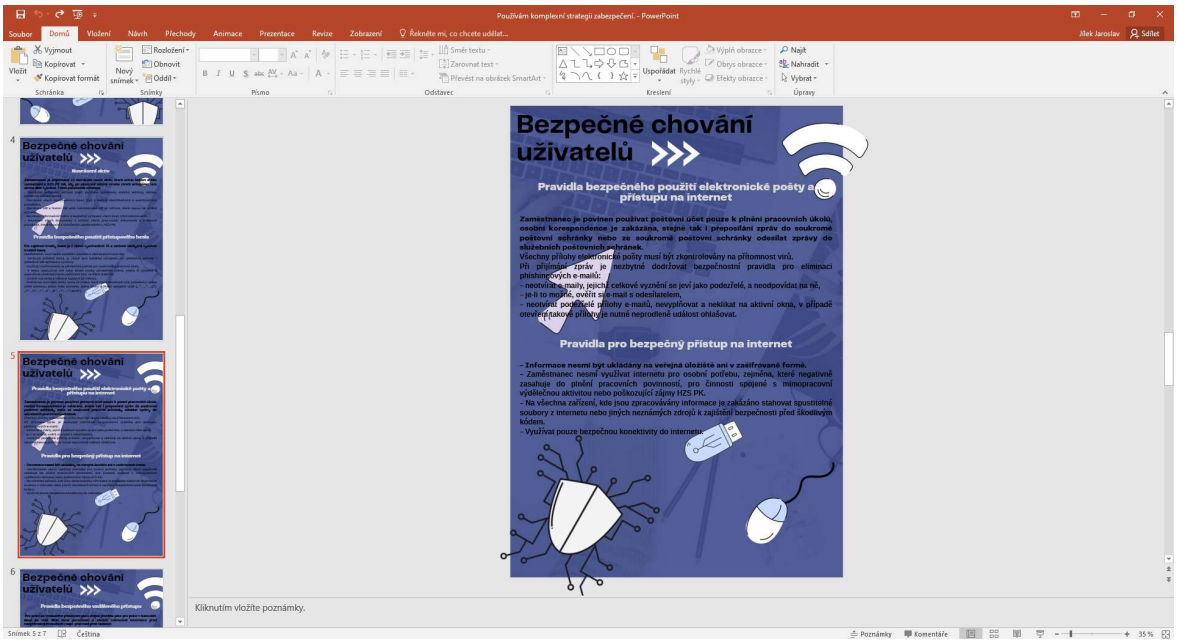
bezpečnosti, svědčící o velké míře obezřetnosti, pravděpodobně způsobenou každodenním používáním e-mailové adresy a podpořeno preventivním působením celého oddělení KIS HZS Pk.

2.6 TVORBA A REALIZACE ŠKOLÍCÍHO VÝUKOVÉHO MATERIÁLU

Jako nejlepší způsob pro zpracování školícího a výukového materiálu bylo společně s oddělením KIS HZS Pk vybráno několik forem. V první řadě byla problematika zpracována v nástroji pro tvorbu obrazových prezentací, např. PowerPoint od společnosti Microsoft (Obr. 27, Obr. 28).



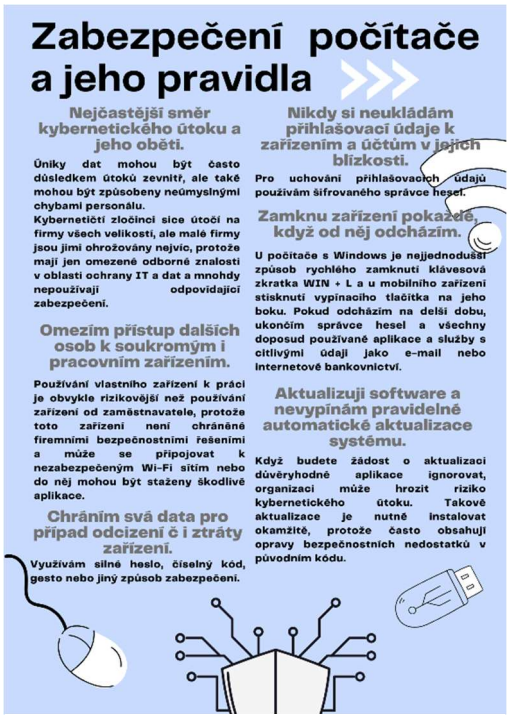
Obr. 27 – Ukázka vytvořené prezentace v PowerPointu.



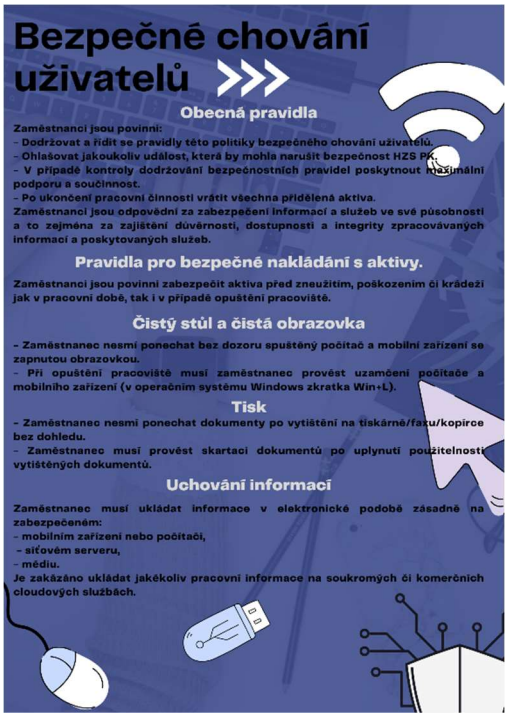
Obr. 28 – Ukázka vytvořené prezentace v PowerPointu.

Z uvedené prezentace jsou zpracovány dva grafické soubory velkoformátových plakátů (Obr. 29, Obr. 30), které oddělení OKIS HZS Pk rozešle na všechna oddělení Krajského ředitelství a také na Územní odbory v celém Plzeňském kraji. Zde budou soubory plakátů vyvěšeny pro dlouhodobou osvětu všech zaměstnanců. První soubor plakátů je zaměřen na všeobecná pravidla zabezpečení počítače a pohybu v kybernetickém prostoru. Zde je také kladen větší důraz na oblasti, ve kterých cílová skupina dosahovala slabších výsledků. Druhá část souboru plakátů již konkrétně popisuje pravidla bezpečného chování zaměstnanců a příslušníků HZS Pk v digitálním světě, tato pravidla musejí všichni znát a dodržovat.

V poslední řadě může být z uvedené prezentace nebo souboru plakátů, pomocí některého volně dostupného a stažitelného programu, vytvořen soubor jako spořič obrazovky. Ten oddělení KIS HZS Pk může umístit do možností nastavení operačních systému u všech stolních počítačů v organizaci, s možností individuálního využití jednotlivými zaměstnanci a příslušníky HZS Pk.



Obr. 29 – Ukázka všeobecných pravidel zabezpečení.



Obr. 30 – Ukázka bezpečného chování zaměstnanců.

2.7 APLIKACE VYTVOŘENÉHO ŠKOLÍCÍHO A VÝUKOVÉHO MATERIÁLU

Vytvořenou prezentací byla v rámci pravidelné odborné přípravy proškolena celá cílová skupina. Části cílové skupiny, kterou tvoří zaměstnanci pracující na ekonomickém úseku, ve finančním oddělení a oddělení provozním a správy majetku krajského ředitelství HZS ČR, byl rozeslán informační e-mail od oddělení KIS HZS Pk. Zde je vznesen požadavek na individuální seznámení se s obrazovou prezentací školícího materiálu. V e-mailu jsou také uvedeny kontaktní údaje na autora bakalářské práce a na pověřeného příslušníka za kybernetickou bezpečnost z oddělení KIS HZS Pk, pro případné objasnění a vysvětlení vyvstalých nejasností. Prezentace byla vložena na intranetovou síť organizace s volným přístupem k jejímu obsahu pro další potřeby a školení ostatních zaměstnanců a příslušníků.

Ve druhé části cílové skupiny, kterou zastupují příslušníci sloužící ve třísměnném modelu střídání směn na hasičských stanicích, jako výjezdoví hasiči, bylo školení provedeno pomocí vypracované prezentace na každé aktuálně sloužící směně osobně autorem bakalářské práce. V tomto bloku školení byl ještě zvýšen důraz na rozbor příchozích e-mailů a rozpoznání potencionálního rizika. Rozeslaný zkušební e-mail a několik posledních e-mailů s možným škodlivým sdělením, poskytnutých od pověřeného příslušníka za kybernetickou bezpečnost u složky HZS Pk, bylo jednotlivě otevřeno a konkrétně

rozebráno. Znovu a s velkým důrazem je připomínáno, v čem je potřeba spatřovat a hledat rizika a jak správně reagovat při takovém zjištění nebo podezření.

Protože reakce na rizikové e-maily byly první částí cílové skupiny velmi dobré, plynoucí z poskytnutých dat oddělením KIS HZS Pk, a ze zvýšeného důrazu při školení druhé části cílové skupiny, kde byl při rozboru uveden autor a účel zkušebního e-mailu, upustilo se od opětovného rozesílání e-mailu. Je předpoklad, že by reakce celé cílové skupiny byla na vysoké úrovni.

Zbylé dvě formy zpracovaného výukového materiálu byly autorem bakalářské práce poskytnuty oddělení KIS HZS Pk, které tyto materiály zapracuje do své koncepce prevence kybernetické bezpečnosti a bude je používat a distribuovat do celé struktury HZS Pk.

Při prověřování možnosti umístění výukového materiálu na intranetové webové stránky HZS Pk byl autorem bakalářské práce zjištěn fakt, že intranetové stránky mají zastaralý vzhled a formou, neodpovídají moderním potřebám a požadavkům. Například oblasti kybernetické bezpečnosti je zde věnován jen minimální prostor. Z konzultace s oddělením KIS HZS Pk vzešlo ujištění, že nové a dnešní době odpovídající intranetové webové stránky budou v nejbližší době spuštěny. Zde již například kybernetické bezpečnosti, ale i kompletně celé problematice ICT, bude věnována celá sekce. Zároveň byl dohodnut další přesah bakalářské práce. Vypracovaný výukový materiál se stane základním kamenem této sekce a budou na něj navazovat další důležitá upozornění a informace, včetně aktuálních kybernetických hrozeb.

2.8 VYHODNOCENÍ APLIKACE A DOPADU VÝUKOVÉHO MATERIÁLU NA CÍLOVOU SKUPINU

Po provedeném komplexním školení v celé cílové skupině byl všem členům opětovně zadán a rozeslán pomocí Google Formuláře text písemného testu, v totožném znění jako byl vstupní. Test byl zpřístupněn nebo rozeslán minimálně s čtrnáctidenním odstupem od podstoupeného školení, aby se zvětšila vypovídající hodnota dopadu výukového materiálu. Z dostupné statistiky vyplývá, že aplikace výukového materiálu měla velice přínosný dopad na všechny členy cílové skupiny. Podle této statistiky se zlepšily a utřídily znalosti v oblasti kybernetické bezpečnosti a celkově se rozšířilo povědomí o pohybu v digitálním světě. Také při osobní konzultaci autora bakalářské práce s některými členy cílové skupiny byl kvitován

individuální přístup k potřebám jednotlivých částí cílové skupiny a jejich zapracování do výukového matriálu.

2.8.1 ZHODNOCENÍ ÚSPĚŠNOSTI OTÁZEK ZKUŠEBNÍHO PÍSEMNÉHO TESTU PŘI JEHO PRVOTNÍM A OPAKOVANÉM ZADÁNÍ

V této části jsou v blocích popsány a vyhodnoceny jednotlivé otázky písemného testu, který byl všem členům cílové skupiny zadán s časovým odstupem od prodělaného školení o kybernetické bezpečnosti, jak bylo popsáno výše.

Ve stejné formě, jako u popisu úrovně vstupního písemného testu, jsou všechny otázky vykopírované z aplikace Google Formuláře a uvedeny v příloze této bakalářské práce (Obr. 31 – Obr. 51).

První otázka testu byla opět jako jediná povinná a popisovala věkové složení cílové skupiny.

V bloku otázek č. 2 – 4., ve kterém byla již ve vstupním testu úspěšnost odpovědí nad úrovní 70 %, se u všech otázek úroveň ještě zlepšila a přiblížila se 90 %. Tato část se týkala variant elektronického podpisu, bezpečnosti ukládání přístupových hesel v prohlížeči a způsobu útoků na uživatele internetu.

U otázky č. 5., ve které při vstupním testu jako u první neuspokojivě zodpovězené otázky byl nízký, maximálně 1/3 počet správných odpovědí, se díky přesně zacílenému školení zvedl počet správných odpovědí až na více jak 78 %. Otázka č. 5., společně s otázkami č. 8. a č. 20. se věnovaly problematice bezpečnosti a způsobu přihlašování do různých typů Wi-Fi sítí a využití šifrovaných internetových protokolů. Byly součástí speciálně a cíleně vytvořenému bloku školení, který se této oblasti podrobněji věnoval. Sice další dvě zmíněné otázky neměly tak nízkou úroveň správných odpovědí, ale hlavně u otázky č. 20 stále vycházelo při možnosti výběru mnoho nesprávných závěrů.

Otázky č. 6., 7., 9., 10., 11., 18. a 21., které se věnovaly spíše technickým záležitostem a názvosloví jako je end-to-end šifrování, anonymní režim, VPN, Hoax, riziku používání vlastního zařízení k pracovní činnosti a principům útoků na mobilní zařízení, si všechny zvýšily většinou již i tak vysokou úspěšnost odpovědí, pohybující se nyní nad hladinou 80 %.

V bloku otázek ohraničujících prostor hrozeb kybernetického útoku, jeho potenciálních tvůrců a obětí, potřeb akceptace a instalování aktualizací, odpovědnosti vyplývající ze zákona o kybernetické bezpečnosti (4) a aspektech komplexního kybernetického

zabezpečení vykazující se ve vstupním testu nejslabšími výsledky, nepřesahující vytýčenou 50% hranici úspěšnost. Uvedené v otázkách 12., 14., 15., 16. a 17., zapůsobilo školení v největší rozsahu a míře. Všechny otázky v opakovaně zadaném písemném testu dosáhly velmi dobré procentuální úspěšnosti pohybující se nad hranicí 70 %.

ZÁVĚR

Svět kolem nás obklopují a protínají moderní technologie a jejich používání se stalo nedílnou součástí našeho života. Jsou rozšířeny do mnoha odvětví, o kterých jsme si ještě donedávna mysleli, že tímto proudem pokroku nebudou nikdy nebo přinejmenším v nebližší době vůbec ovlivněna. S rozmachem a používáním technologií připojených do kybernetického prostoru jde však ruku v ruce i nebezpečí útoku a následné poškození. Proto na bezpečnost a ochranu musí být kladen velký důraz a toto odvětví se musí stále zdokonalovat a vyvíjet. V dnešní době již každý uživatel, bez rozdílu věku nebo vzdělání, musí mít základní povědomí a z toho vyplývající odpovědnost za používání.

Dílčím cílem bakalářské práce bylo na úzké a konkrétní skupině osob ověřit a analyzovat úroveň digitální gramotnosti a povědomí v oblasti její bezpečnosti. Hlavním cílem však zůstalo navržení a vytvoření materiálu, který by měl vést ke zlepšení uživatelských znalostí. Tuto skupinu osob spojoval pouze společný zaměstnavatel a tím i jednotná pravidla pro používání. V praktické části byla včetně upřesnění zásad a podmínek používání ICT prostředků u složky HZS Pk, popsána forma a výběr cílové skupiny uživatelů. Po jejím definování jí byl zadán vstupní test, který se skládal ze dvou částí a stanovil hladinu znalostí o digitálním prostředí a bezpečnosti. Praktická část bakalářské práce vychází z teoretické, ve které je všeobecně vymezen pojem kybernetického útoku jako takového. Je vyzdvihnuta potřeba kybernetické bezpečnosti, stručně popsána základní složka IZS ČR, její moderní historie a základní právní rámec. Taktéž zde byly uvedeny nejdůležitější právní normy týkající se počítačové bezpečnosti a na závěr rozděleny nejčastější druhy kybernetických útoků a všeobecné bezpečnostní zásady.

Zmapování vstupní úrovně se skládalo ze dvou částí, kde byly nezávisle na sobě zadány písemné testy a rozeslány e-maily s externím odkazem a textem o nebezpečnosti chování.

Analýzou vstupního testu bylo zjištěno, že znalosti v cílové skupině jsou na odpovídající úrovni. Většina respondentů měla dostačující povědomí o specifických prostředcích, nástrojích, funkcích a bezpečnostních prvcích.

Z písemného testu vyplynulo, že členové cílové skupiny dostatečně necítí nebezpečí v používání placených veřejných Wi-Fi sítí a přes ně odesílaných dat. Málo si uvědomují rizika útoku, ať v jeho nejčastějším směru nebo zacílení na firmy a organizace, protože

útoky většinou ve větší míře hrozí z vnitřku organizace a jsou cíleny na menší firmy. Další oblastí, ve které mají účastníci slabší úroveň znalosti, je výklad zákona o kybernetické bezpečnosti (4) a z něho vyplývajících práv a povinností. V neposlední řadě mají nedostačující přístup k otázce aktualizací a důležité problematice, která je s tím spojena.

Tato práce vznikala v době, kdy kybernetické útoky nabíraly na vysoké intenzitě, což bylo pravděpodobně podpořeno i probíhajícími ozbrojenými konflikty. Pro tuto nestandartní náladu a stav ve společnosti bylo částečně upuštěno od rozesílání e-mailu se zdánlivě škodlivým obsahem. Bakalářská práce vznikala v úzké spolupráci s oddělením KIS HZS Pk, které spravuje všechny komunikační a informační systémy. Po dohodě s tímto oddělením byla přesně vydefinována a vybrána přibližně jen polovina členů cílové skupiny, které byl e-mail rozeslán. Jako náhradu za chybějící údaje poskytlo oddělení KIS HZS Pk reálná data z posledních záchytů rizikových e-mailů, která měla pro potřeby bakalářské práce větší vypovídající hodnotu.

Analýzou, vzešlou z popsaného ověření znalostí, vyvstala potřeba zpracování výukového a školícího materiálu, který by jednak prohluboval a upřesňoval již tak poměrně dostačující znalosti v cílové skupině, ale ve větší míře se zaměřoval a kladl důraz na výše uvedená slabá místa v rámci kybernetické bezpečnosti a používání pracovních e-mailů.

Jako nejúčinnější forma výukových materiálů byla v první řadě zvolena obrazová prezentace, jejímž proškolením prošla celá cílová skupina. S následným umístěním na intranet HZS Pk, pro další šíření a školení. Na tuto formu navazovalo zpracování celé problematiky do dvou grafických souborů velkoformátových plakátů, které budou v budoucnu oddělením KIS HZS Pk distribuovány do všech struktur HZS Pk. Poslední formou použití podpůrného výukového materiálu bude obrazová prezentace formou spořiče obrazovky. Ten by mohl být implementován do nastavení operačních systémů stolních počítačů používaných u HZS Pk.

Znovu zadáním vstupního testu byla ověřena aplikace a dopad na míru zpracovaného výukového materiálu. Z výsledků vyplývá, že výukový materiál měl vysokou míru účinnosti a jeho forma zpracování je přínosná. Znalosti se v cílové skupině ve všech aspektech zlepšily a ustálily. Včetně utřídění informací v oblastech, ve kterých respondenti vykazovali slabších výsledků.

RESUMÉ

Tato bakalářská práce se věnuje problematice počítačové bezpečnosti v základní složce Integrovaného záchranného systému ČR, konkrétně u Hasičského záchranného sboru Plzeňského kraje.

Dílčím cílem práce je, na úzké a konkrétní skupině osob, ověřit a analyzovat úroveň digitální gramotnosti a povědomí v oblasti její bezpečnosti. Hlavním cílem však zůstává navržení a vytvoření materiálu, který by měl vést ke zlepšení uživatelských znalostí. Tuto skupinu osob spojuje pouze společný zaměstnavatel a tím i jednotná pravidla pro používání. V praktické části je, včetně upřesnění zásad a podmínek používání ICT prostředků, popsána forma a výběr cílové skupiny uživatelů. Po jejím definování jí je zadán vstupní test, který se skládá ze dvou částí a stanoví hladinu znalostí o digitálním prostředí a bezpečnosti. Praktická část bakalářské práce vychází z teoretické, ve které je všeobecně vymezen pojem kybernetického útoku jako takového. Je zde vyzdvihnuta potřeba kybernetické bezpečnosti, stručně popsána základní složka IZS, její moderní historie a základní právní rámec. Taktéž jsou zde uvedeny nejdůležitější právní normy, týkající se počítačové bezpečnosti a na závěr jsou rozděleny nejčastější druhy kybernetických útoků a všeobecné bezpečnostní zásady.

Analýzou vzešlou z popsaného vstupního ověření znalostí vyvstala potřeba zpracování cíleně zaměřeného výukového a školícího materiálu. Jako nejúčinnější forma je zvolena obrazová prezentace, jejímž proškolením prošla celá cílová skupina. Na tento nejdůležitější prostředek dále navazuje zpracování celé problematiky do dvou souborů velkoformátových plakátů pro širší možnosti šíření v organizaci HZS Pk. Jako poslední forma může být výukový materiál uložen do souboru spořiče obrazovky a implementován do nastavení operačních systémů stolních počítačů.

Znovu zadáním vstupního testu je ověřena aplikace a dopad výukového materiálu. Z výsledků vyplývá, že výukový materiál měl vysokou míru účinnosti a jeho forma zpracování byla dobře zvolena a je velice přínosná.

Pro větší a dlouhodobější přesah bakalářské práce bylo její znění a kompletní výukový materiál bezplatně podstoupen HZS Pk a měl by se stát jedním ze základních kamenů, v současnosti nově zpracovávanému tématu kybernetické bezpečnosti.

RESUME

This bachelor thesis is devoted to the problem of computer security in the basic component of the Integrated Rescue System of the Czech Republic, specifically in the Fire Brigade of the Pilsen Region.

This sub-objective of the thesis is to verify and analyze the level of digital literacy and awareness in the field of its security on a small and specific group of persons. However, the main objective remains the design and creation of material that should lead to the improvement of user knowledge. This group of people is solely united by a common employer and thus held to uniform rules of use. In practice, the form and selection of the targeted group of users are described including the specifications, principles, and conditions for the use of ICT resources. Once this has been defined, a two-part entry test is given to determine the level of knowledge about the digital environment and its security. The practical part of the bachelor's thesis is based on the theoretical aspects in which the concept of a cyberattack is generally defined by its very nature. It highlights the need for cyber security, and briefly describes the basic components of the IRS, its modern history, and the basic legal framework. In addition, the most important legal norms related to cyber security are listed, as well as the categorization of the most common types of cyberattacks and general security principles.

The data analysis resulting from the described initial knowledge test has led to the conclusion that there is a lack of targeted teaching and training material. The most effective format was a pictorial presentation, in which the entire targeted group had gone through the necessary training to succeed. This essential tool is followed by the elaboration of the entire issue, divided into two sets of large-format posters for wider dissemination within the organization of the Fire Brigade of the Pilsen Region. In the final format, the training material can be stored in a screensaver file and implemented in the operating system settings of desktop computers.

By re-entering the entry test, the application and impact of the teaching material is verified. The results show that the teaching material had high levels of effectiveness and its format was well chosen and is very beneficial for users.

For larger and long-term overlap of the Bachelor's thesis, its text and the complete teaching material was given free of charge to the Fire Brigade of the Pilsen Region and should become one of the stepping-stones for the newly developed topic of cyber security.

SEZNAM LITERATURY

(1) 133/1985 Sb. Zákon o požární ochraně. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 23.03.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/1985-133#f2804984

(2) 320/2015 Sb. Zákon o hasičském záchranném sboru. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 01.01.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2015-320?citace=1#Sum

(3) Historie - Hasičský záchranný sbor České republiky. *Úvodní strana - Hasičský záchranný sbor České republiky* [online]. Copyright © 2021 Generální ředitelství Hasičského záchranného sboru ČR, všechna práva vyhrazena [cit. 01.01.2022]. Dostupné z: https://www.hzscr.cz/clanek/uvod-hasicsky-zachranny-sbor-cr-historie.aspx

(4) 181/2014 Sb. Zákon o kybernetické bezpečnosti. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 01.01.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181?citace=1

(5) 316/2014 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřen.... *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 01.01.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-316?citace=1

(6) 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 01.01.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-317?citace=1

(7) 365/2000 Sb. Zákon o informačních systémech veřejné správy. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 01.01.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-365?citace=1

(8) KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

(9) Přesměrovat. [online]. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=1021

(10) Kvíz a studijní materiál o kybernetické bezpečnosti | Avast Business. [online]. Dostupné z: https://www.avast.com/cs-cz/business/resources/cybersecurity-quiz#pc

SEZNAM OBRÁZKŮ

Obr. 1 – Otázka č. 1. vstupního ověření. 26
Obr. 2 – Otázka č. 2. vstupního ověření. 26
Obr. 3 – Otázka č. 3. vstupního ověření. 27
Obr. 4 – Otázka č. 4. vstupního ověření. 27
Obr. 5 – Otázka č. 5. vstupního ověření. 28
Obr. 6 – Otázka č. 6. vstupního ověření. 28
Obr. 7 – Otázka č. 7. vstupního ověření. 29
Obr. 8 – Otázka č. 8. vstupního ověření. 29
Obr. 9 – Otázka č. 9. vstupního ověření. 30
Obr. 10 – Otázka č. 10. vstupního ověření. 30
Obr. 11 – Otázka č. 11. vstupního ověření. 31
Obr. 12 – Otázka č. 12. vstupního ověření. 31
Obr. 13 – Otázka č. 13. vstupního ověření. 32
Obr. 14 – Otázka č. 14. vstupního ověření. 32
Obr. 15 – Otázka č. 15. vstupního ověření. 33
Obr. 16 – Otázka č. 16. vstupního ověření. 33
Obr. 17 – Otázka č. 17. vstupního ověření. 34
Obr. 18 – Otázka č. 18. vstupního ověření. 34
Obr. 19 – Otázka č. 19. vstupního ověření. 35
Obr. 20 – Otázka č. 20. vstupního ověření. 35
Obr. 21 – Otázka č. 21. vstupního ověření. 36
Obr. 22 – Text zkušebního emailu. 38
Obr. 23 – Forma webové prezentace pro externí odkaz. 38
Obr. 24 – Popsaná hrozba od manažera kybernetické bezpečnosti. 41
Obr. 25 – Popsaná hrozba od manažera kybernetické bezpečnosti. 41
Obr. 26 – Statistika z Google Analytics. 42
Obr. 27 – Ukázka vytvořené prezentace v PowerPointu. 43
Obr. 28 – Ukázka vytvořené prezentace v PowerPointu. 44
Obr. 29 – Ukázka všeobecných pravidel zabezpečení. 45
Obr. 30 – Ukázka bezpečného chování zaměstnanců. 45
Obr. 31 – Otázka č. 1. z opětovného zadání. VII
Obr. 32 – Otázka č. 2. z opětovného zadání. VII
Obr. 33 – Otázka č. 3. z opětovného zadání. VIII
Obr. 34 – Otázka č. 4. z opětovného zadání. VIII
Obr. 35 – Otázka č. 5. z opětovného zadání. IX
Obr. 36 – Otázka č. 6. z opětovného zadání. IX
Obr. 37 – Otázka č. 7. z opětovného zadání. X
Obr. 38 – Otázka č. 8. z opětovného zadání. X
Obr. 39 – Otázka č. 9. z opětovného zadání. X
Obr. 40 – Otázka č. 10. z opětovného zadání. XI
Obr. 41 – Otázka č. 11. z opětovného zadání. XI
Obr. 42 – Otázka č. 12. z opětovného zadání. XI
Obr. 43 – Otázka č. 13. z opětovného zadání. XII
Obr. 44 – Otázka č. 14. z opětovného zadání. XII
Obr. 45 – Otázka č. 15. z opětovného zadání. XII

Obr. 46 – Otázka č. 16. z opětovného zadání. XIII
Obr. 47 – Otázka č. 17. z opětovného zadání. XIII
Obr. 48 – Otázka č. 18. z opětovného zadání. XIV
Obr. 49 – Otázka č. 19. z opětovného zadání. XIV
Obr. 50 – Otázka č. 20. z opětovného zadání. XV
Obr. 51 – Otázka č. 21. z opětovného zadání. XV

PŘÍLOHY

OTÁZKY PÍSEMNÉHO TESTU

1. Do jaké věkové skupiny se řadíte?

a) 18 – 25

b) 26 – 33

c) 34 – 41

d) 42 – 49

e) 50 – 57

f) 58 – 65

g) 65 a více

2. Jak se označuje vyšší varianta elektronického podpisu?

a) Vyšší elektronický podpis

b) Kvantová identita

c) Kvalifikovaný elektronický podpis

3. Myslíte si, že pokud máte počítač chráněný heslem a ukládáte si svá hesla (od různých služeb jako jsou e-shopy, e-mail, sociální sítě, atd.) do prohlížeče, že jsou tato hesla v bezpečí před útočníky, když je připojen k internetu a navštěvujete nejrůznější webové stránky? Pozn. Pokud je tvrzení jen z části nesprávné, je nesprávné celé.

a) Ano, chrání je počítač s heslem

b) Ne

c) Ano, chrání je prohlížeč

4. Útoky na internet jsou leckdy ve své podstatě jednoduché a spoléhají např. na to, že uživatel něco přehlédne nebo udělá chybu v časové tísni. Útočníci obvykle nemíří na konkrétního uživatele, ale čekají, kdo neznalý se chytí. Některé útoky cílí na strach uživatele a jeho sebeúctu. Typickým příkladem jsou výhružky zveřejněním intimních záběrů z webkamery, pokud uživatel nezaplatí. Útočníci ale často vůbec nic nemají. Pozn. Pokud je tvrzení jen z části nesprávné, je nesprávné cele.

a) Pravda

b) Nepravda

5. Při přihlašování k veřejným Wi-Fi sítím dodržujeme následující pravidla: Pečlivě zvažujeme, k čemu se připojíme. V ideálním případě čteme podmínky využívání a jsme obezřetní. Vyskočil nějaký formulář, který máme vyplnit? Proč? Obecně je zkrátka bezpečnější využít veřejné Wi-Fi pro věci citlivějšího charakteru například pro připojení do internetového bankovnictví. U veřejné Wi-Fi sítě bychom měli mít automaticky pochyby. Ke zvýšení své bezpečnosti můžeme přispět otevíráním webových stránek opatřených HTTPS.

a) Pravda

b) Nepravda

c) Je to jedno na Wi-Fi nezáleží

6. Rozhodněte, zda je toto níže uvedené tvrzení pravdivé. Pokud máme na výběr, preferujeme messengery, které využívají end-to-end šifrování. Absence end-to-end šifrování znamená, že je technicky možné, aby někdo sledoval naši konverzaci.

a) Pravda

b) Nepravda

7. K čemu slouží Anonymní režim?

a) Anonymní režim skryje veškerou naši identitu. Nemáme se čeho obávat.

b) Tento protokol snižuje počet informací a dat, které po našem vyhledávání zůstanou uložená v daném zařízení.

c) Nikdo nepozná, kde jsem nebo ze které země jsem

8. Vyberte správnou odpověď: V momentě, kdy se hodláme přihlašovat do internetového bankovnictví a provádět platby, je důležité, aby naše připojení bylo zabezpečené. Který protokol zajistí bezpečné připojení?

a) HTTPS

b) HTTP

c) POP3

9. Co je to VPN a k čemu slouží?

a) Tato zkratka označuje poskytovatele e-mailových služeb

b) Tato zkratka označuje veřejné Wi-Fi sítě

c) Tato zkratka označuje šifrované spojení mezi dvěma počítači (virtual private network). Využívá se pro bezpečné připojení např. k pracovní síti

10. Co je Hoax?

a) Smyšlená a nesmyslná zpráva, která se snaží tvářit důvěryhodně a které přímo či nepřímo vyzývá uživatele k dalšímu šíření

b) Speciální typ bezpečnostního programu, který blokuje viry při vstupu do počítače

c) Situace, kdy počítač „zatuhne“ a nedá se s ním déle pracovat. Problém pak řeší jen tvrdý restart (např. odpojení od el. sítě)

11. Dokončete větu: „Používání vlastního zařízení k práci je obvykle…“

a) Rizikovější než používání zařízení od zaměstnavatele

b) Stejně rizikové jako používání zařízení od zaměstnavatele

c) Méně rizikové než používání zařízení od zaměstnavatele

12. Kterému z následujících subjektů víc hrozí, že se stane obětí kybernetického útoku?

a) Malá firma

b) Velká firma

c) Občan

13. Které z následujících hesel je nejbezpečnější?

a) 123456

b) drak

c) 10Ma1ych%C3rn0usku!

d) MilujiTe

e) He11oKitty

f) 1q2w3e4r

14. Situace: V počítači se vám zobrazí oznámení, že je k dispozici aktualizace pro důvěryhodnou aplikaci na kontrolu pravopisu, kterou jste si stáhli. Vyberte všechna tvrzení, která jsou podle vás správná.

a) Aktualizace se automaticky nainstaluje i přesto, že na oznámení nekliknete

b) Instaluji jen aktualizace, o jejichž instalaci mě požádá IT oddělení/podpora

c) Raději aktualizaci nenainstaluji, protože oznámení může být součástí kybernetického útoku

d) Aktualizace nejsou důležité, protože pouze přinášejí nové funkce nebo nový vzhled aplikací

e) Aktualizace je nutné instalovat okamžitě

f) Když budu žádost o aktualizaci ignorovat, firmě může hrozit riziko kybernetického útoku

15. Kdo je pro vaši organizaci největší kybernetickou bezpečnostní hrozbou?

a) Lidé v organizaci

b) Lidé z vnějšku

16. Situace: Od nezávislého dodavatele HR služeb („Human Resources“ - lidské zdroje) vaší firmy unikla data, když si nový zaměstnanec nechtěně stáhl malware. Došlo ke krádeži informací z vaší firmy. Kdo za to podle zákona odpovídá? Vyberte všechny vyhovující odpovědi.

a) Firma

b) Nezávislý dodavatel HR služeb

c) Člen personálu, který klikl na odkaz

d) Personál, jehož data byla ukradena

17. Co považujete za nejdůležitější aspekt kybernetického zabezpečení firem? Vyberte všechny vyhovující odpovědi.

a) Používání antiviru/antimalwaru na všech počítačích

b) Školení personálu (včetně zaměstnanců, kteří nejsou z ITC oddělení)

c) Používání silných hesel

d) Používání dvoustupňového ověřování (například potvrzování přihlášení na telefonu)

e) Používání firewallů

f) Možnost správy všech firemních zařízení na dálku

g) Dodržování zákonů na ochranu dat

18. Počítač nemůže být infikován/napaden online, když uživatel aktivně používá VPN?

a) Ano, nemůže být infikován

b) Ne, může být infikován

c) Ano, nemůže být infikován, chrání jej VPN

19. Vyberte tvrzení, které je podle vás nejpřesnější.

a) Veškerý personál musí umět rozpoznat známky kybernetického útoku

b) Konkrétní personál (například ITC pracovníci) musí umět rozpoznat známky kybernetického útoku

c) Pokud firma používá vhodný antivirový software, personál nemusí umět rozpoznat známky kybernetického útoku

20. Ze kterých Wi-Fi sítí se podle vašeho názoru můžete bezpečně připojovat ke svému pracovnímu zařízení, když nejste v práci? Vyberte všechny vyhovující odpovědi.

a) Bezplatné otevřené veřejné Wi-Fi, například v centrech měst

b) Bezplatné otevřené Wi-Fi v kavárnách či restauracích, v museích či na úřadech nebo na letištích či nádražích

c) Placené Wi-Fi v dopravních prostředcích nebo hotelích

d) Soukromé Wi-Fi, například u známých dom

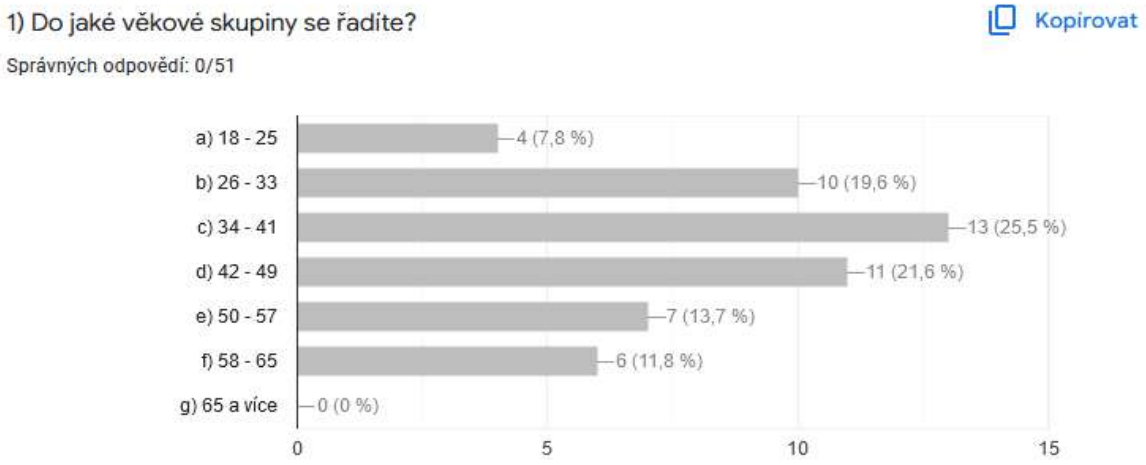
21. Počítačové útoky se mobilních telefonů.

a) Netýkají, mobily mají jiný princip fungování, než počítače a nelze je napadnout

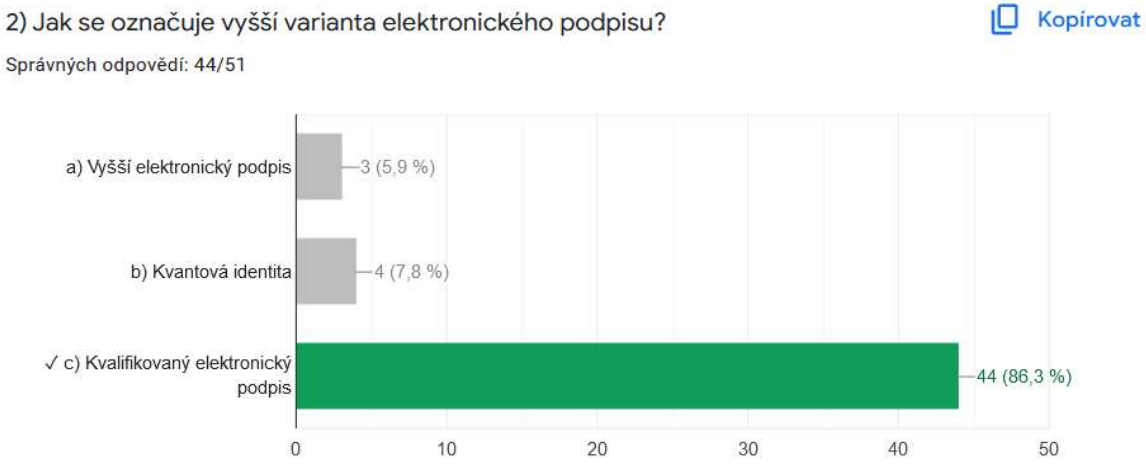
b) Týkají, třeba počítačový virus je program jako každý jiný – pokud dokážeme do mobilu instalovat program, můžeme mít nainstalovaný i virus

c) Netýkají, veškerý provoz v případě mobilů jde skrze operátory, kteří útoky spolehlivě detekují a filtrují

VÝSLEDKY OPĚTOVNÉHO ZADÁNÍ PÍSEMNÉHO TESTU



Obr. 31 – Otázka č. 1. z opětovného zadání.

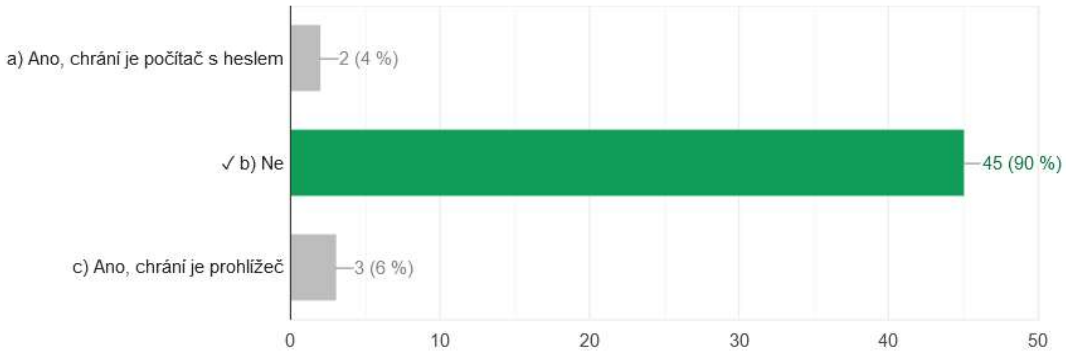


Obr. 32 – Otázka č. 2. z opětovného zadání.

3) Myslíte si, že pokud máte počítač chráněný heslem a ukládáte si svá hesla (od různých služeb jako jsou e-shopy, e-mail, sociální sítě, atd.) do prohlížeče, že jsou tato hesla v bezpečí před útočníky, když je připojen k internetu a navštěvujete nejrůznější webové stránky? Pozn. Pokud je tvrzení jen z části nesprávné, je nesprávné celé.

Kopírovat

Správných odpovědí: 45/50

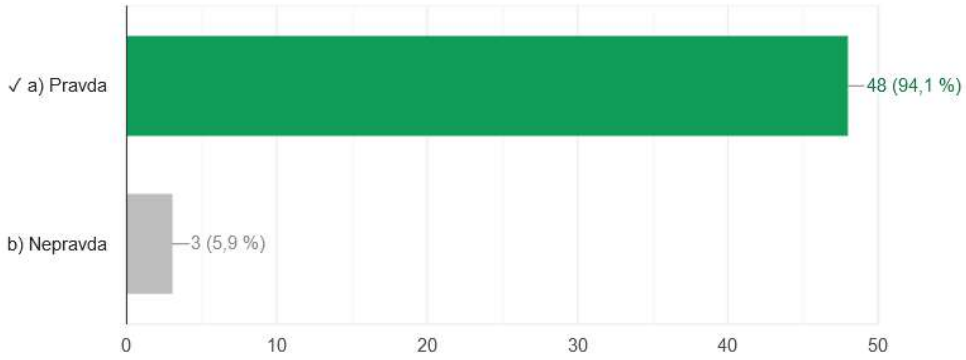


Obr. 33 – Otázka č. 3. z opětovného zadání.

4) Útoky na internet jsou leckdy ve své podstatě jednoduché a spoléhají např. na to, že uživatel něco přehlédne nebo udělá chybu v časové tísni. Útočníci obvykle nemíří na konkrétního uživatele, ale čekají, kdo neznalý se chytí. Některé útoky cílí na strach uživatele a jeho sebeúctu. Typickým příkladem jsou výhrůžky zveřejněním intimních záběrů z webkamery, pokud uživatel nezaplatí. Útočníci ale často vůbec nic nemají. Pozn.: Pokud je tvrzení jen z části nesprávné, je nesprávné cele.

Kopírovat

Správných odpovědí: 48/51

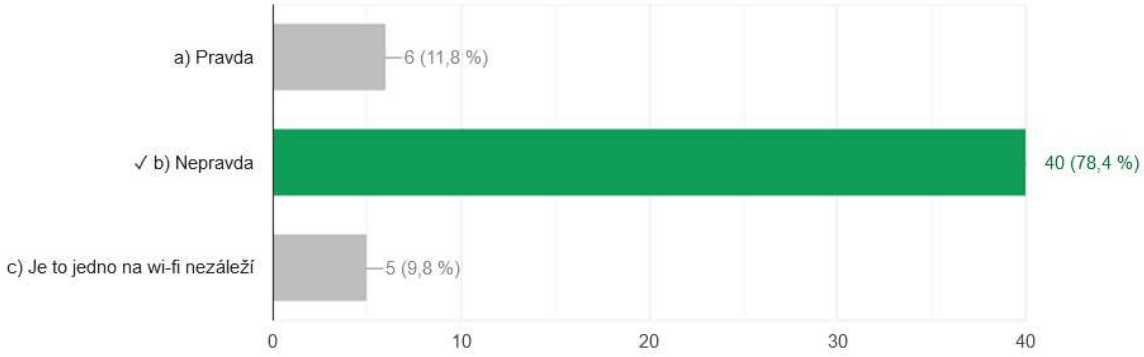


Obr. 34 – Otázka č. 4. z opětovného zadání.

5) Při přihlašování k veřejným wi-fi sítím dodržujeme následující pravidla: Pečlivě zvažujeme, k čemu se připojíme. V ideálním případě čteme podmínky využívání a jsme obezřetní. Vyskočil nějaký formulář, který máme vyplnit? Proč? Obecně je zkrátka bezpečnější využít veřejné wi-fi pro věci citlivějšího charakteru například pro připojení do internetového bankovnictví. U veřejné wi-fi sítě bychom měli mít automaticky pochyby. Ke zvýšení své bezpečnosti můžeme přispět otevíráním webových stránek opatřených HTTPS.

Kopirovat

Správných odpovědí: 40/51

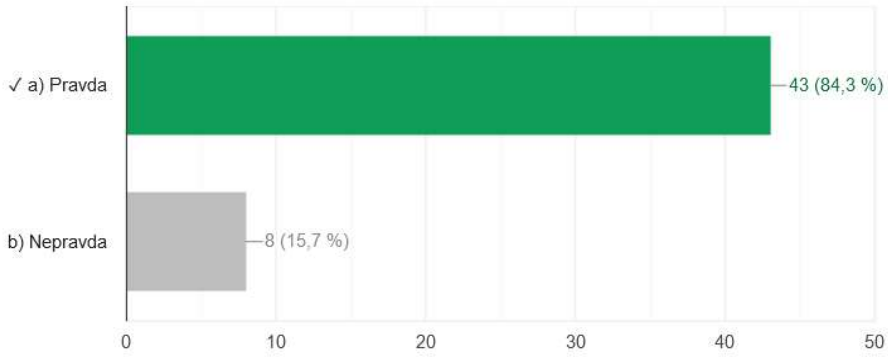


Obr. 35 – Otázka č. 5. z opětovného zadání.

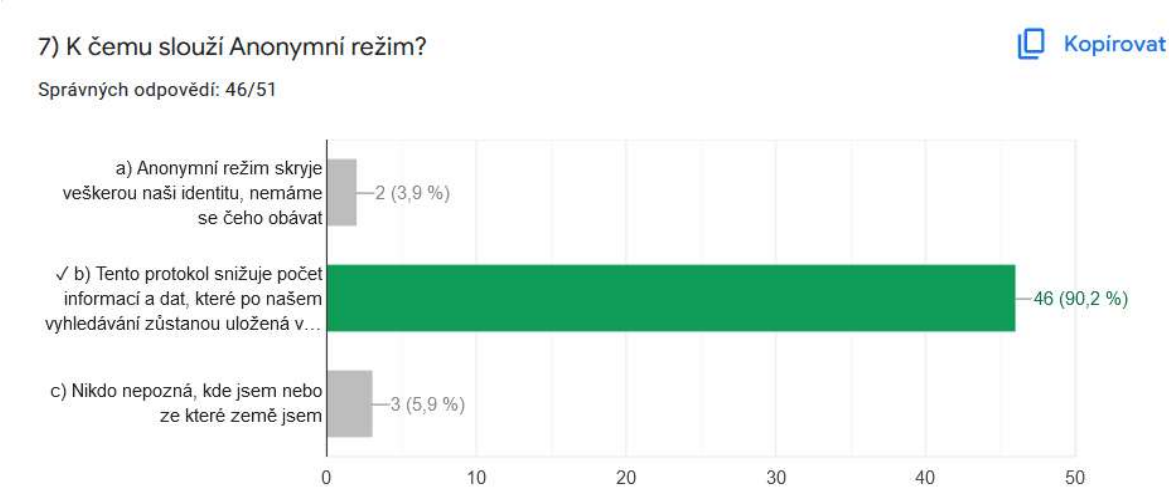
6) Rozhodněte, zda je toto níže uvedené tvrzení pravdivé. Pokud máme na výběr, preferujeme messengery, které využívají end-to-end šifrování. Absence end-to-end šifrování znamená, že je technicky možné, aby někdo sledoval naši konverzaci.

Kopirovat

Správných odpovědí: 43/51

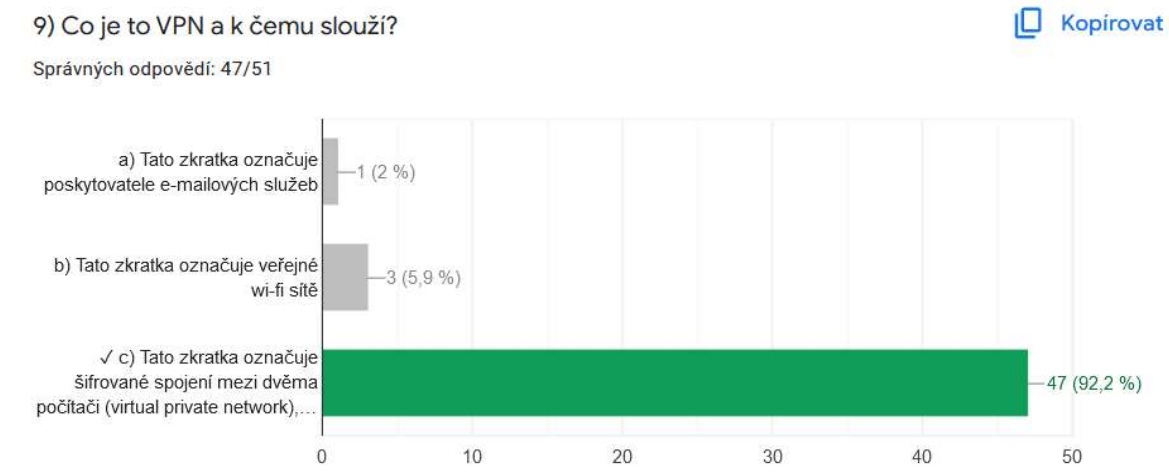


Obr. 36 – Otázka č. 6. z opětovného zadání.

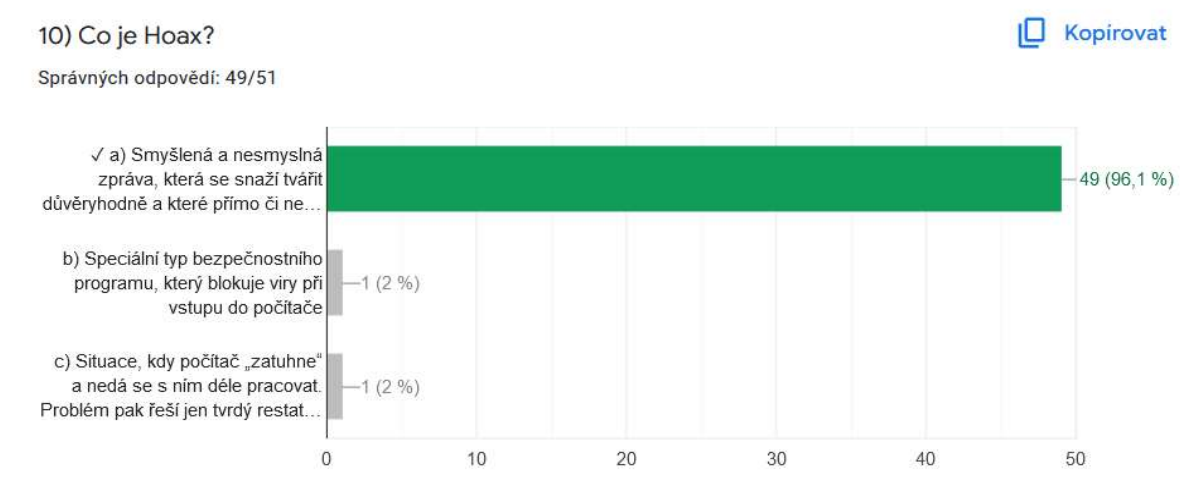


Obr. 37 – Otázka č. 7. z opětovného zadání.

Obr. 38 – Otázka č. 8. z opětovného zadání.

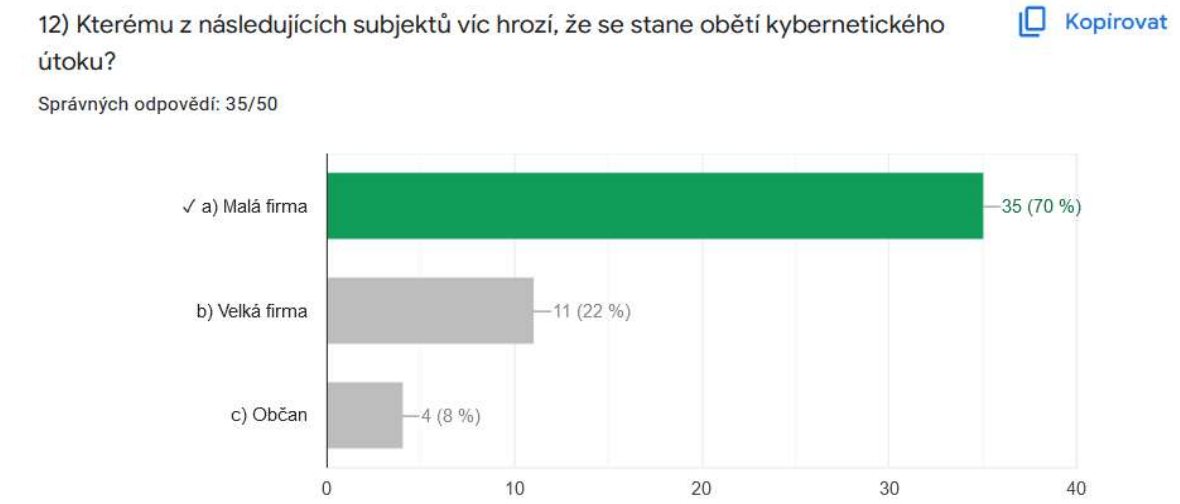


Obr. 39 – Otázka č. 9. z opětovného zadání.



Obr. 40 – Otázka č. 10. z opětovného zadání.

Obr. 41 – Otázka č. 11. z opětovného zadání.

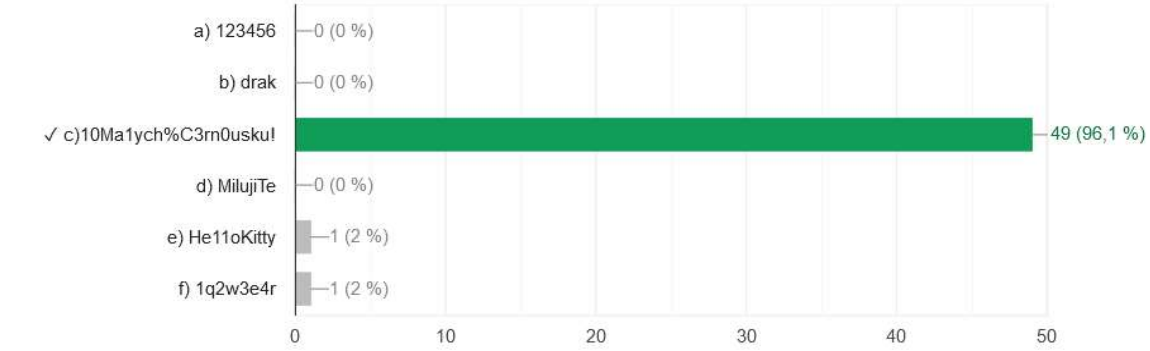


Obr. 42 – Otázka č. 12. z opětovného zadání.

13) Které z následujících hesel je nejbezpečnější?

Kopírovat

Správných odpovědí: 49/51

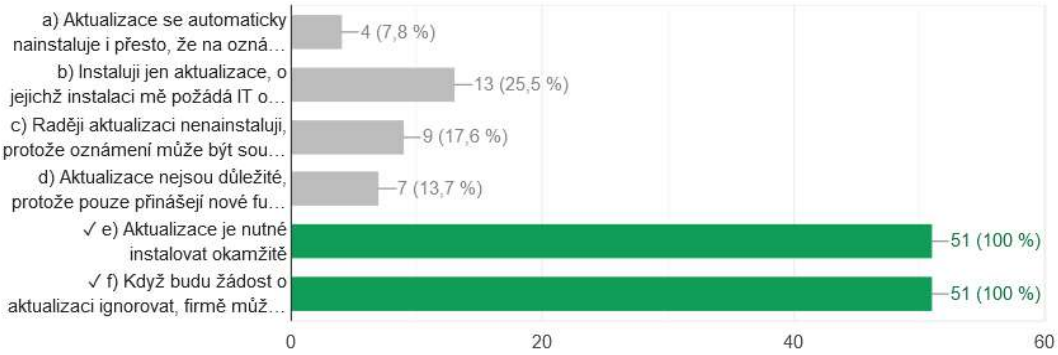


Obr. 43 – Otázka č. 13. z opětovného zadání.

14) Situace: V počítači se vám zobrazí oznámení, že je k dispozici aktualizace pro důvěryhodnou aplikaci na kontrolu pravopisu, kterou jste si stáhli. Vyberte všechna tvrzení, která jsou podle vás správná.

Kopírovat

Správných odpovědí: 38/51

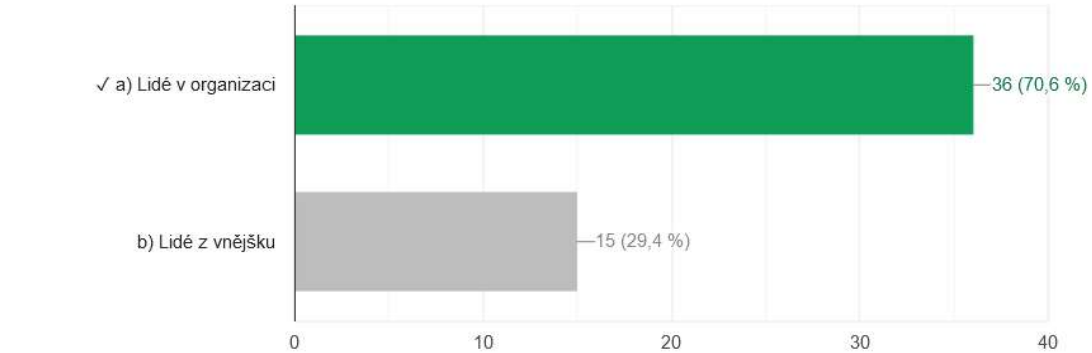


Obr. 44 – Otázka č. 14. z opětovného zadání.

15) Kdo je pro vaši organizaci největší kyberbezpečnostní hrozbou?

Kopírovat

Správných odpovědí: 36/51

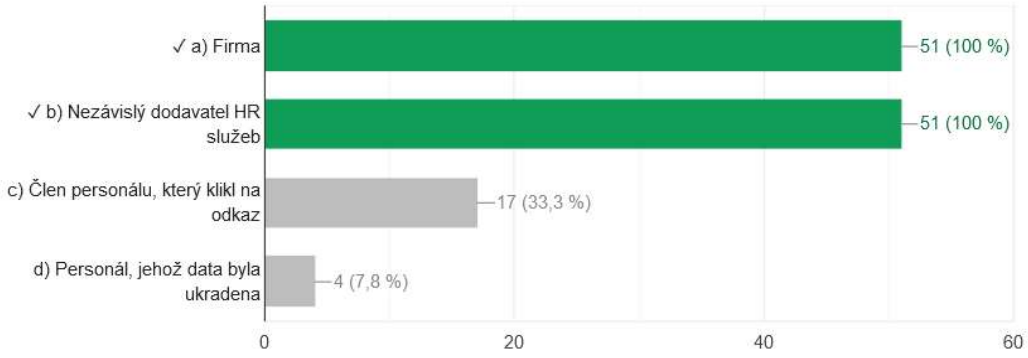


Obr. 45 – Otázka č. 15. z opětovného zadání.

16) Situace: Od nezávislého dodavatele HR služeb („Human Resources“ - lidské zdroje) vaší firmy unikla data, když si nový zaměstnanec nechtěně stáhl malware. Došlo ke krádeži informací z vaší firmy. Kdo za to podle zákona odpovídá? Vyberte všechny vyhovující odpovědi.

Kopírovat

Správných odpovědí: 34/51



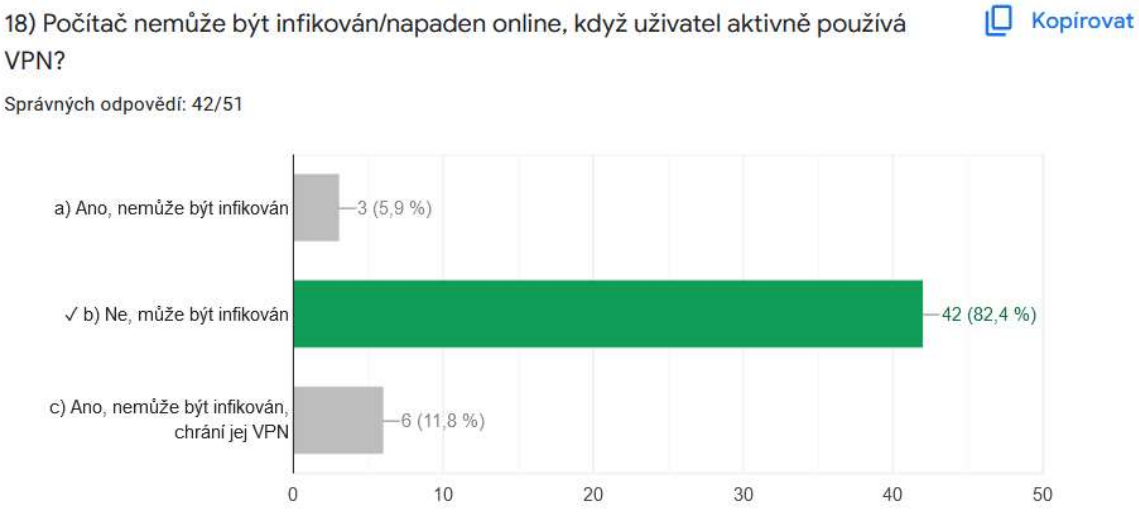
Obr. 46 – Otázka č. 16. z opětovného zadání.

17) Co považujete za nejdůležitější aspekt kybernetického zabezpečení firem? Vyberte všechny vyhovující odpovědi.

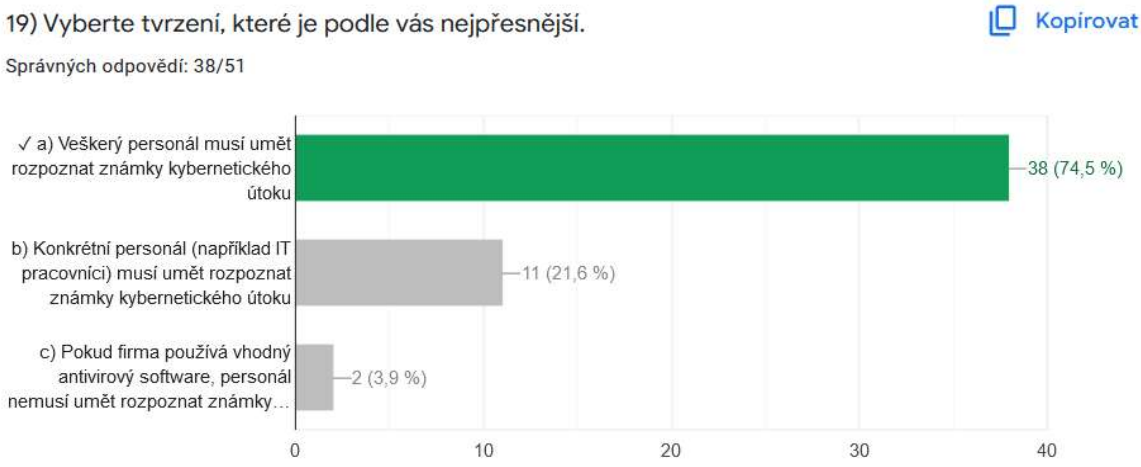
Kopírovat

Správných odpovědí: 41/51

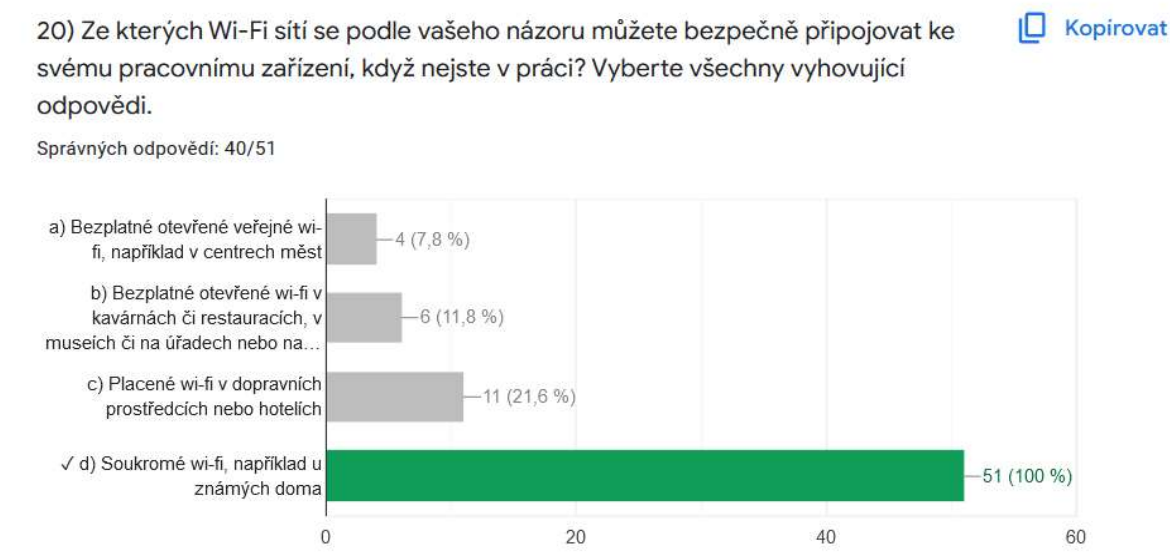
Obr. 47 – Otázka č. 17. z opětovného zadání.



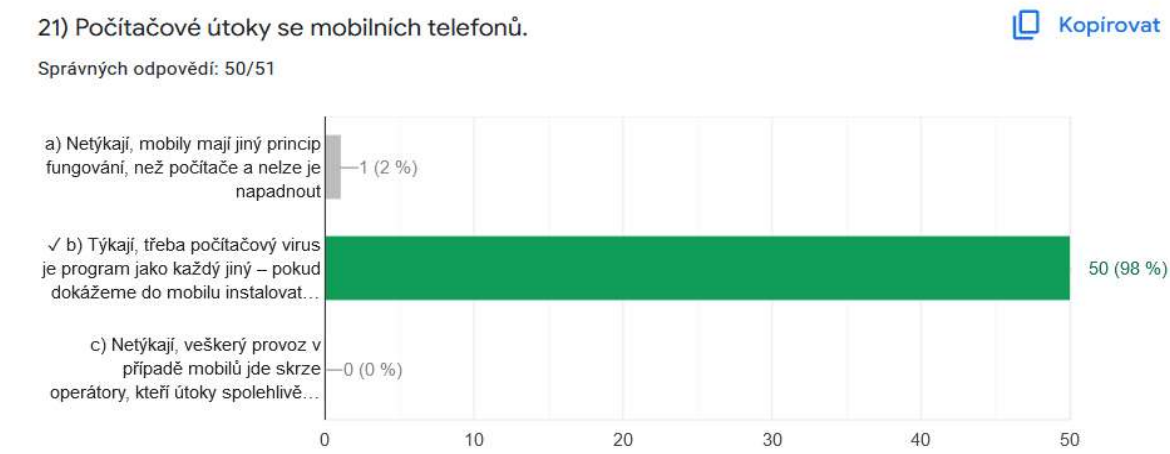
Obr. 48 – Otázka č. 18. z opětovného zadání.



Obr. 49 – Otázka č. 19. z opětovného zadání.



Obr. 50 – Otázka č. 20. z opětovného zadání.



Obr. 51 – Otázka č. 21. z opětovného zadání.