Školení kybernetické bezpečnosti zaměstnanců ve firmách

Karin Žaludová

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav počítačových a komunikačních systémů

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Karin Žaludová**
Osobní číslo:	**A21093**
Studijní program:	**B0688A140008 Informační technologie v administrativě**
Forma studia:	**Prezenční**
Téma práce:	**Školení kybernetické bezpečnosti zaměstnanců ve firmách**
Téma práce anglicky:	**Cyber security training in companies**

Zásady pro vypracování

1. Prozkoumat aktuální stav kybernetického zabezpečení ve firmách a zjistit nejčastější hrozby a slabiny.
2. Analyzovat dostupné metody a formy školení kybernetické bezpečnosti.
3. Prozkoumat vliv legislativních požadavků a regulací týkajících se kybernetické bezpečnosti pro školení ve firmách.
4. Posoudit efektivitu různých metod školení a jejich vliv na školené pracovníky.
5. Navrhnout efektivní školení o kybernetické bezpečnosti pro firmy.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 9788073807375.
2. MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Brno: Computer Press, c2007. ISBN 9788025115114.
3. *Zajištění kybernetické bezpečnosti ve středně velké společnosti*. Praha, 2021. Diplomová práce. Vysoká škola finanční a správní.
4. HRŮZA, Petr. *Kybernetická bezpečnost*. Brno : Univerzita obrany, 2012. ISBN 978-80-7231-914-5.
5. Úplné znění GDPR. *Úřad pro ochranu osobních údajů* [online]. 2016 [cit. 2023-10-24]. Dostupné z: https://www.uoou.cz/uplne%2Dzneni%2Dgdpr/ds-6607/archiv=0&p1=3938

Vedoucí bakalářské práce: **Ing. Lukáš Králík, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **20. listopadu 2023**
Termín odevzdání bakalářské práce: **30. května 2024**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Miroslav Matýsek, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 1. prosince 2023

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.
- že při tvorbě této práce jsem použil/a nástroj generativního modelu AI perplexity.ai; https://www.perplexity.ai za účelem citování obsahu a hledání synonym. Po použití tohoto nástroje jsem provedl/a kontrolu obsahu a přebírám za něj plnou zodpovědnost.

Ve Zlíně, dne …….

podpis studenta

ABSTRAKT

Tato bakalářská práce se zabývá analýzou a hodnocením efektivity školení v oblasti kybernetické bezpečnosti ve firmách. Cílem práce je zhodnotit současný stav v českých firmách a navrhnout efektivní školení, které by mohlo vést k lepší ochraně proti kybernetickým hrozbám. Práce vychází z teoretických základů kybernetické bezpečnosti a dále se zaměřuje na analýzu přístupů k školení kybernetické bezpečnosti v praxi. Metodologie zahrnuje sběr dat prostřednictvím dotazníkového šetření mezi zaměstnanci z různých firem a odvětví. Výsledky jsou analyzovány s ohledem na identifikaci klíčových oblastí pro zlepšení a následně je navrženo výše zmiňované školení pro efektivní postup při školení kybernetické bezpečnosti.

Klíčová slova: Kybernetická bezpečnost, školení, firmy, analýza, hodnocení, efektivita, ochrana, hrozby, dotazníkové šetření, doporučení

ABSTRACT

This bachelor thesis focuses on the analysis and evaluation of the effectiveness of training in the field of cybersecurity in companies. The aim is to assess the current state in Czech companies and propose effective training that could lead to better protection against cyber threats. The thesis is based on the theoretical foundations of cybersecurity and further focuses on analyzing approaches to cybersecurity training in practice. The methodology includes data collection through questionnaire surveys among the public from various companies and industries. The results are analyzed with regard to identifying key areas for improvement, and subsequently, the aforementioned training is proposed for an effective approach to cybersecurity training.

Keywords: Cybersecurity, training, companies, analysis, evaluation, effectiveness, protection, threats, questionnaire survey, recommendations

Poděkování, motto a čestné prohlášení, že odevzdaná verze bakalářské práce a verze elektronická, nahraná do IS/STAG jsou totožné ve znění:

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V dnešní digitální době jsou firmy vystaveny stále rostoucím hrozbám v oblasti kybernetické bezpečnosti. Kybernetické útoky mohou mít katastrofální dopady na podnikání, včetně ztráty důvěryhodnosti, finančních ztrát a poškození firemních aktiv. Jednou z klíčových složek ochrany proti těmto hrozbám je efektivní školení v oblasti kybernetické bezpečnosti pro zaměstnance.

Tato bakalářská práce se zaměřuje na různé druhy školení v oblasti kybernetické bezpečnosti ve firmách. Cílem práce je zhodnotit současný stav školení v českých firmách a navrhnout strategie a postupy pro efektivní školení, které mohou vést k lepší ochraně proti kybernetickým hrozbám.

Práce se opírá o teoretické základy kybernetické bezpečnosti, aby lépe porozuměla potřebám a výzvám školení v této oblasti. Dále analyzuje přístupy k školení kybernetické bezpečnosti v praxi a zkoumá, jakým způsobem jsou tyto přístupy implementovány v různých typech firem a odvětví.

Metodologie této práce zahrnuje sběr dat prostřednictvím dotazníkového šetření mezi zaměstnanci různých firem a odvětví. Získané výsledky budou podrobeny důkladné analýze s cílem identifikovat klíčové oblasti, ve kterých lze provést zlepšení. Na základě těchto analýz bude navrženo vzorové školení, doporučení a postupy pro efektivní školení v oblasti kybernetické bezpečnosti.

Cílem této práce je kromě poskytnutí náhledu na současný stav školení v oblasti kybernetické bezpečnosti, ale hlavně přispět k rozvoji lepších praktik a strategií pro ochranu firem proti kybernetickým hrozbám.

I. TEORETICKÁ ČÁST

1 KYBERNETICKÁ BEZPEČNOST

V dnešní době se informační technologie rozvíjejí poměrně rychle, že je mnohdy pro běžného uživatele pracné udržet se v obraze. V souvislosti s rychlým rozvojem se situace ohledně kybernetické bezpečnosti mění poněkud dramaticky. Firemní aktiva mohou být kopírována, měněna nebo mazána tak rychle, jak si běžní uživatele, ani mnohdy nejsou schopni v reálném čase všimnout.

Kybernetická bezpečnost se v dnešní době považuje za již poněkud rozsáhlý obor, který je nedílnou součásti studia nejen informačních studií. Rostou však nejen zpracovávaná data ale i jejich důležitost.[1]

1.1 Definice

„Kybernetická bezpečnost může být definována několika různými způsoby, ale všeobecně je možné říct, že jde o celkovou ochranu sítí před kybernetickými útoky a hrozbami, aby byla zachována bezpečnost informací.“ [2]

1.2 Kyberprostor

Abychom lépe pochopili téma kybernetické bezpečnosti, musíme si první říct co to vlastně je ten kyberprostor (anglicky „cyberspace“), jak funguje a co platí v rámci kyberprostoru jako takového. Jako první zmínku o kyberprostoru můžeme považovat interview s Williamem Gibsonem z roku 1994, ze Stockholmu, kde Gibson propagoval svou knihu pod názvem „Virtuální světlo“. Kyberprostor je v interview popsán těmito slovy „Kyberprostor je přirovnání, které nám umožňuje uchopit toto místo, kde od časů druhé světové války, jsme udělali stále více věcí, o které můžeme považovat jako prvek naší kultury. Kyberprostor je prostor, kde obchodujeme, jedná se ve skutečnosti o místo, kde banky ukládají naše finance. Je to místo, kde probíhají burzovní obchody. Je to výhodné pro každého, kdo se tohoto účastní, jelikož se jedná o pouhý chod informací.“**Chyba! Nenalezen zdroj odkazů.**[3]

Kyberprostor sám o sobě je používán pro označení virtuální reality interaktivního světa, se kterým se můžeme setkat nejen ve svých, ale i cizích počítačích se kterými přicházíme často do kontaktu. Zjednodušeně řečeno, pojem „kyberprostor“ můžeme vnímat jako digitální prostředí, kde se propojují počítačové sítě, servery a zařízení, umožňující komunikaci, výměnu dat a interakci mezi lidmi a systémy po celém světě. Hlavním cílem kyberprostoru a celého internetu je, aby jednotliví účastníci mohli komunikovat mezi sebou i přes

vzdálenost na co nejlehčí bázi, jak to jen je možné. Tudíž, jde o to provozovat vše nejlépe z pohodlí domova, bez nutnosti se někam přesunovat nebo volat a podobně. Mezi další možnosti kyberprostoru můžeme zařadit přesun dat mezi jednotlivci pomocí cloudových služeb ale i používání platebních systémů k provádění finančních transakcí. Cloudové služby jsou sítě serverů, které jsou vzájemně propojeny a slouží jako úschovna a pro sdílení dat. Pokud se jedná o cloudové služby, tak clouding podléhá kyberprostoru, poněvadž jeho princip je závislý na jeho dispozici. Mluvíme tedy o tom, že cloud je k dispozici odkudkoli, nebo-li z jakéhokoli přístupového bodu. A to je důvodem proč funkce cloudu by bez internetu nebyla možná.

V dnešní době je kyberprostor velmi důležitým místem skoro pro každého z nás. Je tomu tak z důvodu takového, že významná část našeho života se dnes odehrává mimo jiné i v kyberprostoru. Z tohoto důvodu bychom měli kybernetickou bezpečnost brát jako klíčový faktor, pokud cílíme na ochranu našich dat, financí nebo i fyzického světa. Více než spousta průmyslových zařízení, je dneska propojená s kyberprostorem a jsou terčem kybernetických útoků. [3]

2 LEGISLATIVA KYBERNETICKÉ BEZPEČNOSTI

V této kapitole se budeme více věnovat legislativnímu rámci kybernetické bezpečnosti v České republice. Hlavně se budeme věnovat rozboru vyhlášek i zákonů, které se týkají kybernetické bezpečnosti, podíváme se i na některé vybrané normy *International Organization for Standardization* (ISO), metodiky a směrnice.

Dále si uvedeme několik vyhlášek a zákonů, které jsou pro problematiku kybernetické bezpečnosti jedny z hlavních.

Definice zákona je poměrně jednoznačná, jedná se o obecně závazná právní ustanovení, která jsou přijímána mocí legislativní. V České republice je tuto mocí zákonodárný parlament. Na druhou stranu, vyhlášky jsou podzákonnými právními předpisy, které mohou být vydány ústředními správními úřady, obcemi nebo kraji. Tyto vyhlášky stanovují pravidla platná na určitém území nebo v určité oblasti a mají obecně závaznou platnost. [3]

2.1 Zákony o kybernetické bezpečnosti

V následujících podkapitolách nalezneme několik zákonů, které jsou považovány za nezbytné, v oblasti kybernetické bezpečnosti.

2.1.1 Zákon – č. 181/2014 Sb., o kybernetické bezpečnosti

Prvním zákonem týkajícím se kybernetické bezpečnosti v České republice byl Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (známý též jako Zákon o kybernetické bezpečnosti). Tento zákon byl akceptován dne 29. srpna 2014 a v platnost vstoupil od 1. ledna 2015. Regulace práva a povinností jednotlivců a také stanovit kompetence a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti na území České republiky jsou hlavními cíli tohoto zákona. Jako další funkce zákona řadíme nejen zpracovávání příslušných předpisů Evropské Unie, upravování a zajišťování bezpečnosti sítí elektronických komunikací, ale i informačních systémů.

Jako hlavní cíle zákona můžeme považovat 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 v neposlední řadě úpravu činnosti dohledových pracovišť. [4]

2.1.2 Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnosti způsobilosti

Zákon č. 412/2005 Sb., o ochraně utajovaných informací, byl schválen dne 21. září 2005, uděluje komplexní rámec pro ochranu citlivých dat. V první části zákona jsou definovány klíčové pojmy. Mezi těmito pojmy můžeme najít například tyto:

- utajované informace
- národní zájmy
- odpovědné osoby
- neoprávněné osoby

Druhá část je zaměřena na konkrétní opatření k ochraně utajovaných informací, počítaje v to klasifikace, stupňů utajení a bezpečnostních standardů. Další část, třetí, stanovuje požadavky na bezpečnostní kvalifikaci osob zapojených do práce s utajovanými informacemi. Čtvrtá část se zabývá obecnými principy bezpečnostního řízení, zatímco pátá část určuje role a povinnosti státní správy a příslušných institucí. Další části poskytují mechanismy kontroly dodržování předpisů a sankce za jejich porušení. Závěrečná část obsahuje přechodná ustanovení a závěrečné dispozice zákona. Celkově zajišťuje tento zákon důkladnou ochranu utajovaných informací a bezpečnostní způsobilost v souladu s národními zájmy. [5]

2.1.3 Zákon č. 110/2019 Sb. o zpracování osobních údajů

Zákon č. 110/2019 Sb., který vstoupil v platnost dne 24. dubna 2019, vychází z nařízení Evropského parlamentu a Rady Evropské Unie (EU) 2019/679 a rozděluje se do dvou částí, které se zabývají následujícími oblastmi:

- Zpracování osobních údajů.
- Ochranou osobních údajů a jejich zpracováním v souvislosti s trestnou činností, zajišťováním bezpečnosti České republiky nebo veřejného pořádku a vnitřní bezpečnosti.
- Ochranou osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky.
- Úřadem, pověřenými osobami a jejich funkcemi.
- Přečinech vymezených v tomto zákoně.
- Prozatímních, zrušovacích a závěrečných ustanoveních. [6]

2.2 Vyhlášky o kybernetické bezpečnosti

Pokud s bavíme o vyhláškách o kybernetické bezpečnosti představují klíčový legislativní nástroj v oblasti ochrany informačních systémů a dat před kybernetickými hrozbami. Tyto vyhláškou jsou důležitou součástí kybernetického právního rámce, který se zabývá identifikací, prevencí a následně i reakcí na různé formy kybernetických útoků a incidentů. Jejich cílem je stanovit normy, postupy a požadavky pro zajištění kybernetické bezpečnosti v různých sektorech a institucích, aby bylo dosaženo co nejvyšší úrovně ochrany citlivých informací před kybernetickými riziky.

2.2.1 Vyhláška č. 82/2018 – o kybernetické bezpečnosti

Tato vyhláška se zabývá zpracováním příslušného předmětu Evropské unie a upravuje strukturu a obsah bezpečnostní dokumentace, obsah a rozsah bezpečnostních opatření, typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního konfliktu, náležitosti a sdělení o provedení reaktivního nařízení a jeho následku, vzor oznámení kontaktních údajů a jeho formu a v poslední řadě způsob odstranění dat, informacích o provozu, oznámení a jejich kopií. Byla uvedena v platnost 21. května 2018. [7]

2.2.2 Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

Tato vyhláška má za účel stanovit významné informační systémy a kritéria, která jsou klíčová pro jejich identifikaci, v souladu s ustanovením § 6 písm. d) příslušného zákona. Ve znění zákona je stanoveno, že významný informační systém je takový, který spravuje orgán veřejné moci jako organizační složku státu, kraje nebo hlavního města Prahy. Tento systém je využíván při výkonu veřejné moci pro různé účely, jako je například elektronická pošta pro veřejné úřady, kontrolní a inspekční činnosti, státní dozor, příprava a řešení krizových situací, vedení úřední desky a dálkový přístup, mezinárodní spolupráce a zadávání veřejných zakázek.

Dále je specifikováno, že významným informačním systémem není ten, který je spravován obcí. Kritéria pro určení významného informačního systému jsou dále upřesněna v příslušných ustanoveních vyhlášky. Takový systém musí splňovat specifické požadavky a stanovená kritéria pro jeho klasifikaci jako významného. [8]

2.3 Normy a standardy

V České republice se standardizací zabývá primárně Česká agentura pro standardizaci, jež byla zřízena jako příspěvková organizace podle zákona č. 265/2017 Sb., který mění zákon č. 90/2016 Sb., o posuzování shody stanovených výrobků při jejich dodávání na trh a zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů, zřídil Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ).

Mezinárodní organizace pro normalizaci v originále *International Organization for Standardization* (ISO) je federace normalizačních organizací celosvětového rázu, jejíž sídlo nalezneme ve Švýcarsku ve městě Ženeva. Organizace byla založena 23. února v roce 1947. V současné době organizace zahrnuje sto sedmdesát členů, jejichž úkolem je vytváření mezinárodních norem. Organizace je celosvětově známa, avšak největší míru působnosti zaujímá v Evropě.

Řízení bezpečnosti informací a její problematika je vedena pod normami ISO s čísly 27000 a výše. Tyto normy byly zavedeny v roce 2005. Princip, na kterém jsou normy založeny je cyklus Plan-Do-Check-Act (PDCA) což je cyklická metoda o čtyřech krocích. Jedná se o kroky naplánuj, proveď, ověř a jednej.

V rámci první fáze celého cyklu projektu, se zaměřujeme na stanovení cílů, které vycházejí z předešlých poznatků a výzkumů. Tato fáze je důležitá pro identifikaci případných nedostatků v současných bezpečnostních opatřeních, ale i pro definování konkrétních cílů, kterých chce organizace dosáhnout. Během tohoto kroku jsou navrženy konkrétní způsoby řešení, přičemž je kladen důraz na výběr nejefektivnějších opatření pro realizaci projektu. Dále je i zajištěno obsazení projektu kvalifikovanými pracovníky, aby byla zaručena úspěšná implementace navržených opatření. Tato fáze je v projektu klíčová a poskytuje pevný základ pro následující kroky.

Následující krok je zaměřen na praktickou implementaci vytvořeného plánu, kdy navržená řešení jsou realizována a nové procesy jsou začleňovány do provozu. Současně je prováděn aktivní sběr a měření dat, mimo jiné i sběr výsledků realizace. Dokumentace provedených opatření je klíčová z důvodu transparentnosti a efektivního sledování pokroku projektu. Tyto dokumentace slouží jako základ pro další analýzu a optimalizaci bezpečnostního prostředí organizace.

Krok ověření představuje proces kontroly, během kterého jsou analyzována a detailně zkoumána data nasbíraná v předchozí fázi projektu. Skutečné výsledky jsou následně porovnávány s výsledky očekávanými. Tímto identifikujeme případně rozdíly a odchylky od plánu.

Posledním krokem celý cyklus uzavíráme. Jeho úkolem je přijetí a implementace nového standardu, pokud předchozí krok prokázal pozitivní výsledky, které přinesly zdokonalení předchozího standardu. V takovém případě se nový postup stává novým standardem organizace. Ovšem pokud se prokáže opak, tedy výsledky budou negativní, plán se nenasadí jako nový standard organizace, ale předchozí kroky jsou prováděny znovu, dokud organizace nedospěje k výsledkům kladným.[10]

Normy týkající se bezpečnosti informací a její problematikou nalezneme pod čísly 27001 až 2707.

2.3.1 ČSN EN ISO/IEC 27000 (369790) – Informační technologie, Bezpečnostní techniky, Systém řízení bezpečnosti informací - Přehled a slovní zásoba

V tomto dokumentu můžeme najít jakýsi přehled systémů řízení bezpečnosti informaci (ISMS) a zahrnuje také definice a termíny běžně používané, které se vyskytují v rámci nejrůznějších norem ISMS. Použití těchto norem není omezeno velikostí ani typem organizací, do kterých je implementována, rozumíme tím, že její využití je možné jak v obchodních společnostech, tak i ve vládních úřadech nebo neziskových organizacích. Termíny a definice, které jsou v této normě objasněny se řídí následujícími kritérii:

- Zahrnují běžně používané termíny a definice v rámci norem ISMS.
- Nezahrnují všechny termíny a definice, které mohou být použity v rámci norem ISMS.
- Nesnižují schopnost norem ISMS definovat nové termíny a jejich definice.

Tento dokument může mít úlohu referenčního materiálu pro organizace, které implementují ISMS a jeho cílem je zajistit jednotnost a srozumitelnost terminologie v rámci oblasti řízení bezpečnosti informací.[11]

2.3.2 ČSN EN ISO/IEC 27001 (369797) – Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy řízení bezpečnosti informací – Požadavky

Tento dokument specifikuje požadavky na zavedení, udržování a neustálé zlepšování systému managementu informační bezpečnosti v rámci kontextu organizace. Obsahuje také požadavky na posuzování a ošetřování rizik informační bezpečnosti, které jsou přizpůsobeny potřebám konkrétní organizace. Tyto požadavky jsou obecné povahy a mají být použity ve všech organizacích bez ohledu na jejich typ, velikost a povahu činností.

Toto tvrzení zdůrazňuje, že organizace, která deklaruje shodu s daným dokumentem (ve formě normy nebo standard), nemůže vynechat žádné požadavky specifikované v kapitolách čtyři až deset daného dokumentu. Vyloučení těchto požadavků by bylo považováno za nepřijatelné.

Výše uvedené zajišťuje, že pokud organizace chce být v souladu s daným standardem nebo normou, musí splnit všechny uvedené požadavky v uvedených kapitolách, bez jakéhokoli výběru či vyloučení. Díky tomuto způsobu je zajištěn celkový a konzistentní přístup k implementaci daných standardů a udržuje se integrita systému, který je na ně založen.[12]

2.3.3 ČSN EN ISO/IEC 27002 (369798) – Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti

V tomto dokumentu je poskytnut referenční soubor obsahující obecná opatření informační bezpečnosti spolu s pokyny k jejich implementaci. Je určen pro použití organizacemi:

- V rámci systému managementu informační bezpečnosti (ISMS) založeném na normě ISO/IEC 27001.
- Pro zavedení opatření informační bezpečnosti založených na mezinárodně uznávaných osvědčených postupech.
- Pro vytvoření směrnic pro řízení informační bezpečnosti specifických pro danou organizaci.

Tento dokument slouží jako zdroj užitečný pro organizace, které chtějí zlepšit svou organizační bezpečnost a dodržovat standardy a osvědčené postupy v této oblasti, zejména v rámci implementace a udržování ISMS a dalších opatření na ochranu informací.[13]

2.3.4 ČSN ISO/IEC 27003 (369790) – Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Pokyny

Obsahem tohoto dokumentu je poskytnutí vysvětlení a pokyny k normě ISO/IEC 27001:2013. [11]

2.3.5 ČSN ISO/IES 27004 (369790) – Informační technologie - Bezpečnostní techniky - Řízení informační bezpečnosti - Monitorování, měření, analýza a vyhodnocování

Tento dokument obsahuje směrnice, které institucím pomáhají během hodnocení výkonnosti bezpečnosti informací a efektivity systému řízení bezpečnosti informací (ISMS) s cílem splnění požadavků normy ISO/IEC 27001:2013, konkrétně bodu 9.1. Konkrétně stanovuje:

- Monitorování a měření výkonnosti bezpečnosti informací.
- Monitorování a měření efektivity ISMS včetně jeho procesů a opatření.
- Rozbor a vyhodnocení výsledků monitorování a měření.

Tento dokument je použitelný pro organizace všech typů a velikostí. Jeho cílem je poskytnout rámec pro systematické vyhodnocování bezpečnosti informací a účinnosti ISMS v souladu s normou ISO/IEC 27001:2013.[15]

2.3.6 ČSN EN ISO/IEC 27006 (369790) - Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

V této mezinárodní normě jsou stanoveny požadavky a zároveň jsou zde poskytnuty doporučení pro orgány, jež provádí audit a certifikaci systému řízení bezpečnostních informací (ISMS). Tato norma je navržena jako doplněk k požadavkům, kterou jsou obsaženy v normách ISO/IEC 17021-1 (týkajících se požadavků pro certifikační orgány) a ISO/IEC 27001 (týkajících se požadavků pro ISMS).

Jako primární cíl této normy je podpora procesu akreditace certifikačních orgánů, které certifikaci ISMS poskytují. Tato norma obsahuje požadavky, které musí být splněny certifikačními orgány, aby prokázaly nejen svou odbornou způsobilost, ale i spolehlivost. Návody, obsažené v normě pak poskytují dodatečnou interpretaci jednotlivých požadavků pro tyto certifikační orgány.

Tato mezinárodní norma může být použít jako referenční dokument dokument pro procesy akreditace, interního hodnocení a auditních procesů týkající se certifikace ISMS. Součástí této normy je i ucelený rámec jehož součástí jsou standardizované požadavky pro hodnocení a certifikaci systému řízení bezpečnostních informací.[16]

2.3.7 ČSN EN ISO/IES 27007 (369790) – Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Směrnice pro audit systémů řízení bezpečnosti informací

V tomto dokumentu jsou poskytnuty pokyny potřebné k řízení programu auditů systému řízení bezpečnosti informací (ISMS), k provádění auditů a kompetencím auditorů ISMS. Pokyny obsažené v této normě překračují pokyny obsažené v normě ISO 19011, která je zaměřena na obecné principy auditorských činností.

Dokument je vhodný pro ty, kdo potřebují porozumět interním nebo externím auditům ISMS, a také pro ty, kteří tyto audity provádění nebo řídí program auditu ISMS. Jsou zde poskytnuty detailní pokyny i postupy, které jsou zaměřeny specificky na auditování systému řízení bezpečnosti informací a zajišťuje, že auditoři mají odpovídající znalosti a dovednosti k provedení účinného a zároveň kompetentního auditu ISMS.[17]

2.3.8 ČSN ISO/IEC 27033 (369701) – Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 1: Přehled a pojmy

V této části normy je poskytnut komplexní přehled o bezpečnosti sítě a souvisejících definicích. Můžeme, zde najít definované a popsané pojmy spojené s bezpečností sítě. Dále zde nalezneme poskytnutý návod na správu a řízení bezpečnostní sítě. Bezpečnost sítě se v tomto kontextu vztahuje na bezpečnost zařízení, činností týkajících se správy zařízení, aplikací/služeb a koncových uživatelů, s výjimkou bezpečnosti informací přenášených přes komunikační linky.

Tato část normy je relevantní pro každý subjekt, který vlastní, provozuje nebo používá síť. Zde zahrnujeme vysoce postavené manažery, netechnické manažery, uživatele, manažery a administrátory, kteří jsou odpovědní za bezpečnost informací nebo bezpečnost sítě, provozování sítě, a v poslední řadě ty, kteří jsou zodpovědní za celkový program bezpečnosti a rozvoj politiky bezpečnosti organizace. Je rovněž relevantní pro ty, kdo jsou zapojeni do plánování, návrhu a implementace aspektů architektury bezpečnosti sítě.

Tato část normy ISO/IEC 27033 také poskytuje následující:

- Návod, jak identifikovat a analyzovat rizika bezpečnosti sítě a definovat požadavky na bezpečnost sítě na základě této analýzy.
- Přehled opatření podporujících technické architektury bezpečnosti sítě související technická opatření.
- Aspekty rizik, návrhu a řízení spojené s typickými scénáři sítí a oblastmi technologií sítí.
- Způsoby dosažení kvalitních technických architektur bezpečnosti sítě.
- Implementace a provozování opatření síťové bezpečnosti spolu s kontinuální monitorování a přezkoumávání jejich implementace.

Celkově tato část poskytuje přehled a jakousi „cestovní mapu“ pro všechny ostatní části této normy související s bezpečností sítě.[18]

2.4 Směrnice o síti a informačních systémech 2

Směrnice Evropského parlamentu a Rady (EU) 2022/2555, známá také jako Směrnice Network and Information System 2 (NIS2), byla oficiálně přijata dne 14. prosince 2022. Cílem této směrnice je implementovat opatření pro zajištění vysoké společné úrovně kybernetické bezpečnosti v rámci Evropské unie.

Směrnice NIS2, kterou můžeme znát jako druhá směrnice o kybernetické bezpečnosti, stanoví společný regulační rámec pro kybernetickou bezpečnost v Evropské unii (EU). Jejím hlavním cílem je zvýšit úroveň kybernetické bezpečnosti v EU. Směrnice vyžaduje, aby členské státy posílily své kapacity v oblasti kybernetické bezpečnosti a zavedly opatření k řízení kybernetických bezpečnostních rizik a povinnost hlášení incidentů v kritických odvětvích. Kromě toho směrnice stanoví pravidla pro spolupráci, sdílení informací, dohled a prosazování v oblasti kybernetické bezpečnosti. Jejím cílem je tedy posílit ochranu kybernetické infrastruktury a zlepšit schopnost reagovat na kybernetické hrozby a incidenty v EU.

Tato směrnice rozšiřuje povinný okruh osob na různé odvětví, včetně sektoru IT služeb, výrobních podniků, poštovních a kurýrních služeb a organizací působících v oblasti výzkumu. Povinné osoby jsou definovány jako subjekty, které musí splňovat minimálně následující kritéria:

1. Dosahují minimálně velikosti středního podniku.
2. Zaměstnávají minimálně 50 pracovníků.
3. Mají obrat nad 10 milionů eur.

Tyto kritéria mohou být použita k určení, které subjekty spadají do kategorie povinných osob s ohledem na daný kontext nebo právní rámec, ve kterém jsou tato kritéria stanovena. Přesné podmínky mohou být specifikovány v právním textu nebo regulaci, která tuto definici obsahuje. Podle této směrnice jsou povinné osoby rozděleny na základní a důležité. Mezi základní povinné osoby patří podniky z odvětví veřejné správy, zdravotnictví nebo dopravy, které splňují stanovená kritéria velikosti podniku. Na druhou stranu mezi důležité povinné osoby spadají všechny ostatní subjekty, které nejsou zahrnuty mezi základní. Mezi ně mohou patřit například poštovní a kurýrní služby, firmy zabývající se nakládáním s odpady, chemickým nebo potravinářským průmyslem nebo vybrané sektory zpracovatelského průmyslu.

Důležité je zmínit, že mezi povinné osoby dle této směrnice nejsou řazeny orgány veřejné správy, ani subjekty v oblasti národní a veřejné bezpečnosti, obrany, soudní moci, vymáhání práva a národní banky. [20]

2.5 Metodiky pro zajištění bezpečnosti informací

Pro zajištění bezpečnosti informací existuje řada metodik. V této kapitole se zaměříme na dvě nejznámější a nejvíce využívané metodiky**:** ***ITIL*** a ***COBIT***.

ITIL, zkráceně pro Information Technology Infrastructure Library, je soubor osvědčených postupů a metodik pro správu a provoz IT služeb.

COBIT, což je zkratka pro Control Objectives for Information and Related Technology, je další důležitá metodika pro správu IT procesů a řízení rizik.

Obě metodiky, ITIL a COBIT, charakterizují základní vlastnosti bezpečnosti informačních systémů a poskytují ucelený rámec pro certifikaci, klasifikaci a posuzování rizik v rámci IT prostředí organizace. Jejich aplikace může pomoci organizacím zlepšit bezpečnostní postupy a dosáhnout lepší ochrany svých informačních aktiv.

2.5.1 Information Technology Infrastructure Library

Jedná se o metodiku známou jako ITIL (Information Technology Infrastructure Library), kterou lze nalézt ve formě knih a příruček v několika sadách. Tato metodika popisuje způsob řízení informačních a komunikačních technologií (ICT) infrastruktury a služeb. Je založena na praktických zkušenostech a obsahuje knihovny, konzultační služby, certifikace, vzdělávání a další související publikace.

ITIL vznikl ve Velké Británii s cílem vytvořit soubor osvědčených postupů, které lze přizpůsobit potřebám každé organizace. Jeho hlavním cílem je poskytnout rámec pro efektivní řízení IT služeb a infrastruktury.

Největší výhodou zavedení metodiky ITIL do organizací je úspora finančních prostředků. Další přínosy zahrnují zvýšenou spolehlivost IT služeb, lepší komunikaci mezi IT oddělením a uživateli a efektivnější využívání ICT zdrojů. Díky tomu může organizace dosáhnout zlepšení v poskytování služeb a dosažení lepšího výkonu v oblasti IT.[9]

2.5.2 Control Objectives for Information and Related Technology

Metodika COBIT neboli Kontrolní cíle pro informační a související technologie, je zaměřena na zajištění efektivity v oblasti řízení informací a informačních technologií v organizacích. Jejím hlavním cílem je umožnit institucím přizpůsobit si svůj přístup k řízení informací co nejpřesněji podle svých potřeb. COBIT se snaží poskytnout co největší a nejkompatibilnější přizpůsobivost a zároveň umožnit specifikovat postupy při řešení systému řízení informací a správy.

Metodika COBIT se zaměřuje na správnou synchronizaci cílů organizace s IT procesy a zahrnuje hodnocení výkonnosti, sofistikovanost a identifikaci odpovědností spojených s IT procesy. Je vhodná pro aplikaci v rámci organizace s cílem zajištění spolehlivosti, kontroly a kvality informačních systémů. Tato metodika poskytuje rámec pro správu informačních technologií, který organizacím pomáhá dosáhnout lepšího řízení a efektivnějšího využití IT zdrojů.[3]

3 KYBERNETICKÉ HROZBY

Kybernetická hrozba může na nás působit jako jakési působení negativního směru, jehož důsledkem může být změna, narušení nebo i krádež či dokonce zničení informací nebo systému. Tyto hrozby jsou nejčastěji původem z kyberprostoru. Pokud je kybernetická hrozba realizována jedná se v tomto případě již o kybernetický útok.

Kybernetické hrozby můžeme rozdělovat do různých kategorií podle:

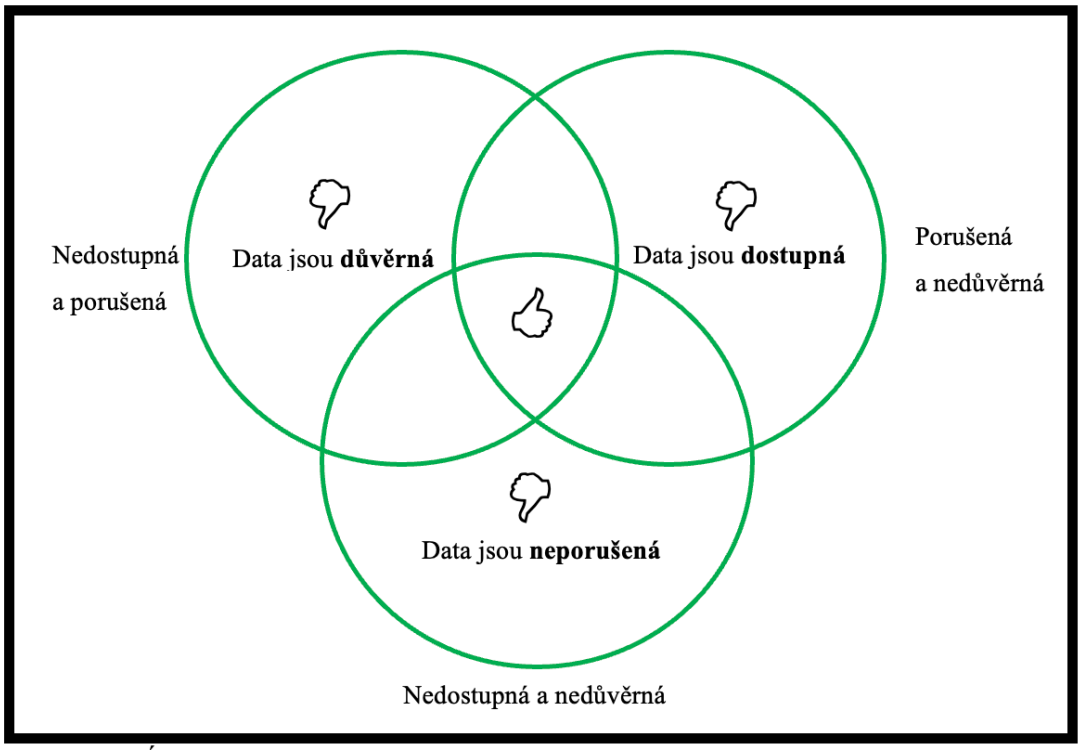
- Zdroje, ze kterého hrozba pochází (lidé, vyšší moc nebo technické chyby).
- Zdroje, ze kterého hrozba působí (vnější nebo vnitřní).
- Motivace, za kterou je hrozba provedena (zničení konkurence, vlastní zisk, dokázání svých schopností apod.).
- Typy hrozeb (DDoS, Phishing, Spamming).

Zdroje hrozeb můžou být různorodé, může se jednat o hrozby, které způsobil člověk, tady se dělí na hrozby úmyslné, jedná se tedy o úmyslné smazání dat či konfigurace systému, můžeme sem ovšem řadit i fyzické poškození jak systému, tak i jiného prvku ICT, krádež dat a informací a kybernetické útoky (malware, phishing, spamming, odposlech bez oprávnění), dále za příčiny člověka zaznamenáváme hrozby z nedbalosti, mezi které patří data, která byla smazána omylem, fyzické poškození (např. pádem nebo překopnutím kabelů) nebo jiné chyby uživatele. Mezi další mimolidské zdroje můžeme řadit například technické chyby (chyba hardware nebo software), vyšší moc (výpadek proudu, přírodní události, katastrofy).

Zdroje působení se mohou nacházet uvnitř organizace, bavíme se tedy o hrozbách vnitřních anebo hrozby, které se nachází mimo organizaci, jedná se tedy o hrozby mimo organizaci.

Stejně jako zdroje hrozeb jsou zde i různé síle hrozeb, jedním z nejčastějších cílů je útok na triádu CIA.

- Důvěrnost (confidentiality) – sem patří například krádeže přístupových údajů nebo klíčů, hardware.
- Neporušenost (integrity) – útoky na chyby v nastavení oprávnění nebo databázích.
- Dostupnost (availability) – výpadky proudu, DDoS a DoS útoky.



Obrázek 1 - Triáda CIA (vlastní tvorba)

Cílem bezpečného systému je zajištění, že všechny tři vlastnosti jsou zachovány. To znamená, že data nebudou zneužita nebo kompromitována, nedojde k nechtěným změnám dat a data budou k dispozici pro oprávněné uživatele v příslušném čase a místě. Zajištění těchto vlastností je základním kamenem pro správnou funkci a spolehlivost jakéhokoli informačního systému.

Útoky mohou být vedeny i na různé prvky kybernetické bezpečnosti jako jsou nejčastěji lidé, zde jsou používány nejčastěji útoky za pomoci sociálního inženýrství, malware nebo phishing. Dalším cílem bývají technologie, hrozby mohou působit na hardware, síť a její infrastrukturu, informace s daty, která jsou uložena v počítačových systémech, databáze nebo software. A v poslední řadě zaznamenáváme i útoky vedené na procesy, čímž se rozumí neoprávněné testování funkčnosti procesů nebo zabezpečení.[3]

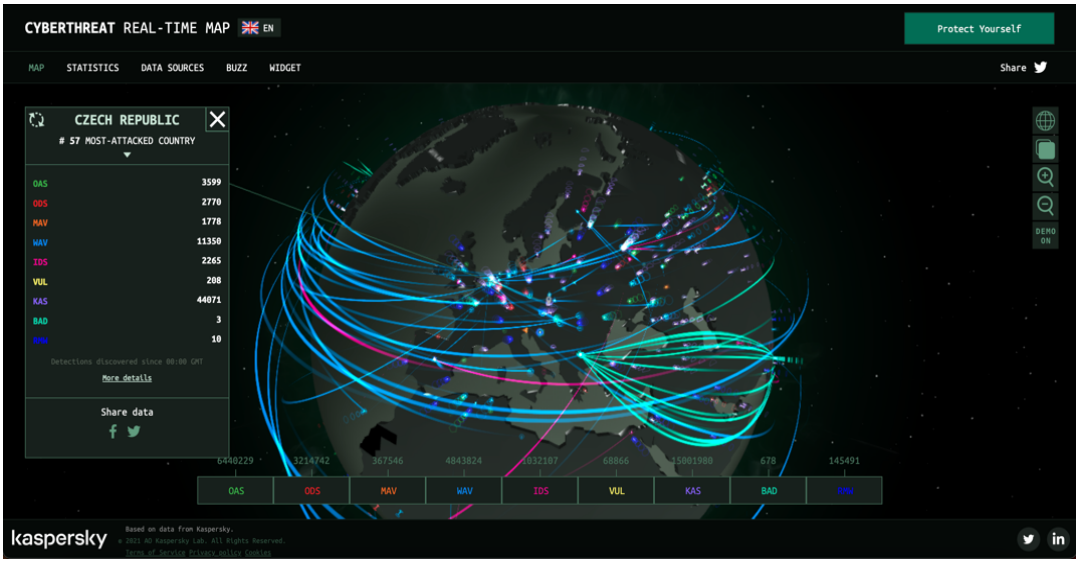
3.1 Kybernetický útok

Definice pojmu kybernetický útok, není úplně jednoznačná, protože existuje řada zdrojů, které se v definici liší. Obecně se tedy jedná o anonymní a neoprávněný pokus o nabourání do počítače nebo jiného elektronického zařízení, za úmyslem způsobit škodu, krádež nebo poškození či dokonce zničení dat a informací. Za kybernetický útok se považuje i případ ve kterém nabouraný počítačový nebo informační systém hodlá útočník použít

k ovládnutí infrastruktury, ovládnutí prostředí nebo také pokud ho plánuje použít ke spuštění dalších útoků.

Kybernetický útok může mít na svědomí jak jednotlivec, tak i organizovaná skupina hackerů. Jako podmět ke kybernetickým útokům může být i státy vyvolávaná politicky motivovaná kybernetická válka nebo také se může jednat o kyberterorismus ze strany teroristů a nestátních aktérů. Jako další motivy bývají nejrozmanitější důvody, může se jedná o špionáž, krádež, podvody a další. Cílem těchto útoků většinou jsou důvody stejné jako když se jedná o útoky nebo zločiny spáchané i mimo kybernetický svět. Jedná se tedy většinou o dosažení nějakých podmínek v podobě výkupného, jelikož se tedy nacházíme v kyberprostoru tak tedy i v měně, která se nachází v kyberprostoru tudíž o kryptoměnu, jelikož to zvýší anonymitu, kterou si útočník nejpodobněji chce udržet.

Jelikož kyberprostor se stále vyvíjí a rozvíjí, je tomu tak i pokud se bavíme o kybernetické útoky. Jejich kvalita se stupňuje se schopností tyto útoky odrážet, tímto však útoky také představují stále vyšší riziko pro národní bezpečnost. [20][21]



Obrázek 2 - Znázornění kybernetického útoku na mapě[22]

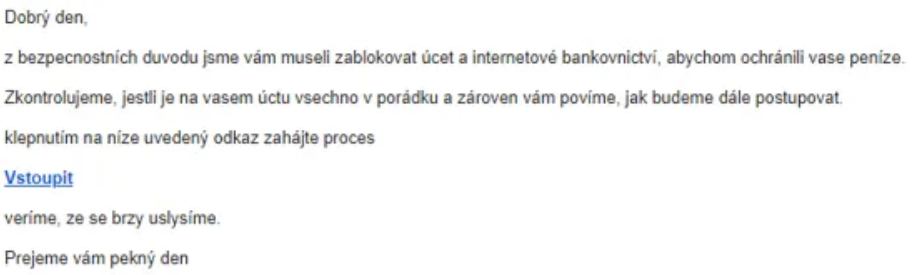
Kybernetické útoky mají celou řadu způsobů, kterými jdou spáchat. Každý typ se liší a vyvíjí neustále. Mezi tyto typy patří: Phishng, sniffing, spamming, malware, ransomware, spyware, trojské koně a DDoS (Distributed Denial od Service).

3.2 Phishing

Pro vznik slova phishing existuje několik různých teorií. Uvedu zde tři teorie, které stojí za vznikem slova. První teorií je, že slovo vzniklo spojením slov „fishing“, jako

rybolov. a „phreaking“ jako odkaz na první útok hackerů, který proběhl v USA, a to na telefonní síť. Další teorií je že první dvě písmenka slova „ph“ slouží jako značení pro specializovanost pachatelů páchajících tyto útoky. Třetí teorií uvádí, že se jedná o zkratku slov „password harvesting fishing“, toto spojení můžeme přeložit do češtiny jako „rybolov sklízením hesel“.

Metoda phishing funguje na bázi podvodu. Probíhá to tak, že hacker, útočník se snaží získat přístup k finančnímu účtu, platební kartě a jakmile se mu to povede snaží se finance zde nalezené odčerpat pro sebe. Nejedná se o útoky směřované směrem na banky, ale o snahu poškodit přímo osobu, která je majitelem účtu, na který je útok prováděn. Oběti těchto útoků bývají často neznalí, příliš důvěřivý nebo lehkomyslní při sdělování svých osobních údajů, které pachateli umožní přístup k jejich bankovním účtům.


Dobrý den,

z bezpecnostních duvodu jsme vám museli zablokovat úcet a internetové bankovnictví, abychom ochránili vase peníze.

Zkontrolujeme, jestli je na vasem úctu vsechno v porádku a zároven vám povíme, jak budeme dále postupovat.

klepnutím na níze uvedený odkaz zahájte proces

Vstoupit

veríme, ze se brzy uslysíme.

Prejeme vám pekný den

Obrázek 3 - Ukázka phishingu[23]

Jak tedy rozpoznat phishing od skutečné komunikace od banky nebo jiné stránky? Podvodníci vždy požadují přístupy a hesla ke klientským účtům. Všechny čísla chtějí celá i s čísly PIN. Vydávají se často za společnosti velmi známé. Většinou se s nimi setkáváme při nákupech a prodejích online. [23]

3.3 Spamming

Slovo „spam“ pochází z názvu konzerv, které se jmenovali totožně a to „SPAM“ jednalo se o zkratku slov Sizzle Pork And Mmm. Jednalo se o šunkové konzervy, které byly distribuovány velmi hojně během druhé světové války firmou Hormel foods. Pokud se bavíme o informačních sítích slovo spam tady nabylo v reakci na toto zboží význam „bláboly“ či „hloupé řeči“.

Slovo spam tedy pokud se bavíme o kybernetické útoky můžeme charakterizovat jako zasílání nechtěné elektronické pošty, většinou se jedná o zprávy s reklamními oznámeními. Všechny spamy mají společnou vlastnost a to tu, že spaměři emaily posílají na co

nejvíce emailových adres, které se jim podaří získat co v nejhojnějším počtu. Při tomto způsobu útoku se nejedná o cílený útok na určitou skupinu lidí, pro které by tyto reklamní sdělení mohly přijít zajímavé. Spameři tyto emaily posílají nehledě na to, jestli se jedná o muže, ženu nebo dítě, všem pošlou to samé.

Jedním ze znaků spamu jsou emailové adresy adresátů, jelikož tyto adresy ve většině případů budou falešné, nebudou existovat. Tudíž pokud se pokusíte odepsat, zablokovat, nebude to mít žádný účinek, jelikož adresa neexistuje tudíž zpráva se nemá kam odeslat.

O spam se nejedná, pokud emaily, které obdržíme jsou námi vyžádány. Například u stránek, kde jsme se k odběru reklamních sdělení přihlásili.

Spameři se k emailovým adresám dostávají především z www stránek, za pomoci externích programů, které obsah stránek analyzují a hledají zde adresy. Jestliže vaše adresa byla zveřejněna na nějaké www stránce, například jako podpis pod vaším článkem nebo také pokud jsme přispěli svým komentářem v diskusi třeba i na stránce www.idnes.cz, spam se ve vaší stránce objeví během prvních dvou týdnu od zveřejnění. Nejspolehlivější prevenci proti spamu si zajistíte tak, že nebudete svůj email zveřejňovat zbytečně na nedůvěryhodných stránkách.[24][25]

3.4 Malware

Slovo malware vzniklo spojením dvou anglických slov jedná se tedy o slova „malicous“ (zákeřný) a software. Mezi malware se řadí veškerý škodlivý kód bez ohledu na způsobu napadání nebo výsledku jeho činnosti, nezáleží ani na jeho chování. Malware můžeme rozřadit do několika podkategorií, řadí se sem podkategorie ransomware, spyware, trojské koně, červi, viry dokonce i třeba bankovní malware. V obecném měřítku můžeme říct, že se jedná o veškerý software, který byl vytvořen se záměrem uškodit.

Malware můžeme poznat hned podle několika skutečností, které na našem zařízení zpozorujeme. Můžeme ho poznat podle změny domovské stránky v našem prohlížeči, zobrazování nežádoucích upozornění, zobrazování nežádoucích vyskakovacích oken, následně to může vést i ke zpomalení funkcí, které vykonáváme na našem zařízení, nesmyslné zvýšení využití paměti nebo pokud se jedná o mobilní telefon tak zvýšená spotřeba mobilních dat, zvýšená spotřeba baterie anebo instalace aplikací na naše zařízení, které jsme si sami instalovat nechtěli.

Účinnou ochranou jsou v tomto případě bezpečnostní programy. V těchto programech můžeme najít řadu technologií, které se útokům typu malware dokáži nejen vyvarovat, ale i je v případě napadení odstranit. Jinými způsoby, jak se škodlivého kódu zbavit je způsob manuální, který je poměrně složitější, jelikož při tomto způsobu je nutné škodlivý soubor najít v počítači, což jak můžeme tušit nebude úplně lehký úkol pro běžného uživatele. Tyto škodlivé soubory v našem zařízení se umí dost dobře schovat, aby odinstalaci zabránila. [26]

Date: Fri, 3 Jan 2020 08:23:35 +0200
From: Valentina Aulisa <carolyn@digitalnews-online.com>
To: [redacted]
Subject: Pohledávky. Dôvodová správa.

Vážení,

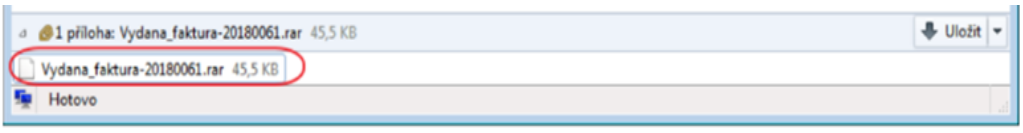
kontrolou naší účetní evidence jsme zjistili, že jste nám dosud neuhradili dlužnou částku ve výši 6.437,- Kč.

Současně vás tímto upozorňujeme, že pokud k úhradě uvedené částky na základě této písemné výzvy dobrovolně nedojde, případně se ani neozvete, a to obratem, za účelem návrhu akceptovatelného řešení této situace, jsme připraveni se domáhat uvedeného nároku právní cestou, především pak podáním žaloby k místně příslušnému soudu

Dôvodová správa v příloze (zahrnuje fakturu a smlouvu).

S pozdravem a přáním hezkého dne,
Valentina Aulisa
advokát/attorney at law
Opatovická 1633/8, Praha 1

Obrázek 4 - Malware[27]



Obrázek 5 - Škodlivý soubor[27]

3.4.1 Ransomware

Slovo ransomware vzniklo opět spojením slov tentokrát jde o slova „ransom“ jako výkupné a „software“.

Ransomware jakožto podkategorie malware také spadá do skupiny škodlivého softwaru. Cílem tohoto kódu je omezení či úplné znemožnění přístupu k napadanému systému a jeho dat, což je následně využito proti napadenému formou vydírání. Útočník, jakmile data znepřístupní, pošle uživateli, výhružnou zprávu a jeho cílem je z uživatele vymámit hlavně peníze, v dnešní době spíše kryptoměnu, pod příslibem následného zpřístupnění dříve napadených dat a systému. Většinou uživateli vytyčí nějaký časový limit, ve kterém chce po něm poslat nějaký finanční obnos pod výhružkou, pokud uživatel nesplní tento časový limit, tak útočník smaže takzvaný soukromý klíč což by vedle k trvalému znemožnění přístupu k datům, které byly útočníkem zašifrovány. Avšak existuje i mnoho dalších způsobů, jak se útočníci snaží z uživatelů vymámit nějakou finanční odměnu. Mohou zvolit i taktiku, kde se vydávají za veřejný orgán a touto lží mámí peníze.

Obrázek 6 - Oznámení o útoku ransomware[29]

Cílem útoku ransomware může být každý od běžného uživatele, podniky nebo společnosti až po veřejné subjekty jako třeba letiště, nemocnice, nebo nádraží. Pokud se bavíme o podnicích a společnostech tak cílem útoků, většinou bývají data o zákaznících, které firma nechce ztratit z důvodu důvěry zákazníka, která by takto mohla býti značně nalomena. Další

obavou pro tyto možné cíle útoku je jejich know-how nebo obchodní tajemství, které je pro ně stejně jako jejich zákazníci nejstřeženějším bodem, který dělá firmu firmou.

Způsob útoku může být velmi jednoduchý, můžeme obdržet email se škodlivou přílohou nebo odkazem na stránku, která obsahuje malware a tady vše může odstartovat pouhé kliknutí myši. Ten způsob útoku se nazývá malspam, toto slovo vzniklo ze dvou anglických slov a to ze „malware“ a „spam“. Pokud útočník využívá metodu malspam jeho cílem je uživatele zaujmout a podvědomě přimět na kliknutí odkazu, který by škodlivý kód na jeho zařízení spustil. Jedná se o reklamní emaily, kde nám nabízí výhru, která nám mnohdy může přijít až přehnaná, třeba smrt nějakého příbuzného, kterého mnohdy ani nemusíme vědět, že máme, avšak najednou jsme zdědili milionové jmění nebo nabídku transakce, která je natolik výhodná, že jen „hlupák“ by ji odmítl. Jak již víme, tahle metoda má název phishing.

V posledních letech se hojně využívá typ ransomware, který je známý pod názvem malvertising. Které můžeme přeložit jako zákeřná reklama, jedná se o pokus infikovat naše zařízení přes škodlivou reklamu, kterou běžně potkáváme dne již na víceméně každém webu. U této možnosti by si laik mohl pomyslet, že se může jednat o reklamy na stránkách, které se nacházejí spíše na té odvrácenější straně internetu, avšak existují i případy, kde se tato reklama objevila na stránkách známých a velmi frekventovaných.

Způsob, kterým se tedy před škodlivými ransomware soubory chránit je jednoduchý. Nejúčinnější je zálohování, pokud si budeme důležitá data zálohovat pravidelně a důkladně, žádný ransomware útok by nás neměl rozhodit. Pro zálohování můžeme použít k nejlepší ochraně zálohování hned několik poměrně známých cloudových uložišť, která se dají použít bezplatně, jako jsou například OneDrive, Google Drive. [29][30]

3.4.2 Spyware

Spyware je druh útoku, který za pomoci internetu odesílá bez vědomí uživatele data z počítače. Jsou odcizována data pouze statistická, mezi které můžeme řadit třeba přehled nainstalovaných aplikací, programů nebo přehled stránek, které námi byli navštívené. Tento počin, může být klasifikován jako pouhé zjišťování potřeb nebo zájmů, které má uživatel za zástěnkou personalizované reklamy. Není však možné zaručit, že tyto informace nikým nebudou zneužita. To vede k hlavnímu nesouhlasu ze strany uživatelů nad existencí legálnosti spyware jako takového. [31]

3.4.3 Trojské koně

Název trojský kůň, je odvozen z řecké mytologie, kde se používal všem velmi známý Trojský kůň jako dar pro bájnou Troju, avšak uvnitř tohoto obrovského dřevěného koně, se ukrývali vojáci, kteří během noci, kdy všichni slavili a nikdo koně nehlídal vylezli z jeho dutých útrob a město Troju dobili, za pomoci této lsti. Můžeme tedy z tohoto usoudit, že se bude jednat o škodlivý kód, který se bude ovšem tvářit jako pomocník v našem zařízení. Můžeme ho najít pod kápí neškodné hry, aplikaci pro spořič obrazovky, ale i jako pro naše zařízení užitečný program pro odstranění malware.

Jeho úkolem tedy je převzetí kontroly nad naším systémem, kde se nenápadně schoval. Jeho cílem je hned několik různých činností jako například získávání hesel, vzdálené ovládání systému nebo manipulace se soubory. Pokud ho porovnáme s jinými viry, není jeho funkcí samovolné rozšiřování.

Setkáním s ním se můžeme vyhnout jednoduše tak, že nebudeme instalovat nic neověřeného nebo nedůvěryhodného. Určitě žádné emailové odkazy nejsou vhodné ani důvěryhodné pro stahování čehokoli.[31]

4 ZÁKLADNÍ PRINCIPY KYBERNETICKÉ BEZPEČNOSTI

Jedná se o klíčové směry a filozofie, které mají schopnost nás navést k efektivní ochraně informačních systému a dat před kybernetickými hrozbami. Pomocí těchto principů nám bude poskytnut rámec pro vytvoření bezpečnostního prostředí, jež bude odolné oproti různým typům útoků a zranitelnostem.

4.1 Autentizace a autorizace

Autentizace je chápána jako proces pro ověření identity uživatele i systému Jako cíl autentizace se považuje potvrzení, že uživatel nebo systém je vskutku tím, za koho se vydává. Existují různé typy autentizace jako nejjednodušší formu známe jednofaktorovou autentizaci, které zahrnuje pouze jeden typ ověření, a to heslo nebo pin. Dalším typem autentizace je dvoufaktorová autentizace, která přidává druhou úroveň zabezpečení. Nejvíce efektivním typem autentizace je ovšem vícefaktorová autentizace, jelikož vyžaduje minimálně dva nebo více způsobů ověření, které na sobě nejsou závislé.

Autorizace je však proces, který určuje, jaká práva a privilegia má ověřený uživatel nebo systém v rámci konkrétního prostředí. Takže na rozdíl od autentizace, jež potvrzuje identitu, autorizace určuje, co uživatel smí dělat. Máme tyto typy autorizace:

- Attribute-Based Access Control (ABAC)
- Discretionary Acces Control (DAC)
- Mandatory Access Control (MAC)

4.2 Šifrování a kryptografie

Kryptografie je věda, která se zabývá zabezpečením komunikace a dat za cílem zajistit důvěrnost, integritu, autentizaci a nepopiratelnost informací. Existují dva hlavní typy šifrování, a to symetrické a asymetrické. Pro symetrické šifrování je používaný jeden tejný klíč, který slouží pro zašifrování a dešifrování dat, což je považováno jako efektivní a rychlé, ale zároveň je vyžadováno bezpečné spravování a distribuce klíče. Avšak asymetrické šifrování tyto klíče používá dva jeden veřejný, jako nástroj pro šifrování a jeden soukromý jako nástroj pro dešifrování.

4.3 Zabezpečení sítí a firewally

Klíčovým prvkem ochrany citlivých dat a informací je zabezpečení sítí. V tomto procesu hrají zásadní roli firewally, jelikož fungují jako bariéra mezi interní sítí organizace a externími sítěmi jako je internet. Funkce firewallu je monitorování a kontrola příchozího a odchozího síťového provozu na základě bezpečnostních pravidel, která jsou definována, a tímto zabraňují neoprávněnému přístupu k síťovým zdrojům. Některé moderní firewally již často obsahují pokročilé funkce jako je třeba detekce a prevence narušení (IDS/IPS) nebo filtrování webového obsahu.[32]

5 OCHRANA CITLIVÝCH DAT

Ochrana dat je jedním z nejzásadnějších aspektů kybernetické bezpečnosti. Je důležité chránit citlivá data jako jsou osobní údaje, obchodní tajemství nebo finanční informace. Ty to data totiž představují cenný majetek pro organizace, ale i pro jednotlivce a jejich zneužití či ztráta může mít mnohdy devastující účinky.

5.1 Klasifikace a kategorizace dat

Jedná se o kritické procesy, které pomáhají organizacím efektivně spravovat a chránit své informace. Klasifikací dat je přiřazena úroveň citlivosti a důležitosti různých typů dat. Kategorizací je dále dosaženo organizace dat do logických skupin podle jejich charakteristik, použití nebo obchodních funkcí. Klasifikace a kategorizace usnadňují správu dat, stanovují priority pro bezpečnostní opatření a díky nim je organizace schopná lépe reagovat na bezpečnostní incidenty.[33]

5.2 Zásady pro bezpečné ukládání a přenos dat

Bezpečné ukládání a přenos dat řadíme mezi základní složky kybernetické bezpečnosti, jejich cíle je zajištění ochrany citlivých informací. Pokud ukládáme data, je stěžejní dodržovat určité zásady jako je například kryptografické šifrování uložených dat nebo pravidelné zálohování a obnova dat. Pokud nastane přenos dat je nezbytné použít šifrované komunikační kanály jako jsou například *Hypertext Transfer Protocol Secure* (HTTPS) nebo *Secure Sockets Layer* (SSL), aby data zůstala zabezpečena při přenosu mezi různými zařízeními a sítěmi. Dodržováním těchto zásad minimalizujeme riziko úniku dat a manipulace s daty.[34]

5.3 Zálohování a obnova dat

Zálohování a obnova dat zajišťují ochranu dat a minimalizují dopady možných bezpečnostních incidentů v organizaci jako jsou například ransomware, poruchy hardware nebo lidský faktor. Zálohováním dat vytváříme duplicitní kopie důležitých dat na externích úložištích, serverech nebo cloudových platformách. V případě zálohování je více než důležité zajistit aktuálnost a úplnost dat. Obnova dat následně zaručí obnovu dat ze záloh v případě výše zmíněných incidentů. Pokud jsou data zálohována je důležité i ověřování funkčnosti zálohovacích procesů, aby bylo zajištěno úspěšné obnovy v případě potřeby. [35]

6 SPRÁVA PŘÍSTUPŮ A IDENTIT

Správa přístupů a identit zaujímá důležitou roli v rámci kybernetické bezpečnosti. Zabývá se řízením a monitorováním přístupových práv uživatelů a aplikací k různým zdrojům v organizaci. Jsou zde zahrnuty proces, technologie a politiky, jejichž úkolem je zajištění přístupu k informacím a zdrojům pouze ze strany oprávněných osob.

6.1 Řízení přístupu založené na rolích

V originálním znění Role-Based Acces Control (RBAC) je strategie řízení přístupu, která určuje přístupová práva k systémovým zdrojům na základě rolí, které mají uživatelé v organizacích. Ke každé roli je možné přiřadit sadu oprávnění, pomocí nichž je určeno, jaké akce může uživatel provádět v rámci systému nebo aplikace. RBAC je zjednodušení pro administrátoru v tom ohledu, že oprávnění přiřazují rolím nikoli jednotlivým uživatelům. Tímto je sníženo riziko chyb v řízení přístupu. [36]

6.2 Princip nejmenších privilegií

Jedná se o zásadu kybernetické bezpečnosti, která říká, že uživateli by měli být předěleny pouze práva, která jsou nezbytná pro výkon jejich úkolů a funkcí. Minimalizování útoků tímto principem se projeví tak, že je snižována možnost zneužití, rozšiřování škody a úniku dat v případě kompromitace účtu uživatele. [37]

6.3 Správa hesel a bezpečnostní politiky

Správa hesel a implementace bezpečnostních politik pomáhají chránit citlivé informace a systémy před neoprávněným přístupem a zneužitím. Pod správu hesel spadá i urgence použití silných hesel, které nejsou tak snadná k prolomení. Dále zde můžeme zahrnout i pravidelnou změnu hesel, omezení počtu neúspěšných pokusů o přihlášení a dvoufaktorovou autentizaci na místech, kde je to možné. V rámci bezpečnostních politik jsou definována pravidla a postupy týkající se právě používání hesel, přístupu k systémům nebo šifrování dat. Pokud je implementace těchto politik důkladná je považována za klíčovou při ochraně a prevenci bezpečnostních incidentů.[38]

7 MONITOROVÁNÍ A DETEKCE HROZEB

7.1 Systémy pro detekci a prevenci narušení

Jedná se o nástroje v oblasti kybernetické bezpečnosti, které pomáhají organizacích při ochraně svých sítí a systémů před škodlivými aktivitami a útoky. Řadíme sem nástroje jako systém pro odhalení průniku (IDS), jeho funkcí je monitorování síťového provozu a hledání známek neautorizovaného přístupu a jiných podezřelých aktivit. Avšak řadíme sem i systém prevence průniku (IPS), jehož funkcí je nejen detekce, ale i zásah a případné blokace nebezpečných typů. Metody využívány tímto systémem jsou například srovnávání síťového provozu s databází povolených a zakázaných vzorů nebo analýzy chování. Implementace těchto systému v organizacích pomáhá zlepšit jejich bezpečnost informačních systémů.[39]

7.2 Řízení bezpečnostních informací a událostí

Tento strategický přístup nese zkratku SIEM a slouží pro správu informací o bezpečnosti a analýzu bezpečnostních informací. S tímto systémem mají organizace možnost efektivně monitorovat a detekovat na bezpečnostní incidenty a hrozby v reálném čase. SIEM agreguje data z různých zdrojů a poskytuje organizacím pohled na stav jejich kybernetické bezpečnosti. Tím je organizacím umožněna rychlá identifikace potencionálních bezpečnostních incidentů, analýzu jejich závažnosti a odpovídající reakci na tyto incidenty.[40]

7.3 Pravidelné audity a zátěžové testování

Pravidelně audity a zátěžové testy pomáhají organizacím posoudit úroveň bezpečnosti svých informačních systémů a procesů, čímž mohou identifikovat potencionální slabiny a nedostatky. Pravidelné audity mohou být provádění interními nebo externími auditory a zajišťují povědomí o tom, zda-li je možné nějaké zlepšení bezpečnostních politik a zda-li jsou tyto politiky dodržovány. Pokud mluvíme o zátěžovém testování, to simuluje reálně kybernetické útoky a posléze zkoumá odolnost organizace na tyto scénáře. Těmito audity organizace může identifikovat slabá místa a následně je posílit podle potřeby. [30]

8 ŠKOLENÍ A VZDĚLÁVÁNÍ ZAMĚSTNANCŮ

Zde se zaměříme na význam školení a vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti. Jelikož lidský faktor je mnohdy ten nejzranitelnější musí organizace tomuto faktoru věnovat speciální pozornost.

8.1 Význam vzdělávání v oblasti kybernetické bezpečnosti

Význam školení kybernetické bezpečnosti by zejména v dnešní době, kdy kybernetické hrozby se neustále vyvíjí a jsou čím dál více sofistikovanými, neměl být opomíjený. Vzdělávání zaměstnanců je klíčové pro udržení kroku s nejnovějšími technologiemi, bezpečnostními postupy a hrozbami. Proces vzdělávání zaměstnancům umožňuje vetší prostor pro seberozvoj a posílení schopností rozpoznání a reakce na potencionální hrozby. Žádanými aspekty vzdělávání je zvýšení úrovně bezpečnostního povědomí v organizaci, což vede k lepší schopnosti identifikovat potencionální hrozby. Dalším aspektem je to, že zaměstnancům je umožněno lépe porozumět bezpečnostním postupům a politikách. Nebo také to, že neustálé vzdělávání předchází riziko lidských chyb, které mohou vést k bezpečnostním incidentům.[42]

8.2 Bezpečné chování na internetu a používání firemních zařízení

Zaměstnanci by měli být obeznámeni s nebezpečím spojeným s neopatrným chováním na internetu, jako jsou klikáni na podezřelé odkazy, stahování neověřeného software nebo sdílení dat, které jsou citlivé jak pro zaměstnance, tak i pro firmu. Důležité je i bezpečné používání firemních zařízení. Zaměstnanci by měli být instruování s dodržováním bezpečnostních politik a postupů pro práci s firemními zařízeními jako jsou například pravidelné aktualizace, používání silných hesel nebo zapnutí firewallu a antivirové ochrany. Bezpečnostní opatření v případě odcizení nebo ztráty dat by měla být implementována také.[43]

II. PRAKTICKÁ ČÁST

9 PLÁN REALIZACE ŠKOLENÍ O KYBERNETICKÉ BEZPEČNOSTI

Tento plán podrobně popisuje cíle školení, potřebné materiály a metody výuky, který zajistí, že školení bude efektivní a přizpůsobené specifickým potřebám naší organizace. Důraz je kladen na praktickou aplikaci získaných znalostí a na vytvoření prostředí, ve kterém se zaměstnanci cítí motivovaní k aktivnímu zapojení do kybernetické bezpečnosti.

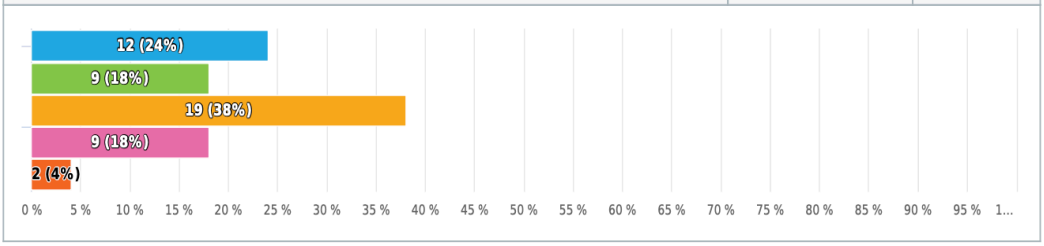
9.1 Sběr dat z ankety o kybernetické bezpečnosti ve firmách

Pomocí ankety byly sebírány data, která jsou následně použita v následujících odstavcích. Data byla svírána kvůli lepšímu pochopení aktuální úrovně povědomí a připravenosti zaměstnanců čelit kybernetickým hrozbám.

9.2 Stanovení cílů školení

Stanovení cílů školení je klíčové pro úspěch v jakémkoli vzdělávacím programu. Tyto cíle poskytují jasný směr a určují očekávané výsledky, které organizace chce dosáhnout prostřednictvím školení. Definování cílů umožňuje lépe zaměřit obsah a metodiku školení tak, aby efektivně reagovala na potřeby účastníků a specifické hrozby, jimž organizace čelí. Díky jasně stanoveným cílům mají účastníci lepší představu o tom, co mohou očekávat, a mají motivaci se aktivně zapojit do školení. Tím se zvyšuje pravděpodobnost úspěšného přenosu znalostí a dovedností a dosažení pozitivních změn v chování a postojích zaměstnanců v oblasti kybernetické bezpečnosti. Stanovení cílů také usnadňuje evaluaci školení a hodnocení jeho účinnosti, protože umožňuje porovnat skutečné výsledky s očekávanými výstupy a identifikovat případné nedostatky a oblasti potřebující zlepšení. Celkově tedy stanovení cílů školení posiluje jeho efektivitu a přispívá k posílení kybernetické bezpečnosti v organizaci.

Možnosti odpovědí	Responzí	Podíl
1x ročně (minimální bezpečnostní standard)	12	24,0%
Častěji	9	18,0%
Méně než 1x ročně	19	38,0%
Neúčastním se	9	18,0%
Jiná	2	4,0%



Obrázek 7 - Četnost školení v organizacích

Když byli respondenti ankety dotazování na to, jak často se účastní školení o kybernetické bezpečnosti, nejčastěji volili odpověď, „méně než 1x ročně“, což není ideálním stavem vzhledem k rychlosti objevování nových hrozeb kybernetické bezpečnosti.

Pro Českou republiku by hlavní cíle školení o kybernetické bezpečnosti můžeme definovat následovně:

1. Zvýšení povědomí o kybernetických hrozbách:
   - Informovat zaměstnance o aktuálních kybernetických hrozbách a jejich potenciálních dopadech na firmu a jednotlivce.
   - Zdůraznit důležitost prevence a ochrany před různými typy kybernetických útoků, včetně phishingu, ransomwaru, malware a sociálního inženýrství.
2. Zdokonalení dovedností v reakci na útoky:
   - Poskytnout zaměstnancům praktické dovednosti a know-how k rychlé a efektivní reakci v případě kybernetického incidentu.
   - Trénovat týmy pro identifikaci, izolaci a řešení bezpečnostních incidentů, včetně zálohování dat a obnovení služeb.
3. Posílení bezpečnostní kultury v organizaci
   - Vytvořit a podporovat bezpečnostní kulturu, ve které jsou zaměstnanci aktivními účastníky ochrany informací a prevence kybernetických rizik.
   - Vyzdvihnout důležitost bezpečnostních postupů a politik a podpořit dodržování a respektování těchto pravidel ve všech úrovních organizace.

Zavedení těchto cílů do školení o kybernetické bezpečnosti by mělo pomoci organizacím zlepšit svou schopnost odolávat kybernetickým hrozbám a posílit ochranu citlivých dat a informací. Je také důležité zohlednit specifika českého právního a podnikatelského prostředí při formulaci konkrétních opatření a strategií kybernetické bezpečnosti.

9.3 Cílová skupina

Identifikace zaměstnanců, kteří budou podstupovat školení o kybernetické bezpečnosti, by měla zahrnovat ty, kteří mají přímý vliv na bezpečnost informací a IT infrastruktury. Mezi tyto zaměstnance by měli patřit:

1. Manažeři

Vedoucí pracovníci a manažeři mají často přístup k citlivým informacím a jsou zodpovědní za rozhodování v oblasti bezpečnosti. Je důležité, aby měli hlubší porozumění kybernetickým hrozbám a schopnost vést své týmy k dodržování bezpečnostních postupů.

2. IT pracovníci

IT odborníci jsou první linií obrany proti kybernetickým útokům a mají klíčovou roli při správě a ochraně IT infrastruktury. Jejich školení by mělo zahrnovat detailní znalost různých typů útoků a moderních bezpečnostních technologií.

3. Zaměstnanci pracující s citlivými daty

Kromě manažerů a IT pracovníků je důležité školit i zaměstnance, kteří mají přímý přístup k citlivým datům. To může zahrnovat zaměstnance oddělení lidských zdrojů, finančních oddělení, právních služeb a dalších oblastí, kde se manipuluje s důvěrnými informacemi.

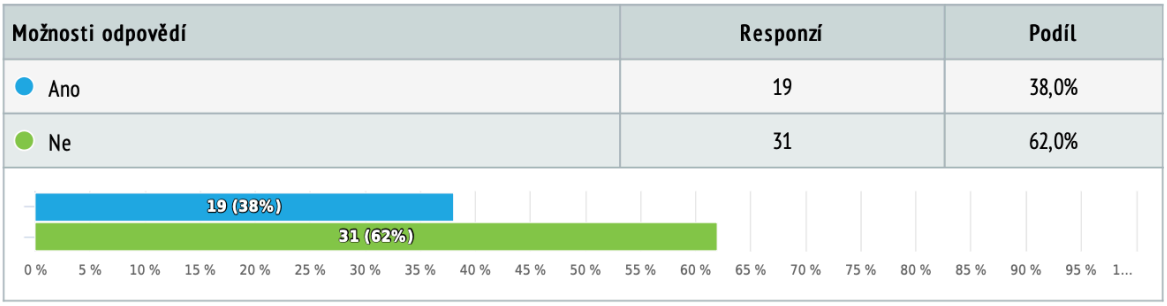
4. Ostatní zaměstnanci

I ostatní zaměstnanci by měli projít základním školením o kybernetické bezpečnosti, aby byli schopni rozpoznat potenciální hrozby a jednat v souladu s bezpečnostními politikami organizace. To platí zejména v případě zaměstnanců, kteří pracují s počítači a internetem jako součást své práce.

Identifikace těchto klíčových skupin zaměstnanců umožní organizaci efektivně cílit své školení o kybernetické bezpečnosti a zajistit, že ti, kteří mají největší vliv na bezpečnost organizace, budou dobře informováni a připraveni k akci v případě kybernetického incidentu.

Zde můžeme vidět, podle výsledků z ankety, kde otázka zněla, jestli školení respondentů v jejich organizaci je dostatečně přizpůsobené potřebám a pozici ve firmě, že více něž

polovina dotazovaných není spokojena, což značí, že dělení do cílových skupin, pro které je školení určeno, může pro zaměstnance znamenat poměrně značný rozdíl, než pokud tomu tak není.



Obrázek 8 - Přizpůsobení školení pozici ve firmě

9.4 Výběr školení

Zvolení vhodného formátu školení je klíčové pro efektivní přenos znalostí a dovedností v oblasti kybernetické bezpečnosti. Zde jsou možné formáty školení, které by byly vhodné pro firmu:

- Prezentace

Prezentace jsou efektivní pro předávání základních informací o kybernetických hrozbách, bezpečnostních postupech a nejlepších praktikách. Může se jednat o prezentace vedoucího pracovníka, externího experta nebo interního IT týmu.

- Interaktivní semináře

Interaktivní semináře umožňují účastníkům aktivně se zapojit do školení prostřednictvím diskusí, skupinových cvičení a praktických příkladů. Tento formát umožňuje lepší zapojení a sdílení zkušeností mezi účastníky.

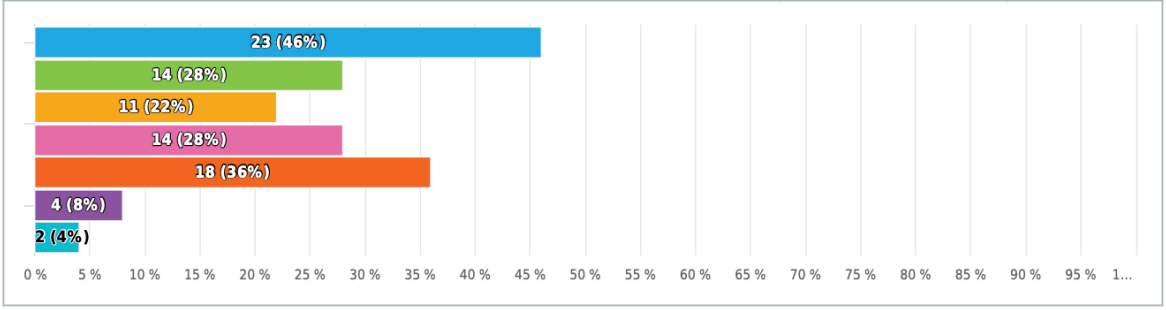
- Online kurzy

Online kurzy poskytují flexibilitu a možnost učit se vlastním tempem. Mohou obsahovat videa, testy, interaktivní prvky a diskusní fóra. To je ideální pro zaměstnance, kteří nemusí být přítomni v jednom místě nebo mají omezený čas.

- Praktická cvičení

Praktická cvičení simuluji skutečné kybernetické situace a umožňují účastníkům procvičovat své dovednosti v reálném prostředí. To může zahrnovat simulované útoky, scénáře řízení incidentů a testování bezpečnostních opatření.

Možnosti odpovědí	Responzí	Podíl
Online kurzy	23	46,0%
Workshopy	14	28,0%
Papírová podoba	11	22,0%
Školení zaměstnavatelem (vedoucím)	14	28,0%
Školení externí osobou	18	36,0%
Neúčastním se	4	8,0%
Jiná	2	4,0%



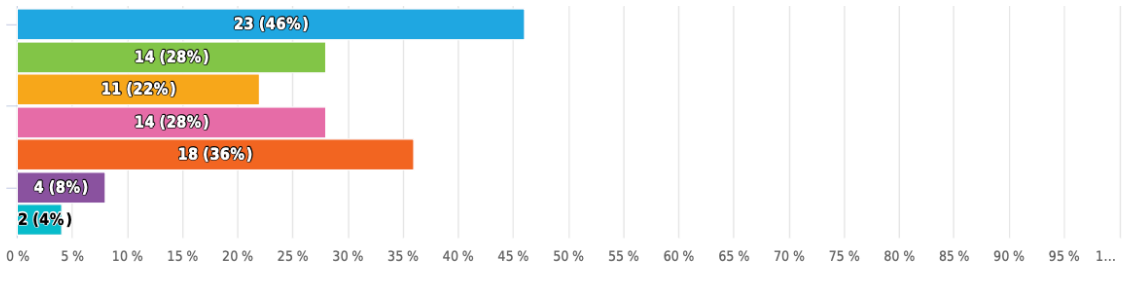
Obrázek 9 - Aktuální typy školení

Když byli respondenti dotazování, jaké formy školení jsou jim k dispozici v rámci jejich organizace nejčastější odpovědí byli online kurzy, jelikož se jedná o nejméně finančně a časově náročnou možnost, avšak jelikož na průběh školení nikdo nedohlíží tudíž ho nelze považovat jako nejefektivnější.

Pro optimální výsledky může být užitečné kombinovat různé formáty školení, aby se pokryly různé učební styly a potřeby účastníků. Například lze začít s prezentací o základech kybernetické bezpečnosti, pokračovat interaktivním seminářem k diskusi a zdůraznění konkrétních témat a zakončit praktickými cvičeními k procvičení dovedností v reálném prostředí.

Při dotazu jakým stylem by zaměstnanci školení v organizaci preferovali, repondeti reagovali následovně:

Možnosti odpovědí	Responzí	Podíl
Online kurzy	23	46,0%
Workshopy	14	28,0%
Papírová podoba	11	22,0%
Školení zaměstnavatelem (vedoucím)	14	28,0%
Školení externí osobou	18	36,0%
Neúčastním se	4	8,0%
Jiná	2	4,0%



Obrázek 10 - Typy školení preferované zaměstnanci

9.5 Plánovaný obsah

Specifikování obsahu školení je klíčové pro zajištění toho, aby školení poskytovalo komplexní a vyvážené pokrytí témat souvisejících s kybernetickou bezpečností. Obsah by měl zahrnovat jak teoretické základy, tak praktické dovednosti potřebné pro ochranu digitálních systémů a dat. Teoretické prvky poskytují účastníkům základní povědomí o kybernetických hrozbách a strategiích obrany, zatímco praktické prvky umožňují účastníkům procvičit své dovednosti a aplikovat je v reálném prostředí.

Obsah školení by mohl zahrnovat témata jako:

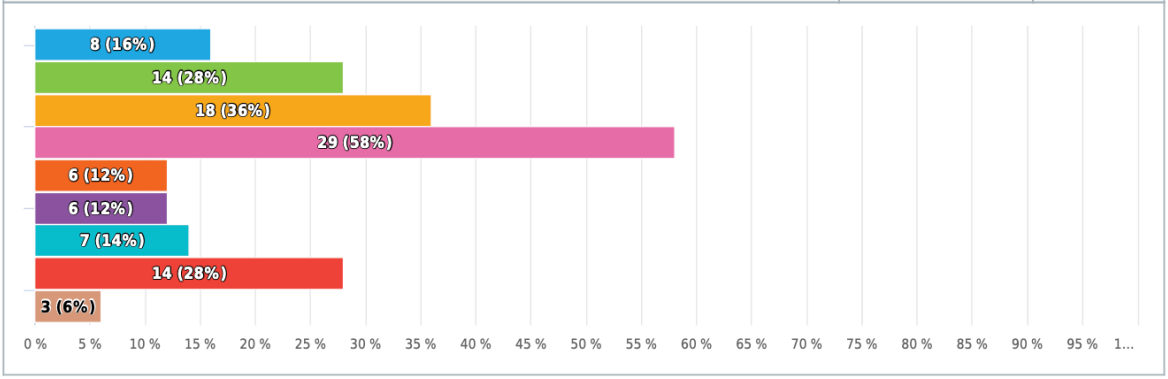
- Identifikace různých typů kybernetických hrozeb a útoků
- Bezpečnostní politiky a postupy v organizaci
- Bezpečnostní technologie a nástroje, včetně firewall, antivirové ochrany a šifrování
- Řízení incidentů a postupy pro reakci na kybernetické útoky

- Bezpečnostní aspekty práce s cloudovými technologiemi a mobilními zařízeními
- Zabezpečení síťového prostředí a endpointů
- Sociální inženýrství a ochrana před phishingovými útoky
- Zálohování dat a obnovení služeb po útoku

V souladu s navrženým obsahem by mělo být školení strukturováno tak, aby poskytovalo vyváženou kombinaci teoretických prezentací, praktických cvičení, diskusí a případových studií. To umožní účastníkům získat nejen teoretické znalosti, ale také praktické dovednosti a zkušenosti potřebné k úspěšné ochraně organizace před kybernetickými hrozbami.

Zde můžeme podle ankety vidět, které hrozby jsou v organizacích nejaktuálnější:

Možnosti odpovědí	Responzí	Podíl
Ochrana před malwarovými útoky	8	16,0%
Firewally a síťová bezpečnost	14	28,0%
Školení zaměstnanců v kybernetické bezpečnosti	18	36,0%
Správa hesel a autentizace	29	58,0%
Incidentní reakce a rekonstrukce	6	12,0%
Kybernetické hrozby IoT (Internet of Things)	6	12,0%
Bezpečnostní analýza a monitorování	7	14,0%
Šifrování a bezpečnost dat	14	28,0%
Vlastní odpověď	3	6,0%



Obrázek 11 - Aktuální témata kybernetické bezpečnosti

9.6 Výběr dodavatele

Prozkoumání možností externích dodavatelů školení a interních odborníků je klíčové pro zajištění kvalitního a relevantního školení o kybernetické bezpečnosti. Externí dodavatelé mohou poskytnout odborní znalosti a perspektivu zvenčí, zatímco interní odborníci

mohou mít hlubší porozumění specifickým potřebám a procesům organizace. Zde jsou některé faktory, které je třeba zvážit při výběru externích dodavatelů nebo interních odborníků.

Nutno je především zajistit, že externí dodavatelé nebo interní odborníci mají dostatečné znalosti a zkušenosti v oblasti kybernetické bezpečnosti. Měli by mít certifikace a referenční případy úspěšných školení v této oblasti.

Dále zvažte, zda externí dodavatelé nebo interní odborníci mají specializaci v konkrétních oblastech kybernetické bezpečnosti, které jsou relevantní pro vaši organizaci. To může zahrnovat síťovou bezpečnost, bezpečnost endpointů, správu identit, ochranu před ransomwarem atd.

Zohlednění potřeby a preference vaší organizace ohledně formátu a časování školení. Externí dodavatelé by měli být schopni nabídnout školení v souladu s vašimi požadavky a případně je přizpůsobit specifickým potřebám.

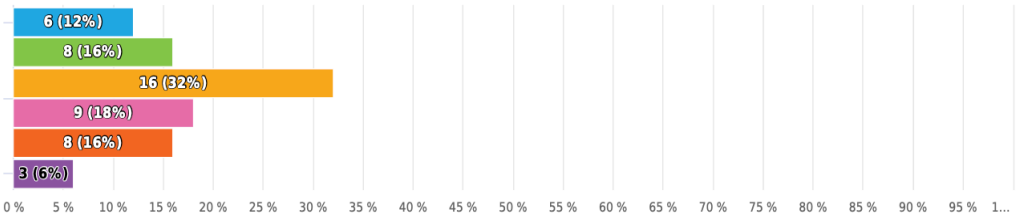
Zkoumání kvality materiálů a obsahu školení poskytovaných externími dodavateli nebo interními odborníky. Měli by být aktualizovaní v souladu s nejnovějšími trendy a technologiemi v oblasti kybernetické bezpečnosti. Dále by měli být schopni poskytnout pozitivní zpětnou vazbu a podporu po ukončení školení.

Porovnání nákladů spojené s externími dodavateli školení a interními odborníky a zvažte, která možnost je pro vaši organizaci nejvíce ekonomická a efektivní.

Prozkoumání těchto faktorů a porovnání možností externích dodavatelů školení a interních odborníků vám pomůže vybrat tu nejlepší možnost pro vaši organizaci a dosáhnout maximálního prospěchu z školení o kybernetické bezpečnosti.

V anketě respondenti byli dotázány, aby ohodnotili aktuální stav kvality školení v rámci kybernetické bezpečnosti ve své organizaci na škále jedna až pět, kdy jedna je nejhorší hodnocení a pět nejlepší. Zde, můžeme vidět, že většina odpovědí zaujímá hodnocení číslem tři, z čehož plyne, že prostor pro zlepšení školení kybernetické bezpečnosti je poměrně značný.

Možnosti odpovědí	Responzí	Podíl
1	6	12,0%
2	8	16,0%
3	16	32,0%
4	9	18,0%
5	8	16,0%
Neúčastním se	3	6,0%



Obrázek 12 - Hodnocení kvality školení

9.7 Plánování rozvrhu

Stanovení data a délky školení je důležité pro efektivní plánování a organizaci školení o kybernetické bezpečnosti. To může být provedeno buď jako jednorázová událost nebo sérii školení rozložených v čase, v závislosti na potřebách a preferencích organizace. Zde jsou některé faktory, které je třeba zvážit při stanovení data a délky školení.

- Délka školení

Zohlednění a komplexita obsahu školení a dostupnost zaměstnanců. Kratší školení může být vhodné pro základní koncepty, zatímco rozsáhlejší školení může být nezbytné pro pokročilé dovednosti a strategie.

- Frekvence školení

Je třeba rozhodnout, zda bude školení provedeno jako jednorázová událost nebo jako série školení rozložených v čase. Rozložení školení do série může umožnit lepší absorpci informací a průběžné zlepšování dovedností.

- Dostupnost zaměstnanců

Zvážení pracovních harmonogramů a povinností zaměstnanců při stanovování data školení. Vyberte čas, který minimalizuje rušení pracovního procesu, a zaručuje maximální účast zaměstnanců.

- Příprava a logistika

Zabezpečení potřebných zdrojů, místnost, technické vybavení a materiály před datem školení. Ujistěte se, že všichni účastníci mají přístup k potřebným informacím a že jsou informováni o čase a místě konání školení.

- Evaluace a zpětná vazba

Zahrnutí času pro evaluaci a zpětnou vazbu od účastníků do plánu školení. To umožní identifikovat příležitosti k vylepšení školení a zlepšit jeho účinnost v budoucnu.

Stanovení data a délky školení by mělo být provedeno s ohledem na tyto faktory a potřeby organizace. Cílem je zajistit, aby školení bylo efektivní, dobře organizované a přizpůsobené potřebám účastníků.

9.8 Komunikace a propagace

Informování zaměstnanců o školení o kybernetické bezpečnosti a zdůraznění jeho důležitosti je klíčové pro zajištění maximální účasti a zapojení. Toho lze dosáhnout prostřednictvím různých interních komunikačních kanálů a propagace v rámci firmy. Zde jsou některé způsoby, jak efektivně informovat zaměstnance.

Poslat emailovou zprávu všem zaměstnancům s informacemi o školení, jeho datu, čase a důležitosti účasti. Zdůraznění, proč je kybernetická bezpečnost důležitá pro každého zaměstnance a jaké jsou očekávané výstupy školení.

Účinnou formou komunikace také může být pozvánka od vedoucích pracovníků, aby osobně oslovili své podřízené a zdůraznili důležitost účasti na školení o kybernetické bezpečnosti. Osobní doporučení může mít silnější dopad než hromadné komunikace.

Využití pravidelných pracovních schůzek a týmových setkání k přímému oslovení zaměstnanců a sdělení důležitosti školení o kybernetické bezpečnosti.

Důležité je zajistit, aby informace o školení byly dostatečně dostupné a srozumitelné pro všechny zaměstnance a aby byla zdůrazněna jejich role a zodpovědnost při ochraně kybernetické bezpečnosti v rámci organizace.

9.9 Implementace školení

Zabezpečení dostupnosti prostředků a zařízení potřebných pro školení, zajištění účasti zaměstnanců a správné provedení samotného školení jsou klíčové krok pro úspěšné školení o kybernetické bezpečnosti.

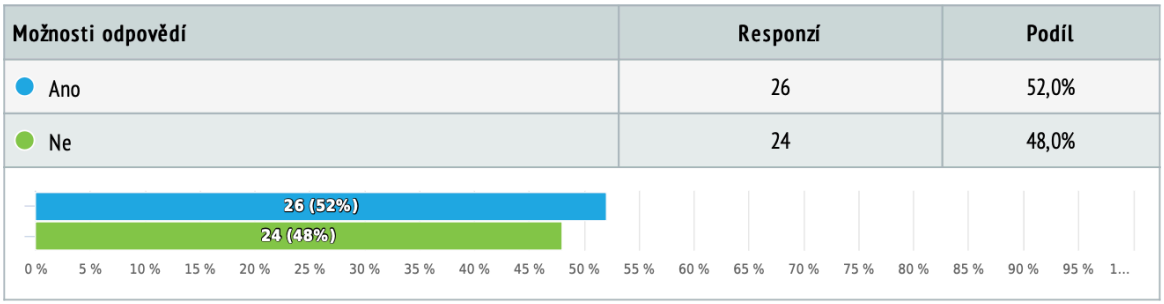
Důkladně zabezpečené školení s dostatečnou účastí zaměstnanců a správně provedeným průběhem má zásadní význam pro úspěšnou implementaci a dodržování bezpečnostních opatření v oblasti kybernetické bezpečnosti v organizaci.

9.10 Evaluace a zpětná vazba

Zhodnocení úspěšnosti školení o kybernetické bezpečnosti je klíčové pro posouzení jeho účinnosti a identifikaci oblastí potřebujících zlepšení. K dosažení tohoto cíle lze použít několik metod jakou jsou například:

- Hodnocení účastníků
- Sledování změn v povědomí o kybernetické bezpečnosti
- Analýza případných incidentů
- Průběžná evaluace
- Zapojení manažerského týmu

Kombinace těchto metod vám poskytne komplexní pohled na účinnost školení o kybernetické bezpečnosti a umožní vám přijmout opatření ke zlepšení, pokud je to potřeba. Tento průběžný proces zhodnocování a zlepšování je klíčový pro udržení vysoké úrovně kybernetické bezpečnosti v organizaci v dlouhodobém horizontu.



Obrázek 13 - Efektivita školení

Zde byli respondenti dotazováni, zde školení je pro ně efektivní či nikoli, vidíme, že většina odpověděla kladně, avšak výsledky jsou poměrně vyrovnané. Tudíž z toho můžeme usoudit, že efektivita školení je něco na čem by mohli organizace zapracovat.

10 NÁVRH ŠKOLENÍ O KYBERNETICKÉ BEZPEČNOSTI

Návrh tohoto školení je klíčovým momentem na zvýšení úrovně ochrany citlivých informací a systémů v rámci organizace. Cílem tohoto školení je vybavit zaměstnance potřebnými znalostmi a dovednostmi, které jim umožní rozpoznat a efektivně reagovat na kybernetické hrozby. Důraz bude kladen především na vytvoření kultury bezpečného chování a povědomí, která je nezbytná pro udržení vysoké úrovně ochrany v dynamickém a neustále se měnícím digitálním prostředí. Školení bude určeno především pro vedoucí pracovníky organizace, kteří povědomí o kybernetické bezpečnosti mohli šířit mezi své podřízené.

10.1 Zásady pro sestavení školení

Sestavení efektivního školení vyžaduje pečlivé plánování a zaměření na několik klíčových oblastí. Nejprve je nutné stanovit jasné cíle školení a identifikovat potřeby účastníků. Obsah školení by měl být rozdělen do logických bloků a doplněn o příslušné materiály, jako jsou prezentace. Důležitý je výběr metod výuky, které by měly zahrnovat interaktivní aktivity a využití moderních technologií. Lektor musí být dobře připravený a obeznámený s obsahem, stejně jako mít silné komunikační dovednosti. Organizačně je třeba zajistit vhodné místo, technické vybavení a harmonogram školení. Během školení je klíčové podporovat aktivní účast a poskytovat průběžné i závěrečné hodnocení. Získaná zpětná vazba by měla být využita k dalšímu zlepšení školení.

10.2 Vizuál a nosič školení

Jelikož se jedná o výukový materiál, který pod vedením kvalifikovaného školitele bude přednášen pro pracovníky, zvolila jsem si formu prezentace, jelikož je to nejznámější nositel školících materiálů, je dostupný volně pro jakoukoli firmu, dá se přenášet i jako formát PDF, čímž je použitelný dalo by se říct na jakémkoli počítači ve firmě i za předpokladu, že firma nemá placenou verzi balíčku Microsoft Office nebo jakoukoli jinou i neplacenou formu aplikace pro zobrazení prezentací.

Zvolila jsem tedy online stránku canva.com, kde je velmi hezký a profesionální výběr šablon pro prezentace, zároveň export z téhle stránky je možný jak ve formátu pro Microsoft PowerPoint, tak i jak jsem výše zmiňovala, je zde i možnost exportu ve formátu PDF tudíž je pro mnou potřebu ideálním kandidátem.

Ze školení by si účastník měl odnést nové poznatky o pojmu kybernetické bezpečnosti, potřebné informace pro zajištění kybernetické bezpečnosti jak ve firmě, kde je školení prováděno, ale i ve svém osobním životě, jakožto uživatele internetu.

10.3 Cíle školení

Hlavním, ne však jediným cílem tohoto školení kybernetické bezpečnosti ve firmách, je zvýšení povědomí o kybernetických hrozbách nejen ve firemním prostředí, ale i v životě mimo pracovní dobu a prostředí. Jelikož jsme uživateli internetu, různých aplikací, stránek a celkově online prostředí dalo by se říct na denní bázi, čelíme kybernetickým hrozbám na skoro každém kroku. Očekáváným výstupem školení je, že účastník školení ze školení odejde s těmito vědomostmi:

- Identifikace kybernetických hrozeb
- Pochopení základních bezpečnostních postupů
- Pochopení důsledků kybernetických útoků
- Praktické dovednosti v oblasti detekce a reakce
- Ochrana osobních údajů
- Zlepšení povědomí o sociálním inženýrství
- Zlepšení povědomí o právních aspektech

10.4 Školitel

Školitel/lektor by měl být osoba, která nemá problém s komunikací s neznámou skupinou lidí. Měl by být znalý problematiky kybernetické bezpečnosti na vyšší úrovni, než jsou školené subjekty. Lektorem tohoto školení může býti osoba se zkušenostmi jak z praxe, tak z vlastního spektra jinak řečeno samoukem, avšak v tomto případě, by měla školící osoba tohle řešit s nadřízeným neboli vedoucím firmy nebo kolektivu, který je školen.

Pokud by byl lektor znalý v cizích jazycích minimálně tedy v jazyce anglickém bylo by to jedině výhodou, jelikož by školení poté mohlo býti provázeni v jiném jazyce pro širší spektrum posluchačů. Výklad by měl býti pro posluchače zajímavý, měl by přitáhnout jejich pozornost, aby si ji udrželi během celého školení, měl by aktivně účastníky zapojovat do školení, aby se dozvěděl jejich postoj k věci nebo jejich osobní zkušenosti v daném tématu. Lektor by měl být seznámen velmi důkladně s obsahem školení i s jeho průběhem, avšak pokud by byl schopen improvizace nebylo by tomu na škodu, jelikož osobní zkušenosti jsou poutavější částí jakéhokoli školení.

10.5 Subjekty školení

Školení je zaměřen především na vzájemné porozumění, tudíž v případě jakékoli nejasnosti je kladen důraz na komunikace se školitelem. V návaznosti na tento cíl školení je důležité školení nepřehltit, tedy každé školení by mělo býti pro maximálně 10 osob zároveň. Školení je cíleno spíše obecněji tudíž koncovým cílem školení je považován spíše zaměstnanec vyšší pozice, který nabyté vědomosti může předat svému týmu, popřípadě svým podřízeným. Věkové omezení pro školení není žádné. Školení je vedeno v českém jazyce.

10.6 Zásady pro sestavení školení

Rozdílné typy firem vyžadují odlišné přístupy k tvorbě školení. Proto tohle školení bylo vytvořeno s ohledem na konkrétní potřeby daného prostředí a zaměřuje se na posílení schopnosti zaměstnanců rozpoznat a reagovat na bezpečnostní hrozby specifické pro jejich pracovní prostředí.

10.7 Grafická stránka školení

Práce s grafikou při tvorbě jakéhokoli školení je důležitým prvkem pro vytvoření efektivních a přitažlivých vzdělávacích materiálů. Použity by měly být jasné a srozumitelné grafické prvky, čímž jsou myšleny například obrázky a grafy, které slouží pro vizualizaci složitých konceptů a usnadnění zapamatování informací. Ilustrativní příklady a scénáře, zasazené do grafických prvků, umožňují účastníkům lépe si představit reálné situace a jejich důsledky. Stejně jako důsledky nevhodného chování. Důležité je zaměřit se na důležité body školení a přizpůsobit grafiku specifickým potřebám a pracovnímu prostředí účastníků. Data obsažena na jednotlivých slidech by měla být napsána výstižně, formou odrážek nikoli jako souvislý dlouhý a nepřehledný text. Zároveň by velikost písma textu v prezentaci měla odpovídat možnosti prezentování ve vyšším rozlišení nebo možné místnosti, kde prezentace by mohla být prezentována.

11 NÁPLŇ ŠKOLENÍ

Školení bylo rozděleno na osm kategorií, které jsou následně více rozebrány na následujících slidech. V seznamu příloh můžeme najít prezentaci (Příloha č. 3) a dokument (Příloha č. 2) který slouží jako podpůrný materiál pro školitele. Školení může školitel obohatit o své poznatky nebo své zkušenosti. Cílem tohoto školení je předat důležité informace subjektům školení tak, aby si na konci školení odnesli komplexní a nejideálněji o něco rozšířený pohled na oblast kybernetické bezpečnosti ve firmě, jak předcházet určitým kybernetickým rizikům a vylepšit politiku kybernetické bezpečnosti ve firmě na vyšší úroveň.

Prezentace je rozdělena na základ a tři možné diverzifikace firemního prostředí, jelikož různá prostředí mají specifické požadavky, co se týče kybernetické bezpečnosti.

11.1 Kategorie „Úvod do kybernetické bezpečnosti“

V první části školení je klíčové seznámení účastníků s obecným konceptem kybernetické bezpečnosti. Proto je na prvním slidu představena definice pojmu kybernetické bezpečnosti, aby účastníci měli jasnou představu o tom, co je v této oblasti zahrnuto a zároveň aby věděli jaký je význam kybernetické bezpečnosti v dnešním digitálním prostředí. Následující slide je věnován důležitosti implementace kybernetických bezpečnostních opatření a jejím dopadu na ochranu firemních aktiv a zajištění kontinuity provozu.

Dále je v prezentaci věnována část aktuálním hrozbám a trendům v oblasti kybernetické bezpečnosti. Účastníky je zde cílem informovat o nejnovějších technikách a útocích používaných kybernetickými útočníky a o tom, jakým způsobem se tyto hrozby mohou projevit v jejich pracovním prostředím.

V závěrečné části první kapitoly se zabývá právním rámcem problematiky kybernetické bezpečnosti v České republice. Jsou zde velmi přehledně uvedeny klíčové body právního aspektu kybernetické bezpečnosti. Tato část je klíčová pro porozumění právního kontextu a zajištění dodržování příslušných legislativních prostředků.

11.2 Kategorie „Bezpečnostní povědomí“

Tato část školení je zaměřena na seznámení účastníků s reálnými hrozbami, jednotlivé hrozby jim budou postupně představeny současně s jejich charakteristikou. Účastníci budou podrobně seznámeni s metodami, které jsou využívaný útočníky za cílem proniknout do

systémů, jedná se o útoky, které byly zmíněny v teoretické části této bakalářské práce již dříve. Důraz je zde kladen na identifikaci hlavních znaků těchto útoků a možnosti jejich prevence.

Na druhém slidu jsou účastníci seznámeni s konkrétními případy a zkušenostmi z praxe, kdy byla firma vystavena zmíněným kybernetickým útokům. Prostřednictvím praktických poznatků a zkušeností budou tyto hrozby představeny účastníkům spolu s jejich efektivním řešením. Tato část bude především zaměřena na aplikace praktických a teoretických znalostí a poskytne účastníkům cenné informace pro identifikaci a zvládání kybernetických hrozeb.

11.3 Kategorie „Bezpečnostní politiky a postupy“

V rámci podkategorie vytvoření a implementace bezpečnostních politik, zde je zmíněno několik nejdůležitějších bodů, které jsou následně rozebrány jeden po druhém, aby účastníci školení měli lepší přehled, jak docílit bezpečných podmínek ve firmě v oblasti kybernetické bezpečnosti.

Dalším důležitým tématem prezentace je rozvoj bezpečnostní kultury v organizaci, kde je poukázáno na klíčové body, které je potřeba dodržovat, aby bylo dosaženo správného dodržování bezpečnostních politik v organizaci, které jsme si zmínili v předchozím slidu. To zahrnuje:

- Vedení odshora
- Školení a osvěta
- Jasná komunikace
- Odpovědnost
- Motivace
- Příklady z praxe
- Pravidelné revize a zpětná vazba
- Zapojení všech zaměstnanců

Všechny body jsou vysvětleny v pomocné osnově prezentace, kterou můžeme najit jako přílohu (Příloha č.2). Poslední slide této kategorie je věnován odpovědnosti zaměstnanců v kybernetickém bezpečnosti, kde cílem účastníky seznámit s čím jsou zaměstnanci organizace zavázání, pokud se jedná o dodržování postupů bezpečnostní politiky v oblasti kybernetické bezpečnosti ve firmě. Každý zaměstnanec by měl být informován o svých

povinnostech a odpovědnostech v této oblasti a měl by být aktivně zapojen, pokud je bavíme o ochraně před kybernetickými hrozbami a útoky.

11.4 Kategorie „Bezpečnostní technologie a nástroje“

Tato kategorie se dělí do dvou podkategorií a síťová a endpointová bezpečnost.

V podkategorii síťové bezpečnosti je rozvedeno, jaké prvky bezpečnosti by měly býti použity v organizaci pro zajištění kybernetické bezpečnosti a omezení kybernetických hrozeb na minimum. Účastníci jsou seznámení s různými technologiemi a postupy, které mohou být implementovány pro ochranu sítě a infrastruktury organizace před útoky, jakou jsou firewall, rozšířená reakce a detekce, Security Information and Event Management, virtuální privátní sítě nebo segmentace sítě.

Druhou podkategorií je endpointová bezpečnost, ve které jsou účastníci seznámeni s metodami ochrany koncových zařízení před kybernetickými hrozbami. To zahrnuje instalaci antivirových softwarů, firewallů a dalších softwarových nástrojů na koncových zařízeních jako jsou počítače, mobilní telefony a tablety. Účastníci jsou informováni o důležitosti ochrany koncových zařízení.

11.5 Kategorie „Řízení incidentů a reakce na útoky“

Tato kategorie se věnuje řízení incidentů a reakci na kybernetické útoky, ačkoliv velmi stručně. Je zde zdůrazněna důležitost reportování kybernetických incidentů jak interně, tak externě. Účastníci jsou povzbuzeni k aktivnímu hlášení všech podezřelých aktivit a incidentů, aby mohly být rychle identifikovány a řešeny.

Kromě toho jsou prezentovány příklady reakcí na kybernetické incidenty, které jsou používány na základě útoku, který byl použit na strukturu organizace. Tyto příklady jsou zde uvedeny jako inspirace pro účastníky, aby byli lépe připraveni na potencionální kybernetické hrozby a mohli rychle a efektivně reagovat v. případě potřeby.

11.6 Kategorie „Praktické cvičení“

V této kategorii je zdůrazněna důležitost praktického testování zaměstnanců organizace a jejich znalostí v oblasti kybernetické bezpečnosti. Účastníci jsou seznámeni s cíli takovýchto cvičení a jejich postupem.

Cílem praktických testů zaměstnanců organizace je ověřit jejich schopnost rozpoznat a reagovat na různé kybernetické hrozby a útoky v reálném prostředí.

Praktická testování zaměstnanců organizace jsou klíčovým prvkem celkového bezpečnostního programu a pomáhají zvýšit úroveň bezpečností organizace tím, že posilují povědomí zaměstnanců o kybernetických hrozbách a připravují je na adekvátní reakci v případě útoku.

11.7 Kategorie „Aktualizace a udržování dovedností“

Poslední kategorie zastoupená na jednom z posledních slidů, obsahuje tři klíčové body: školení zaměstnanců, aktualizace bezpečnostních postupů a podpora motivace zaměstnanců.

Prvním bodem je školení zaměstnanců, což je opravdu jeden z hlavních a základních kroků pro zajištění efektivní ochrany proti kybernetickým hrozbám. Pravidelné a komplexní školení zaměstnanců umožňuje nejen zlepšení jejich povědomí o kybernetických hrozbách.

Druhým bodem je aktualizace bezpečnostních postupů, což je také nezbytným procesem v rámci neustále měnícího se kybernetického prostředí. Pravidelná aktualizace bezpečnostních politik a postupů v organizacích je nutná vzhledem k zajištění účinné ochrany svých aktiv a dat.

Posledním bodem je podpora a motivace zaměstnanců, což hraje klíčovou roli v úspěšné implementaci bezpečnostních opatření. Každá organizace by měla nejen podporovat, ale i motivovat své zaměstnance k dodržování bezpečnostních postupů a politik

11.8 Diverzifikace prostředí pro školení

V prezentaci nalezneme tři možnosti pro různá firemní prostředí, kde by školení mohlo probíhat. Každé prostředí má totiž různé požadavky a nároky na školení. Vybrala jsem si tři typy firemního prostředí, které jsou v dnešní době nejvíce rozšířené a vypracovala jsem verzi školení i pro ně. Jedná se o tyto prostředí:

- Výrobní prostředí
- Mediální domy
- IT firmy s citlivými daty

11.9 Diverzifikace pro výrobní prostředí

Kybernetická bezpečnost ve výrobní prostředí je kritická pro zajištění kontinuity výroby, ochranu duševního vlastnictví a předcházení finančním ztrátám. Vzhledem k rostoucí digitalizaci a propojení průmyslových systémů s internetem se výrobní prostředí stává zranitelnějším a atraktivním cílem pro kybernetické útočníky. Výrobní prostředí se potýká s hrozbami jako jsou průmyslová špionáž, sabotáž, ransomware útoky. Tyto hrozby mohou mít pro infrastrukturu společnosti zdrcující důsledky, pokud by došlo k bezpečnostním incidentům. Proto implementování komplexních opatření je považováno za nezbytné pro síťová oddělení, zálohování a aktualizace průmyslových systémů a použití specializovaných technologií. Důležitým faktorem je i investice do vzdělání zaměstnanců a vytváření bezpečnostní kultury, která posiluje vědomi o kybernetických hrozbách.

11.10 Diverzifikace pro mediální domy

Pokud se nacházíme v prostředí mediálních domů, tak klíčovými faktory kybernetické bezpečnosti je ochrana citlivých informací, obsahu a provozních procesů proti hrozbám a útokům. Mediální domy čelí různorodým bezpečnostním výzvám, včetně úniku dat, sabotáží, dezinformační kampaní a útoků na webové platformy. Jelikož média jsou v dnešní době již převážně digitalizována je mediální prostředí náchylnější na kybernetické útoky, což může ohrozit jak důvěryhodnost, tak i reputaci těchto domů.

Aby kybernetická odolnost v mediálních domech byl zvýšena, je kladen důraz na implementaci bezpečnostních opatření jako je šifrování dat, dvoufaktorová autentizace, pravidelné zálohování obsahu, monitoring sítě a ochrana před phishingem. Důležitost je také přikládána pro vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti, včetně rozpoznání možných hrozeb a zacházení s citlivými informacemi. Aktuálnost softwaru a bezpečnostních politik může mnohdy sehrát důležitý faktor.

11.11 Diverzifikace pro IT firmy s citlivými daty

Pokud se bavíme o kybernetické bezpečnosti v IT firmách jedná se o naprosto zásadní faktor pro ochranu před různorodými kybernetickými hrozbami a útoky. Tyto firmy často zpracovávají, přenášejí nebo ukládají informace, jako jsou osobní údaje, finanční data, zdravotní záznamy nebo duševní vlastnictví, což je staví do pozice přímo ideální pro terč kybernetický útoků.

Aby v těchto organizacích byla zajištěna adekvátní ochrana citlivých dat je nutné implementovat opravdu robustní bezpečnostní opatření. Mezi tyto opatření můžeme zahrnout šifrování dat, pravidelné zálohy a obnovu dat a využívání bezpečnostních technologií jako jsou firewally a antivirové programy. Kromě technologických opatření je podstatné provádění pravidelných bezpečnostních auditů a zátěžových testů, pro identifikování možných slabin v bezpečnostní infrastruktuře.

ZÁVĚR

Kybernetická bezpečnost je v dnešní době nezbytnou součástí provozu každé firmy. Prozkoumali jsme aktuální stav kybernetického zabezpečení ve firmách a identifikovali nejčastější hrozby a slabiny. Z analýzy vyplývá, že firmy čelí různým typům kybernetických útoků, včetně phishingu, ransomwaru a úniku dat, přičemž nedostatečné povědomí a nedostatečně zabezpečené systémy patří mezi hlavní slabiny.

Dále byly analyzovány dostupné metody a formy školení kybernetické bezpečnosti. Bylo zjištěno, že školení může zahrnovat prezentace, interaktivní semináře, online kurzy a praktická cvičení, přičemž kombinace těchto metod může být nejefektivnější.

Vliv legislativních požadavků a regulací týkajících se kybernetické bezpečnosti pro školení ve firmách je významný. Zákonodárný rámec často stanovuje povinnosti pro firmy v oblasti školení zaměstnanců a ochrany dat, což může mít vliv na strategii školení.

Byla posouzena efektivita různých metod školení a jejich vliv na školené pracovníky. Dále bylo zjištěno, že interaktivní a praktické přístupy často vedou k lepší absorpci informací a zlepšení dovedností zaměstnanců.

Na základě těchto analýz bylo navrženo efektivní školení o kybernetické bezpečnosti pro firmy, které bude zahrnovat kombinaci různých metod a důraz na praktické cvičení.

Implementace takového školení by měla pomoci firmám zvýšit povědomí o kybernetických hrozbách, zdokonalit dovednosti v reakci na útoky a posílit celkovou bezpečnostní kulturu v organizaci.

SEZNAM POUŽITÉ LITERATURY

[1] HRŮZA, Petr, 2024. Kybernetická bezpečnost. In: *Kybernetická bezpečnost* [online]. s. 1-59 [cit. 2024-05-21]. ISBN 978-80-7231-914-5. Dostupné z: https://vlada.gov.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/

[2] Kybernetická bezpečnost, 2021. *Vláda České republiky*[online]. [cit. 2024-05-21]. Dostupné z: https://vlada.gov.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/

[3] BC. ŠERÁKOVÁ, Kristýna, 2023. Kybernetická bezpečnost a její význam pro společnost. Brno. Diplomová práce. AMBIS vysoká škola a.s.

[4] Legislativa KB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2024-05-21]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[5] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, 2024. *Příručka pro personální agendu a odměňování zaměstnanců* [online]. [cit. 2024-05-21]. Dostupné z: https://ppropo.mpsv.cz/zakon_412_2005

[6] Zákon č. 110/2019 Sb., 2024. *Zákony pro lidi* [online]. [cit. 2024-05-21]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110

[7] Vyhláška č. 82/2018 Sb., 2024. *Zákony pro lidi* [online]. [cit. 2024-05-21]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

[8] Vyhláška č. 317/2014 Sb., 2024. *Zákony pro lidi*[online]. [cit. 2024-05-21]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-317

[9] FIALKOVÁ, Karin, 2023. Kybernetická bezpečnost subjektu. Uherské Hradiště. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

[10] HROMKOVÁ, Ludmila a Zuzana TUČKOVÁ. Reengineering podnikových procesů. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2008. 139 s. ISBN 978-80-7318-759-0

[11] ČSN EN ISO/IEC 27000 (369790) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník, 2024. *Technické*

normy ČSN [online]. [cit. 2024-05-21]. Dostupné z: https://www.technicke-normy-csn.cz/csn-en-iso-iec-27000-369790-199764.html

[12] ČSN EN ISO/IEC 27001 (369797) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti – Požadavky, 2024. *Technické normy ČSN* [online]. [cit. 2024-05-21]. Dostupné z: https://www.technicke-normy-csn.cz/csn-en-iso-iec-27001-369797-250275.html

[13] ČSN EN ISO/IEC 27002 (369798) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti, 2024. *Technické normy ČSN* [online]. [cit. 2024-05-21]. Dostupné z: https://www.technicke-normy-csn.cz/csn-en-iso-iec-27002-369798-249194.html

[14] ČSN ISO/IEC 27003 (369790) Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací, 2024. *Technické normy ČSN* [online]. [cit. 2024-05-21]. Dostupné z: https://www.technicke-normy-csn.cz/csn-iso-iec-27003-369790-199773.html

[15] ČSN ISO/IEC 27004 (369790) Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Monitorování, měření, analýza a hodnocení, 2024. *Technické normy ČSN* [online]. [cit. 2024-05-21]. Dostupné z: https://www.technicke-normy-csn.cz/csn-iso-iec-27004-369790-199776.html

[16] ČSN EN ISO/IEC 27006 (369790) Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací, 2024. *Technické normy ČSN* [online]. [cit. 2024-05-21]. Dostupné z: https://www.technicke-normy-csn.cz/csn-en-iso-iec-27006-369790-199765.html

[17] ČSN EN ISO/IEC 27007 (369790) Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí - Směrnice pro audit systémů řízení bezpečnosti informací, 2024. *Technické normy ČSN* [online]. [cit. 2024-05-21]. Dostupné z: https://www.technicke-normy-csn.cz/csn-en-iso-iec-27007-369790-199786.html

[18] ČSN ISO/IEC 27033-1 (369701) Informační technologie - Bezpečnostní techniky - Bezpečnost sítě - Část 1: Přehled a pojmy, 2024. *Technické normy ČSN* [online].

[cit. 2024-05-21]. Dostupné z: https://www.technicke-normy-csn.cz/csn-iso-iec-27033-1-369701-199502.html

[19] Co je kybernetický útok? 2024. *Microsoft* [online]. [cit. 2024-05-21]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-a-cyberattack

[20] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 9788073807375.

[21] KOLOUCH, Jan. *Kybernetické útoky* [online]. [cit. 2024-05-21]. Dostupné z: https://csirt.cesnet.cz/_media/cs/documents/kyberneticke_utoky.pdf

[22] CYBERTHREAT Real-time map, 2024. In: *Kaspersky*[online]. [cit. 2024-05-21]. Dostupné z: https://cybermap.kaspersky.com

[23] Falešná komunikace přes SMS, e-maily a chatování na internetu, 2024. *Česká spořitelna* [online]. [cit. 2024-05-21]. Dostupné z: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/phishing

[24] Úvod - Co je SPAM a jak se mu bránit, 2024. *Univerzita Karlova* [online]. [cit. 2024-05-21]. Dostupné z: https://uvt1.cuni.cz/email/spam/uvod.html

[25] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Ochrana osobních údajů [online]. Dostupné z: https://uoou.gov.cz/cinnost/ochrana-osobnich-udaju

[26] KPBO. Bezpečnost v online prostředí [online]. 2023. Dostupné z: https://www.kpbo.cz/wp-content/dokumenty/prilohy/bezpecnost_v_online_prostredi.pdf

[27] Varování: Podvodné zprávy žádají zaplacení pohledávek, 2024. *MUNI - CSIRT MU* [online]. [cit. 2024-05-21]. Dostupné z: https://csirt.muni.cz/varovani/varovani-podvodne-zpravy-zadaji-zaplaceni-pohledavek

[28] Schreier, J. Kybernetické útoky a jejich detekce. 2020. Dostupné z: https://is.slu.cz/th/rc929/FPF_bakalarska_2020_Kybernetickeutokyajejichdetekce_SchreierJan.pdf

[29] RANSOMWARE CRYPTOLOCKER STÁLE ÚTOČÍ, 2024. EABM [online]. [cit. 2024-05-22]. Dostupné z: https://eabm.cz/1288-ransomware-cryptolocker-stale-utoci

[30] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Brno: Computer Press, c2007. ISBN 9788025115114.

[31] *Zajištění kybernetické bezpečnosti ve středně velké společnosti.* Praha, 2021. Diplomová práce. Vysoká škola finanční a správní

[32] What Is a Firewall?, 2020. *Cisco* [online]. [cit. 2024-05-22]. Dostupné z: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

[33] Top 3 Best Practices of Data Classification to Boost Your Organization's Security, 2024. Seclore [online]. [cit. 2024-05-22]. Dostupné z: https://www.seclore.com/blog/top-3-best-practices-of-data-classification-to-boost-your-organizations-security/

[34] 10 Best Practices for Secure Data Transfers, 2024. Ifax [online]. [cit. 2024-05-22]. Dostupné z: https://www.ifaxapp.com/blog/secure-data-transfer/

[35] Data backup and recovery best practices for the manufacturing industry, 2024. Acronis[online]. [cit. 2024-05-22]. Dostupné z: https://www.acronis.com/en-us/blog/posts/data-backup-and-recovery-best-practices-for-the-manufacturing-industry/

[36] What is Role-Based Access Control (RBAC)? Examples, Benefits, and More, 2024. *Digital Gueardian* [online]. [cit. 2024-05-22]. Dostupné z: https://www.digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more

[37] Principle of Least Privilege, 2024. *Techopedia* [online]. [cit. 2024-05-22]. Dostupné z: https://www.techopedia.com/definition/13676/principle-of-least-privilege-polp

[38] Password management best practices, 2024. *SailPoint* [online]. [cit. 2024-05-22]. Dostupné z: https://www.sailpoint.com/identity-library/password-management-best-practices/

[39] What is an Intrusion Detection System?, 2024. *Barracuda* [online]. [cit. 2024-05-22]. Dostupné z: https://www.barracuda.com/support/glossary/intrusion-detection-system

[40] What is SIEM?, 2024. *Microsoft* [online]. [cit. 2024-05-22]. Dostupné z: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

[41] Ensuring Data Security in Retail ERP, 2024. *Cybersecurity Insider* [online]. [cit. 2024-05-22]. Dostupné z: https://www.cybersecurity-insiders.com/ensuring-data-security-in-retail-erp/

[42] The Importance of Cybersecurity Training, 2024. *United States Cybersecurity Magazine* [online]. [cit. 2024-05-22]. Dostupné z: https://www.uscybersecurity.net/cybersecurity-training-important/

[43] 10 critical steps to help protect yourself online, 2024. *Norton* [online]. [cit. 2024-05-22]. Dostupné z: https://us.norton.com/blog/how-to/5-ways-you-can-help-yourself-stay-secure-online

[44] Plesník, P. Viry [online]. Dostupné z: http://home.tiscali.cz/petr.plesnik/Viry.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ISO	International Organization for Standardization
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
PDCA	Plan-Do-Act-Check
ISMS	Systém řízení bezpečnosti informace
IEC	International Electrotechnical Commision
NIS2	Network and Information System 2
EU	Evropská unie
ITIL	Information Technology Infrastructure Library
COBIT	Control Objectives for Information and Related Technology
ICT	Information and Communication Technologies
IT	Information Technology
DDoS	Distributed Denial of Service
CIA	Confidentialy, integrity and availability
USA	United States of America
PIN	Personal Identifiacation Number
SPAM	Sizzle Pork and Mmm
ABAC	Attribute-Based Access Control
DAC	Discretionary Access Control
MAC	Mandatory Access Control
IDS	Intrusion Detection Systém
IPS	Intrusion Protection Systém
HTTPS	Hypertext Transfer Protocol Secure
SSL	Secure Sockets Layer
RBAC	Role-Based Access Control

SIEM Security Information and Event Management

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

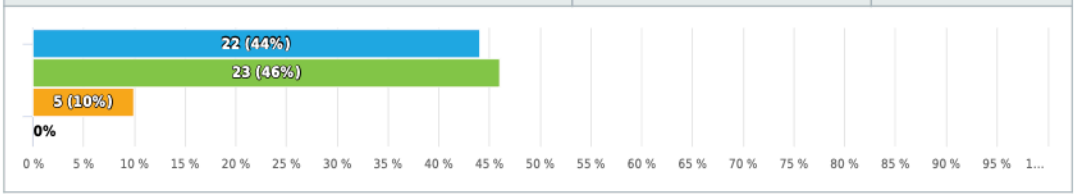
PŘÍLOHA P I: VÝSLEDKY ANKETY

Výsledky

1 Jaké je Vaše pohlaví?

Výběr z možností , zodpovězeno 50 x, nezodpovězeno 0 x

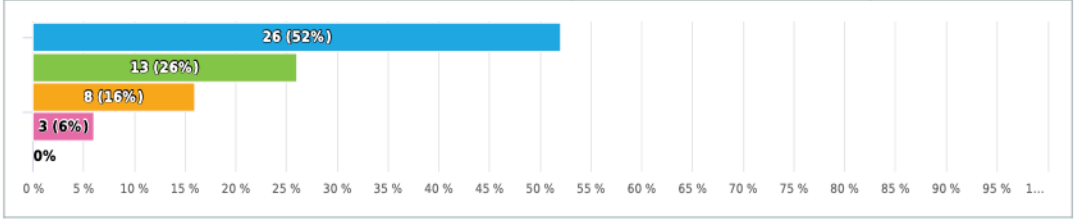
Možnosti odpovědí	Responzí	Podíl
Žena	22	44,0%
Muž	23	46,0%
Nechci uvádět	5	10,0%
Jiná	0	0,0%



2 Kolik je Vám let?

Výběr z možností , zodpovězeno 50 x, nezodpovězeno 0 x

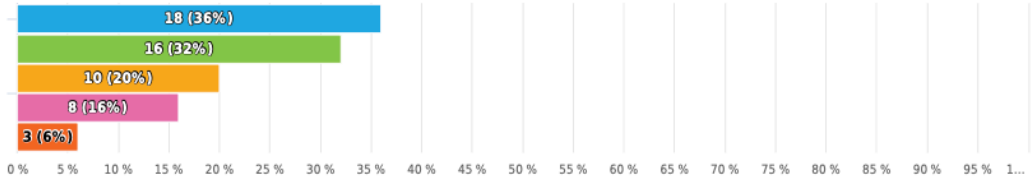
Možnosti odpovědí	Responzí	Podíl
18-25 let	26	52,0%
26-50 let	13	26,0%
50 let a více	8	16,0%
Nechci uvádět	3	6,0%
Jiná	0	0,0%



3 Jaký je Váš pracovní poměr, vyberte správnou odpověď:

Výběr z možností, více možných, zodpovězeno 50 x, nezodpovězeno 0 x

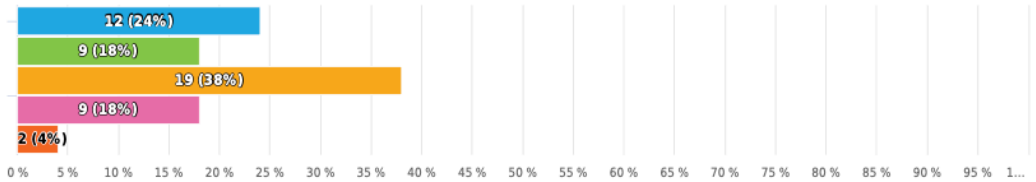
Možnosti odpovědí	Responzí	Podíl
HPP - hlavní pracovní poměr	18	36,0%
DPP - dohoda o provedení práce	16	32,0%
DPČ - dohoda o pracovní činnosti	10	20,0%
OSVČ	8	16,0%
Jiná	3	6,0%



4 Jak často se účastníte školení týkajících se kybernetické bezpečnosti ve vaší firmě?

Výběr z možností, více možných, zodpovězeno 50 x, nezodpovězeno 0 x

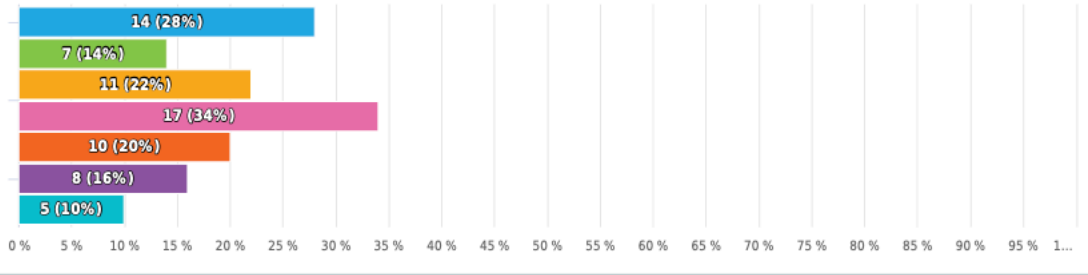
Možnosti odpovědí	Responzí	Podíl
1x ročně (minimální bezpečnostní standard)	12	24,0%
Častěji	9	18,0%
Méně než 1x ročně	19	38,0%
Neúčastním se	9	18,0%
Jiná	2	4,0%



5 Jaké typy kybernetického školení jsou vám k dispozici (např. online kurzy, workshopy, simulace atd.)?

Výběr z možností, více možných , zodpovězeno 50 x, nezodpovězeno 0 x

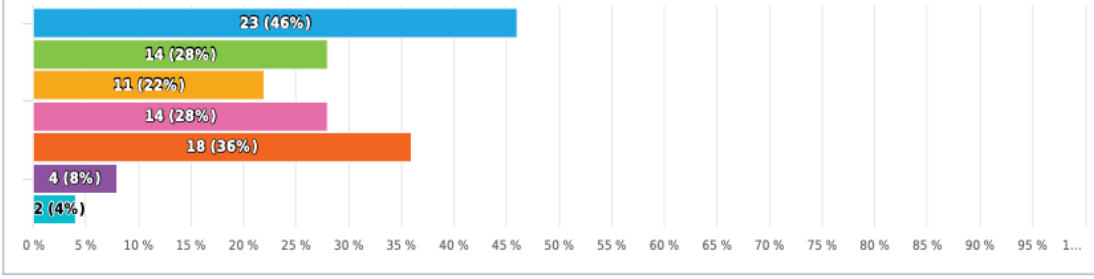
Možnosti odpovědí	Responzí	Podíl
Online kurzy	14	28,0%
Workshopy	7	14,0%
Papírová podoba	11	22,0%
Školení zaměstnavatelem (vedoucím)	17	34,0%
Školení externí osobou	10	20,0%
Neúčastním se	8	16,0%
Jiná	5	10,0%



6 Jakou formou preferujete absolvovat školení v oblasti kybernetické bezpečnosti (např. online, v rámci firemních seminářů, individuální kurzy atd.)?

Výběr z možností, více možných , zodpovězeno 50 x, nezodpovězeno 0 x

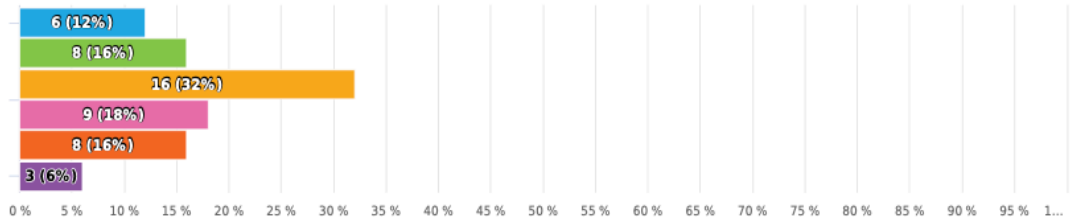
Možnosti odpovědí	Responzí	Podíl
Online kurzy	23	46,0%
Workshopy	14	28,0%
Papírová podoba	11	22,0%
Školení zaměstnavatelem (vedoucím)	14	28,0%
Školení externí osobou	18	36,0%
Neúčastním se	4	8,0%
Jiná	2	4,0%



7 Jak hodnotíte kvalitu školení, která jsou Vám poskytována v rámci firmy? (na škále 1-5, kde 1 je neuspokojivá a 5 je vynikající)

Výběr z možností , zodpovězeno 50 x, nezodpovězeno 0 x

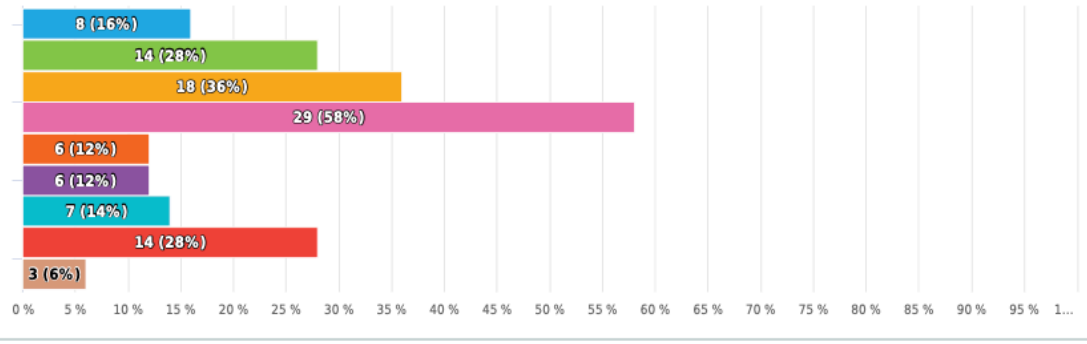
Možnosti odpovědí	Responzí	Podíl
1	6	12,0%
2	8	16,0%
3	16	32,0%
4	9	18,0%
5	8	16,0%
Neúčastním se	3	6,0%



8 Jaká témata kybernetické bezpečnosti jsou vám nejvíce relevantní ve vaší práci?

Výběr z možností, více možných , zodpovězeno 50 x, nezodpovězeno 0 x

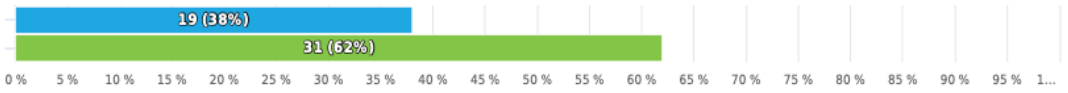
Možnosti odpovědí	Responzí	Podíl
Ochrana před malwarovými útoky	8	16,0%
Firewally a síťová bezpečnost	14	28,0%
Školení zaměstnanců v kybernetické bezpečnosti	18	36,0%
Správa hesel a autentizace	29	58,0%
Incidentní reakce a rekonstrukce	6	12,0%
Kybernetické hrozby IoT (Internet of Things)	6	12,0%
Bezpečnostní analýza a monitorování	7	14,0%
Šifrování a bezpečnost dat	14	28,0%
Vlastní odpověď	3	6,0%



9 Máte pocit, že školení v oblasti kybernetické bezpečnosti jsou dostatečně přizpůsobena vašim potřebám a pozici ve firmě?

Výběr z možností , zodpovězeno 50 x, nezodpovězeno 0 x

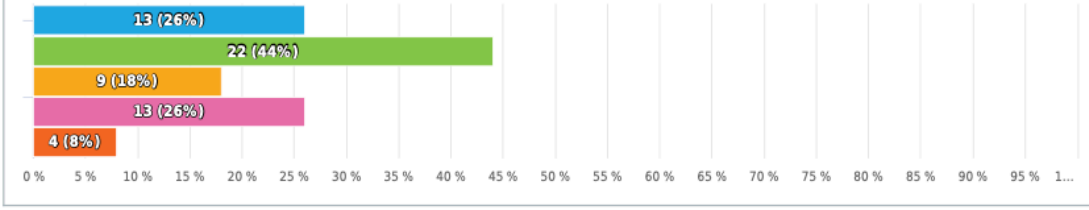
Možnosti odpovědí	Responzí	Podíl
Ano	19	38,0%
Ne	31	62,0%



10 Jaká metoda hodnocení vaší dovednosti a znalostí v oblasti kybernetické bezpečnosti se v rámci firmy používá (např. certifikace, testy, simulace atd.)?

Výběr z možností, více možných , zodpovězeno 50 x, nezodpovězeno 0 x

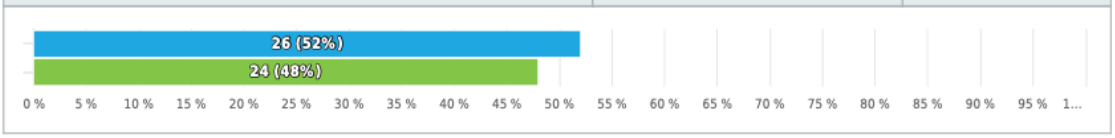
Možnosti odpovědí	Responzí	Podíl
Certifikace	13	26,0%
Testy	22	44,0%
Simulace	9	18,0%
Žádná z uvedených možností	13	26,0%
Jiná	4	8,0%



11 Jaký je váš názor na efektivitu školení v oblasti kybernetické bezpečnosti ve firmě? Cítíte, že vám pomáhají zvýšit bezpečnost a povědomí o kybernetických hrozbách?

Výběr z možností, zodpovězeno 50 x, nezodpovězeno 0 x

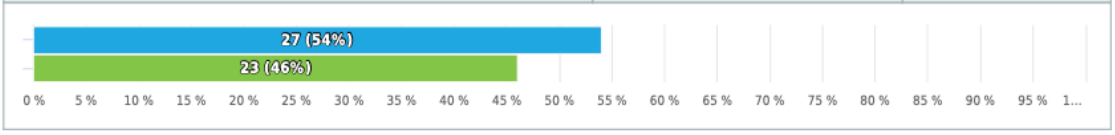
Možnosti odpovědí	Responzí	Podíl
Ano	26	52,0%
Ne	24	48,0%



12 Máte přístup k dostatečným zdrojům a technologiím pro zdokonalení svých dovedností v oblasti kybernetické bezpečnosti?

Výběr z možností, zodpovězeno 50 x, nezodpovězeno 0 x

Možnosti odpovědí	Responzí	Podíl
Ano	27	54,0%
Ne	23	46,0%



13 Jakými způsoby byste navrhovali zlepšit školení v oblasti kybernetické bezpečnosti ve vaší firmě?

Textová odpověď, zodpovězeno 50 x, nezodpovězeno 0 x

- (39x)
- Aby vůbec nějaké bylo
- Dělám to podle svého nejlepšího svědomí a vědomí.
- Není jak
- Nijak
- Online formou
- Pravidelným školením bezpečnosti od odborníků.
- Uvádět ve smlouvě povinnou účast na sezení ohledně bezpečnosti
- Více kurzů, školení zábavnou formou (interaktivní)
- Vytvořit jako předmět

- Začít ho dělat
- Žádným

14 Jak se v rámci firmy řeší otázka motivace zaměstnanců ke studiu kybernetické bezpečnosti?

Textová odpověď, zodpovězeno 50 x, nezodpovězeno 0 x

- (41x)
- Často vidíme co se stane když něco někde uteče a je to bolest
- (2x) Neřeší
- Nevím
- Premie
- Spam emaily a bububu v chatu
- TeamBuilding
- X
- zdůrazňuje se důležitost školení, ukázka reálných příkladů

15 Jaká omezení, pokud nějaká, vnímáte ve školení kybernetické bezpečnosti ve vaší firmě?

Textová odpověď, zodpovězeno 50 x, nezodpovězeno 0 x

- (41x)
- Kde nic není, ani security nebere
- Kybernetické hrozby přibývají každým dnem, školení jsou málo častá.
- Nedostatečně vzdělaní školitelé
- Nevím
- Nezájem ostatních
- X
- Zadna
- Žádné
- Žádnou

16 Máte vědomosti o incidentech spojených s kybernetickou bezpečností ve vaší firmě? Jak byly tyto incidenty řešeny?

Textová odpověď, zodpovězeno 50 x, nezodpovězeno 0 x

- (39x)
- Ano
- Ano, borce jsme zaměstnali
- Ano. Incidenty mají formu řešení okamžité odezvy na daný incident, následné vyhodnocení a doporučení dalšího postupu, aby se daný incident neopakoval, případně se snížil jeho dopad.
- Ano, policií
- Momentálně nemám povědomí o žádném bezpečnostním incidentu

- Ne
- Nevím
- Vyhození
- X
- Z prvu domluva, pak banování na všech platformách a snažit se informace nepotrvzovat ani na téma nereagovat
- Žádné si nevybavuji

17 Máte nějaké další připomínky nebo nápady týkající se školení kybernetické bezpečnosti ve firmách?

Textová odpověď, zodpovězeno 50 x, nezodpovězeno 0 x

- (42x)
- Chtělo by to zlepšit
- Měly by být častěji.
- Náš připad je moc specifický pro firmy.
- (2x) Ne
- Nevím
- X
- Začít ho dělat a neco z toho taky praktikovat

Anketa o školení kybernetické bezpečnosti ve firmách

Tato anketa se zaměřuje na vaše pohledy, zkušenosti a potřeby ohledně školení v oblasti kybernetické bezpečnosti ve firmě, kde pracujete. Vaše názory a odpovědi budou nesmírně cenným zdrojem informací pro naši bakalářskou práci, která má za cíl analyzovat a zkoumat efektivitu těchto školení, stejně jako jejich vliv na kybernetickou bezpečnost firmy.

Vaše účast v této anketě je zcela dobrovolná a vaše odpovědi budou zachovány v absolutním soukromí a důvěrnosti. Dotazník by neměl trvat déle než několik minut a vaše zpětná vazba je pro nás nesmírně cenná.

1 Jaké je Vaše pohlaví?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Žena ◯ Muž ◯ Nechci uvádět

◯ Jiná

2 Kolik je Vám let?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ 18-25 let ◯ 26-50 let ◯ 50 let a více ◯ Nechci uvádět

◯ Jiná

3 Jaký je Váš pracovní poměr, vyberte správnou odpověď:

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

☐ HPP - hlavní pracovní poměr ☐ DPP - dohoda o provedení práce ☐ DPČ - dohoda o pracovní činnosti ☐ OSVČ

☐ Jiná

4 Jak často se účastníte školení týkajících se kybernetické bezpečnosti ve vaší firmě?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

☐ 1x ročně (minimální bezpečnostní standard) ☐ Častěji ☐ Méně než 1x ročně ☐ Neúčastním se

☐ Jiná

5 Jaké typy kybernetického školení jsou vám k dispozici (např. online kurzy, workshopy, simulace atd.)?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

- [ ] Online kurzy
- [ ] Workshopy
- [ ] Papírová podoba
- [ ] Školení zaměstnavatelem (vedoucím)
- [ ] Školení externí osobou
- [ ] Neúčastním se
- [ ] Jiná

6 Jakou formou preferujete absolvovat školení v oblasti kybernetické bezpečnosti (např. online, v rámci firemních seminářů, individuální kurzy atd.)?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

- [ ] Online kurzy
- [ ] Workshopy
- [ ] Papírová podoba
- [ ] Školení zaměstnavatelem (vedoucím)
- [ ] Školení externí osobou
- [ ] Neúčastním se
- [ ] Jiná

7 Jak hodnotíte kvalitu školení, která jsou Vám poskytována v rámci firmy? (na škále 1-5, kde 1 je neuspokojivá a 5 je vynikající)

Nápověda k otázce: *Vyberte jednu odpověď*

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ Neúčastním se

8 Jaká témata kybernetické bezpečnosti jsou vám nejvíce relevantní ve vaší práci?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

- [ ] Ochrana před malwarovými útoky
- [ ] Firewally a síťová bezpečnost
- [ ] Školení zaměstnanců v kybernetické bezpečnosti
- [ ] Správa hesel a autentizace
- [ ] Incidentní reakce a rekonstrukce
- [ ] Kybernetické hrozby IoT (Internet of Things)
- [ ] Bezpečnostní analýza a monitorování
- [ ] Šifrování a bezpečnost dat
- [ ] Vlastní odpověď

14 Jak se v rámci firmy řeší otázka motivace zaměstnanců ke studiu kybernetické bezpečnosti?

15 Jaká omezení, pokud nějaká, vnímáte ve školení kybernetické bezpečnosti ve vaší firmě?

16 Máte vědomosti o incidentech spojených s kybernetickou bezpečností ve vaší firmě? Jak byly tyto incidenty řešeny?

17 Máte nějaké další připomínky nebo nápady týkající se školení kybernetické bezpečnosti ve firmách?

9 Máte pocit, že školení v oblasti kybernetické bezpečnosti jsou dostatečně přizpůsobena vašim potřebám a pozici ve firmě?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano ◯ Ne

10 Jaká metoda hodnocení vaší dovednosti a znalostí v oblasti kybernetické bezpečnosti se v rámci firmy používá (např. certifikace, testy, simulace atd.)?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

☐ Certifikace ☐ Testy ☐ Simulace ☐ Žádná z uvedených možností

☐ Jiná

11 Jaký je váš názor na efektivitu školení v oblasti kybernetické bezpečnosti ve firmě? Cítíte, že vám pomáhají zvýšit bezpečnost a povědomí o kybernetických hrozbách?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano ◯ Ne

12 Máte přístup k dostatečným zdrojům a technologiím pro zdokonalení svých dovedností v oblasti kybernetické bezpečnosti?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano ◯ Ne

13 Jakými způsoby byste navrhovali zlepšit školení v oblasti kybernetické bezpečnosti ve vaší firmě?

PŘÍLOHA P 2: MANUÁL PRO PREZENTACI

1 MANUÁL PREZENTACE – ŠKOLENÍ KYBERNETICKÉ

1.1 SLIDE 1 – Představení

Školitel představí sebe a téma prezentace.

1.2 SLIDE 2 - Obsah

Na tomto slidu budou subjekty školení seznámeni s obsahem školení v bodech.

1.3 SLIDE 3 – První kategorie

Na tomto slidu bude uvedena první kategorie školení zároveň s krátkým popisem kybernetické bezpečnosti.

1.4 SLIDE 4 - Definice

Zde budou posluchači seznámeni s definicí kybernetické bezpečnosti podle zdroje vlády České republiky.

1.5 SLIDE 5 – Význam kybernetické bezpečnosti

Na tomto slidu budou od školitele rozebrány všechny body postupně a význam kybertické bezpečnosti pro firmu jako takovou.

- *Ochrana dat* - Pod což spadají citlivá data ve firmě jakožto například firemní informace, finanční údaje, osobní údaje a podobné- Tyto data jsou chráněny před neoprávněným přístupem, krádeží, poškozením nebo ztrátou.
- *Ochrana před kybernetický útoky* - Například malware, ransomware, phishing a jiné útoky, které mohou poškodit nejen zaměstnance firmy, ale i firmu samotnou. Takže cílem kybernetické bezpečnosti je se těmto útokům vyhnout nebo je odvrátit či minimalizovat jejich dopad.
- *Ochrana kritické infrastruktury* - Čímž rozumíme například servery nebo fyzickou ochranu před živelními pohromami, neoprávněným přístupem a zásahy. Kybernetická bezpečnost zajišťuje ochranu těchto prvků jako jsou servery apod.
- *Zajištěním důvěry v digitálním prostředí* - Je ujištění firem nebo uživatelů, že naše digitální aktiva firmy jsou chráněny před vnějšími i vnitřními hrozbami. Takže jde o to ujistit naše okolí, že jsme důvěryhodným činitelem.
- *Plány kontinuity* – Je myšleno jako promítání různých scénářů, které by mohli ohrozit běžnou činnost firmy a jejich.

1.6 SLIDE 6 – Aktuální hrozby a trendy

Na tomto slidu je možná úprava, jelikož se jedná o aktuální trendy mohou se postupem času měnit. Tudíž je možné sem zakomponovat i vlastní zkušenosti nebo přidat aktuálnější data. Pro data stávající odpovídají tyto informace:

- *Zvýšené cílené útoky na firmy a instituce* - Za cílem z firem ukradnout data zákazníků/pracovníků nebo omezit jejich provozu schopnost.
- *Ransomware útoky* – Jedná se o zašifrování dat v počítači a následné vydírání za krypto převod (nejčastěji).
- *Zranitelnost IoT (Internet of Things) zařízení* - Znamená, že v dnešní době, kdy používání zařízení s přístupem k internetu je velmi rozsáhlé a jejich zabezpečení mnohdy není úplně dostačující mohou být tyto zařízení zneužita k provádění útoků nebo krádeže dat.
- *Sociální inženýrství* - Je v dnešní době jeden z nejpoužívanějších útoků na běžného uživatele internetu. A rozumíme tím tedy falešné emaily, podvodné telefonáty nebo

SMS zprávy nebo také podvodné webové stránky za účelem získání důvěrných údajů.

- *Nedostatečná ochrana osobních údajů* - Zadávání citlivých informací na stránky, které nejsou důvěryhodné nebo sdělování těchto informací ve veřejném prostředí, kde může být odposlechnuto lidmi, kterým by tyto informace neměly být odhaleny. Ale můžeme k odhalení těchto dat přijít i přes firmy, které jsou cílem útoků sociálního inženýrství.
- *Zvýšena spolupráce mezi organizacemi* – Jedná se o organizace hackerů, které mezi sebou spolupracují na útocích.

1.7 SLIDE 7 – Právní aspekty

Na tomto slidu stačí je zmínit tyto tři hlavní body jako je hlavní zákon v České republice, pokud se bavíme o kybernetické bezpečnosti v plném znění jej můžeme naleznout na stránkách národního úřadu kybernetické bezpečnosti.

Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatření náležitostech podání v oblasti kybernetické bezpečnosti a likvidace dat.

ISO normy 2700X jsou soubory instrukcí a požadavků na firmu v oblasti kybernetické bezpečnosti. Pokud firma má certifikace ISO je to pro ni přínosné z hlediska lepších zakázek například i státních zakázek.

1.8 SLIDE 8 – Druhá kategorie

Seznámení posluchačů s další kategorií školení.

1.9 SLIDE 9 – Hrozby a útoky

Seznámení s hrozbami, které jsou typickými případy kybernetických útoku, na tomto slidu by mělo být ke každé odrážce minimálně vysvětleno, jak daný způsob probíhá, jak může uživatel rozlišit podvod.

- *Malware* - Škodlivý kód, který můžeme rozeznat pomocí nějakých nežádoucích činností našeho zařízení jako jsou například vyskakují reklamy/okénka na našem prohlížeči.
- *Phishing* - Útok za pomocí sociálního inženýrství, cílem je z uživatelů dostat citlivá data, nejčastěji se můžeme setkat s podvodnými emaily.
- *DoS útoky* - Snaho o přetížení serveru jednoho místa, které inscenuje útočník.
- *DDoS* – Podkategorie DoS, avšak častěji používaná, snaho o přetížení serveru z náhodných různých více míst takzvaných botnetů (zombie stanice), které inscenuje útočník z jednoho místa.
- *Úniky dat* – Úniky dat zákazníků od firem, které byly cílem útoku, nebo nepozorností špatně proškolených zaměstnanců.
- *Sociální inženýrství* – Bylo zmíněno již výše, stačí pouze zrychleně připomenout posluchačům.
- *Zranitelnost IoT zařízení* - Bylo zmíněno již výše, stačí pouze zrychleně připomenout posluchačům.
- *Ransomware* - Bylo zmíněno již výše, stačí pouze zrychleně připomenout posluchačům.

Jsou tři věci, které jsme si již vysvětlily tudíž je nemusíme vysvětlovat znovu, ale patří sem také.

1.10 SLIDE 10 – Příklady z praxe

Prezentované příklady z praxe mohou být nahrazeny lektorovými vlastními nebo těmi, které považuje za praktičtější v oblasti organizace. Příklady, které jsou zde zmíněné patří mezi nejčastěji, zároveň je zde popsáno i jejich řešení v praxi.

- *Brute force*
  - Útočník se snaží dostat na secure shell (ssh) prolomením hesel.
  - Řešením je použití místo hesel ssh klíče s šifrováním pro administrátory.
  - Takže jsou dvě části klíče pro připojení jednu má uživatel/administrátor u sebe například v souboru a druhá je součástí ssh a funguje to na principu, že k sobě musí obě části pasovat.
- *DDoS*
  - Snaho o přetížení serveru z náhodných a různých více míst takzvaných botnetů (zombie stanice) které inscenuje útočník.
  - Řešení může být posílení infrastruktury o prvky filtrující DDoS, aby útoku obstáli.
  - Limitace, avšak zde je potřeba velmi výkonných serverů, aby útoky byly zablokovány a omezeny. Finančně nepraktické tudíž se používá spíše pro menší firmy, které nemají dosahy do zahraničí.
- *Ransomware*
  - Útok na data uvnitř počítače, ke kterým je znemožněn přístup a jsou zaheslována a podmínkou útočníka je nějaké výkupné za návrat přístupu k datům.
  - Řešením je firewall a antivirus pro uživatelské stanice, ale i hlavní servery.
- *Phishing*
  - Útok za pomocí sociálního inženýrství a cílem je z uživatelů dostat citlivá data, nejčastěji se s tím můžeme setkat jako s podvodnými emaily.
  - Schopnost rozpoznat podvodnou stránku od reálné, čehož dosáhneme řádným školením a aktuálními trendy ve školení.

1.11 SLIDE 11 – Třetí kategorie

Lektor uvede další kategorii školení.

1.12 SLIDE 12 – Bezpečnostní politiky v organizaci 1/2

Tento slide se věnuje vytvoření a implementaci bezpečnostních politik, což je důležitým bodem školení, je důležité zde probrat každý bod a vysvětlit jej na struktuře firmy.

- *Analýza rizik* – Dostaneme seznam rizik a jejich dopad (nízký x vysoký) a jejich řešení.
- *Stanovení cílů* – Seznam cílů v rámci kybernetické bezpečnosti, kterých se snažíme dosáhnout (a průběh toho, jak jich dosáhnout = plán), obsahuje aktuální a požadovaný stav.
- *Vytvoření bezpečnostních politik* – Soubor nařízení, jak by se měli chovat zaměstnanci firmy v rámci zachování kybernetické bezpečnosti.
- *Zahrnutí zaměstnanců* – Školení!

1.13 SLIDE 13 – Bezpečnostní politiky v organizaci 2/2

- *Implementace* – Použití postupů, které si stanovíme pro dostatečné zabezpečení v organizaci.
- *Monitorování a hodnocení* – Postupy, které jsme si zavedly tak monitorujeme jejich účinnost či neúčinnost.
- *Kontinuální vylepšení* – Aktualizace podle aktuálních potřeb.

- *Zajištění souladu* – Aby vše fungovalo se vším. Mohou zde být zahrnuty i audity.
- *Prohlášení a aplikovatelnosti* – Dokument, který nás odkáže na jednotlivé dokumenty, ve kterých nalezneme aktuální bezpečnostní opatření.

1.14 SLIDE 14 – Rozvoj bezpečnostní kultury

Na tomto slidu se zaměříme na rozvoj bezpečnostní kultury uvnitř organizace, tudíž na to, jak dosáhnout nejlepších.

- *Vedení odshora* - Musíme zapojit i vedení, vedení by mělo spolupracovat (schvalování směrnic atp.).
- *Školení a osvěta* – Školit zaměstnance, v případě nových trendů aktualizovat.
- *Jasná komunikace* - V případě nejasností nebát se zeptat, a v opačném případě přiznat si, pokud nějaké hrozby jsou reálné.
- *Odpovědnost* - Každý zaměstnanec by měl vědět, za co je zodpovědný.
- *Motivace* - Motivace dodržovat pravidla a postupy.
- *Příklady z praxe* - Zdůraznění úspěšných bezpečnostních opatření a podpora a povzbuzení ze strany nadřízeného.
- *Pravidelné revize a zpětná vazba* - Kontrola bezpečnostních politik a jejich účinnost.
- *Zapojení všech zaměstnanců* - Sdílení bezpečnostní kultury a podporování všemi zaměstnanci bez ohledu na jejich pozici v organizaci.

1.15 SLIDE 15 – Odpovědnosti zaměstnanců

Tento slide je zamřený hlavně na zaměstnance, jak mohou být součástí kybernetické bezpečnosti ve firmě. Je důležité, aby tento slide byl obzvlášť implementován pro řadové zaměstnance v organizaci.

- *Ochrana hesel a přihlašovacích údajů* – Hesla nesmí být veřejně přístupná, žádné lepení papírků s hesly na obrazovku apod., žádná jednoduchá hesla a jiné často praktikované postupy u zaměstnanců.
- *Rozpoznání phishingu* – Zaměstnanci by měli dostávat školení o tom, jak rozpoznají phishingovou zprávu od zprávy reálné, nejlepším způsobem je, obdržené phishingové zprávy vystavit, aby byli na očím všem.
- *Aktualizace softwaru* – Aktualizace všech softwarů ve firmě je důležitým bodem, abychom předešli vystavení kybernetickým hrozbám, důležité je brát zřetel i na zařízení, které jsou „out-of-date“, tím je myšleno, pokud jejich software je zastaralý a aktualizace na něm již neprobíhají, je považován za kybernetickou hrozbu.
- *Fyzická bezpečnost* – Zaměstnanci jsou odpovědní za svěřené fyzická zařízení včetně kabelových rozvodů apod., neumožňují přístup do budovy neoprávněným osobám.
- *Reportování incidentů* – Pokud má zaměstnanec podezření na možnou bezpečnostní hrozbu nebo zranitelnost měl by to nahlásit.
- *Spolupráce s bezpečnostním týmem* – Při podezření na bezpečnostní hrozbu nebo při ní by zaměstnanci měli spolupracovat s bezpečnostním týmem, aby situace byla vyřešena co nejplynuleji a nejrychleji.

1.16 SLIDE 16 – Čtvrtá kategorie

Zde by přednášející opět uvede posluchače do další kategorie.

1.17 SLIDE 17 – Síťová bezpečnost

Síťová bezpečnost, tedy co musíme mít/dělat abychom udrželi naši síť nejlépe zabezpečenou.

- *Firewally* – Zjednodušeně se dá říct, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje.
- *Rozšířená detekce a reakce* – Zabezpečení, které využívá automatizaci a umělou inteligenci ke zkrácení doby odezvy ve více běžících procesech.
- *Security Information and Event Management* – Řešení zabezpečení, které shromažďuje data analyzuje aktivity a podporuje tak v organizacích ochranu před hrozbami.
- *Virtuální privátní sítě* – Maskování IP adresy navenek. Napojeni do firmy z domu bezpečně, dnes při časté práci z domu důležitým faktorem.
- *Segmentace sítě* – Vytvoření nějakého počtu lokálních sítí, které jsou odděleny pomocí firewallů a přistup k nim je možné modifikovat.

1.18 SLIDE 18 – Endpoinotvá bezpečnost

Na tomto slidu lektor seznámí posluchače s endpointovou bezpečností ve firmě. Bezpečnost koncových zařízení jako jsou uživatelské stanice.

- *Antivirový software* – Pomáhá uživatelům rozlišit podvodné stránky a škodlivé soubory.
- *Mobile Device Management* – Správa zařízení na dálku například pro případ ztráty nebo odcizení (uzamknutí, smazání dat).
- *Firewally* – Bavili jsme se dříve, stačí připomenout.
- *Ochrana před ransomware* – Bavili jsme se dříve, stačí připomenout.
- *Aktualizace* - Bavili jsme se dříve, stačí připomenout.
- *Šifrování dat* – Jedná se o proces, kdy data jsou zašifrována pomocí kryptografie a přístup k nim má pouze majitel dešifrovacího klíče.
- *Školení zaměstnanců* - Bavili jsme se dříve, stačí připomenout.
- *Správa zařízení* – Uživatelé nemají stejné pravomoce jako administrátoři.

1.19 SLIDE 19 – Pátá kategorie

Lektor uvede následující kategorii.

1.20 SLIDE 20 – Reportování a reakce

Zde se lektor bude věnovat reportování a reakcím na incidenty, je zde nutné zdůraznit, že všechny podezření apod. se musí hlásit, vždy!

- *Interní incident* – Incident, který se může stát interně (falešný e-mail od účetní).
- *Externí incident* – Náš klient může být osloven naším jménem zá záminkou nás poškodit nebo poškodit našeho klienta.

Reakce na incidenty jsou:

- *Izolace a neutralizace* – Bavíme se o způsobených škodách.
- *Šetření a opravy* – Zjištění slabých míst, díky kterým kybernetický incident vznikl.
- *Implementace bezpečnostních opatření* – Můžeme zde použít PDCA (Plan-Do-Control-Act) model.
- *Školení zaměstnanců* – Již bylo zmíněno víckrát, avšak můžeme připomenout!

1.21 SLIDE 21 – Ukázka malware (Interní incident)

E-mail odeslaný z běžně používané adresy. Avšak můžeme si zde všimnout klasického znaku falešného e-mailu a to jméno, které není skloněné.

1.22 SLIDE 22 – Šestá kategorie

Posluchači jsou uvedeni do šesté kategorie školení.

1.23 SLIDE 23 – Praktické cvičení

Na tomhle slidu lektor bude apelovat na provádění praktických cvičení. Tato cvičení mohou probíhat právě formou závadného e-mailu nebo například vystavit ve firmě formulář pro změnu hesla, kde zaměstnanci musí napsat svá citlivá data.

1.24 SLIDE 24 – Sedmá kategorie

Lektor uvede další kategorii.

1.25 SLIDE 25 – Zmínění důležitých bodů

Na tomto slidu můžeme nalézt body, které jsme již probrali dřív, avšak jsou důležité pro zlepšení kybernetické bezpečnosti v organizacích proto můžeme znovu připomenout.

1.26 SLIDE 26 – Závěr

Lektor pomalu vede školení ke konci, řekne pár závěrečných vět a postoupí k posledním dvou slidům.

1.27 SLIDE 27 – Poznatky

Zde se lektor může zeptat školených subjektů na jejich poznatky, které si odnesli ze školení. Účinnou formou je zeptat se zúčastněných aspoň na jednu věc, která jim zůstala v paměti ze školení což vyvolá menší brainstorming na konec a donutí zúčastněné si upořádat všechny myšlenky a informace, které vstřebali.

1.28 SLIDE 28 – Prostor pro dotazy

Lektor dá zúčastněným prostranství pro dotazy a zhodnocení lektora samotného a ukončí školení.

2 DIVERZIFIKAČNÍ MOŽNOSTI ŠKOLENÍ (VÝROBNÍ PROSTŘEDÍ)

2.1 SLIDE výrobní prostředí 1/5

Lektor uvede úvodní slide pro výrobní prostředí.

2.2 SLIDE Ochrana výrobních zařízení a systémů 2/5

- *Implementace robustních autentizačních mechanismů* - Zavedení silných autentizačních metod, jako je dvoufaktorová autentizace, zajišťuje, že přístup k citlivým systémům a datům mají pouze oprávněné osoby.
- *Pravidelná aktualizace softwaru a hardwaru* - Pravidelné aktualizace softwaru a firmwaru výrobních zařízení pomáhají eliminovat známé bezpečnostní zranitelnosti a chránit před novými hrozbami.
- *Segmentace sítě* - Segmentace sítě odděluje kritické výrobní systémy od méně citlivých částí sítě, což omezuje šíření kybernetických útoků a minimalizuje potenciální škody.

2.3 SLIDE Kontrola přístupu a autentizace 3/5

- *Vícefaktorová autentizace (MFA)* - Vyžaduje, aby uživatelé prokázali svou identitu prostřednictvím dvou nebo více nezávislých metod (např. heslo a mobilní aplikace) před přístupem k citlivým systémům nebo datům.
- *Správa přístupových práv na základě role (RBAC)* - Umožňuje organizacím přiřazovat uživatelům specifické přístupové úrovně a oprávnění na základě jejich pracovních rolí, čímž zvyšuje bezpečnost a efektivitu řízení přístupu.
- *Pravidelné audity uživatelských přístupů* - Pravidelné audity uživatelských přístupů kontrolují a vyhodnocují oprávnění uživatelů v systému, aby se zajistilo, že mají pouze nezbytné přístupy a že nedochází k neoprávněnému nebo zastaralému přístupu.

2.4 SLIDE Monitorování a detekce hrozeb 4/5

- *Systémy pro detekci narušení (IDS)* - Monitorují síťový provoz a systémové aktivity, aby identifikovaly podezřelé nebo škodlivé chování, které může signalizovat kybernetický útok.
- *Systémy pro prevenci narušení (IPS)* - Nejen detekují potenciální útoky, ale také automaticky podnikají kroky k jejich zablokování a zmírnění škod v reálném čase.
- *Pravidelné testování a simulace útoků* - Jako je penetrační testování a cvičení typu "red team", pomáhají organizacím identifikovat zranitelnosti a zlepšit své obranné strategie proti reálným kybernetickým hrozbám.

2.5 SLIDE Školení a povědomí zaměstnanců 5/5

- *Školení o bezpečnostních postupech* - Poskytuje zaměstnancům znalosti a dovednosti potřebné k dodržování osvědčených praktik kybernetické bezpečnosti.
- *Školení o správném zacházení* – Zaměřuje se na zásady bezpečného používání firemních zařízení a přístupů k citlivým informacím.
- *Informovanost zaměstnanců* - zahrnuje pravidelné informování o aktuálních kybernetických hrozbách a metodách obrany proti nim.
- *Kultura bezpečnosti* - podporuje prostředí, kde je kybernetická bezpečnost prioritou a všichni zaměstnanci jsou zapojeni do jejího udržování a posilování.

3 DIVERZIFIKAČNÍ MOŽNOSTI ŠKOLENÍ (MEDIÁLNÍ DOMY)

3.1 SLIDE Mediální domy 1/5

Lektor uvede kategorii pro mediální domy.

3.2 SLIDE Ochrana redakčních systémů a dat 2/5

- *Implementace silného šifrování dat* - Zajišťuje, že citlivé informace jsou chráněny před neoprávněným přístupem během přenosu i při ukládání.
- *Zabezpečení redakčních systémů* - Zahrnuje ochranu publikačních platforem před kybernetickými útoky a neoprávněným přístupem.
- *Kontrola přístupu k citlivým souborům* - Omezuje přístup pouze na oprávněné uživatele, čímž snižuje riziko úniku nebo zneužití dat.
- *Pravidelné zálohování dat a aktualizace* - Chrání data před ztrátou a zajišťuje, že software je zabezpečen proti nejnovějším hrozbám.

3.3 SLIDE Zabezpečení online platforem a webových stránek 3/5

- *Webové firewally (WAF)* - Chrání webové aplikace před útoky tím, že filtrují a monitorují HTTP provoz mezi webovou aplikací a internetem.
- *Ochrana před DDoS útoky* - Zahrnuje implementaci technologií a postupů k detekci a zmírnění distribuovaných útoků na vyčerpání zdrojů a přetížení serverů.
- *Pravidelné skenování zranitelností a bezpečnostní testování* - Pomáhají identifikovat a opravit slabá místa v systému předtím, než mohou být zneužita útočníky.
- *Zajištění bezpečného přenosu dat pomocí HTTPS* - šifruje komunikaci mezi webovými servery a klienty, čímž chrání data před odposlechem a manipulací.

3.4 SLIDE Kontrola přístupu a autentizace 4/5

- *Vícefaktorová autentizace (MFA)* - Zvyšuje bezpečnost přihlášení tím, že vyžaduje ověření identity uživatele pomocí více než jednoho nezávislého faktoru, například hesla a mobilního ověřovacího kódu.
- *Správa přístupových práv na základě role (RBAC)* - Zajišťuje, že uživatelé mají přístup pouze k těm zdrojům a funkcím, které potřebují k výkonu své role v organizaci.
- *Pravidelné audity uživatelských přístupů* - kontrolují a ověřují oprávnění uživatelů, aby se zajistilo, že mají odpovídající přístupová práva v souladu s jejich pracovními povinnostmi.

3.5 SLIDE Školení a povědomí zaměstnanců 5/5

- *Školení o bezpečnostních postupech* - Poskytuje zaměstnancům znalosti a dovednosti potřebné k dodržování osvědčených praktik kybernetické bezpečnosti.
- *Školení o správném zacházení* – Zaměřuje se na zásady bezpečného používání firemních zařízení a přístupů k citlivým informacím.
- *Informovanost zaměstnanců* - zahrnuje pravidelné informování o aktuálních kybernetických hrozbách a metodách obrany proti nim.
- *Kultura bezpečnosti* - podporuje prostředí, kde je kybernetická bezpečnost prioritou a všichni zaměstnanci jsou zapojeni do jejího udržování a posilování.

4 DIVERZIFIKAČNÍ MOŽNOST ŠKOLEÍ (IT FIRMY S CITLIVÝMI DATY)

4.1 SLIDE IT firmy s citlivými daty 1/5

Lektor uvede úvodní slide pro IT firmy s citlivými daty

4.2 SLIDE Ochrana redakčních systémů a dat 2/5

- *End-to-end šifrování* - Zajišťuje, že data jsou šifrována od odesílatele k příjemci, což zabraňuje jakýmkoli neoprávněným zásahům během přenosu.
- *Implementace šifrování na úrovni souborů a disků* - Zabezpečuje data uložená na zařízení nebo v cloudu tím, že je šifruje a chrání před neoprávněným přístupem.
- *Pravidelné revize a aktualizace šifrovacích protokolů* - Zajišťují, že používané šifrovací metody jsou stále odolné vůči aktuálním hrozbám a zranitelnostem.

4.3 SLIDE Kontrola přístupu a identita managementu 3/5

- *Vícefaktorová autentizace (MFA)* - Zvyšuje bezpečnost tím, že vyžaduje více než jednu formu ověření totožnosti, jako jsou heslo, token nebo biometrické údaje.
- *Správa přístupových práv na základě role (RBAC)* - Umožňuje přidělovat oprávnění na základě rolí v organizaci, což usnadňuje řízení přístupu a minimalizuje riziko zneužití.
- *Implementace principu privilegií* - Zajišťuje, že uživatelé mají pouze potřebná oprávnění k provádění svých pracovních úkolů, čímž minimalizuje riziko nesprávného použití dat nebo systémů.

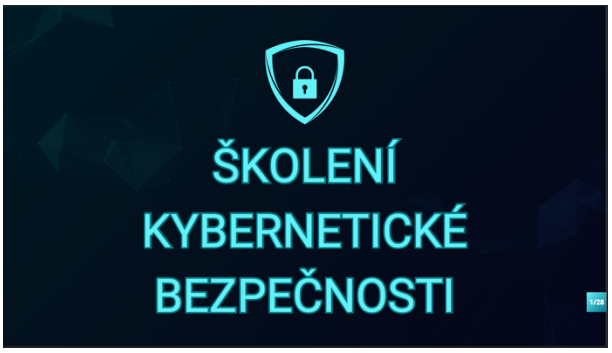
4.4 SLIDE Monitorování a detekce hrozeb 4/5

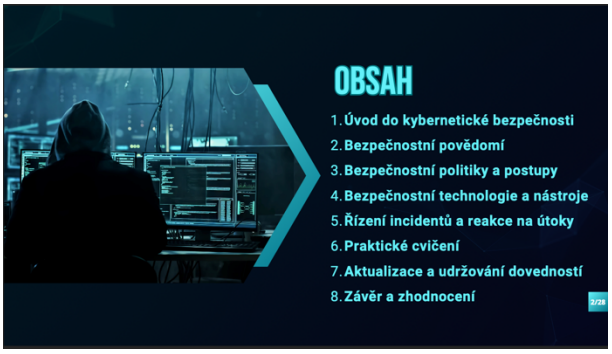
- *Systémy pro detekci a prevenci narušení (IDS/IPS)* - Monitorují síťový provoz a detekují potenciální hrozby (IDS) nebo aktivně reagují na narušení (IPS), čímž chrání síťovou infrastrukturu.
- *Systémy pro řízení bezpečnostních informací a událostí (SIEM)* - Agregují, analyzují a reagují na události z různých zdrojů v reálném čase, poskytují celkový přehled o bezpečnosti a umožňují rychlou reakci na incidenty.
- *Pravidelné testování zranitelností* - identifikuje slabiny v síťové infrastruktuře, aplikacích a systémech pomocí simulovaných útoků, což umožňuje organizacím aktualizovat svá bezpečnostní opatření a minimalizovat riziko úspěšného útoku.

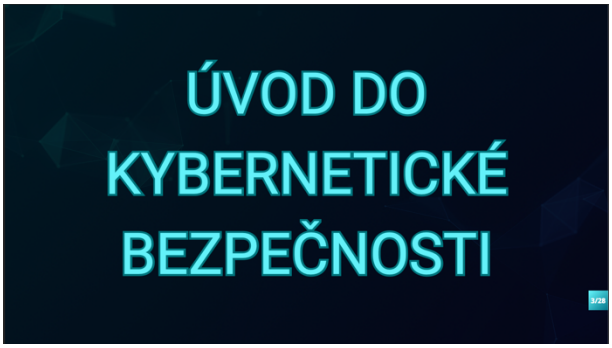
4.5 SLIDE Školení a povědomí zaměstnanců 5/5

- *Školení o bezpečnostních postupech* - Poskytuje zaměstnancům znalosti a dovednosti potřebné k dodržování osvědčených praktik kybernetické bezpečnosti.
- *Školení o správném zacházení* – Zaměřuje se na zásady bezpečného používání firemních zařízení a přístupů k citlivým informacím.
- *Informovanost zaměstnanců* - zahrnuje pravidelné informování o aktuálních kybernetických hrozbách a metodách obrany proti nim.
- *Kultura bezpečnosti* - podporuje prostředí, kde je kybernetická bezpečnost prioritou a všichni zaměstnanci jsou zapojeni do jejího udržování a posilování.

PŘÍLOHA P 3: PREZENTACE







IDENTIFIKACE TYPICKÝCH KYBERNETICKÝCH HROZEB A ÚTOKŮ

01 Malware
02 Phishing
03 Ransomware
04 Denial-of-Service (Dos) útoky
05 Úniky dat
06 Sociální inženýrství
07 Zranitelnost IoT zařízení

9/28

PRAKTICKÉ PŘÍKLADY ÚTOKŮ A JEJICH DOPADY

01 Brute Force
02 DDoS
03 Ransomware
04 Phishing

10/28

BEZPEČNOSTNÍ POLITIKY A POSTUPY

11/28

VYTVOŘENÍ A IMPLEMENTACE BEZPEČNOSTNÍCH POLITIK

01 Analýza rizik
02 Stanovení cílů
03 Vytvoření bezpečnostních politik
04 Zahrnutí zaměstnanců

12/28

VYTVOŘENÍ A IMPLEMENTACE BEZPEČNOSTNÍCH POLITIK

05 Implementace
06 Monitorování a hodnocení
07 Kontinuální vylepšení
08 Zajištění souladu
09 Prohlášení o aplikovatelnosti

13/28

ROZVOJ BEZPEČNOSTNÍ KULTURY V ORGANIZACI

01 Vedení odshora
02 Školení a osvěta
03 Jasná komunikace
04 Odpovědnost
05 Motivace
06 Příklady z praxe
07 Pravidelné revize a zpětná vazba
08 Zapojení všech zaměstnanců

14/28

ODPOVĚDNOSTI ZAMĚSTNANCŮ V KYBERNETICKÉ BEZPEČNOSTI

01 Ochrana hesel a přihlašovacích údajů
02 Rozpoznání phishingu
03 Aktualizace softwaru
04 Reportování incidentů
05 Spolupráce s bezpečnostním týmem

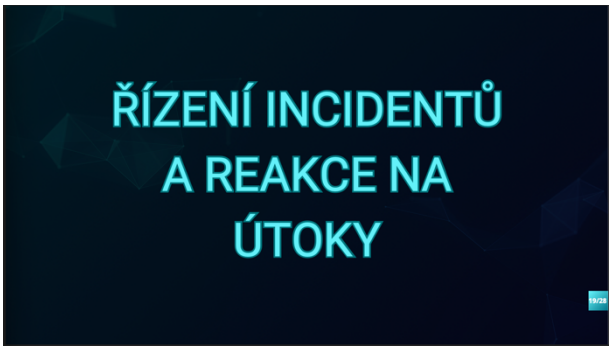
15/28

BEZPEČNOSTNÍ TECHNOLOGIE A NÁSTROJE

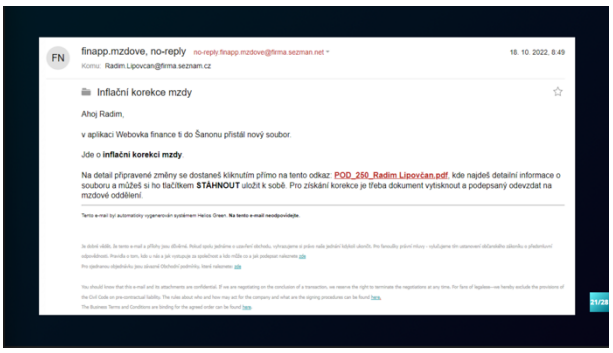
16/28


SÍŤOVÁ BEZPEČNOST
01 Firewally
02 Rozšířená detekce a reakce (XDR)
03 Security Infromation and Event Management (SIEM)
04 Virtuální privátní sítě (VPN)
05 Segmentace sítě
17/28

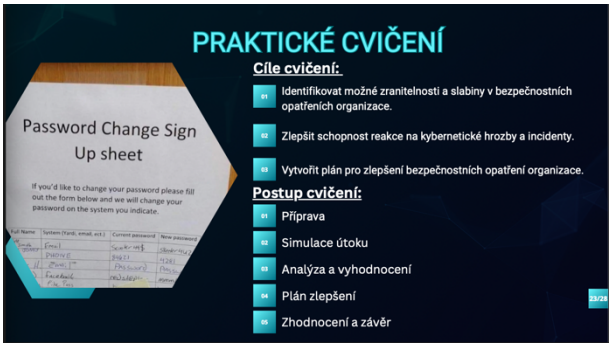

ENDPOINTOVÁ BEZPEČNOST
01 Antivirový software
02 Mobile Device Management (MDM)
03 Firewally
04 Ochrana před ransomware
05 Aktualizace
06 Šifrování dat
07 Omezení práv uživatelů
08 Školení zaměstnanců
18/28


ŘÍZENÍ INCIDENTŮ A REAKCE NA ÚTOKY
19/28


REPORTOVÁNÍ KYBERNETICKÝCH INCIDENTŮ
01 Interní reportování
02 Externí reportování
REAKCE NA KYBERNETICKÉ INCIDENTY
01 Izolace a neutralizace
02 Šetření a opravy
03 Implementace bezpečnostních opatření
04 Školení zaměstnanců
20/28


FN
finapp.mzdove, no-reply no-reply.finapp.mzdove@firma.seznam.net
18. 10. 2022, 8:49
Komu: Radim.Lipovcan@firma.seznam.cz
Inflační korekce mzdy
Ahoj Radim,
v aplikaci Webovka finance ti do Šanonu přistál nový soubor.
Jde o inflační korekci mzdy.
Na detail připravené změny se dostaneš kliknutím přímo na tento odkaz: POD_250_Radim Lipovčan.pdf, kde najdeš detailní informace o souboru a můžeš si ho tlačítkem STÁHNOUT uložit k sobě. Pro získání korekce je třeba dokument vytisknout a podepsaný odevzdat na mzdové oddělení.
21/28


PRAKTICKÉ CVIČENÍ
22/28


PRAKTICKÉ CVIČENÍ
Password Change Sign Up sheet
If you'd like to change your password please fill out the form below and we will change your password on the system you indicate.
Cíle cvičení:
01 Identifikovat možné zranitelnosti a slabiny v bezpečnostních opatřeních organizace.
02 Zlepšit schopnost reakce na kybernetické hrozby a incidenty.
03 Vytvořit plán pro zlepšení bezpečnostních opatření organizace.
Postup cvičení:
01 Příprava
02 Simulace útoku
03 Analýza a vyhodnocení
04 Plán zlepšení
05 Zhodnocení a závěr
23/28


AKTUALIZACE A UDRŽOVÁNÍ DOVEDNOSTÍ
24/28

PRŮBĚŽNÉ ŠKOLENÍ ZAMĚSTNANCŮ A AKTUALIZACE BEZPEČNOSTNÍCH POSTUPŮ

01 Pravidelné školení zaměstnanců

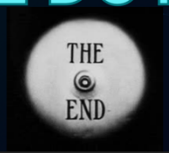
02 Aktualizace bezpečnostních postupů

03 Podpora a motivace zaměstnanců

ZÁVĚR

KLÍČOVÉ POZNATKY? ZHODNOCENÍ!

PROSTOR PRO VAŠE DOTAZY



Zdroje

- VLÁDA ČESKÉ REPUBLIKY. Kybernetická bezpečnost [online]. 13.4.2024 [cit. 2024-04-26]. Dostupné z: https://vlada.gov.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/
- GIPHY. Hoppip Art Film [online]. 2024-04-26 [cit. 2024-04-26]. Dostupné z: https://giphy.com/gifs/hoppip-art-film-eujb1tWaj3ZxS[6]
- ŽALUDOVÁ, Karin. Kybernetická bezpečnost ve firmách. Bakalářská práce. Zlín: Univerzita Tomáše Bati ve Zlíně, 2024.
- RANSOMWARE CRYPTOLOCKER STÁLE ÚTOČÍ, 2024. EABM [online]. [cit. 2024-05-22]. Dostupné z: https://eabm.cz/1288-ransomware-cryptolocker-stale-utoci
- Varování: Podvodné zprávy žádají zaplacení pohledávek, 2024. MUNI - CSIRT MU [online]. [cit. 2024-05-21]. Dostupné z: https://csirt.muni.cz/varovani/varovani-podvodne-zpravy-zadaji-zaplaceni-pohledavek

VÝROBNÍ PROSTŘEDÍ

OCHRANA VÝROBNÍCH ZAŘÍZENÍ A SYSTÉMŮ

01 Implementace robustních autentizačních mechanismů

02 Pravidelná aktualizace softwaru a hardwaru

03 Segmentace sítě

KONTROLA PŘÍSTUPU A AUTENTIZACE

01 Vícefaktorová autentizace (MFA)

02 Správa přístupových práv na základě role (RBAC)

03 Pravidelné audity uživatelských přístupů

MONITOROVÁNÍ A DETEKCE HROZEB

01 Systémy pro detekci narušení (IDS)

02 Systémy pro prevenci narušení (IPS)

03 Pravidelné testování a simulace útoků

ŠKOLENÍ A POVĚDOMÍ ZAMĚSTNANCŮ

01 Školení o bezpečnostních postupech

02 Školení o správném zacházení

03 Informovanost zaměstnanců

03 Kultura bezpečnosti

MEDIÁLNÍ DOMY

OCHRANA REDAKČNÍCH SYSTÉMŮ A DAT

01 Implementace silného šifrování dat

02 Zabezpečení redakčních systémů

03 Kontrola přístupu k citlivým souborům

03 Pravidelné zálohování dat a aktualizace

ZABEZPEČENÍ ONLINE PLATFOREM A WEBOVÝCH STRÁNEK

01 Webové firewally (WAF)

02 Ochrana před DDoS útoky

03 Pravidelné skenování zranitelností a bezpečnostní testování

03 Zajištění bezpečného přenosu dat pomocí HTTPS

KONTROLA PŘÍSTUPU A AUTENTIZACE

01 Vícefaktorová autentizace (MFA)

02 Správa přístupových práv na základě role (RBAC)

03 Pravidelné audity uživatelských přístupů

ŠKOLENÍ A POVĚDOMÍ ZAMĚSTNANCŮ

01 Školení o bezpečnostních postupech

02 Školení o správném zacházení

03 Informovanost zaměstnanců

03 Kultura bezpečnosti

IT FIRMY S CITLIVÝMI DATY

OCHRANA REDAKČNÍCH SYSTÉMŮ A DAT

01 Použití end-to-end šifrování

02 Implementace šifrování na úrovni souborů a disků

03 Pravidelné revize a aktualizace šifrovacích protokolů

KONTROLA PŘISTUPU A IDENTITA MANAGEMENTU

01 Vícefaktorová autentizace (MFA)

02 Správa přístupových práv na základě role (RBAC)

03 Implementace principu privilegií

MONITOROVÁNÍ A DETEKCE HROZEB

01 Systémy pro detekci a prevenci narušení (IDS/IPS)

02 Systémy pro řízení bezpečnostních informací a událostí (SIEM)

03 Pravidelné testování zranitelností

ŠKOLENÍ A POVĚDOMÍ ZAMĚSTNANCŮ

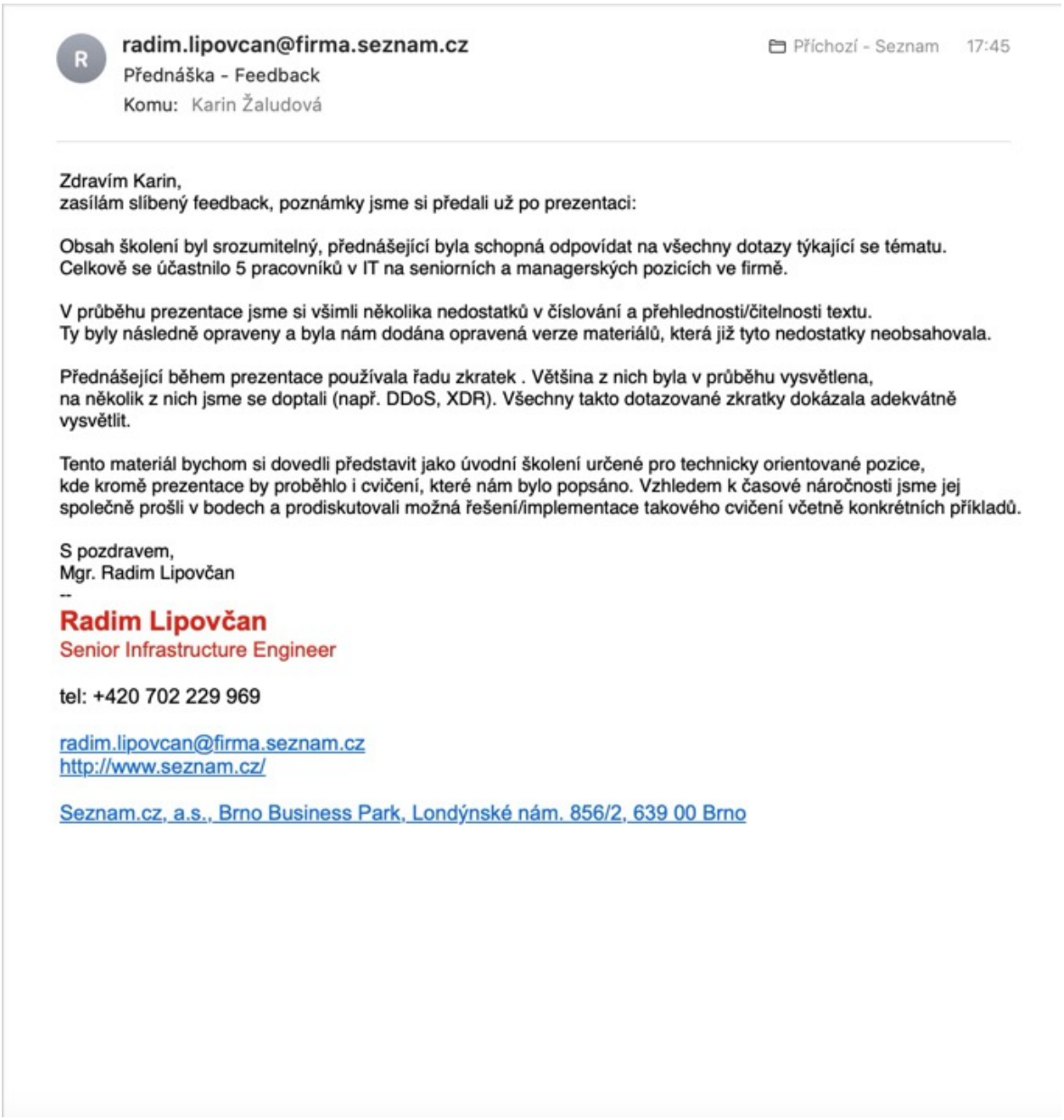
01 Školení o bezpečnostních postupech

02 Školení o správném zacházení

03 Informovanost zaměstnanců

03 Kultura bezpečnosti

PŘÍLOHA P 4: ZPĚTNÁ VAZBA ZE ŠKOLENÍ



R **radim.lipovcan@firma.seznam.cz** Příchozí - Seznam 17:45

Přednáška - Feedback

Komu: Karin Žaludová

Zdravím Karin,
zasílám slíbený feedback, poznámky jsme si předali už po prezentaci:

Obsah školení byl srozumitelný, přednášející byla schopná odpovídat na všechny dotazy týkající se tématu.
Celkově se účastnilo 5 pracovníků v IT na seniorních a managerských pozicích ve firmě.

V průběhu prezentace jsme si všimli několika nedostatků v číslování a přehlednosti/čitelnosti textu.
Ty byly následně opraveny a byla nám dodána opravená verze materiálů, která již tyto nedostatky neobsahovala.

Přednášející během prezentace používala řadu zkratek . Většina z nich byla v průběhu vysvětlena,
na několik z nich jsme se doptali (např. DDoS, XDR). Všechny takto dotazované zkratky dokázala adekvátně vysvětlit.

Tento materiál bychom si dovedli představit jako úvodní školení určené pro technicky orientované pozice,
kde kromě prezentace by proběhlo i cvičení, které nám bylo popsáno. Vzhledem k časové náročnosti jsme jej společně prošli v bodech a prodiskutovali možná řešení/implementace takového cvičení včetně konkrétních příkladů.

S pozdravem,
Mgr. Radim Lipovčan
--

Radim Lipovčan
Senior Infrastructure Engineer

tel: +420 702 229 969

radim.lipovcan@firma.seznam.cz
http://www.seznam.cz/

Seznam.cz, a.s., Brno Business Park, Londýnské nám. 856/2, 639 00 Brno