Nástroj pro analýzu rizik kybernetické bezpečnosti podle platné legislativy

Erik Podešva

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Erik Podešva**
Osobní číslo:	**A21070**
Studijní program:	**B0613A140020 Softwarové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Nástroj pro analýzu rizik kybernetické bezpečnosti podle platné legislativy**
Téma práce anglicky:	**Cybersecurity Risk Analysis Tool According to Current Legislation**

Zásady pro vypracování

1. Proveďte stručnou analýzu dostupných kybernetických bezpečnostních předpisů a nařízení v různých zemích a vytvořte přehledné srovnání.
2. Navrhněte nástroj, který by mohl pomoci organizacím dodržovat tyto předpisy.
3. Pro vývoj multiplatformního softwaru pro řízení rizik kybernetické bezpečnosti zvolte vhodný programovací jazyk, technologii a detailně popište proces vývoje nástroje.
4. Zdokumentujte implementaci jednotlivých funkcí nástroje a zajištění multiplatformního přístupu.
5. Navrhněte a implementujte uživatelské rozhraní s ohledem na širokou škálu uživatelů.
6. Otestujte vytvořený nástroj a to včetně bezpečnostního testování a testování funkčnosti.
7. Popište, jaké bezpečnostní mechanismy a postupy jsou implementovány do nástroje, aby byl chráněn před kybernetickými hrozbami.

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

Seznam doporučené literatury:

1. SCAMBRAY, Joel a Allan FRIEDMAN. Cybersecurity and Cyberwar: What Everyone Needs to Know. Illustrated. Oxford University Press, 2014. ISBN 978-0199918119.
2. MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. Hacking Exposed 7: Network Security Secrets and Solutions. 7th edition. McGraw Hill, 2012. ISBN 978-0071780285.
3. STEINBERG, Joseph. Cybersecurity For Dummies. 1th edition. For Dummies, 2022. ISBN 978-1119867180.
4. CAPPELLI, Dawn M., Andrew P. MOORE a Randall F. TRZECIAK. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes. 1th edition. Addison-Wesley Professional, 2012. ISBN 978--0321812575.
5. STUTTARD, Dafydd a Marcus PINTO. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. 2th edition. Wiley, 2011. ISBN 978-1118026472.
6. HADNAGY, Christopher. Social Engineering: The Science of Human Hacking. 2th edition. Wiley, 2018. ISBN 978--1119433385.
7. VACCA, John R. Computer and Information Security Handbook. 3th edition. Morgan Kaufmann, 2017. ISBN 978--0128038437.

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

Datum zadání bakalářské práce: **5. listopadu 2023**
Termín odevzdání bakalářské práce: **13. května 2024**

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

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

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 5. ledna 2024

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.

Ve Zlíně, dne Erik Podešva v.r.

ABSTRAKT

Bakalářská práce se zabývá vytvořením nástroje pro analýzu kybernetické bezpečnosti podle platné legislativy. Cílem je vytvořit multiplatformní software, který poskytne firmám možnost efektivně dodržovat příslušné kybernetické bezpečnostní předpisy a nařízení. Teoretická část se zabývá srovnáním kybernetických bezpečnostních předpisů v různých zemích, srovnání předpisů k regulaci, účinnost regulace a jak dodržovat kybernetické předpisy. Praktická část představuje návrh a vývoj samotného nástroje, vybrání technologií a implementace bezpečnostních mechanismů. Důraz byl taky kladen na uživatelské rozhraní a funkčností nástroje.

Klíčová slova:

kybernetická bezpečnost, analýza rizik, legislativa, multiplatformní software, nástroj pro řízení rizik

ABSTRACT

This bachelor thesis focuses on the development of a cybersecurity risk analysis tool according to current legislation. The aim is to create a multiplatform software solution enabling companies to effectively comply with current cybersecurity regulations. The theoretical part compares cybersecurity regulations across different countries, assessing their effectiveness and methods for compliance. The practical segment presents the design and development of the tool, including technology selection and implementation of security measures. Emphasis was also placed on user interface design and tool functionality.

Keywords:

cybersecurity, risk analysis, legislation, multiplatform software, risk management tool

Tímto bych chtěl poděkovat svému vedoucímu panu Ing. Lukáši Králíkovi Ph.D. za ochotu, rady a odborný dohled během procesu vypracování bakalářské práce, rodině za podporu a motivaci během studia.

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

Prohlašuji, že při tvorbě této práce jsem použil nástroj generativního modelu AI [ChatGPT; https://chat.openai.com] za účelem vytváření textu. Po použití tohoto nástroje jsem provedl kontrolu obsahu a přebírám za něj plnou zodpovědnost.

OBSAH

ÚVOD **9**

I TEORETICKÁ ČÁST **10**

1 KYBERNETICKÉ BEZPEČNOSTNÍ PŘEDPISY VE VYBRANÝCH ZEMÍCH **11**

1.1 Spojené Státy Americké 11

1.1.1 Zákon o zvýšení kybernetické bezpečnosti 11
1.1.2 Federální zákon o modernizaci bezpečnosti informací (FISMA) 12
1.1.3 Zákon o sdílení informací o kybernetické bezpečnosti (CISA) 13
1.1.4 Národní institut pro standarty a technologie (NIST) 14
1.1.5 Národní institut pro standarty a technologie (NIST) 2.0 16
1.1.6 Zákon o hlášení kybernetických incidentů pro kritickou infrastrukturu 18

1.2 Evropská únie 19

1.2.1 Obecné nařízení o ochraně osobních údajů (GDPR) 19
1.2.2 Směrnice o bezpečnosti sítí a informačních systémů (směrnice NIS) 20
1.2.3 Akt o kybernetické bezpečnosti 21
1.2.4 ePrivacy Regulation 21

1.3 Česká Republika 22

1.3.1 Zákon o kybernetické bezpečnosti (Act No. 181/2014 Coll.) 22

1.4 Srovnání přístupů k regulaci 23

1.5 Jak dodržovat kybernetické předpisy 23

II PRAKTICKÁ ČÁST **25**

2 NÁVRH NÁSTROJE PRO DODRŽOVÁNÍ KYBERNETICKÝCH PŘEDPISŮ **25**

2.1 Systém řízení bezpečnosti informací 25

2.2 Řízení aktiv 28

2.3 Řízení rizik 31

2.4 Organizační bezpečnost 33

2.5 Řízení dodavatelů 37

2.6 Další okruhy otázek 38

3 VÝVOJ MULTIPLATFORMNÍHO SOFTWARU **40**

3.1 Multiplatformní přístup 40

3.2 Front-end 40

3.3 Back-hand 45

4 ANALÝZA FUNKCÍ A SOUBORŮ NÁSTROJE **47**

4.1 Konfigurační soubor 48

4.1.1 Registrace a přihlášení uživatele 50
4.1.2 Analýza a algoritmus 51
4.1.3 Výpočet výsledné analýzy 53

5 NÁVRH A IMPLEMENTACE DATABÁZE....54
5.1 Návrh databáze....54
5.2 Šifrování databáze....55
6 BEZPEČNOSTNÍ A FUNKČNÍ TESTOVÁNÍ....58
6.1 Bezpečnostní testování....58
6.2 Funkční testování....60
7 BEZPEČNOSTNÍ MECHANISMY....63
7.1 Autentizace a autorizace....63
7.2 HTTPS....64
7.3 Cross-Site Request Forgery....64
7.4 Brute force attack....65
ZÁVĚR....67
SEZNAM POUŽITÉ LITERATURY....69
SEZNAM OBRÁZKŮ....72

ÚVOD

V dnešní digitální éře se kybernetická bezpečnost stává stále důležitějším aspektem pro organizace všech velikostí a odvětví. S neustálým vzrůstajícím počtem kybernetických hrozeb a přísnějšími legislativními požadavky se firmy musí aktivně snažit chránit své informační systémy a citlivá data. S nedostatkem kvalifikovaných odborníků zabývajících se ochranou firem proti kybernetickým útokům je stále naléhavější potřeba vyvíjet nástroje a technologie, které by mohly pomoci organizacím lépe porozumět a efektivněji reagovat na tyto výzvy.

Bakalářská práce se zabývá vytvořením nástroje, který pomůže firmám chránit se před kybernetickými útoky a zlepšit jejich kybernetickou bezpečnost. Cílem této práce je vyvinout multiplatformní software, který umožní organizacím efektivně analyzovat jejich kybernetické prostředí.

Teoretická část se zabývá kybernetickou bezpečností v dnešní době pro organizace a státy v Evropské unii a Spojených státech amerických. V téhle části jsou zkoumány klíčové legislativní dokumenty a předpisy v oblasti kybernetické bezpečnosti, které mají vliv na provoz a ochranu informačních systémů a dat. Cílem je porozumět jejich klíčovým prvkům, cílům a dopadům na organizace a společnosti, které se podílejí na dnešní digitální ekonomice.

V praktické části je popsán návrh nástroje, který organizacím by mohl pomoct s dodržováním těchto předpisů. Dále je popsán vývoj toho dle nástroje, multiplatformní řešení, zvolený programovací jazyk, popsání jednotlivých funkcí nástroje a zajištění multiplatformního přístupu. Poté je zde popsán vývoj uživatelského rozhraní pro širokou škálu uživatelů, otestování funkčnosti, bezpečnostní testování a popis bezpečnostních mechanismů a postupů, které zajistí, že nástroj bude chráněn před kybernetickými hrozbami.

I. TEORETICKÁ ČÁST

1 KYBERNETICKÉ BEZPEČNOSTNÍ PŘEDPISY VE VYBRANÝCH ZEMÍCH

V moderním digitálním prostředí je kybernetická bezpečnost klíčovým aspektem, který významně ovlivňuje globální i místní úroveň. Organizace a státy se stále potýkají s nedostatkem kvalifikovaných odborníků v této oblasti a neustálým nárůstem kybernetickým hrozeb a útoků, které ohrožují bezpečnost informačních systému a citlivých dat. Proto se v různých zemích vyvíjejí a uplatňují legislativní opatření a předpisy, které mají za cíl ochránit digitální infrastrukturu a minimalizovat tak rizika kybernetických útoků.

1.1 Spojené Státy Americké

Kybernetická bezpečnost ve Spojených státech tvoří základ pro ochranu digitální infrastruktury a citlivých dat v zemi. Její systém je složen z federálních, státních a odvětvových předpisů, které společně tvoří ochranu informačních systémů a sítí před kybernetickými hrozbami.

Federální úroveň vytváří politiky a strategie týkajících se kybernetické bezpečnosti. Agentury jako Národní institut pro standarty a technologie (NIST) a Úřad pro kybernetickou bezpečnost a infrastrukturu (CISA) vypracovávají směrnice, standardy a doporučení, které slouží jako ochrana kybernetické infrastruktury.

Na státní úrovni každý stát má své vlastní předpisy a iniciativy v oblasti kybernetické bezpečnosti, které mohou doplňovat federální právní předpisy nebo přinášet specifická opatření relevantní pro daný stát.

Odvětvové předpisy jsou zaměřeny na konkrétní odvětví, jako jsou finanční služby, zdravotnictví nebo energetika, upravují specifické požadavky a standardy pro kybernetickou bezpečnost v těchto oblastech. Tyto předpisy mohou být vytvářeny federálními agenturami nebo regulátory v daném odvětví.

1.1.1 Zákon o zvýšení kybernetické bezpečnosti

Základem předpisu o posílení kybernetické bezpečnosti je důraz na podporu inovací prostřednictvím značných investic do výzkumných a vývojových iniciativ. Vzhledem k dynamické povaze kybernetických rizik zákon vyčleňuje finanční prostředky na podporu

nejmodernějších technologií a metod kybernetické bezpečnosti. Tento proaktivní přístup zajišťuje, že Spojené státy zůstanou v čele pokroku v oblasti kybernetické bezpečnosti a budou schopny řešit vyvíjející se problémy.

Hlavním principem tohoto zákona je podpora spolupráce, která posiluje partnerství mezi vládními agenturami, soukromým průmyslem a akademickou obcí. Tento ekosystém spolupráce má vytvořit synergický přístup ke kybernetické bezpečnosti. Využitím silných stránek jednotlivých sektorů je cílem zlepšit sdílení informací, vypracovat společné strategie a společně posílit obranu země proti kybernetickým útokům.

Předpis o posílení kybernetické bezpečnosti si uvědomuje kritický nedostatek kvalifikovaných odborníků a přijímá opatření k řešení tohoto nedostatku. Zákon podporuje rozvoj pracovních sil prostřednictvím podpory vzdělávacích a školicích programů. Investováním do iniciativ, které vychovávají kvalifikovanou a znalou pracovní sílu, je cílem vytvořit silný kádr odborníků schopných zvládat dynamické výzvy, které kybernetický prostor představuje.

Za nedodržení tohodle předpisu firmy mohou čelit pokutám, správním opatřením, ztrátu licence nebo povolení, zveřejnění nedodržení, či jiné sankce. Tyto sankce jsou typicky stanoveny v u příslušného legislativního systému a mohou se lišit v závislosti na závažnosti porušení a opatřeních, která byla přijata jako k prevenci porušení zákona. [1]

1.1.2 Federální zákon o modernizaci bezpečnosti informací (FISMA)

Zákon o modernizaci federální informační bezpečnosti (Federal Information Security Modernization Act, FISMA) je základním kamenem pro vytvoření komplexního systému pro zajištění bezpečnosti federálních informačních systémů. FISMA se zabývá kritickými aspekty a představuje závazek k důkladným postupům kybernetické bezpečnosti.

Jádrem systému FISMA je přijetí přístupu založeného na rizicích prostřednictvím rámce řízení rizik (RMF). Tento přístup vyžaduje průběžné hodnocení a monitorování bezpečnostních kontrol. Federální agentury mají povinnost kategorizovat své informační systémy podle úrovně rizika, což umožňuje přizpůsobit bezpečnostní kontroly tak, aby odpovídaly konkrétním hrozbám a zranitelnostem.

FISMA klade velký důraz na průběžné monitorování informačních systémů. Tento proaktivní přístup je zásadní pro včasnou identifikaci a reakci na vznikající bezpečnostní hrozby. Pravidelná hodnocení jsou nedílnou součástí zajištění trvalého souladu se

Obrázek 1: *The Federal Information Security Management Act [2]*

zavedenými bezpečnostními standardy a pokyny a odrážejí závazek adaptace tváří v tvář rozvíjejícím se kybernetickým výzvám.

V rámci svého závazku k transparentnosti a odpovědnosti nařizuje systém FISMA federálním agenturám pravidelně podávat zprávy o stavu kybernetické bezpečnosti. Tento požadavek na podávání zpráv poskytuje komplexní přehled o účinnosti zavedených bezpečnostních opatření. FISMA navíc zavádí mechanismy odpovědnosti, které zajišťují, aby agentury v reakci na zjištěná zranitelná místa přijaly nezbytná opatření. [3]

1.1.3 Zákon o sdílení informací o kybernetické bezpečnosti (CISA)

Zákon o sdílení informací o kybernetické bezpečnosti (CISA) hraje klíčovou roli při podpoře spolupráce mezi vládou a organizacemi soukromého sektoru s cílem zlepšit celkovou kybernetickou bezpečnost.

CISA zavádí silné pobídky k podpoře sdílení indikátorů kybernetických hrozeb soukromými organizacemi. To zahrnuje poskytování právní ochrany, která zaručuje, že organizace, které sdílejí klíčové informace o kybernetické bezpečnosti, budou chráněny před právními následky. Zákon aktivně podporuje kulturu spolupráce prostřednictvím včasné výměny relevantních informací o kybernetických hrozbách mezi zúčastněnými stranami.

CISA uznává mimořádný význam soukromí jednotlivců a obsahuje ustanovení na ochranu osobních údajů. Před sdílením indikátorů kybernetických hrozeb zákon vyžaduje odstranění informací umožňujících identifikaci osob.

Obrázek 2: logo *zákonu o sdílení informací o kybernetické bezpečnosti [4]*

Kromě ustanovení podporujících spolupráci mezi vládou a soukromým sektorem zajišťuje CISA, že organizace soukromého sektoru mají právní jistotu při sdílení důležitých informací o kybernetické bezpečnosti. Důraz na ochranu osobních údajů a anonymizaci před sdílením indikátorů hrozeb je dalším klíčovým aspektem tohoto zákona, který odráží jeho ohleduplný přístup k ochraně soukromí jednotlivců.

CISA také klade důraz na vytvoření prostředí důvěry a spolupráce mezi organizacemi soukromého sektoru a vládními institucemi. Tímto způsobem se snaží maximalizovat efektivitu a účinnost v boji proti kybernetickým hrozbám a posiluje tak celkovou ochranu v tomto odvětví. [5]

1.1.4 Národní institut pro standarty a technologie (NIST)

NIST slouží jako klíčový průvodce pro organizace, které se snaží efektivně řídit rizika kybernetické bezpečnosti. Klade důraz na klíčové složky a poskytuje stručný, ale komplexní přístup k dokonalé kybernetické bezpečnosti.

Obrázek 3: Základní funkce *NIST*
[6]

Základem je 5 funkcí, které tvoří základ komplexního programu kybernetické bezpečnosti. Tyto funkce – identifikace, ochrana, detekce, reakce a zotavení zajišťuje komplexní a strategický přístup ke kybernetické bezpečnosti.
Identifikace pomáhá při vybudování organizačního porozumění řízení kybernetického rizika v systémech, lidech, aktivech, datech a schopnostech.

Ochrana je Funkce která popisuje vhodná opatření k zajištění dodávky kritických infrastrukturních služeb.

Detekce je funkce, která zahrnuje vypracování a implementaci vhodných aktivit k identifikaci výskytu kybernetické události.

Funkce reakce podporuje schopnost přijmout opatření ohledně zjištěné kybernetické události.

Obnova je funkce, která identifikuje vhodné aktivity k udržení plánů odolnosti a obnovení jakýchkoli schopností nebo služeb, které byly narušeny v důsledku kybernetické události.

NIST zavádí stupňovitý přístup k vyspělosti kybernetické bezpečnosti. Tento flexibilní model umožňuje organizacím hodnotit a zlepšovat jejich pozici v oblasti kybernetické bezpečnosti na základě jejich specifických potřeb a ochoty riskovat. Přestože NIST není povinný, jeho široké přijetí napříč odvětvími svědčí o jeho účinnosti. Organizace dobrovolně přijímají rámec jako osvědčený postup pro zvýšení odolnosti kybernetické bezpečnosti.

NIST není jenom dokument, ale také přední autorita ve vývoji a implementaci standardů a postupů kybernetické bezpečnosti. Jeho materiály poskytují podrobné pokyny, doporučení a nástroje, které organizacím pomáhají identifikovat, ochránit, detekovat, reagovat a zotavit se z kybernetických hrozeb a útoků.

NIST neustále aktualizuje své systémy a dokumenty, aby reflektovaly aktuální trendy a výzvy v oblasti kybernetické bezpečnosti. To znamená, že organizace, které se řídí NIST, mají přístup k nejnovějším informacím a postupům, které jim pomáhají zůstat krok před neustále se vyvíjejícími hrozbami.

Většina průmyslových odvětví a vládních agentur v USA používá NIST jako referenční bod pro své strategie a programy kybernetické bezpečnosti. Jeho flexibilita umožňuje širokou škálu organizací, od malých podniků až po velké korporace, přizpůsobit si svůj přístup k bezpečnosti podle svých potřeb a možností.

NIST je často spojován s konkrétními dokumenty, jako je například NIST Special Publication 800-53, který poskytuje rozsáhlý systém pro správu informační bezpečnosti v federálním sektoru. Tyto dokumenty jsou pečlivě navrženy tak, aby organizacím poskytovaly jasný a strukturovaný postup pro posílení své kybernetické obrany. [7]

1.1.5 Národní institut pro standarty a technologie (NIST) 2.0

Nová verze NIST 2 také nazývané jako Rámec kybernetické bezpečnosti NIST (CSF) 2.0 zavádí k původním pěti funkcím ještě šestou funkci "Řídit": Identifikace, ochrana, detekce, reakce a zotavení. Tato funkce zdůrazňuje význam výsledků souvisejících s řízením a zabývá se strategií, očekáváními a politikami řízení rizik kybernetické bezpečnosti. Tato změna znamená, že řízení přesahuje všechny ostatní funkce, a zdůrazňuje jeho klíčovou roli v efektivní kybernetické bezpečnosti.

CSF 2.0 je určen pro všechny cílové skupiny, průmyslová odvětví a typy organizací, od nejmenších škol a neziskových organizací až po největší agentury a korporace, a to bez ohledu na stupeň jejich vyspělosti v oblasti kybernetické bezpečnosti. Různým skupinám poskytuje na míru šité cesty k CSF a usnadňuje zavádění CSF 2.0 do praxe.

Dokumentace CSF 2.0 zahrnuje praktické prostředky, jako jsou příručky pro rychlý start, příklady implementace a katalogy mapování, které subjektům usnadňují přijetí tohoto rámce a jeho začlenění do běžné praxe.

Analýza případových studií je klíčovým prvkem pro pochopení praktické aplikace teoretických konceptů. Ukázkově může být středně velká technologická společnost, která implementovala CSF 2.0 jako součást své strategie kybernetické bezpečnosti. Tato implementace začala identifikací klíčových aktiv a jejich mapováním na funkce CSF 2.0, následovanou analýzou rizik a stanovením priorit.

Obrázek 4: *Národní institut pro standarty a technologie [8]*

Identifikace a správa dat jsou klíčové pro úspěšné zajištění kybernetické bezpečnosti. Firma by měla mít přehled o svých údajích a jejich umístění, což jí umožní efektivněji je chránit. Důležité je také schopnost hodnotit rizika a slabiny, abychom identifikovali potenciální nebezpečí a slabiny, které mohou ohrozit bezpečnost dat a informací.

Ochrana dat a informací je klíčová. Zajištění přístupu k nim pouze autorizovaným osobám a ochrana před zneužitím jsou základními kroky pro bezpečnostní strategii firmy. Provádění odborného vzdělávání zaměstnanců je dalším důležitým prvkem, který pomáhá vytvořit povědomí o bezpečnostních rizicích a postupech.

Bezpečnost IT infrastruktury je klíčová pro ochranu dat a informací. To zahrnuje nejen hardwarové a softwarové prvky, ale také aplikace, které jsou využívány pro zpracování a ukládání údajů. Správa dodavatelů IT služeb je důležitá pro sledování bezpečnosti poskytovaných cloudových služeb a dalších IT řešení, které firma využívá.

Prevence před útoky je důležitá pro minimalizaci rizika. Implementace opatření na ochranu proti útokům a schopnost rychle reagovat na incidenty jsou klíčové pro zachování integrity a bezpečnosti dat.

Zajištění obnovy provozu po útoku nebo havárii je rovněž důležité. Firma by měla být schopna rychle obnovit provoz a procesy, aby minimalizovala dopad na své operace.

Implementace směrnic informační bezpečnosti je zásadní pro definování a prosazení bezpečnostních politik a postupů. Neustálé zdokonalování bezpečnostních opatření a procesů je nezbytné, aby firma udržela krok s neustále se měnícími kybernetickými hrozbami a technologickým prostředím.

Výsledkem bylo efektivní řízení rizik kybernetické bezpečnosti a zlepšení ochrany proti kybernetickým hrozbám. Tento příklad ukazuje sílu a flexibilitu CSF 2.0 a jeho schopnost přizpůsobit se potřebám různých subjektů. [9]

1.1.6 Zákon o hlášení kybernetických incidentů pro kritickou infrastrukturu

Známý také jako zákon o hlášení kybernetických incidentů, nebo také (CIRCIA), je americký zákon, který organizacím kritické infrastruktury ukládá povinnost hlásit podstatné kybernetické incidenty Agentuře pro kybernetickou bezpečnost a bezpečnost infrastruktury (CISA) do 72 hodin. Tato povinnost se týká jakákoli událost, která může ohrozit integritu, dostupnost nebo důvěrnost kritických informací či systémů. Pokud je v reakci na kybernetický útok provedena platba výkupného, je organizace povinna ji nahlásit do 24 hodin, což zvyšuje důležitost rychlého a přesného vyhodnocení situace a následné reakce. [10]

Tento zákon je navržen tak, aby zlepšil celkovou americkou kybernetickou bezpečnost tím, že poskytuje systém pro rychlou reakci a koordinaci při kybernetických incidentech. Jedním z klíčových cílů je umožnit agentuře CISA rychle nasadit zdroje a poskytnout pomoc postiženým organizacím, což je zásadní pro minimalizaci škod způsobených kybernetickými útoky.

Dalším důležitým aspektem zákona je analýza příchozích hlášení napříč různými odvětvími, což umožňuje odhalit vzory a trendy v kybernetických hrozbách a rychle sdílet tyto informace s ostatními organizacemi pro lepší ochranu. [11]

Zákon rovněž uděluje CISA pravomoc předvolávat podniky, které neohlásí bezpečnostní incidenty nebo platby výkupného, což je další opatření směřující k zajištění účinného dodržování zákonů v oblasti kybernetické bezpečnosti. Tyto nové pravomoci však vyžadují, aby CISA dokončila povinné činnosti související s tvorbou pravidel předtím, než požadavky na hlášení vstoupí v platnost, což znamená, že se očekává transparentní a systematický postup při implementaci a dodržování těchto nových pravidel.

Tento program je také provázán z dalšími programy a iniciativami, které mají za cíl posílit obranyschopnost země proti kybernetickým hrozbám. Mezi tyto iniciativy může patřit například investice do výzkumu a vývoje v oblasti kybernetických technologií, posílení spolupráce mezi veřejným a soukromým sektorem v oblasti kybernetické bezpečnosti nebo vytváření lepších mechanismů pro sdílení informací o hrozbách a incidentech. Tyto

komplexní opatření mají za cíl vytvořit robustní a efektivní kybernetickou obranu, která bude schopna reagovat na stále se měnící hrozby a výzvy v digitálním prostředí. [12]

1.2 Evropská unie

Kybernetickou bezpečnost v Evropské unii upravuje řada legislativních opatření a směrnic, jejichž cílem je zajistit ochranu digitální infrastruktury a osobních údajů občanů EU. Jedním z klíčových dokumentů je obecné nařízení o ochraně osobních údajů (GDPR), které stanoví povinnosti týkající se ochrany a zpracování osobních údajů.

Dalším významným dokumentem je směrnice o bezpečnosti sítí a informačních systémů (směrnice NIS), která stanoví minimální požadavky na zajištění kybernetické bezpečnosti a národní strategie ochrany kritické infrastruktury v členských státech EU.

Kromě těchto legislativních opatření existuje v jednotlivých členských státech EU mnoho dalších iniciativ a strategií, které se zabývají specifickými aspekty kybernetické bezpečnosti v rámci jejich jurisdikce.

1.2.1 Obecné nařízení o ochraně osobních údajů (GDPR)

Obrázek 5: *Obecné nařízení o ochraně osobních údajů [13]*

Obecné nařízení o ochraně osobních údajů (GDPR) je klíčovým právním rámcem v oblasti ochrany osobních údajů v Evropské unii.

GDPR ukládá zdůrazněný důraz na ochranu dat a pomáhá firmám zachovávat soukromí a důvěrnost citlivých informací. Této zdůrazněné úrovně ochrany údajů je dosaženo tím, že firmy musí zavést přísná bezpečnostní opatření a záruky. Kromě toho nařízení GDPR vyžaduje, aby firmy specifikovaly, jaké údaje shromažďují, proč je shromažďují a jak je zpracovávají, čímž podporuje transparentnost, která může posílit důvěru zákazníků, což je

klíčový prvek pro růst podnikání. Dodržování nařízení GDPR nejen pomáhá vyhnout se významným pokutám, ale také prokazuje závazek společnosti k ochraně údajů. Nařízení zajišťuje práva subjektů údajů, včetně přístupu k jejich údajům, opravy, výmazu a dalších. Zavedením registru zpracování dat získávají firmy přehled o svých organizačních datech, což zvyšuje efektivitu podnikání a hodnotu investic do datové analytiky. GDPR nařizuje v případě porušení ochrany dat okamžitě informovat orgány a dotčené osoby, čímž posiluje bezpečnostní opatření, která potenciálně snižují počet případů porušení ochrany. Kromě toho GDPR upravuje přeshraniční předávání údajů, čímž zajišťuje, aby takové předávání dodržovalo ochranu osobních údajů mimo EU.

Klíčoví zaměstnanci ve firmě, zvláště ti, kteří pracují s osobními údaji, by měli být informováni o požadavcích GDPR a jejich významu. Školení zaměstnanců zvyšuje povědomí o bezpečnostních postupech a procesech pro zacházení s osobními údaji. [14]

Firma by měla provádět pravidelné audity svých datových procesů a dokumentovat veškeré osobní údaje, které shromažďuje, zpracovává a uchovává. To zahrnuje informace o způsobu shromažďování dat, jejich účelu a způsobu zpracování. GDPR také vyžaduje implementaci odpovídajících bezpečnostních opatření k zajištění důvěrnosti, integrity a dostupnosti těchto údajů. To zahrnuje informace o způsobu shromažďování dat, jejich účelu a způsobu zpracování. [15]

1.2.2 Směrnice o bezpečnosti sítí a informačních systémů (směrnice NIS)

Směrnice NIS je významným právním opatřením v rámci Evropské unie, jehož cílem je zvýšit celkovou úroveň kybernetické bezpečnosti v členských státech. Směrnice o bezpečnosti sítí a informací, která byla přijata v srpnu 2016, představuje první legislativní akt EU zaměřený konkrétně na kybernetickou bezpečnost a tvoří nedílnou součást širší politiky a strategií Unie v oblasti kybernetické bezpečnosti. Jejím hlavním cílem je zajistit vysokou společnou úroveň bezpečnosti síťových a informačních systémů v celé Unii, přičemž se zohledňuje vzájemná propojenost těchto systémů a potenciální rozsáhlé dopady narušení. Směrnice ukládá povinnost zavést vhodná bezpečnostní opatření, která zahrnují jak kybernetickou, tak fyzickou odolnost, a zdůrazňuje tak nezbytnost ochrany síťových a informačních systémů.

Zavedení směrnice NIS 2 v lednu 2023 navíc dále posiluje rámec kybernetické bezpečnosti EU tím, že zavádí požadovanou strukturu kybernetického krizového řízení. Pro firmy

dodržování směrnice NIS vyžaduje pečlivá bezpečnostní opatření na ochranu síťových a informačních systémů, čímž se snižuje riziko narušení bezpečnosti dat a zajišťuje integrita systému.

Transparentnost činností při zpracování údajů navíc posiluje důvěru zákazníků a zúčastněných stran, zatímco dodržování právních předpisů zabraňuje možným sankcím a zdůrazňuje závazek firmy k ochraně údajů. Vedením registru činností zpracování dat mohou firmy získat cenné informace o svém datovém prostředí, což usnadňuje efektivnější obchodní operace a účinnou analýzu dat. [16]

1.2.3 Akt o kybernetické bezpečnosti

Akt o kybernetické bezpečnosti je významným právním krokem v rámci Evropské unie, jehož cílem je zvýšit celkovou úroveň kybernetické bezpečnosti v členských státech. Na základě tohoto aktu byla posílena Agentura Evropské unie pro kybernetickou bezpečnost (ENISA), která získala trvalý mandát, větší zdroje a další úkoly. Agentura ENISA přebírá klíčovou úlohu při vytváření a udržování evropského certifikačního rámce kybernetické bezpečnosti, což je základní iniciativa zavedená aktem o kybernetické bezpečnosti.

Tento rámec zahrnuje celoevropský mechanismus certifikace produktů, služeb a procesů IKT, který zjednodušuje certifikační procesy pro společnosti působící v EU a usnadňuje uznávání certifikátů v celé Unii. Navrhovaná změna zákona o kybernetické bezpečnosti navíc rozšiřuje jeho působnost na řízené bezpečnostní služby, které zahrnují oblasti, jako je reakce na incidenty, penetrační testy, bezpečnostní audity a poradenství.

Firmám dodržování zákona o kybernetické bezpečnosti ukládá povinnost zavést pečlivá bezpečnostní opatření k ochraně síťových a informačních systémů, a tím posílit obranu proti narušení bezpečnosti dat a zachovat integritu systému. Transparentnost činností souvisejících se zpracováním údajů navíc posiluje důvěru zákazníků a zúčastněných stran, zatímco dodržování právních předpisů zdůrazňuje oddanost firmy ochraně údajů. [17]

1.2.4 ePrivacy Regulation

Cílem nařízení o ochraně soukromí a elektronických komunikací, které je navrhováno v rámci Evropské unie, je zvýšit normy ochrany soukromí a zajistit osobní údaje v elektronické komunikaci. Mezi jeho klíčové aspekty patří rozšíření působnosti na nově vznikající poskytovatele služeb elektronických komunikací a zajištění rovnocenných standardů důvěrnosti napříč různými komunikačními platformami. Kromě toho nařízení

slibuje přísnější předpisy o ochraně soukromí, které by jednotlivcům a podnikům poskytovaly jednotnou ochranu v celé EU. Záruky ochrany soukromí se týkají jak obsahu komunikace, tak metadata, s ustanoveními o anonymizaci nebo vymazání metadat bez souhlasu uživatele. Kromě toho se nařízení zaměřuje na zjednodušení ustanovení o souborech cookie a posiluje kontrolu uživatelů nad sledovacími soubory cookie prostřednictvím nastavení prohlížeče. [18]

Pro firmy znamená dodržování předpisů zavedení pečlivých bezpečnostních opatření k posílení síťových a informačních systémů, čímž se zabrání narušení bezpečnosti údajů a zachová se integrita systému. Transparentnost činností zpracování údajů je povinná, což posiluje důvěru zákazníků a zúčastněných stran, zatímco dodržování předpisů zdůrazňuje závazek k ochraně údajů. Nařízení o ochraně soukromí a elektronických komunikací nakonec přesahuje rámec dodržování právních předpisů a podporuje kulturu ochrany soukromí v organizacích. Přijetím jeho směrnic mohou firmy posílit svůj postoj k ochraně soukromí, zvýšit důvěru zákazníků, optimalizovat provoz a podpořit obchodní růst. [19]

1.3 Česká republika

Česká republika implementuje řadu mezinárodních a evropských předpisů týkajících se kybernetické bezpečnosti, včetně GDPR a směrnice NIS.

1.3.1 Zákon o kybernetické bezpečnosti (Act No. 181/2014 Coll.)

Zákon o kybernetické bezpečnosti je klíčovým předpisem v České republice, který určuje právní rámec pro kybernetickou bezpečnost. Zákon stanovuje práva a povinnosti jednotlivců a pravomoci veřejných institucí v oblasti kybernetické bezpečnosti. Jeho účelem je zajistit bezpečnost v kybernetickém prostoru prostřednictvím definice povinností a nástrojů pro ochranu kybernetické infrastruktury. Společnosti jsou povinny dodržovat tento zákon. Nedodržení tohoto předpisu může mít za následek pokuty nebo právní postihy. Dále společnosti musí implementovat robustní bezpečnostní opatření k ochraně citlivých dat. To může zahrnovat šifrování dat, použití silných hesel a pravidelné aktualizace softwaru.

Zákon také vyžaduje, aby společnosti byly transparentní ohledně svých aktivit v oblasti zpracování dat, plány pro reakci na bezpečnostní incidenty, což zahrnuje také hlášení incidentů příslušným úřadům a informování postižených jedinců. V neposlední řadě by také společnosti měly hodnotit své bezpečnostní postupy a provádět potřebné úpravy, aby zůstaly v souladu s měnícími se předpisy a hrozbami. [20]

1.4 Srovnání přístupů k regulaci

Srovnání přístupů k regulaci nebo také nazývané harmonizaci předpisů o kybernetické bezpečnosti je proces, který se snaží sjednotit a standardizovat právní rámce různých zemí. Cílem je snížit složitost a náklady na dodržování pro firmy a zároveň zvýšit účinnost a efektivitu ochrany kybernetické bezpečnosti.

Globální harmonizace kybernetických předpisů je stále v procesu a je předmětem diskuse na různých úrovních. Existují určité kroky směrem k harmonizaci, ale je zde také mnoho výzev, které je třeba překonat.

Různé jurisdikce mohou mít odlišné definice kybernetického incidentu a požadavky na hlášení, což vede k nejednoznačnosti a zmatku. Existují také rozdíly v časových rámcích a spouštěčích pro hlášení incidentů a v rychlosti, jakou je třeba incident nahlásit. Dále, různé jurisdikce mohou požadovat různé úrovně detailů v hlášeních o incidentech a mohou mít odlišné mechanismy pro hlášení. Zatímco regulační nezávislost je zásadním principem tvorby pravidel, přispívá k obtížím při dosažení harmonizace. [21]

Kybernetické předpisy se staly složitými, nákladnými a obtížně se zabezpečují kvůli síti národních a regionálních předpisů, které se vyvinuly v posledních letech. Firmy se také musí vyrovnávat se složitými a nákladnými procesy pro splnění povinností v rámci různých jurisdikcí. [22]

1.5 Jak dodržovat kybernetické předpisy

V první řadě je pro firmu důležité porozumět jednotlivým nařízením o kybernetické bezpečnosti, která se na firmu vztahují, a pochopit, jak je dodržovat, aby nedocházelo k pokutám, které hrozí za nedodržení těchto nařízení.

V první řadě je pro firmu důležité porozumět jednotlivým nařízením o kybernetické bezpečnosti, která se na firmu vztahují, a pochopit, jak je dodržovat, aby nedocházelo k pokutám, které hrozí za nedodržení těchto nařízení. FISMA vyžaduje, aby federální agentury implementovaly komplexní rámec pro zabezpečení informací, který je založen na NIST normách. Pro dodržování NIST standardů poskytuje tento rámec soubor standardů a pokynů, které organizace mohou použít k zajištění bezpečnosti svých informačních systémů. Dále NIST požaduje, aby organizace prováděly hodnocení rizik, zavedly politiky

a postupy pro zabezpečení informací a zajistily školení zaměstnanců v oblasti bezpečnosti informací. [23]

Certifikace CISA se koná dvakrát ročně (v červnu a prosinci) ve více než 220 městech po celém světě. Pro úspěšné získání certifikátu je nutné také prokázat 5letou praxi v oblasti auditu, řízení a bezpečnosti informačních systémů. Držitelé CISA musí dodržovat etický kodex ISACA a jsou zodpovědní za své kontinuální vzdělávání v oboru. [24]

Abychom dodrželi akt o kybernetické odolnosti, existuje 6 pravidel, která opakují směrnici NIS 2. Tedy pokud dodržujeme NIS 2, dodržujeme i akt o kybernetické bezpečnosti. [26]

Dodržování pravidel ePrivaci Regulation, firmy by měly tyto důležité aspekty. Všechny osoby a firmy v EU budou mít stejnou úroveň ochrany svých elektronických komunikací. Pro obsah komunikace a metadat je nutné zaručit soukromí. Další pravidlo se týče ochrany proti spamu, tedy zákazu nevyžádané elektronické komunikace e-mailem, SMS a automatizovanými volacími stroji. Pravidla soukromí se také vztahují na služby jako je WhatsApp, Facebook, Messenger a Skype. [27]

II. PRAKTICKÁ ČÁST

2 NÁVRH NÁSTROJE PRO DODRŽOVÁNÍ KYBERNETICKÝCH PŘEDPISŮ

V následující kapitole je popsán postup návrhu nástroje pro dodržování kybernetických předpisů. Pro začátek vývoje tohoto nástroje bylo nejdůležitější určení jeho základních principů a funkčnosti. Muselo se rozhodnout, jaké otázky budou klíčové pro výpočet celkové úrovně zabezpečení proti kybernetickým hrozbám a jakým způsobem bude algoritmus pracovat.

Pro tento účel byla vybrána Vyhláška č. 82/2018 Sb., která se zaměřuje přímo na bezpečnostní incidenty, opatření, reaktivní opatření a kontaktní údaje. Tato vyhláška poskytuje komplexní rámec pro identifikaci a řízení kybernetických rizik, což ji činí vhodným základem pro náš nástroj.

2.1 Systém řízení bezpečnosti informací

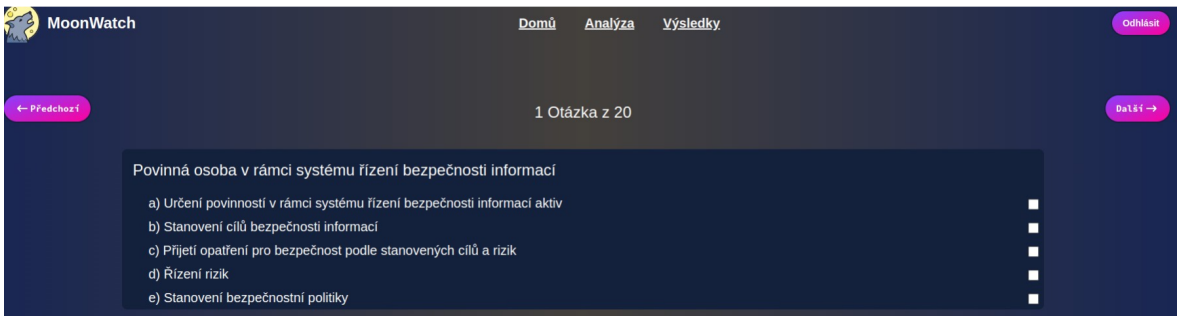
První otázka v nástroji spadá do kategorie organizačních opatření a týče se povinné osoby, která ve firmě řídí bezpečnost informací. Je nutno si stanovit rozsah systému řízení bezpečnosti informací. Tedy povinná osoba určuje, jaké části organizace a které informace,

technologie a procesy budou zahrnuty do systému řízení bezpečnosti informací. Při stanovení rozsahu se berou také v úvahu požadavky všech dotčených stran, což mohou být například zákazníci, zaměstnanci, dodavatelé nebo také organizační orgány. Povinná osoba také zohledňuje interní organizační strukturu a procesy a určuje, jak bude mít systém řízení bezpečnosti informací vliv na jednotlivé části organizace. To zahrnuje identifikaci týmů, oddělení, procesů a aktiv, které budou mít svou roli a odpovědnost v systému řízení bezpečnosti informací.

Další část téhle otázky se zaměřuje na stanovení cílů pro systém řízení bezpečnosti informací. Povinná osoba identifikuje konkrétní cíle, které chce dosáhnout pomocí systému řízení bezpečnosti informací. Tyto cíle by měly být měřitelné, relevantní a dosažitelné. Mohou zahrnovat snížení rizik, ochranu citlivých dat nebo například; zlepšení odolnosti vůči kybernetickým hrozbám.
Další část otázky se zabývá implementací bezpečnostních opatření na základě stanovených cílů. Povinná osoba definuje, jaké části organizace a aktiva budou zahrnuty do systému řízení bezpečnosti informací. To zahrnuje určení rozsahu a aplikace bezpečnostních opatření. Implementace bezpečnostních opatření by měla být informována hodnocením rizik, které identifikuje potenciální hrozby a zranitelnosti a posuzuje jejich dopady a pravděpodobnosti. Bezpečnostní opatření by měla být navržena tak, aby minimalizovala nebo eliminovala identifikovaná rizika.

Povinná osoba také musí vytvořit a schválit bezpečnostní politiku, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací. Na základě bezpečnostních potřeb a výsledků hodnocení rizik povinná osoba stanoví bezpečnostní politiku i pro další oblasti a zavede přiměřená bezpečnostní opatření.

Otázka vždy obsahuje pět položek, jak je vidět na (Obr. 6), na které uživatel odpovídá pomocí zakliknuti checkboxu. Každá položka má své hodnocení, které vychází z toho, jak důležitá je tato položka v rámci organizačních opatření firmy.



Obrázek 6: Ukázka první otázky v nástroji

Hodnocení každé otázky spadá tedy do tří kategorií. Hodnocení je označeno písmeny A, B, C. Písmeno A znamená, že na otázku bylo zodpovězeno kladně, a tedy znamená plusové skóre, které se pak přičítá do celkového vyhodnocení. B naopak je záporně zodpovězená otázka a odečítá se z celkového vyhodnocení bod. Písmeno C spadá do kategorie, kdy je porušena velmi důležitá položka, která má značný vliv na porušení kybernetické bezpečnosti ve firmách. Taková otázka může být například "Přijetí opatření pro bezpečnost podle stanovených cílů a rizik". Výsledkem bude, že uživatel neprojde vyhodnocovacím algoritmem.

Volba písmen A, B, C bylo také z důvodu, aby nedocházelo k složitým výpočtům, která mohou nastat, kdybychom použili číslice. V algoritmu se budou počítat množství písmen a podle nich se vyhodnotí celkový výsledek analýzy. Použití číselných hodnot bychom mohli dojít do záporných hodnot, nebo u vážného porušení by stanovená konstanta nemusela vyhovovat celkovému vyhodnocení, a tak by nesplnila svůj účel. Použití písmen umožňuje jednoduchý a přehledný způsob vyhodnocení, který minimalizuje riziko chyb při výpočtech. Tímto způsobem můžeme snadněji sledovat a interpretovat výsledky analýzy a efektivněji reagovat na potřebné úpravy nebo změny.

Druhá otázka se zabývá taktéž bezpečnosti informací ve firmách. Firmy by měli provádět audity kybernetické bezpečnosti. Audit by měl být prováděn pravidelně a slouží k posouzení úrovně bezpečnosti systému a identifikaci případných nedostatků.

Povinná osoba musí také provádět pravidelné vyhodnocování účinnosti systému řízení bezpečnosti informací. Toto vyhodnocování zahrnuje revizi hodnocení rizik, posouzení výsledků provedených auditů kybernetické bezpečnosti a zhodnocení dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací. Tahle položka je velmi důležitá. Tato činnost je velmi důležitá, protože poskytuje klíčové informace o aktuálním stavu kybernetické bezpečnosti a umožňuje identifikaci oblastí, které vyžadují zlepšení.

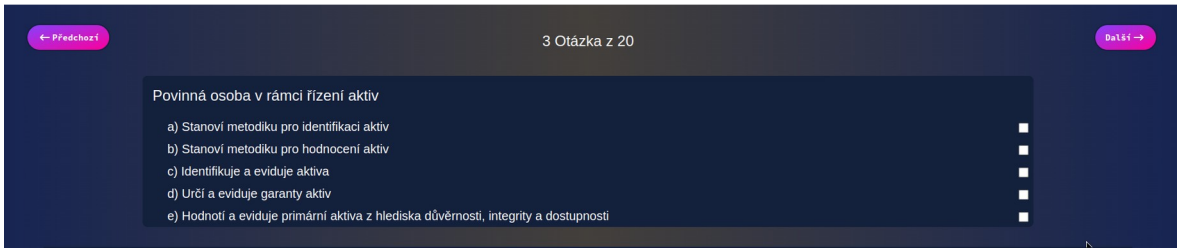
Řízení významných změn povinná osoba musí průběžně identifikovat a řídit významné změny, které patří do rozsahu systému řízení bezpečnosti informací. Tyto změny mohou ovlivnit bezpečnost informačních aktiv a je důležité je řídit tak, aby byla zachována úroveň bezpečnosti.

Aktualizace systému povinná osoba musí provádět pravidelně a také vést příslušnou dokumentaci. Tyto aktualizace jsou založeny na zjištěních z auditů kybernetické

bezpečnosti, vyhodnocení účinnosti systému a v souvislosti s prováděnými významnými změnami.

Povinná osoba musí řídit provoz a zdroje systému řízení bezpečnosti informací a zaznamenávat činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik. Tím se zajišťuje efektivní fungování systému a správa zdrojů pro dosažení stanovených bezpečnostních cílů. [28]

2.2 Řízení aktiv



Obrázek 7: Ukázka otázky pro řízení aktiv

Stanovení řízení aktiv je důležitou částí vyhodnocení analýzy (Obr. 7). Povinná osoba se zabývá správou a ochranou organizace. Každá položka otázky se zaměřuje na specifickou činnost spojenou s řízení aktiv.

Stanovení metodiky pro identifikaci aktiv stanovuje povinná osoba, cílem je určit jak identifikovat aktiva organizace. Identifikace aktiv je důležitá pro správné pochopení toho, co organizace vlastní a co je třeba chránit. Dobrá metodika pro identifikaci aktiv umožňuje efektivní správu a ochranu aktiv.

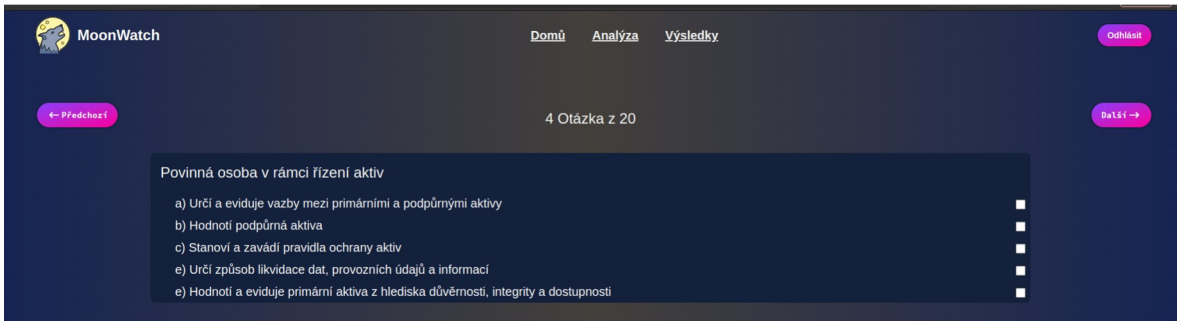
Stanovení metodiky pro hodnocení aktiv stanoví poviná osoba, která obsahuje posouzení jejich hodnot, rizik a významu organizace. Tato činnost pomáhá prioritizovat ochranná opatření a alokovat zdroje na základě důležitosti jednotlivých aktiv.

Povinná osoba identifikuje a eviduje veškerá aktiva organizace. To zahrnuje nejen fyzická aktiva jako zařízení a vybavení, ale i nehmotná aktiva jako informace, data a duševní vlastnictví. Jedná se o velmi důležitou položku v otázce, protože správná identifikace a evidence aktiv je základem pro úspěšné řízení a ochranu.

Povinná taktéž osoba určuje a eviduje garanty aktiv, tedy osoby nebo subjekty, které jsou zodpovědné za správu a ochranu konkrétních aktiv. Zajištění jasných rolí a odpovědností

pomáhá zajistit účinné řízení aktiv a minimalizuje rizika spojená s jejich nedostatečnou ochranou.

Hodnocení a evidence primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti je položka která je velmi důležitá. Povinná osoba hodnotí a eviduje primární aktiva z hlediska tří základních principů kybernetické bezpečnosti a to je důvěrnosti, integrity a dostupnosti. Tato činnost je velmi důležitá, protože pomáhá identifikovat a adresovat případné nedostatky v ochraně aktiva a minimalizuje riziko jejich neoprávněného přístupu, poškození nebo nedostupnosti.



Obrázek 8: Otázka *č.4 řízení aktiv*

Určení a evidence vazeb mezi primárními a podpůrnými aktivy (Obr. 8) určuje a eviduje povinná osoba vazby mezi primárními a podpůrnými aktivy organizace. To zahrnuje identifikaci závislostí mezi různými aktivy a určení jejich vzájemného vztahu. Tato činnost pomáhá organizaci lépe porozumět tomu, jak jsou aktiva propojena a jaké jsou důsledky jejich změn.

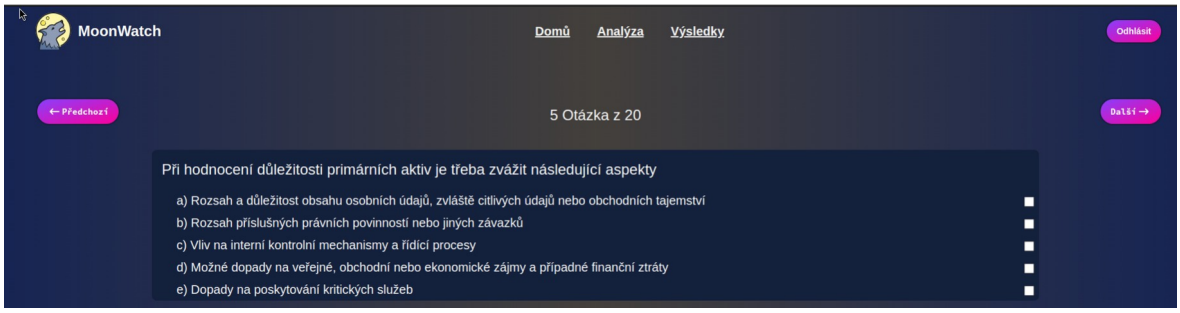
Hodnocení podpůrných aktiv hodnotí povinná osoba podpůrná aktiva, což jsou ta, která nepřímo podporují primární aktiva organizace. Hodnocení těchto aktiv je důležité pro posouzení jejich důležitosti a významu pro organizaci a pro stanovení adekvátních opatření k jejich ochraně.

Stanovení a zavedení pravidel ochrany aktiv stanovuje a zavádí povinná osoba pro ochranu aktiv organizace. Tato pravidla určují, jak mají být aktiva chráněna, jaké bezpečnostní opatření mají být uplatněna a jaké jsou příslušné postupy pro zacházení s nimi. Velký důraz je kladen na zajištění důvěrnosti, integrity a dostupnosti aktiv.

Stanovení přípustných způsobů používání aktiv stanoví a zavádí povinná osoba přípustné způsoby používání aktiv organizace. To zahrnuje definici pravidel a omezení pro užívání

aktiv a určení, jaké činnosti jsou povoleny a jaké jsou zakázány. Cílem je minimalizovat riziko neoprávněného nebo nevhodného použití aktiv.

Povinná osoba také určuje způsob, jak mají být data, provozní údaje a informace likvidovány, pokud už nejsou potřebné. To zahrnuje stanovení postupů pro bezpečné a trvalé odstranění nebo zneškodnění dat a informací tak, aby nedošlo k jejich neoprávněnému získání nebo zneužití po skončení jejich životního cyklu.



Obrázek 9: Otázka *Hodnocení primárních aktiv*

Rozsah a důležitost obsahu osobních údajů (Obr. 9), zvláště citlivých údajů nebo obchodních tajemství se zaměřuje na to, jaký obsah aktiv obsahuje, zejména pokud jde o osobní údaje, a zda jsou mezi nimi citlivé informace nebo obchodní tajemství. Hodnocení důležitosti těchto informací je klíčové pro stanovení úrovně ochrany a bezpečnostních opatření.

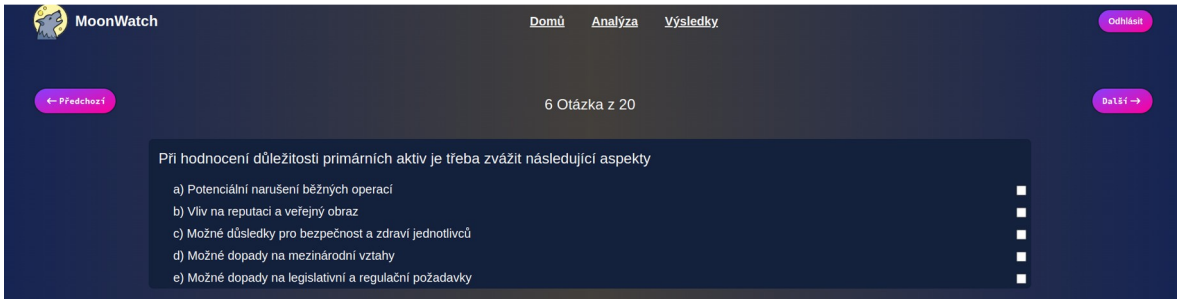
Při hodnocení důležitosti aktiv je důležité zohlednit veškeré právní povinnosti a závazky, které organizace musí dodržovat. To může zahrnovat dodržování právních předpisů v oblasti ochrany dat, průmyslového vlastnictví nebo jiných právních norem.

Vliv na interní kontrolní mechanismy a řídící procesy se zabývá tím, jaký vliv má dané aktivum na interní kontrolní mechanismy a řídící procesy organizace. Hodnocení této oblasti pomáhá identifikovat potenciální slabiny v kontrolních mechanismech a procesech a zlepšit jejich účinnost.

Při posuzování důležitosti aktiv je důležité zvážit jejich možné dopady na veřejné, obchodní nebo ekonomické zájmy. To může zahrnovat potenciální finanční ztráty nebo reputační škody, které by mohly nastat v důsledku ohrožení těchto aktiv.

Dopady na poskytování kritických služeb znamená, jaký má vliv na dané aktivum na poskytování kritických služeb organizace. Hodnocení této oblasti pomáhá identifikovat

klíčové aktivity, které jsou nezbytné pro chod organizace a pro ochranu těchto aktiv před možnými hrozbami a riziky.



Obrázek 10: Otázka *hodnocení primárních aktiv*

Potenciální narušení běžných operací (Obr. 10) zkoumá, jaké důsledky by mělo poškození nebo ztráta klíčových aktiv na běžné operace organizace. Jedná se o posouzení, jakým způsobem by takové události mohly ovlivnit rutinní činnosti a procesy a jaké by byly jejich možné dopady.

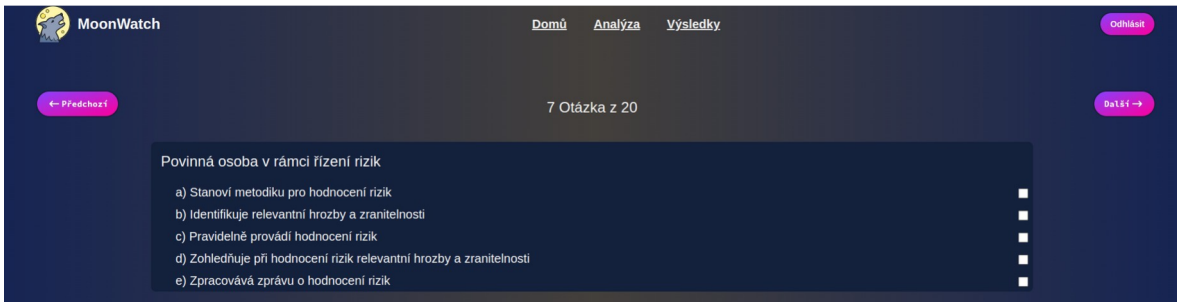
Vliv na reputaci a veřejný obraz analyzuje, jaký by mohl mít poškození či ztráta klíčových aktiv vliv na pověst a vnímání organizace ze strany veřejnosti a zainteresovaných stran. Jedná se o posouzení rizika pro pověst společnosti a potenciálních důsledků pro její veřejný obraz.

Možné důsledky pro bezpečnost a zdraví jednotlivců se zaměřuje na zhodnocení, jaké by mohlo mít poškození klíčových aktiv dopady na bezpečnost a zdraví jednotlivců spojených s organizací. Posuzuje se potenciální riziko pro bezpečnost a zdraví zaměstnanců, zákazníků nebo jiných osob spojených s činnostmi organizace.

Položka možné dopady na mezinárodní vztahy se zaměřuje, jaké by mohly být důsledky poškození nebo ztráty klíčových aktiv na mezinárodní spolupráci a vztahy s jinými subjekty nebo zeměmi. Zohledňuje se možný vliv na obchodní vztahy, diplomatické interakce a mezinárodní reputaci organizace.

Možné dopady na legislativní a regulační požadavky je položka, která se zabývá posouzením, jaké by mohly být důsledky poškození klíčových aktiv pro dodržování platných právních předpisů a regulací. Zjišťuje se, jakým způsobem by takové události mohly ovlivnit právní prostředí, v němž organizace působí, a jak by mohly ovlivnit její povinnosti a závazky vůči regulátorům a legislativním orgánům. [28]

2.3 Řízení rizik



Obrázek 11: Otázka *řízení rizik*

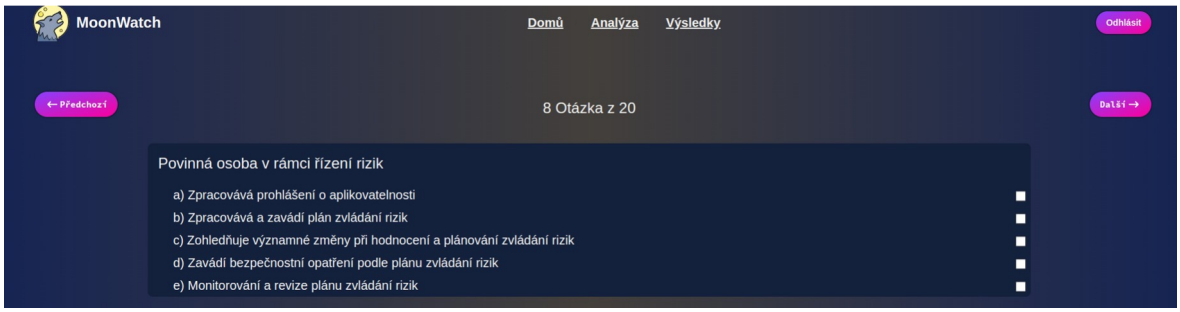
Stanovení metodiky pro hodnocení rizik (Obr. 11) je fáze, která zahrnuje definici postupů a metod pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik. Metodika by měla být komplexní a zahrnovat procesy pro identifikaci, analýzu a hodnocení rizik.

Identifikace relevantní hrozby a zranitelnosti identifikuje povinná osoba, které by mohly ohrozit bezpečnost informací a systémů organizace. Zohledňuje přitom nejen vnější hrozby, ale také interní nedostatky a slabiny, které mohou vést k rizikům.

Pravidelné provádění hodnocení rizik je činnost, která zahrnuje pravidelné provádění hodnocení rizik s cílem aktualizovat informace o aktuálních bezpečnostních hrozbách a zranitelnostech. Pravidelné hodnocení je klíčové pro udržení aktuálnosti a účinnosti opatření pro řízení rizik.

Zohledňuje při hodnocení rizik relevantní hrozby a zranitelnosti povinná osoba bere v úvahu relevantní hrozby a zranitelnosti v souladu s identifikovanými bezpečnostními potřebami. To zahrnuje posouzení možných dopadů těchto hrozeb a zranitelností na aktiva organizace.

Na základě provedeného hodnocení povinná osoba připravuje zprávu obsahující výsledky identifikace a analýzy rizik, jejich prioritizaci a doporučená opatření pro jejich řízení. Zpráva slouží jako podklad pro rozhodování a plánování bezpečnostních opatření v organizaci.



Obrázek 12: Otázka *řízení rizik*

Povinná osoba připravuje prohlášení (Obr. 12) o aplikovatelnosti, které obsahuje přehled bezpečnostních opatření požadovaných touto vyhláškou. Prohlášení identifikuje, která opatření byla aplikována a jakým způsobem, a která nebyla aplikována, a to včetně důvodů pro neaplikování.

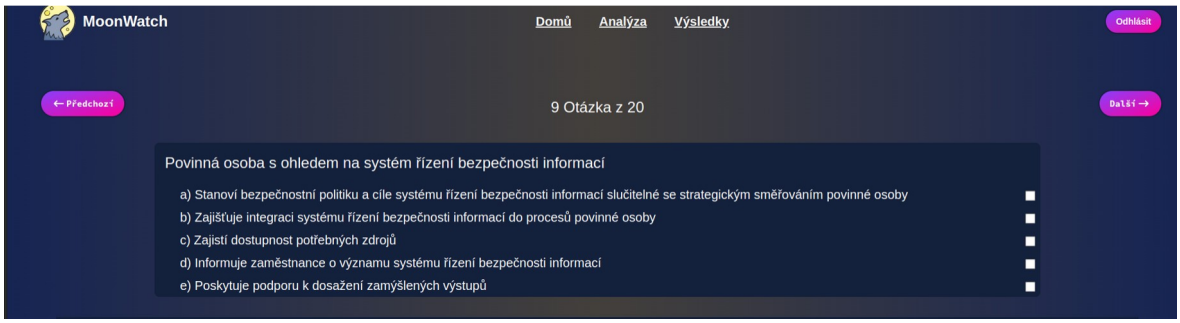
Povinná osoba také připravuje a implementuje plán zvládání rizik, který obsahuje stanovení cílů a přínosů bezpečnostních opatření pro zvládání jednotlivých rizik. Plán specifikuje potřebné zdroje a termíny zavedení bezpečnostních opatření, a také popisuje vazby mezi riziky a příslušnými opatřeními.

Při hodnocení rizik a plánování zvládání rizik povinná osoba bere v úvahu významné změny, které mohou ovlivnit bezpečnostní prostředí organizace. Tato činnost zahrnuje aktualizaci plánu zvládání rizik v souladu s novými informacemi a podmínkami.

Zavádění bezpečnostních opatření podle plánu zvládání rizik implementuje povinná osoba bezpečnostní opatření v souladu s plánem zvládání rizik. To zahrnuje realizaci konkrétních opatření určených k řešení identifikovaných rizik a minimalizaci jejich dopadů na organizaci.

Monitorování a revize plánu zvládání rizik povinná osoba pravidelně monitoruje účinnost a implementaci bezpečnostních opatření specifikovaných v plánu zvládání rizik. V případě potřeby provádí revize plánu a upravuje ho tak, aby reflektoval aktuální bezpečnostní potřeby a hrozby. [28]

2.4 Organizační bezpečnost



Obrázek 13: Otázka *organizační bezpečnost*

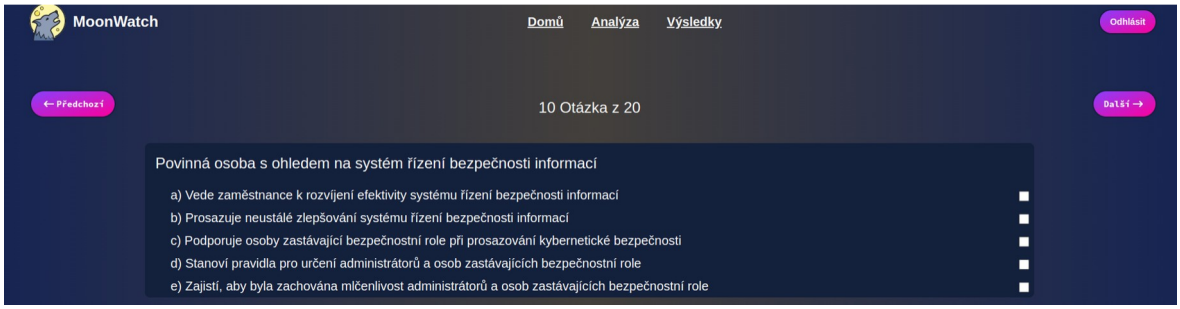
Povinná osoba vypracovává bezpečnostní politiku (Obr. 13) a stanoví cíle systému řízení bezpečnosti informací, které jsou v souladu se strategickými cíli a směřováním organizace. Tato politika a cíle poskytují rámec pro ochranu informací a zajišťují soulad s obecnými cíli a hodnotami organizace.

Povinná osoba také zajistí, že systém řízení bezpečnosti informací je účinně integrován do všech procesů a činností organizace. To zahrnuje začlenění bezpečnostních opatření a postupů do každodenních pracovních procesů a provádění pravidelných kontrol a revizí.

Povinná osoba taktéž zajistí, že jsou k dispozici potřebné zdroje pro úspěšnou implementaci a provoz systému řízení bezpečnosti informací. To může zahrnovat financování, personál, technologie a další podpůrné prostředky nezbytné k dosažení stanovených cílů bezpečnosti informací.

Povinná osoba zajišťuje, že zaměstnanci jsou informováni o důležitosti a významu systému řízení bezpečnosti informací pro organizaci. To zahrnuje poskytování školení, komunikaci a informační kampaně, které pomáhají zaměstnancům porozumět jejich rolím a odpovědnostem v rámci ochrany informací.

Povinná osoba poskytuje podporu a pomoc všem členům organizace, aby mohli dosáhnout stanovených cílů a výsledků systému řízení bezpečnosti informací. To může zahrnovat poskytování poradenství, sdílení osvědčených postupů a podpora při implementaci bezpečnostních opatření.



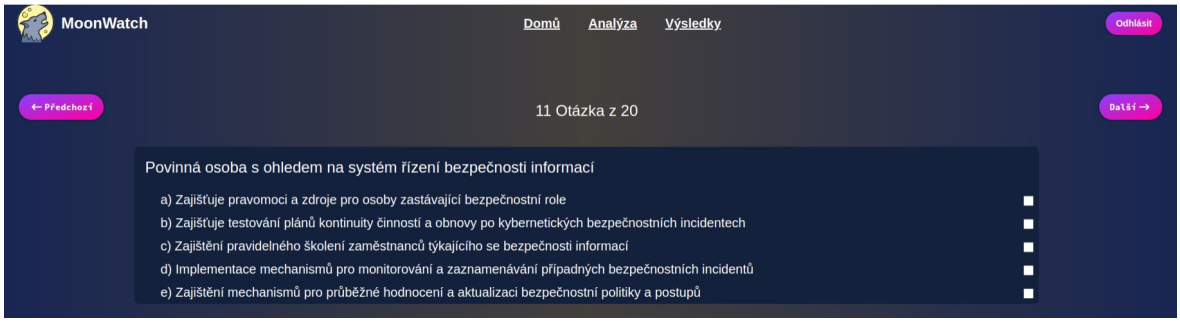
Obrázek 14: Otázka *organizační bezpečnost*

Povinná osoba aktivně podporuje zaměstnance (Obr. 14) v jejich úsilí o zvyšování efektivity systému řízení bezpečnosti informací. To zahrnuje poskytování školení, sdílení osvědčených postupů a podporu při implementaci bezpečnostních opatření s cílem posílit povědomí o bezpečnostních rizicích a zlepšit ochranu informací.

Povinná osoba aktivně podporuje kulturu neustálého zlepšování systému řízení bezpečnosti informací. To zahrnuje identifikaci slabých míst, analýzu incidentů a implementaci nápravných opatření s cílem zvyšovat odolnost organizace vůči kybernetickým hrozbám a zlepšovat celkovou bezpečnostní situaci.

Povinná osoba taktéž aktivně podporuje osoby zastávající bezpečnostní role v organizaci při jejich úsilí o prosazování kybernetické bezpečnosti. To zahrnuje poskytování zdrojů, školení a motivaci pro úspěšné plnění jejich úkolů a povinností v oblasti kybernetické bezpečnosti.

Povinná osoba stanovuje jasná pravidla a postupy pro určení administrátorů a osob zastávajících bezpečnostní role v organizaci. To zahrnuje definici jejich povinností, odpovědností a pravomocí, stejně jako postupy pro jejich výběr, školení a dohled.



Obrázek 15: Otázka *organizační bezpečnost*

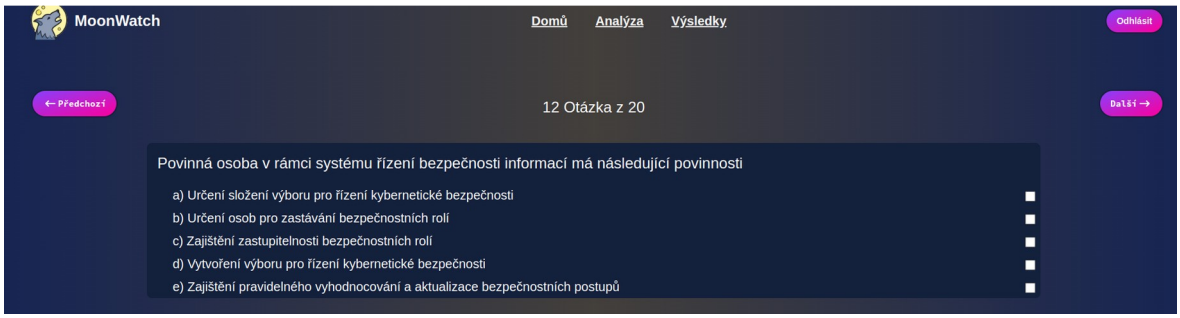
Povinná osoba zajistí (Obr. 15), že osoby zastávající bezpečnostní role mají dostatečné pravomoci a zdroje k úspěšnému plnění svých úkolů. To zahrnuje poskytnutí odpovídajících finančních prostředků, technických nástrojů a autority potřebné k prosazování bezpečnostních opatření a ochraně informací.

Povinná osoba zajistí, že plány kontinuity činností a obnovy jsou pravidelně testovány, včetně simulace kybernetických bezpečnostních incidentů. To umožňuje organizaci ověřit účinnost svých postupů a připravenost na případné krizové situace.

Povinná osoba zajistí, že zaměstnanci jsou pravidelně školeni v otázkách bezpečnosti informací. To zahrnuje seznámení s bezpečnostními politikami a postupy, identifikací kybernetických hrozeb a prevencí proti únikům dat a jiným bezpečnostním incidentům.

Povinná osoba taktéž implementuje mechanismy pro monitorování sítě a systémů, aby bylo možné detekovat případné bezpečnostní incidenty včas. Zaznamenávání a analýza těchto incidentů umožňuje organizaci lépe porozumět hrozbám a přijmout odpovídající opatření k jejich řešení.

Povinná osoba zajistí, že bezpečnostní politiky a postupy jsou průběžně hodnoceny a aktualizovány v souladu s nejnovějšími hrozbami a změnami v prostředí organizace. To zahrnuje revizi a aktualizaci politik, postupů a technických opatření s cílem zlepšit ochranu informací a reagovat na nové bezpečnostní výzvy.



Obrázek 16: Otázka *organizační bezpečnost*

Povinná osoba určí (Obr. 16) složení výboru pro řízení kybernetické bezpečnosti a bezpečnostní role, včetně práv a povinností souvisejících se systémem řízení bezpečnosti informací.

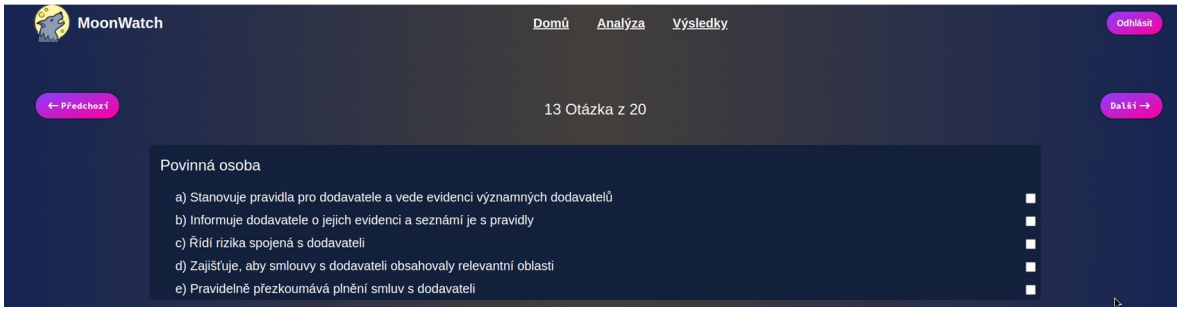
Povinná osoba určí osobu pro zastávání bezpečnostních rolí jako manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti, garanta aktiva a auditora kybernetické bezpečnosti.

Je nutné zajistit, aby bezpečnostní role byly vždy plněny a zastoupeny. Povinná osoba má tohle na starosti.

Povinná osoba vytvoří výbor pro řízení kybernetické bezpečnosti, který bude tvořen osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj systému řízení bezpečnosti informací.

Povinná osoba zajistí pravidelné vyhodnocování a aktualizaci bezpečnostních postupů v souladu s aktuálními bezpečnostními standardy a nejlepšími postupy v oboru. [28]

2.5 Řízení dodavatelů



Obrázek 17: Otázka *řízení dodavatelů*

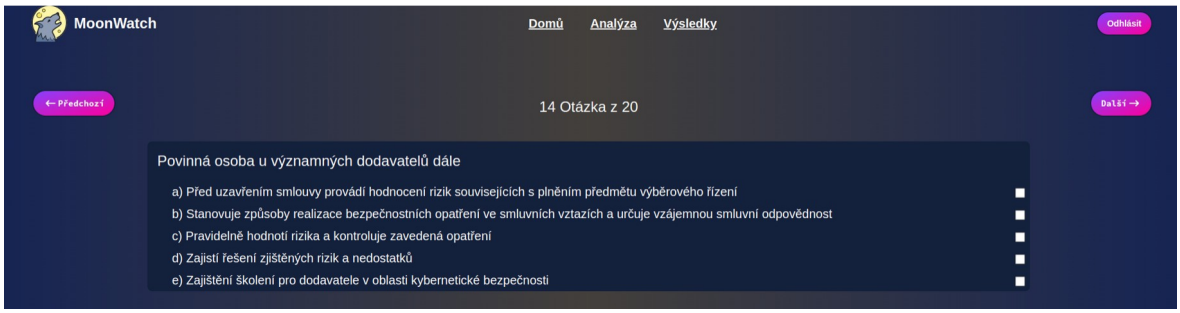
Povinná osoba definuje pravidla (Obr. 17), která dodavatelé musí dodržovat, a udržuje evidenci všech významných dodavatelů organizace. To pomáhá zajistit soulad dodavatelů s bezpečnostními standardy a požadavky organizace.

Povinná osoba sděluje dodavatelům, že jsou evidováni, a zároveň je seznámí s pravidly a požadavky, které musí dodržovat při poskytování svých služeb nebo výrobků.

Povinná osoba aktivně řídí rizika, která mohou vzniknout ve spojení s dodavateli. To zahrnuje identifikaci, hodnocení a monitorování rizik a zavedení odpovídajících opatření k jejich minimalizaci nebo eliminaci.

Povinná osoba se zajišťuje, že smlouvy uzavřené s dodavateli obsahují veškeré relevantní oblasti týkající se kybernetické bezpečnosti a ochrany dat. To zahrnuje klauzule o ochraně osobních údajů, ochraně duševního vlastnictví a další bezpečnostní požadavky.

Povinná osoba pravidelně monitoruje a přezkoumává dodavatelské smlouvy, aby zajistila jejich dodržování a plnění stanovených požadavků. To pomáhá udržovat bezpečnostní standardy a zajišťuje, že dodavatelé plní své závazky v souladu s dohodnutými podmínkami.



Obrázek 18: Otázka *řízení dodavatelů*

Před uzavřením smlouvy povinná osoba (Obr.18) provádí důkladné hodnocení rizik spojených s plněním předmětu výběrového řízení. To zahrnuje identifikaci potenciálních hrozeb a zranitelností a posouzení jejich dopadů na organizaci.

Povinná osoba stanovuje konkrétní způsoby, jak realizovat bezpečnostní opatření ve smluvních vztazích s dodavateli. To zahrnuje stanovení smluvních povinností týkajících se kybernetické bezpečnosti a určení odpovědnosti za dodržování těchto opatření.

Povinná osoba pravidelně hodnotí rizika spojená s dodavatelskými vztahy a kontroluje účinnost zavedených bezpečnostních opatření. To zahrnuje průběžné monitorování rizik a provádění auditů ke kontrole dodržování bezpečnostních standardů.

Povinná osoba aktivně řeší identifikovaná rizika a nedostatky ve spolupráci s dodavateli. To může zahrnovat implementaci nových bezpečnostních opatření, revizi smluvních podmínek nebo jiné kroky k minimalizaci rizik.

Povinná osoba zajistí, že dodavatelé jsou školeni v oblasti kybernetické bezpečnosti a jsou seznámeni s nejnovějšími bezpečnostními postupy a požadavky. To pomáhá zlepšit povědomí dodavatelů o bezpečnostních hrozbách a jejich schopností je řádně řešit. [28]

2.6 Další okruhy otázek

Do nástroje byly přidány i další typy otázek z oblasti organizačních opatření, které směřují k posílení kybernetické bezpečnosti organizací. Těmito otázkami se zaměřujeme na oblasti jako je bezpečnost lidských zdrojů, řízení provozu a komunikací, řízení změn, řízení přístupu, akvizice, vývoj a údržba systémů, zvládání kybernetických bezpečnostních událostí a incidentů, řízení kontinuity činností a audit kybernetické bezpečnosti. Tyto otázky mají organizacím pomoci lépe porozumět principům kybernetické bezpečnosti a aplikovat je v jejich vlastním prostředí.

Dále nástroj zahrnuje otázky z oblasti technických opatření, jako je fyzická bezpečnost, zabezpečení komunikačních sítí, správa a ověřování identit, řízení přístupových práv, ochrana proti škodlivému kódu, záznam událostí v informačních a komunikačních systémech, detekce kybernetických hrozeb, sběr a analýza kybernetických bezpečnostních incidentů, bezpečnost aplikací, použití kryptografických prostředků, zajištění dostupnosti informací a ochrana průmyslových, řídících a dalších specifických systémů. Tyto otázky mají za cíl posílit technické aspekty kybernetické bezpečnosti a pomoci organizacím lépe ochránit své informace a systémy. [28]

3 VÝVOJ MULTIPLATFORMNÍHO SOFTWARU

Pro vývoj nástroje bylo nejprve nezbytné stanovit jeho cíle a funkcionality. Nástroj musí poskytovat multiplatformní přístup, uživatelské rozhraní vhodné pro širokou škálu uživatelů a zajistit integritu, dostupnost a důvěrnost uložených dat. Dále je nutné, aby umožňoval provádění analýzy rizik kybernetické bezpečnosti a prezentoval výsledky této analýzy. Zahrnuje také autentizaci, validaci a ochranu dat. Po definování těchto požadavků je nutné je otestovat, včetně testování bezpečnosti aplikace, což zahrnuje i penetrační testování.

3.1 Multiplatformní přístup

Snaha vývoje toho dle nástroje se snaží být jednoduchá, tedy pro multiplatformní přístup webová aplikace poskytuje jednoduchý způsob přístupu a použití bez nutnosti instalace dalšího softwaru. Uživatelé pouze potřebují internetový prohlížeč a připojení k internetu, což minimalizuje nároky na jejich zařízení a usnadňuje jim práci s nástrojem odkudkoli.

Použití webové aplikace eliminuje potřebu investovat do infrastruktury pro nasazení a správu aplikace na každém jednotlivém zařízení uživatele. Webové aplikace také mohou využívat moderní zabezpečení a šifrování dat při přenosu, což pomáhá chránit citlivé informace uživatelů a zajišťuje jejich soukromí.

3.2 Front-end

Zde bylo za potřebí si vybrat front-end framework, který by pomohl se stylováním uživatelského rozhraní a přinesl výhody, které by pomohly k lepší uživatelskému zážitku. Pro vývoj nástroje tedy byl zvolen Tailwind CSS framework. Tailwind z prvního pohledu vypadá velice nepřehledně, ale ve skutečnosti každá funkce v Tailwind CSS je přehledně zdokumentována. Od ostatních frameworků navíc neposkytuje výchozí téma, které je zapotřebí použít. Můžeme každému projektu dát jiný vzhled, i když použijeme stejné prvky.

Další výhodou proč byl zvolen pro stylování front-endu byla jeho rychlost. Díky vestavěným a zdokumentovaným třídám, je rychlost vytvoření front-endu rychlá a lehká.

Pro integraci Tailwind CSS do projetku je zapotřebí ho nainstalovat. Za pomocí dvou příkazů npm install -D tailwindcss a npx tailwindcss init jsme schopni si vytvořit konfigurační soubor. Poté musíme přidat @tailwind pro každou vrstvu Tailwind do hlavního CSS souboru. Následuje příkaz na build npx tailwindcss -i ./src/input.css -o

./src/output.css –watch, který kompiluje vstupní CSS soubor do výstupního CSS souboru. Tento příkaz se spouští vždy před samotným spouštěním webové aplikace. Pro ulehčení je možno si na tenhle dlouhý příkaz udělat script, který spustí Tailwind CSS jednoduchým příkazem jako je například npm run Tailwind (Obr. 19).

Obrázek 19: Script pro *Tailwind CLI build*

Poté, co je Tailwind CSS úspěšně nainstalován a nakonfigurován v projektu, můžeme přejít k vytváření uživatelského rozhraní. Díky bohaté sadě předdefinovaných tříd poskytovaných Tailwind CSS není nutné se spoléhat na již hotové šablony pro jednotlivé komponenty. Každý komponent lze jednoduše naprogramovat a opakovaně použít na dalších stránkách aplikace.

Důležité bylo také brát v potaz responzivní design pro širokou škálu zařízení. Aplikace byla vyvíjena tak, aby byla optimalizovaná nejen pro desktopová rozlišení, ale i pro tablety a mobilní zařízení. Tím bylo zajištěno, že uživatelé mohou bez problémů přistupovat k aplikaci a využívat ji na různých typech zařízení s různými obrazovkami a rozlišeními.

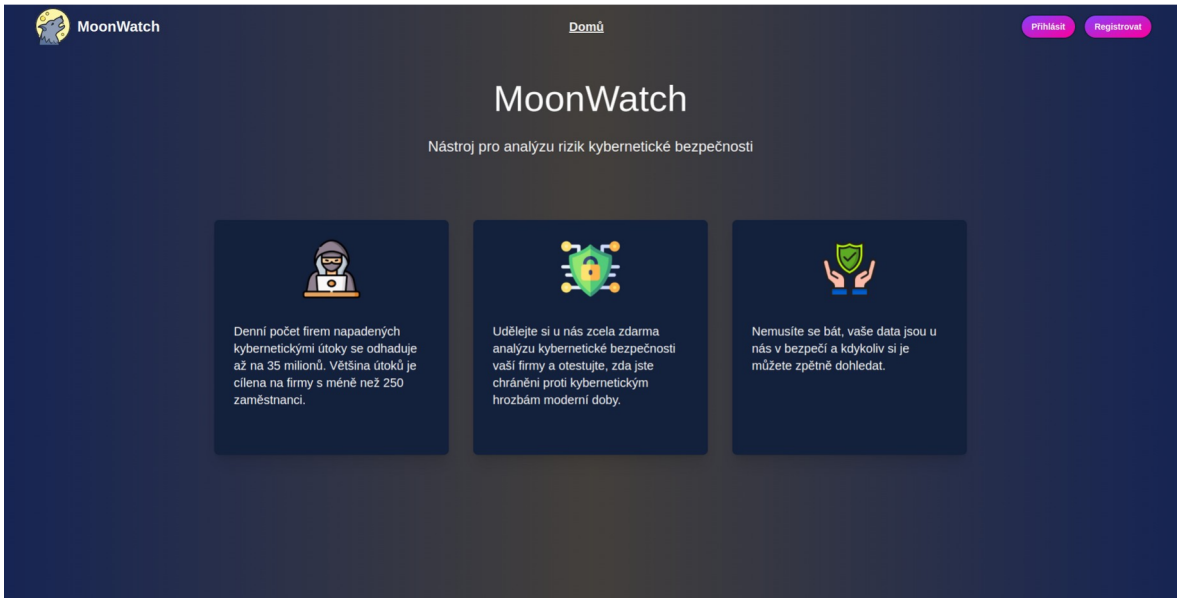
Jako první krok v procesu vytváření uživatelského rozhraní byl implementován header (Obr. 20). Tento klíčový prvek uživatelského rozhraní poskytuje uživatelům navigační možnosti a umožňuje jim snadný přechod mezi různými částmi aplikace. Pro jeho vytvoření byly využity třídy a komponenty poskytované frameworkem Tailwind CSS, což umožnilo rychlou a efektivní implementaci s minimálním množstvím vlastního CSS kódu.

Header obsahuje navigaci "Domů" pro nepřihlášeného uživatele a tlačítko pro přihlášení, které po stisknutí přesměruje uživatele na formulář pro přihlášení. Kromě toho obsahuje také tlačítko pro registraci, které přesměruje na formulář pro registraci nového uživatele. Součástí headeru je též obrázek loga webové aplikace a její název, "MoonWatch" (Obr. 21).

Po dokončení headeru je dalším krokem v procesu vytváření uživatelského rozhraní naprogramování indexové stránky. Indexová stránka představuje vstupní bod do aplikace a obsahuje důležité navigační prvky, které uživatelé potřebují k orientaci a interakci s aplikací.

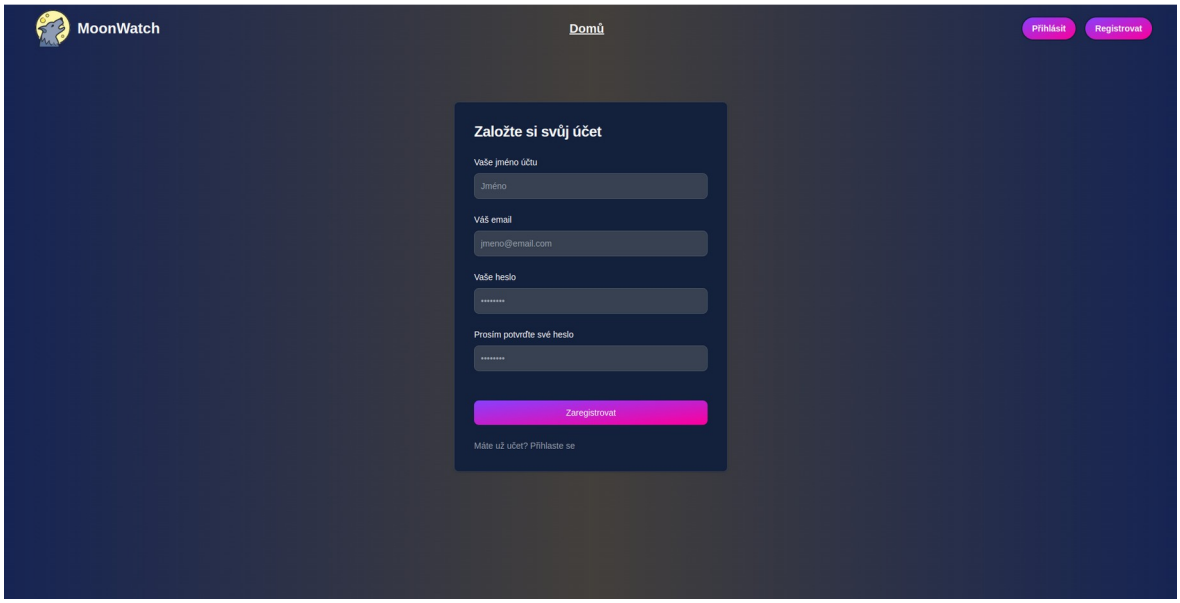
```
<header
    class=' max-md:py-4 max-md:px-4 sm:px-10 bg-gradient-to-r from-blue-950 via-stone-700 to-blue-950 font-[sans-serif] mi
    <div class='flex flex-wrap items-center justify-between gap-2 relative'>
        <a href="{{url_for('home_page')}}">
            <div class="flex flex-row justify-center items-center font-bold text-2xl text-white"><img
                src="{{ url_for('static', filename='images/icon.png') }}" alt="" class="w-20 max-sm:hidden">
                <p>
                    MoonWatch</p>
            </div>
        </a>
        <div class='flex lg:order-1 max-sm:ml-auto'>
            <a href="{{ url_for('login_page') }}">

                <button
                    class='px-4 py-2 text-sm rounded-full font-bold text-white border-2 border-[#14213D] bg-gradient-to-tl
            </a>
            <a href="{{ url_for('register_page') }}">
                <button
                    class='px-4 py-2 text-sm rounded-full font-bold text-white border-2 border-[#14213D] bg-gradient-to-tl

                </button>
            </a>
            <button id="toggle" class='lg:hidden ml-7'>
                <svg class="w-7 h-7" fill="#000" viewBox="0 0 20 20" xmlns="http://www.w3.org/2000/svg">
                    <path fill-rule="evenodd"
                        d="M3 5a1 1 0 011-1h12a1 1 0 110 2H4a1 1 0 01-1-1zM3 10a1 1 0 011-1h12a1 1 0 110 2H4a1 1 0 01-1-1zM3 15a
                        clip-rule="evenodd"></path>
                </svg>
            </button>
        </div>
        <ul id="collapseMenu" class='lg:!flex lg:space-x-5 max-lg:space-y-2 max-lg:hidden max-lg:py-4 max-lg:w-full'>
            <li
                class='max-lg:border-b max-lg:bg-gradient-to-tl from-[#ff009d] to-[#8a41ff] max-lg:py-2 px-3 max-lg:rounded'
                <a href="{{ url_for('home_page') }}"
                    class='lg:hover:text-[#007bff] text-[#fafafa] max-lg:text-white block font-semibold text-[20px] hover:
                    index}}</a>
            </li>
        </ul>
```

Obrázek 20: Ukázka *Tailwind CSS* header komponenty



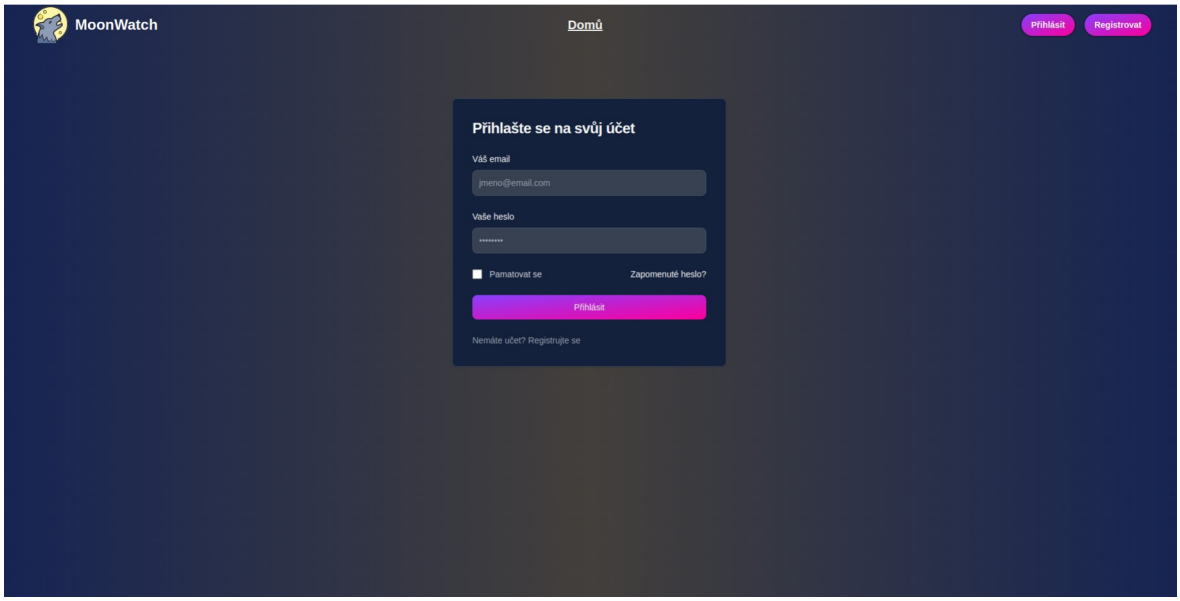
Obrázek 21: *Index* stránka

Registrační formulář slouží k registraci nového uživatele (Obr. 22). Obsahuje políčka pro uživatelské jméno, emailovou adresu, heslo a potvrzení hesla.



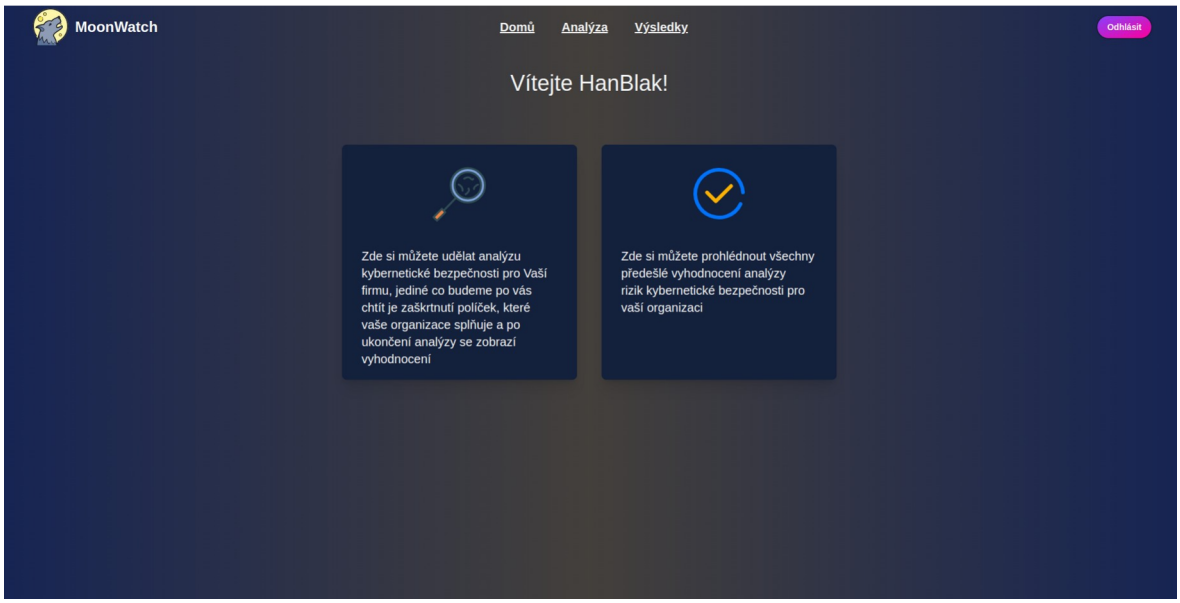
Obrázek 22: Stránka registrace

Stránka login slouží k přihlášení uživatele. Formulář obsahuje dvě políčka, email a heslo registrovaného uživatele. Je zde možnost taky si nechat zapamatovat údaje pro příští použití.



Obrázek 23: Přihlašovací stránka

Po přihlášení se uživatel dostane na domovskou stránku pro přihlášené uživatele (Obr. 24). Zde má možnost provést analýzu kybernetické bezpečnosti nebo si zobrazit předešlé výsledky analýz. K dispozici je také možnost odhlášení, která nahradila tlačítka pro přihlášení a registraci.



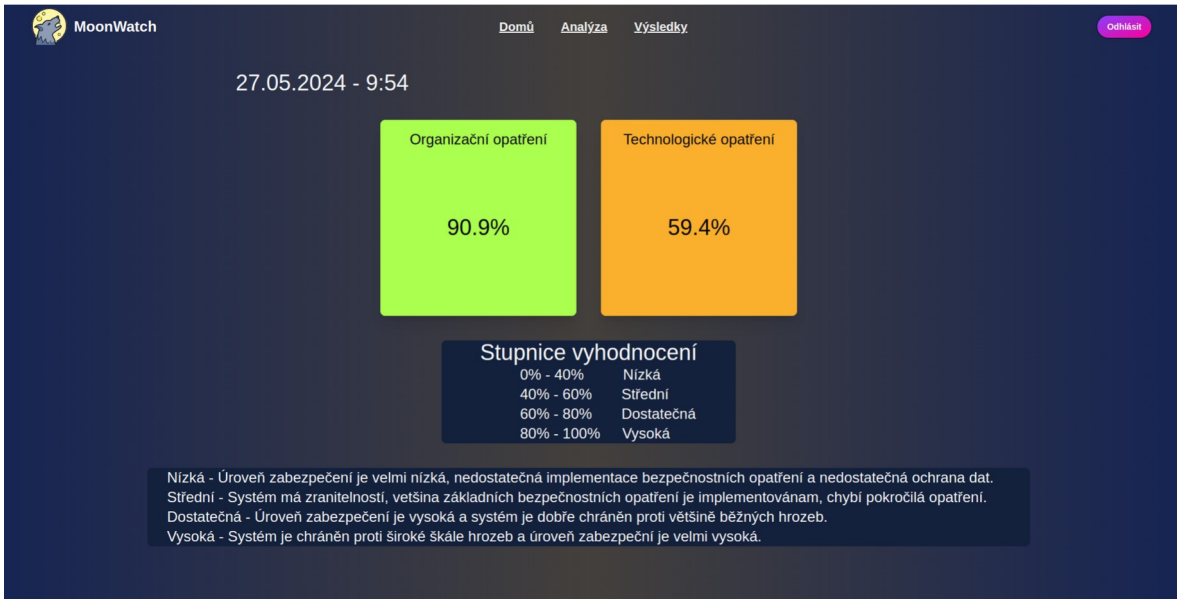
Obrázek 24: Domovská stránka pro přihlášené uživatelé

Stránka "analyze" (Obr. 25) slouží jako rozhraní, kde uživatelé mohou odpovídat na sadu otázek týkajících se kybernetické bezpečnosti. Každá otázka je doplněna checkboxem, který umožňuje uživatelům vybrat odpověď podle svého uvážení.

Pro zjednodušení procesu je na stránce "analyze" povolena pouze jedna otázka najednou. Jakmile uživatel odpoví na danou otázku a stiskne tlačítko "Další", přesune se na následující otázku. Naopak, stisknutím tlačítka "Zpět" se uživatel může vrátit k předchozí otázce v případě, že chce svou odpověď změnit nebo upravit. Tímto způsobem je proces analýzy postupně proveden a uživatel má kontrolu nad svými odpověďmi až do konce procesu.

Poslední stránkou je samotná "result" stránka (Obr. 26), kde uživatelé naleznou výsledky provedené analýzy. Zde jsou zobrazeny výsledky organizačních opatření a technických opatření. Kontejnery, ve kterých jsou zobrazeny číselné hodnoty, jsou zbarveny podle dosažené hodnoty. Výsledná stupnice poskytuje informace o dosažených výsledcích. Stránka také obsahuje datum a čas dokončení analýzy, aby uživatelé měli přehled o aktuálnosti výsledků.

Obrázek 25: Stránka *analýzy* ve které se provádí vyplnění otázky



Obrázek 26: Stránka *result a* výsledek analýzy

3.3 Back-hand

Volba back-handové části spočívala ve výběru správného programovacího jazyka a frameworku. Pro front-end byl zvolen Tailwind CSS, proto bylo potřeba uvažovat nad frameworkem, který umožňuje importovat Tailwind CSS a integrovat ho. Nabízelo se více možností, ale nakonec byl vybrán mikro framework Flask pro jeho jednoduchost a flexibilitu v kombinaci s možností snadné integrace s Tailwind CSS.

Flask je mikro webový frameworkDůležité bylo také brát v potaz responzivní design pro širokou škálu zařízení. Aplikace byla vyvíjena tak, aby byla optimalizovaná nejen pro desktopová rozlišení, ale i pro tablety a mobilní zařízení. Tím bylo zajištěno, že uživatelé mohou bez problémů přistupovat k aplikaci a využívat ji na různých typech zařízení s různými obrazovkami a rozlišeními. napsaný v jazyce Python, známý svou jednoduchostí a flexibilitou. Jeho funkcionalita je založena na konceptu routování, kde specifické URL adresy, nazývané také routy, jsou propojeny s funkcemi, jež zpracovávají požadavky na tyto adresy a vracejí odpovídající obsah. Toto se často realizuje pomocí dekorátorů Pythonu, které označují funkce jako obslužné funkce pro konkrétní URL adresy.

Flask také poskytuje podporu pro šablony (templates) a statické soubory, což umožňuje snadné vykreslování dynamických webových stránek a využití statických zdrojů, jako jsou například obrázky, CSS nebo JavaScriptové soubory. Flask je používán s programovacím jazykem Python, který disponuje bohatou sadou knihoven.

Instalace mikro frameworku Flask je prvním krokem pro vytvoření back-endové části webové aplikace. Poté, co je nainstalován Python, je možné přistoupit k instalaci Flaska. Bylo zapotřebí vytvořit nový adresář projektu a vytvořit virtuální prostředí, což umožňuje izolovat aplikaci od ostatních projektů a zároveň zajistí, že budou použity pouze ty knihovny, které jsou specificky potřebné pro daný projekt. Po vytvoření virtuálního prostředí lze nainstalovat Flask pomocí nástroje pip, který je standardním správcem balíčků pro Python. Stačí použít příkaz "pip install flask" a tím je Flask úspěšně nainstalován v daném virtuálním prostředí. Poté je možné začít implementovat back-endovou logiku aplikace a stavět na ní celý její funkcionalitu.

Potom co je nainstalován mikro framework Flask do virtuálního prostředí, můžeme vytvořit konfigurační soubor. Jeho pojmenování se doporučuje "app.py" a obsahuje konfiguraci aplikace a routování URL. Následně je nutno vytvořit adresář "templates", ve kterém budou uloženy HTML šablony, které budou využity k vytváření dynamických stránek webové aplikace.

Následně je nutno vytvořit adresář "static“, který bude obsahovat uložené soubory typu CSS stylů, obrázků, JavaScript soubory apod.

4 ANALÝZA FUNKCÍ A SOUBORŮ NÁSTROJE

V následující kapitule provedeme rozbor klíčových funkcí a souborů nástroje, které společně tvoří funkční celek webové aplikace. Zároveň se zaměříme na multimediální přístup do aplikace a představíme použité knihovny a technologie.

4.1 Konfigurační soubor

Jak již bylo zmíněno v předchozí kapitole, konfigurační soubor "app.py" obsahuje definici tras a další důležité nastavení aplikace. V této části se detailněji zaměříme na konfiguraci tras a význam jednotlivých částí souboru pro funkčnost webové aplikace.

Při nakonfigurování souboru (Obr. 27) je třeba nejdříve si naimportovat "SQLalchemy“. Dále musíme vytvořit instanci aplikace Flask příkazem "app = Flask(__name__)", který umožnuje Flask frameworku identifikovat, kde se nachází zdrojový kód aplikace a jaké soubory jsou součástí nástroje. Tím se definuje rozsah aplikace a umožňuje Flasku provádět různé operace, jako je načítání šablon, trasování URL adres a správa relací. Pro funkci trasování URL, je nutné taky importovat moduly pro Flask framework. Modul na vykreslování HTML šablon nazývaný "render_template", umožňuje načíst HTML šablony s dynamickými daty. Modul "url_for" slouží k vytváření URL adres pro jednotlivé trasy ve webové aplikace, případně se dá použít například při volání obrázků ze static adresáře. Modul "request" umožnuje získat data z HTTP požadavků, jako jsou data z formulářů, parametry adres a další. Modul "redirect" slouží k přesměrování uživatele na jinou URL adresu ve webové aplikaci. Je používána v situacích, kdy je potřeba přesměrovat uživatele na jinou stránku, například po odeslání formuláře. Modul "session" umožnuje ukládat data o relaci uživatele při interakcí s webovou aplikací. Lze tak ukládat datové informace například o přihlášení.

Dále je v konfiguraci instance aplikace Flask nastavena URI (Uniform Resource Identifier) pro připojení k SQLite databázi (Obr. 27). Tento řetězec, který je přiřazen klíči "SQLALCHEMY_DATABASE_URI" v konfiguračním souboru specifikuje umístění a název databázového souboru.

Dále je taky v konfiguračním souboru generován tajný klíč pomocí funkce "secrets.token_hex()", který je využíván k zabezpečení aplikace, kde se používá k podepisování a ověřování dat, která jsou uložena v relaci uživatele.

```python
from flask import Flask, render_template, url_for, request, redirect, session
from flask_sqlalchemy import SQLAlchemy
from static import translations
from generate import is_strong_password
from datetime import datetime
from models import db, User, LargerQuestion, SubQuestion, Answer, Results, Active_results
from werkzeug.security import generate_password_hash, check_password_hash
from sqlalchemy.exc import IntegrityError
from sqlalchemy.sql import text
from flask_wtf.csrf import CSRFProtect
import secrets



app = Flask(__name__)

secret_key = secrets.token_hex(16)
app.secret_key = secret_key
csrf = CSRFProtect(app)

app.config['SQLALCHEMY_DATABASE_URI'] = 'sqlite:///Rend.db'
db.init_app(app)

with app.app_context():
    db.create_all()

@app.route("/")
def home_page():
```

Obrázek 27: Ukázka konfiguračního souboru *app.py*

Následně vygenerovaný klíč je přiřazen k atributu "secret_key". Tím se zajistí, že aplikace používá specifikovaný tajný klíč pro své zabezpečení.

Nakonec je vytvořen objekt CSRFProtect, který poskytuje ochranu před CSRF útoky. CSRFProtect je rozšíření Flasku, které poskytuje nástroje pro ochranu před útoky, které mohou zneužít autorizovaného uživatele k provedení neautorizovaných akcí v jeho jménu. Tím, že je CSRFProtect inicializován s instancí aplikace Flask, je aktivována ochrana před CSRF útoky pro všechny cesty aplikace.

```python
with app.app_context():
    db.create_all()

@app.route("/")
def home_page():
    browser_language = translations.get_browser_language(request)

    if browser_language.startswith('cs'):
        selected_translations = translations.czech_translations
    else:
        selected_translations = translations.english_translations

    return render_template("index.html", **selected_translations)
```

Obrázek 28: Ukázka trasování a vytvoření databáze

V tomto kódu (Obr. 28) se vytváří tzv. "application context" (kontext aplikace) pomocí funkce "app.app_context()", což je potřeba pro práci s databází. Uvnitř tohoto kontextu je volána metoda "create_all()" na objektu db, který představuje naši instanci SQLAlchemy. Tímto způsobem se zajišťuje, že všechny definované tabulky v modelu budou vytvořeny v databázi, pokud ještě neexistují.

Domovská stránka je nastavena jako index v konfiguračním souboru (Obr. 28). Dále je každé další trasování nastaveno tak, aby zavolalo funkci pro překlad stránky. To umožňuje uživatelům s různými jazykovými preferencemi přístup k webové aplikaci. Primární jazyk aplikace je čeština, avšak pro uživatele hovořící jinými jazyky je k dispozici anglický překlad, který je závislý na nastavení jejich webového prohlížeče. Takže pokud není webový prohlížeč nastaven na češtinu, webová aplikace se automaticky přepne do angličtiny.

4.1.1 Registrace a přihlášení uživatele

Registrace (Obr. 30) uživatele začíná tím, že se zjistí jazyk uživatelova prohlížeče. Pokud je detekován jako český, budou se používat české překlady, jinak se použijí anglické překlady. Když uživatel vyplní registrační formulář a odešle ho, aplikace přijme data pomocí metody POST. Poté jsou z formuláře získány informace jako uživatelské jméno, e-mail, heslo a potvrzení hesla. Pro ověření, zda uživatel s daným e-mailem již existuje, se provede dotaz do databáze. Pokud je e-mail již registrován, uživatel obdrží chybovou zprávu o existujícím e-mailu.

```
def is_strong_password(password):
    min_length = 8
    has_lowercase = any(char.islower() for char in password)
    has_uppercase = any(char.isupper() for char in password)
    has_digit = any(char.isdigit() for char in password)
    special_characters = "!@#$%^&*()\-_=+{};:'\",<.>/?[\]\\"
```

Obrázek 29: Funkce pro silné heslo

Následně je ověřeno, zda heslo splňuje požadavky na sílu hesla (Obr. 29). Pokud ne, uživatel obdrží odpovídající chybovou zprávu. Poté se zkontroluje, zda se zadaná hesla shodují. Pokud ne, zobrazí se chybová zpráva. Před uložením do databáze je heslo hashováno pomocí funkce "generate_password_hash" z balíčku Flask-Bcrypt. Nakonec je

nový uživatel uložen do databáze s hashovaným heslem. V případě chyby při zápisu do databáze je uživateli zobrazena odpovídající chybová zpráva. Pokud je registrace úspěšná, uživatel je přesměrován na stránku přihlášení. Pokud uživatel navštíví stránku pro registraci, ale nepošle žádný formulář, zobrazí se mu stránka s registračním formulářem a případně i s příslušnými překlady podle jazyka jeho prohlížeče.

```python
@app.route("/register", methods=['GET', 'POST'])
def register_page():
    browser_language = translations.get_browser_language(request)
    if browser_language.startswith('cs'):
        selected_translations = translations.czech_translations
    else:
        selected_translations = translations.english_translations
    if request.method == 'POST':
        username = request.form['username']
        email = request.form['email']
        password = request.form['password']
        password_confirm = request.form['password_confirm']
        existing_user = User.query.filter_by(_email=email).first()
        if existing_user:
            error_message = selected_translations['email_exist']
            return render_template("register.html", error_message=error_message, **selected_translations)
        if not is_strong_password(password):
            error_message = selected_translations['password_req']
            return render_template("register.html", error_message=error_message, **selected_translations)
        if password != password_confirm:
            error_message = selected_translations['notsamepassword']
            return render_template("register.html", error_message=error_message, **selected_translations)
        hashed_password = generate_password_hash(password)
        try:
            query = text("INSERT INTO User (_username, _email, _password) VALUES (:username, :email, :password)")
            db.session.execute(query, {'username': username, 'email': email, 'password': hashed_password})
            db.session.commit()
        except Exception as e:
            error_message = "An error occurred while registering. Please try again later."
            return render_template("register.html", error_message=error_message, **selected_translations)
        return redirect(url_for('login_page'))
    return render_template("register.html", **selected_translations)
```

Obrázek 30: Registrace v konfiguračním souboru

Pro přihlášení uživatel odesílá formulář na přihlášení, aplikace přijme data pomocí metody POST. Z formuláře jsou následně získány informace o e-mailu a heslu uživatele. Následně je proveden dotaz do databáze, aby se ověřilo, zda existuje uživatel s daným e-mailem. Pokud je uživatel nalezen a zadané heslo odpovídá hashovanému heslu v databázi, je uživatel přihlášen. Pokud je ověření úspěšné, uživateli je nastavena relace s identifikátorem uživatele a je přesměrován na stránku určenou pro přihlášené uživatele. V případě neúspěšného přihlášení je uživatel přesměrován zpět na přihlašovací stránku. Pokud uživatel pouze navštíví přihlašovací stránku a nepošle žádný formulář, zobrazí se mu stránka s přihlašovacím formulářem a s případnými překlady podle jazyka jeho prohlížeče.

4.1.2 Analýza a algoritmus

Cesta "submit_answer" (Obr. 31) slouží k zpracování požadavků typu POST pro získání odpovědí z analýzy. Data z front-endu jsou získána pomocí request.form. Je nutné nastavit

formulář v HTML tak, aby data byla odeslána na správnou URL pomocí metody POST. Poté, co získáme data, projdeme je a uložíme jednotlivé odpovědi do databáze. Nakonec provedeme commit změn do databáze. Je důležité poznamenat, že uživatel se získává z relace, aby nedocházelo k promíchání uživatelů, a tak poté načítání nesprávného uživatele z databáze.

```python
@app.route("/submit_answer", methods=['POST'])
def submit_answer():
    user_id = session.get('user_id')

    if user_id is None:
        return jsonify({"error": "Uživatel není přihlášen."}), 401

    question_id = request.form.get("question_id")
    answers = request.form.getlist("answers[]")

    for answer in answers:
        new_answer = Answer(question_id=question_id, user_id=user_id, answer=answer)
        db.session.add(new_answer)

    db.session.commit()

    return jsonify({"message": "Odpovědi byly úspěšně uloženy do databáze."}), 200
```

Obrázek 31: Uložení dat z front-endu do databáze

```python
@app.route("/calculate_results")
def calculate_results():
    user_id = session.get('user_id')

    if user_id is None:
        return jsonify({"error": "Uživatel není přihlášen."}), 401

    answers = Answer.query.all()

    count_A = 0
    count_B = 0
    count_C = 0

    for answer in answers:
        if answer.answer == 'A':
            count_A += 1
        elif answer.answer == 'B':
            count_B += 1
        elif answer.answer == 'C':
            count_C += 1

    new_result = Results(user_id=user_id, A_count=count_A, B_count=count_B, C_count=count_C)
    db.session.add(new_result)
    db.session.commit()

    return jsonify({"message": "Vypočtené hodnoty byly úspěšně uloženy do tabulky 'results'."}), 200
```

Obrázek 32: Výpočet hodnot odpovědí a zapsání do tabulky Results

Algoritmus "calculate_results" slouží k výpočtu a uložení výsledků odpovědí uživatele do databáze. Nejprve algoritmus získává user_id z aktuální relace uživatele. Algoritmus poté získává všechny uložené odpovědi z databáze z tabulky "Answers" ve které jsou zapsány odpovědí uživatele. Po spočítání odpovědí algoritmus zapíše do tabulky "Results" celkový počet odpovědí A, B a C.

4.1.3 Výpočet výsledné analýzy

Algoritmus "calculate_coverage" slouží k výpočtu procentuálního pokrytí odpovědí uživatele v celkové analýze kybernetické bezpečnosti. Nejprve se získá ID přihlášeného uživatele z aktuální relace. Pokud uživatel není přihlášen, algoritmus vrátí chybovou zprávu. Poté se získá první záznam z tabulky "Results", který obsahuje odpovědi kladných (označené jako A), záporných (označené jako B) a kritických (označené jako C) aspektů kybernetické bezpečnosti.

Dalším krokem algoritmu je výpočet procentuálního pokrytí. To se provede tak, že se celkový počet kladných odpovědí vydělí součtem kladných a záporných odpovědí a výsledek se vynásobí 100. Tím získáme celkové pokrytí v procentech. Pokud existují odpovědi typu C, což jsou odpovědi na kritické otázky, algoritmus nastaví celkové pokrytí na 0%. Důvodem je skutečnost, že porušení kritických aspektů kybernetické bezpečnosti představuje vážné riziko pro firmu a může ohrozit bezpečnostní opatření jako celek.

```python
@app.route("/calculate_coverage")
def calculate_coverage():
    user_id = session.get('user_id')

    if user_id is None:
        return jsonify({"error": "Uživatel není přihlášen."}), 401

    total_answers = Results.query.first()
    total_A = total_answers.A_count
    total_B = total_answers.B_count
    total_C = total_answers.C_count

    total_possible_A = total_A + total_B

    if total_possible_A != 0:
        coverage_percentage = (total_A / total_possible_A) * 100
    else:
        coverage_percentage = 0

    if total_C > 0:
        coverage_percentage = 0

    new_analyze_result = Analyze_results(user_id=user_id, coverage_percentage=coverage_percentage)
    db.session.add(new_analyze_result)
    db.session.commit()

    return jsonify({"message": "Procentuální pokrytí bylo úspěšně vypočítáno a uloženo do tabulky 'Analyze_results'."}), 200
```

Obrázek 33: Výpočet analýzy rizik kybernetické bezpečnsti

5 NÁVRH A IMPLEMENTACE DATABÁZE

Pro správu dat ve webové aplikaci pro analýzu kybernetické bezpečnosti byla navržena a implementována relační databáze. Databáze je klíčovým prvkem systému, neboť uchovává informace o uživatelích, jejich odpovědích na otázky a výsledcích analýzy.

5.1 Návrh databáze

Zdá se, že text obsahuje několik pravopisných a gramatických chyb, ale obsahově je v pořádku. Zde je opravená verze: Podle relačního modelu databáze (Obr. 34) byla vytvořena tabulka "User" pro uchovávání informací o uživatelích. Každý záznam v této tabulce obsahuje identifikátor (ID), který slouží jako primární klíč tabulky. Každý uživatel má jedinečné ID. Sloupec "username" uchovává uživatelská jména, která musí být unikátní, aby nedošlo k duplikaci jmen v databázi. Stejně tak je i sloupec pro e-mailovou adresu uživatele navržen tak, aby obsahoval pouze unikátní údaje. Poslední sloupec je určen pro uchovávání hesla uživatele. Tyto údaje jsou následně využívány při ověřování a autorizaci uživatelů, při správě jejich účtů a při dalších operacích spojených s uživatelským prostředím aplikace.

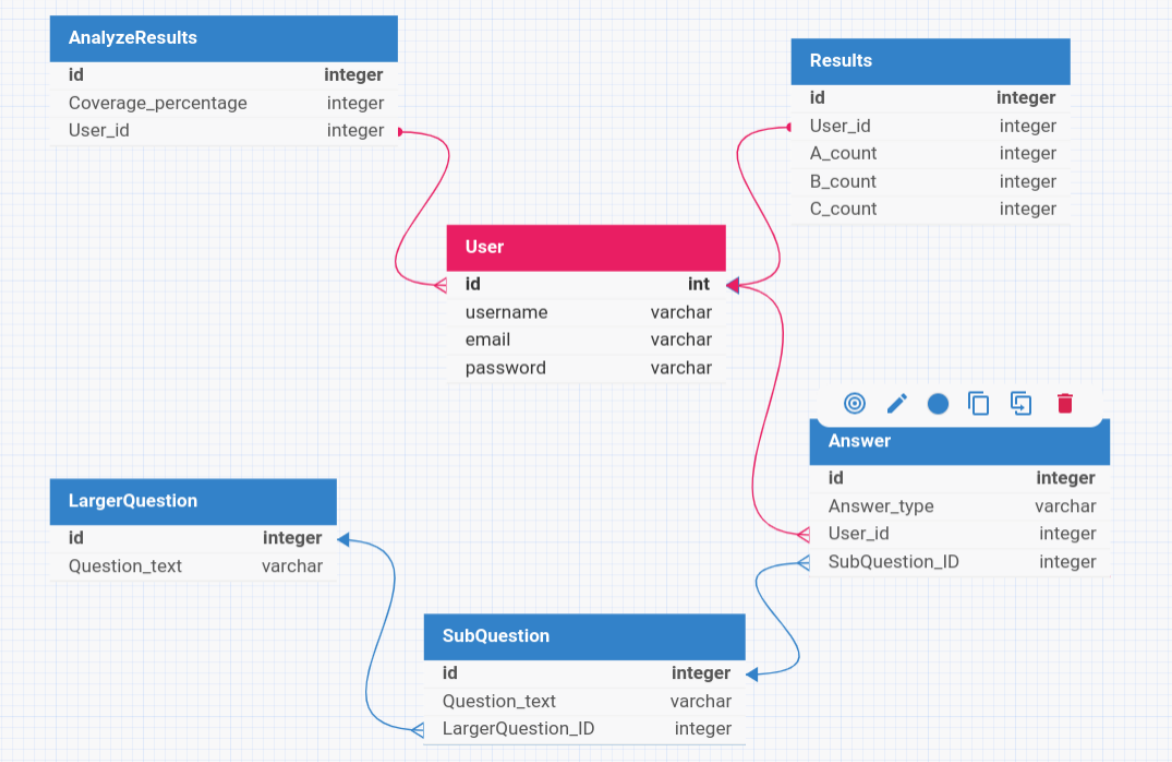
Tabulka "LargeQuestion" slouží k uchování textu každé otázky. "LargeQuestion" má své id, které slouží jako primární klíč tabulky, a text otázky.

Tabulka "SubQuestion" slouží k uchování informací o konkrétních položkách otázek. Každá otázka má 5 položek, které jsou uchovány v tabulce "SubQuestion". Tabulka má své id, text položky a následně cizí klíč "LargeQuestion_ID" pro vztah mnoha položek k jedné otázce.

Další tabulka "Answer" ukládá informace o odpovědích, které uživatelé poskytli na otázky v analýze kybernetické bezpečnosti. Tabulka obsahuje své id, sloupec "Answer_Type" obsahující typ odpovědi (A pro kladnou, B pro zápornou, C pro kritickou odpověď), cizí klíč "user_id", který odkazuje na tabulku uživatelů a vztah mnoha odpovědí k jednomu uživateli. Sloupec "SubQuestion_ID" je cizí klíč z tabulky, která obsahuje informaci o tom, na kterou položku uživatel odpověděl, s vztahem 1 odpovědi k 1 položce.

Tabulka "Results" slouží k ukládání agregovaných informací o počtu odpovědí jednotlivých typů (A, B, C) pro každého uživatele. Tabulka má své id, sloupce pro uložení kladných odpovědí "A_count", záporných odpovědí "B_count" a kritických odpovědí "C_count". Cizí klíč "user_id" slouží pro identifikaci uživatele s vztahem mnoha výsledků k jednomu uživateli.

Omlouvám se za to. Zde je opravená verze: Poslední tabulka "AnalyzeResults" slouží k uložení informací o procentuálním pokrytí kybernetické bezpečnosti organizace. Tabulka obsahuje své id, sloupec "Coverage_percentage", který obsahuje hodnotu procentuálního pokrytí kybernetické bezpečnosti, a cizí klíč "user_id" pro identifikaci uživatele s vztahem jednoho uživatele k více výsledkům.



Obrázek 34: Relační model databáze

5.2 Šifrování databáze

Samozřejmě, rád pomůžu s úpravou textu: Šifrování databáze představuje klíčovou praxi v dnešní době. Je zásadní šifrovat citlivá data, jako jsou hesla, a to je právě implementováno v tomto nástroji. Citlivé informace jsou v nástroji hashovány pomocí knihovny "wekzeug", která poskytuje bezpečné hashování hesel s jednoduchou programovatelnou logikou.

Uživatel zadá své heslo do formuláře, který ho přijme a následně provede funkce "generate_password_hash(password)" (Obr. 35) pro vytvoření hashe. Tento hash je poté uložen do databáze. Při následném ověření při přihlášení se hash použije k porovnání s uloženým hashem v databázi, tedy se zavolá funkce "check_password_hash(decrypt_email._password, password)".

```
    if existing_user:
        error_message = selected_translations['email_exist']
        return render_template("register.html", error_message=error_message, **selected_translations)
    if not is_strong_password(password):
        error_message = selected_translations['password_req']
        return render_template("register.html", error_message=error_message, **selected_translations)
    if password != password_confirm:
        error_message = selected_translations['notsamepassword']
        return render_template("register.html", error_message=error_message, **selected_translations)
    hashed_password = generate_password_hash(password)
    encrypted_username = encrypt_data(username)
    encrypted_email = encrypt_data(email)
    try:
        query = text("INSERT INTO User (_username, _email, _password) VALUES (:username, :email, :password)")
        db.session.execute(query, {'username': encrypted_username, 'email': encrypted_email, 'password': hashed_password})
        db.session.commit()
    except Exception as e:
        error_message = "An error occurred while registering. Please try again later."
        return render_template("register.html", error_message=error_message, **selected_translations)
    return redirect(url_for('login_page'))
return render_template("register.html", **selected_translations)
```

Obrázek 35: Ukázka hashování a šifrování dat do databáze

Pro šifrování se běžně využívá bloková šifra AES-256 (Obr. 36), která je ideální pro šifrování velkých objemů dat a zároveň je velmi rychlá. Pro zajištění bezpečnosti webové aplikace je klíč uložen v prostředí operačního systému. V případě online verze je klíč přímo vložen do prostředí serveru.

```
def encrypt_data(data):
    cipher = AES.new(key, AES.MODE_EAX)
    ciphertext, tag = cipher.encrypt_and_digest(data.encode('utf-8'))
    return base64.b64encode(cipher.nonce + tag + ciphertext).decode('utf-8')

def decrypt_data(encrypted_data):
    encrypted_data = base64.b64decode(encrypted_data.encode('utf-8'))
    nonce = encrypted_data[:16]
    tag = encrypted_data[16:32]
    ciphertext = encrypted_data[32:]
    cipher = AES.new(key, AES.MODE_EAX, nonce)
    decrypted_data = cipher.decrypt_and_verify(ciphertext, tag)
    return decrypted_data.decode('utf-8')
```

Obrázek 36: Implementování šifry *AES-256*

Data jsou šifrována (Obr. 35) před uložením do databáze. Při zadávání údajů do přihlašovacího formuláře jsou tato data před ověřením dešifrována (Obr. 37). Stejný postup šifrování je aplikován i na ostatní data v tabulkách, což zajišťuje ochranu proti případnému úniku dat z databáze.

```
if request.method =='POST':
    email = request.form.get("email")
    password = request.form.get("password")
    user = User.query.filter_by(_email=email).first()
    decrypt_email = decrypt_data(email)
    if user and check_password_hash(decrypt_email._password, password):
        session['user_id'] = user.id
        return redirect(url_for('logged_page'))
    else:
        return redirect(url_for('login_page'))

return render_template("login.html", **selected_translations)
```

Obrázek 37: Ukázka dešifrování a kontrola hashe

6 BEZPEČNOSTNÍ A FUNKČNÍ TESTOVÁNÍ

Pro bezpečnostní testování aplikace byla provedena analýza proti SQL injection, Cross-Site Scripting, Cross Site Request Forgery, autentizačních mechanismů, oprávnění, úniku informací a útokům typu Denial of Service.

Funkční testování zahrnovalo ověření funkcionality dotazů v analýze, jejich správné ohodnocení, správné ukládání do databáze, testování uživatelského rozhraní, výkonu a kompatibility.

6.1 Bezpečnostní testování

Webová aplikace používá parametrizovaný dotaz za pomocí SQLAlchemy, který chrání proti útokům SQL injection. Tento způsob (Obr. 38) zpracování dotazů zajišťuje, že uživatelské vstupy jsou správně escapovány a nejsou interpretovány jako část SQL syntaxe. Díky tomu je minimalizováno riziko útoků SQL injection, které mohou ohrozit bezpečnost aplikace a integritu dat v databázi.

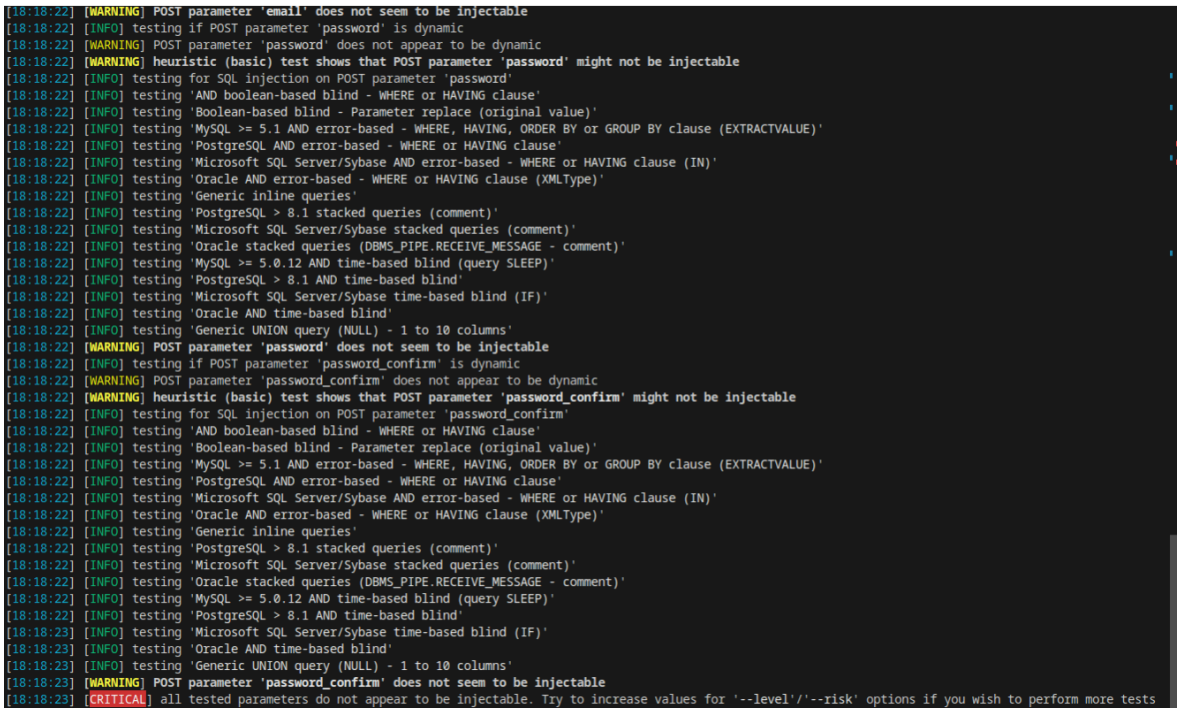
```
try:
    query = text("INSERT INTO User (_username, _email, _password) VALUES (:username, :email, :password)")
    db.session.execute(query, {'username': encrypted_username, 'email': encrypted_email, 'password': hashed_password})
    db.session.commit()
except Exception as e:
    error_message = "An error occurred while registering. Please try again later."
    return render_template("register.html", error_message=error_message, **selected_translations)
```

Obrázek 38: Ochrana proti SQL injection

Pro ověření bezpečnosti webové aplikace proti SQL injection (Obr. 39) byl použit nástroj SQLMap, který je specializovaný na testování zranitelností spojených s SQL injection útoky.

SQLMap je výkonný nástroj určený k automatickému testování zranitelností spojených s SQL injection útoky. Jeho hlavním účelem je identifikovat a exploataci potenciálních bezpečnostních chyb v aplikacích, které používají SQL databáze. Tento nástroj funguje tím, že analyzuje vstupní parametry aplikace a pokouší se vložit různé SQL dotazy, aby odhalil možné zranitelnosti.

Následně byly takhle otestovány všechny formuláře, které by mohli nést tuhle zranitelnost vůči tomuhle útoku.



Obrázek 39: SQLmap testování aplikace

Při testování Cross Site Scripting byly identifikovány potenciální zranitelnosti (Obr. 40). Proces testování umožnil detekci potenciálně nebezpečných skriptů, které by mohly být zneužity pro útoky. Tyto zranitelnosti byly následně řádně analyzovány a adresovány, aby webová aplikace nebyla ohrožena těmito typy útoků.

Obrázek 40: XSS zranitelnost

Pro testování zranitelností Cross Site Scripting byl využit specializovaný nástroj, který umožňuje automatizované testování a identifikaci potenciálních slabých míst v kódu. Tento nástroj je navržen tak, aby detekoval různé formy XSS útoků a poskytoval důležité informace pro další zabezpečení aplikace.

Obrázek 41: Kontrola Cross Site Scripting zranitelnosti

6.2 Funkční testování

Otestování správné funkcionality je zaměřeno na ověření, zda jednotlivé algoritmy pracují korektně. Například, testování správného výpočtu odpovědí na otázky zajistí, že algoritmus provádí správné výpočty a výsledky jsou adekvátně uloženy v databázi za pomocí unit testů importované z knihoven.

V testu (Obr. 42) této funkcionality jsou nejprve vytvořeny falešné odpovědi v databázi, simulující odpovědi uživatele na otázky. Poté je zaslán požadavek na výpočet výsledků pomocí GET požadavku na endpoint "/calculate_results".

V tomto endpointu se prochází všechny odpovědi v databázi a na základě jejich typu se zvyšuje příslušné počítadlo (A_count, B_count, C_count). Tyto výsledky jsou následně uloženy do tabulky "Results".

V rámci testu je poté ověřováno (Obr. 43), zda byly výsledky korektně uloženy v databázi. Očekává se, že počty odpovědí typu A, B a C jsou správně spočítány. Pokud test proběhne úspěšně, znamená to, že výpočet výsledků funguje korektně a data jsou úspěšně ukládána do databáze.

Testování uživatelského rozhraní probíhalo za pomocí manuálního testování, kdy se použilo ruční testování. To znamená, že testování probíhalo prostřednictvím interakce s uživatelským rozhraním aplikace přímo v prohlížeči nebo na zařízení, aniž by byly použity automatizované testovací nástroje.

```python
class TestCalculateResults(unittest.TestCase):

    def setUp(self):
        app.config['TESTING'] = True
        app.config['SQLALCHEMY_DATABASE_URI'] = 'sqlite:///:memory:'
        self.app = app.test_client()

        self.app_context = app.app_context()
        self.app_context.push()

        db.create_all()

    def tearDown(self):
        db.session.remove()
        db.drop_all()

        self.app_context.pop()

    @patch('app.session', {'user_id': 1})
    def test_calculate_results(self):
        question_id = 1
        answer1 = Answer(user_id=1, question_id=question_id, answer_type='A')
        answer2 = Answer(user_id=1, question_id=question_id, answer_type='A')
        answer3 = Answer(user_id=1, question_id=question_id, answer_type='C')
        answer4 = Answer(user_id=1, question_id=question_id, answer_type='A')
        answer5 = Answer(user_id=1, question_id=question_id, answer_type='B')

        db.session.add_all([answer1, answer2, answer3, answer4, answer5])
        db.session.commit()

        response = self.app.get('/calculate_results')

        self.assertEqual(response.status_code, 200)

        results = Results.query.filter_by(user_id=1).first()
        print("Results from database:", results)
```

Obrázek 42: Unit test pro algoritmus *calculate_results*

Během manuálního testování se prováděly různé akce a interakce s uživatelským rozhraním, jako jsou klikání na odkazy, vyplňování formulářů, odesílání požadavků a kontrola výstupů. Cílem bylo ověřit, že uživatelské rozhraní je intuitivní, funkční a odpovídá očekáváním uživatele.

Také se zkoumalo, zda jsou všechny funkce dostupné a pracují správně, ať už jde o navigaci mezi stránkami, odesílání formulářů nebo zobrazování dat. Při manuálním testování byly také sledovány scénáře použití, abychom se ujistili, že aplikace funguje přesně tak, jak bylo zamýšleno.

```
(.venv) [han@archlinux tool]$ python test.py
Results from database: <Results 1>
Total counts: A=3, B=1, C=1
.
----------------------------------------------------------------------
Ran 1 test in 0.091s

OK
```

Obrázek 43: Výsledek unit testu pro algoritmus *calculate_results*

Testování rychlosti aplikace bylo provedeno s cílem zjistit, jak rychle aplikace reaguje na různé uživatelské požadavky a operace.

V neposlední řadě bylo provedeno manuální testování kompatibility, kdy byla webová aplikace testována v různých prohlížečích s cílem zajistit, že neztratila žádnou funkcionalitu.

7 BEZPEČNOSTNÍ MECHANISMY

Poslední kapitola se zabývá bezpečnostními mechanismy implementovanými ve webové aplikaci. Bezpečnostní opatření jsou klíčovým prvkem každé webové aplikace, zejména v kontextu ochrany uživatelských dat a zabránění potenciálním hrozbám jako je zneužití, únik dat nebo neoprávněný přístup.

7.1 Autentizace a autorizace

Pro ověření totožnosti uživatele byl implementován systém autentizace, který vyžaduje přihlášení pomocí uživatelského jména a hesla. Dále byl implementován systém autorizace, který řídí oprávnění uživatelů a určuje, které části aplikace mohou jednotliví uživatelé přistupovat.

Nepřihlášení uživatelé jsou přesměrováni na indexovou stránku, kde mají možnost přihlášení nebo registrace, tedy provedení autentizace. Obě tyto stránky jsou přístupné i bez autorizace, což umožňuje všem uživatelům přistupovat k těmto formulářům.

Po úspěšném přihlášení je uživatel přesměrován na domovskou stránku, která je určena pro autentizované uživatele. Na této stránce je uživateli přiděleno session ID, které slouží jako identifikátor uživatele v rámci webové aplikace.

Následně má uživatel přístup ke všem stránkám, které vyžadují autorizaci. To zahrnuje jak stránky pro analýzu kybernetické bezpečnosti a prohlížení výsledků analýzy. Po vykonání uživatelských potřeb ve webové aplikaci má uživatel zbavit se své autorizaci odhlášením z webové aplikace. Session se taky uzavře za 30 minut po posledním požadavku (Obr. 44).

```python
@app.before_request
def update_last_activity():
    session.permanent = True
    session.modified = True
    session['last_activity'] = datetime.now()


def check_session_timeout():
    last_activity = session.get('last_activity')
    if last_activity is not None:
        delta = datetime.now() - last_activity
        if delta.seconds > 1800:
            session.clear()
            return redirect(url_for('login_page'))

@app.before_request
def before_request():
    check_session_timeout()
    session['last_activity'] = datetime.now()
```

Obrázek 44: Uzavření session po 30minutovém intervalu

7.2 HTTPS

Jedním z klíčových aspektů zabezpečení webových aplikací je používání protokolu HTTPS (Hypertext Transfer Protocol Secure) pro veškerou komunikaci mezi klientem a serverem. HTTPS využívá šifrování dat pomocí protokolu SSL/TLS (Secure Sockets Layer/Transport Layer Security), což zajišťuje důvěrnost, integritu a autenticitu dat přenášených mezi klientem a serverem.

Webová aplikace bude hostována na platformě Render.com, která poskytuje robustní a uživatelsky přívětivé řešení pro nasazení a provoz webových aplikací v cloudu. Platforma Render.com poskytuje zabezpečené prostředí pro provoz vaší aplikace v cloudu a automaticky poskytuje certifikáty SSL/TLS pro zabezpečení přenosu dat pomocí HTTPS.

7.3 Cross-Site Request Forgery

K ochraně před CSRF (Cross-Site Request Forgery) útoky byla v aplikaci implementována ochrana pomocí tokenů. Každý formulář v aplikaci obsahuje unikátní CSRF token, který je ověřován při odesílání formulářů a chrání aplikaci před neoprávněným předáváním požadavků.
Do webové aplikace bylo tohle zabezpečení importované pomocí knihovny from "flask_wtf.csrf import CSRFProtect". Dalším krokem po importu CSRFProtect je generování a nastavení tajného klíče, který bude použit pro podepisování CSRF tokenů a ověřování jejich pravosti. Tento tajný klíč musí být dostatečně náhodný a bezpečný a nezveřejněný, aby předešel odhalení a zneužití.

Nakonec se pro každý formulář vygeneruje CSRF token (Obr. 45). Tento kód zajistí, že při odesílání formulářů na server bude automaticky přidán CSRF token do hlaviček požadavku. Tím je zajištěno, že každý formulářový požadavek je chráněn proti CSRF útokům. Tímto způsobem je zabezpečení jak na straně serveru, tak i na straně klienta, což poskytuje robustní ochranu webové aplikace proti různým bezpečnostním hrozbám.

```
<script>
    function getCSRFToken() {
        var cookieValue = null;
        if (document.cookie && document.cookie !== '') {
            var cookies = document.cookie.split(';');
            for (var i = 0; i < cookies.length; i++) {
                var cookie = cookies[i].trim();
                if (cookie.substring(0, 'csrf_token'.length + 1) === (' ' + 'csrf_token' + '=')) {
                    cookieValue = decodeURIComponent(cookie.substring('csrf_token'.length + 1));
                    break;
                }
            }
        }
        return cookieValue;
    }

    document.getElementById('registerForm').addEventListener('submit', function (event) {
        event.preventDefault();

        var csrfToken = getCSRFToken();

        var headers = new Headers();
        headers.append('X-CSRFToken', csrfToken);

        fetch(this.action, {
            method: 'POST',
            headers: headers,
            body: new FormData(this)
        }).then(response => {
        }).catch(error => {
        });
    });
</script>
```

Obrázek 45: Script pro generování *CSRF* tokenu

7.4 Brute force attack

Efektivní obrana proti brute force útokům ve webové aplikaci je realizována několika způsoby. Pro formuláře jsou nastaveny tzv. limiter, které nám zaručují, že od jedné IP adresy je možné poslat požadavky na server pouze v určitém množství za daný časový interval. Tímto dojde k výraznému zpomalení procesu útoku, jelikož útočník bude limitován v počtu pokusů během daného časového období.

Kromě toho je zde implementován další limiter (Obr. 48), který po každém neúspěšném požadavku na přihlášení zpomalí odpověď serveru. Tím se minimalizuje riziko úspěšného útoku a ztíží se automatizovaným nástrojům možnost rychle provádět opakované pokusy.

Pro implementaci limiteru (Obr. 46) do webové aplikace je nejprve zapotřebí importovat knihovnu "from flask_limiter import Limiter" a poté je třeba tuto knihovnu zavolat nad trasováním jednotlivých formulářů (Obr. 47), aby bylo možné nastavit omezení pro konkrétní cesty nebo funkce. Tímto způsobem je možné nastavit limity pro maximální počet požadavků z jedné IP adresy v daném časovém intervalu, což poskytuje účinnou ochranu proti brute force útokům.

```python
limiter = Limiter(
    app,
    key_func=get_remote_address,
    default_limits=["5 per minute"]
)
```

Obrázek 46: Implementace limitéru

```python
@app.route("/login", methods=["GET", "POST"])
@limiter.limit("5 per minute")
def login_page():
    browser_language = translations.get_browser_language(request)

    if browser_language.startswith('cs'):
        selected_translations = translations.czech_translations
    else:
        selected_translations = translations.english_translations
```

Obrázek 47: Zavolání limitéru do trasování

```python
@limiter.request_filter
def slow_down_responses():
    if request.endpoint == 'login_page' and g.login_failed:
        sleep(2)
```

Obrázek 48: Ukázka limitéru pro zpoždění odpovědi od serveru

ZÁVĚR

Cílem bakalářské práce bylo vytvoření webové aplikace, která by firmám pomohla s analýzou kybernetické bezpečnosti, a tak usnadnila rozpoznávání a reakci na kybernetické hrozby. Práce se zaměřila na vývoj jednoduchého softwarového nástroje, který umožní firmám efektivně analyzovat jejich kybernetické prostředí a identifikovat potenciální slabiny a rizika. Tento nástroj by měl poskytovat uživatelům přehledné a srozumitelné informace o stavu jejich kybernetické bezpečnosti.

V teoretické části práce byla provedena analýza legislativního prostředí týkajícího se kybernetické bezpečnosti v různých částech světa. V rámci Spojených států amerických byly zkoumány klíčové zákony jako Zákon o zvýšení kybernetické bezpečnosti, Federální zákon o modernizaci bezpečnosti informací (FISMA), a Zákon o sdílení informací o kybernetické bezpečnosti (CISA). V Evropské unii byla analyzována legislativa jako Obecné nařízení o ochraně osobních údajů (GDPR), Směrnice o bezpečnosti sítí a informačních systémů (směrnice NIS) a ePrivacy Regulation. V České republice byl zkoumán Zákon o kybernetické bezpečnosti (Act No. 181/2014 Coll.). Srovnání různých přístupů k regulaci kybernetické bezpečnosti a ochrany osobních údajů bylo provedeno s cílem identifikovat nejlepší postupy pro dodržování kybernetických předpisů v podnikovém prostředí.

V praktické části práce byl navržen nástroj pro dodržování kybernetických předpisů, který měl organizacím pomoci s jejich implementací a udržováním. Systém byl zaměřen na řízení bezpečnosti informací, které zahrnovalo řízení aktiv, řízení rizik, organizační bezpečnost, a řízení dodavatelů. Další okruhy otázek zahrnovaly oblasti jako politiky a postupy, školení a vzdělávání, a incidentní řízení.

Následně byl vyvinut multiplatformní software s důrazem na jeho dostupnost a použitelnost. Front-end aplikace byl navržen tak, aby byl intuitivní a uživatelsky přívětivý, zatímco back-end byl implementován s důrazem na efektivní zpracování dat a analýzu.

Analýza funkcí a souborů nástroje byla provedena s cílem identifikovat klíčové prvky a procesy, které budou implementovány v aplikaci. To zahrnovalo konfigurační soubor pro nastavení uživatelských preferencí, funkce pro registraci a přihlášení uživatele, algoritmus pro analýzu dat, a mechanismus pro výpočet výsledků analýzy.

Dále byl navržen a implementován databázový model pro ukládání a správu dat v aplikaci. Bylo zajištěno šifrování dat v databázi pro ochranu citlivých informací před neoprávněným přístupem.

Aplikace prošla bezpečnostním a funkčním testováním, aby bylo ověřeno, že splňuje stanovené požadavky a je chráněna před kybernetickými hrozbami. Mezi testované oblasti patřilo bezpečnostní testování, zaměřené na odhalení možných zranitelností a nedostatků v bezpečnosti, a funkční testování, které ověřilo správnou funkčnost a uživatelskou přívětivost aplikace.

Nakonec byly implementovány bezpečnostní mechanismy jako autentizace a autorizace, použití protokolu HTTPS pro zabezpečení přenosu dat, ochrana proti Cross-Site Request Forgery (CSRF) útokům a obrana proti brute force útokům.

SEZNAM POUŽITÉ LITERATURY

[1] S.3600 - Strengthening American Cybersecurity Act of 2022. Online. Congress.gov. 2022. Dostupné z: https://www.congress.gov/bill/117th-congress/senate-bill/3600. [cit. 2024-03-01].

[2] The Federal Information Security Management Act. Online. In: Hyperproof. 2023. Dostupné z: https://hyperproof.io/wp-content/uploads/2023/06/framework-informational-page_hero-badges-fisma.png. [cit. 2024-05-10].

[3] Federal Information Security Management Act of 2002. Online. 2023. Dostupné z: https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002. [cit. 2024-02-28].

[4] Cybersecurity and Infrastructure Security Agency. Online. In: Wikipedia. [2023]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/thumb/6/6d/Seal_of_Cybersecurity_and_Infrastructure_Security_Agency.svg/220px-Seal_of_Cybersecurity_and_Infrastructure_Security_Agency.svg.png. [cit. 2024-05-10].

[5] CYBERSECURITY AND INFRASTRUCTURE SECURITY. Online. 2021. Dostupné z: https://www.cisa.gov/sites/default/files/publications/CISA-Factsheet_16-Dec-2021-V4_508.pdf. [cit. 2024-02-28].

[6] An Introduction to the Functions. Online. In: Nist. 2018. Dostupné z: https://www.nist.gov/sites/default/files/styles/220_x_220_limit/public/images/2018/04/12/ipdrr_circle.png?itok=qV5agiH5. [cit. 2024-05-10].

[7] Framework for Improving Critical Infrastructure Cybersecurity. Online. Nist.gov. 2018. Dostupné z: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. [cit. 2024-03-27].

[8] An Introduction to the Functions. Online. In: Nist. 2018. Dostupné z: https://eu-images.contentstack.com/v3/assets/blt6d90778a997de1cd/blt339126f871d3f624/64f17d993fae843f4d51fbf7/CSF-wheel-revamp-final-white.png?width=850&auto=webp&quality=95&format=jpg&disable=upscale. [cit. 2024-05-10].

[9] The NIST Cybersecurity Framework (CSF) 2.0. Online. 2024. Dostupné z: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. [cit. 2024-02-28].

[10] Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Online. 2022. Dostupné z: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia. [cit. 2024-03-01].

[11] Cyber Incident Reporting Act: What it means for your organization. Online. 2022. Dostupné z: https://www.cshub.com/executive-decisions/news/cyber-incident-reporting-act-what-it-means-for-your-organization. [cit. 2024-03-01].

[12] Cyber Incident Reporting for Critical Infrastructure Act. Online. 2021. Dostupné z: https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Overview%20of%20Cyber%20Incident%20Reporting%20Legislation.pdf. [cit. 2024-03-01].

[13] GDPR logo. Online. In: Atlassian. [2018]. Dostupné z: https://wac-cdn.atlassian.com/dam/jcr:4da170c1-40f1-434d-9595-854785de7bd5/gdpr.png?cdnVersion=1715. [cit. 2024-05-10].

[14] 4 key benefits for companies complying with GDPR. Online. Advisera. [2018]. Dostupné z: https://advisera.com/articles/4-key-benefits-for-companies-complying-with-gdpr/. [cit. 2024-03-27].

[15] Top 10+ Benefits of GDPR for Businesses. Online. Theknowledgeacademy. 2023. Dostupné z: https://www.theknowledgeacademy.com/blog/benefits-of-gdpr/. [cit. 2024-03-27].

[16] Directive on security of network and information systems (NIS Directive). Online. Europarl.europa. 2020. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI%282020%29654198_EN.pdf. [cit. 2024-03-27].

[17] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Online. Eur-lex.europa. 2019. Dostupné z: https://eur-lex.europa.eu/eli/reg/2019/881/oj. [cit. 2024-03-27].

[18] Proposal for an ePrivacy Regulation. Online. Digital-strategy.ec.europa. 2023. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation. [cit. 2024-03-27].

[19] What will Europe’s e-privacy regulation mean for your business? Online. Mckinsey. 2019. Dostupné z: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/what-will-europes-eprivacy-regulation-mean-for-your-business. [cit. 2024-03-27].

[20] ACT No 181/2014 Coll. Online. Nukib.gov. 2014. Dostupné z: https://nukib.gov.cz/download/publications_en/legislation/Act_181_2014_EN.pdf. [cit. 2024-03-27].

[21] DHS Calls for Critical Harmonization of Cyber Incident Reporting. Online. Wiley. 2023. Dostupné z: https://www.wiley.law/alert-DHS-Calls-for-Critical-Harmonization-of-Cyber-Incident-Reporting. [cit. 2024-04-08].

[22] Why global harmonisation of cybersecurity would be music to everyone's ears. Online. Weforum. 2022. Dostupné z: https://www.weforum.org/agenda/2022/03/why-global-harmonisation-of-cybersecurity-regulations-would-be-like-music-to-our-ears/. [cit. 2024-04-08].

[23] PENALTIES FOR NON-COMPLIANCE WITH FISMA (AND HOW TO AVOID THEM). Online. Blog.rsisecurity. 2018. Dostupné z: https://blog.rsisecurity.com/penalties-for-non-compliance-with-fisma-and-how-to-avoid-them/. [cit. 2024-04-08].

[24] Certifikace CISA - Požadavky. Online. Isaca. [2021]. Dostupné z: http://www.isaca.cz/cs/certifikace-cisa-pozadavky. [cit. 2024-04-08].

[25] Co je NIS2. Online. Aptien. 2023. Dostupné z: https://aptien.com/cs/kb/articles/what-is-nis2. [cit. 2024-04-08].

[26] Legislativa KB. Online. Nukib.gov. [2023]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/. [cit. 2024-04-08].

[27] Proposal for an ePrivacy Regulation. Online. Commission.europa. 2023. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation. [cit. 2024-04-08].

[28] Vyhláška č. 82/2018 Sb. Online. Zákony pro lidi. 2018. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#cast2. [cit. 2024-05-11].

SEZNAM OBRÁZKŮ

Obrázek 1: The Federal Information Security Management Act [2].....13
Obrázek 2: logo zákonu o sdílení informací o kybernetické bezpečnosti [4].....14
Obrázek 3: Základní funkce NIST [6].....15
Obrázek 4: Národní institut pro standarty a technologie [8].....17
Obrázek 5: Obecné nařízení o ochraně osobních údajů [13].....19
Obrázek 6: Ukázka první otázky v nástroji.....26
Obrázek 7: Ukázka otázky pro řízení aktiv.....28
Obrázek 8: Otázka č.4 řízení aktiv.....29
Obrázek 9: Otázka Hodnocení primárních aktiv.....30
Obrázek 10: Otázka hodnocení primárních aktiv.....31
Obrázek 11: Otázka řízení rizik.....32
Obrázek 12: Otázka řízení rizik.....33
Obrázek 13: Otázka organizační bezpečnost.....34
Obrázek 14: Otázka organizační bezpečnost.....34
Obrázek 15: Otázka organizační bezpečnost.....35
Obrázek 16: Otázka organizační bezpečnost.....36
Obrázek 17: Otázka řízení dodavatelů.....37
Obrázek 18: Otázka řízení dodavatelů.....38
Obrázek 19: Script pro Tailwind CLI build.....41
Obrázek 20: Ukázka Tailwind CSS header komponenty.....42
Obrázek 21: Index stránka.....42
Obrázek 22: Stránka registrace.....43
Obrázek 23: Přihlašovací stránka.....43
Obrázek 24: Domovská stránka pro přihlášené uživatelé.....44
Obrázek 25: Stránka *analýzy* ve které se provádí vyplnění otázky.....45
Obrázek 26: Stránka result a výsledek analýzy.....45
Obrázek 27: Ukázka konfiguračního souboru app.py.....49
Obrázek 28: Ukázka trasování a vytvoření databáze.....49
Obrázek 29: Funkce pro silné heslo.....50
Obrázek 30: Registrace v konfiguračním souboru.....51
Obrázek 31: Uložení dat z front-endu do databáze.....52
Obrázek 32: Výpočet hodnot odpovědí a zapsání do tabulky Results.....52
Obrázek 33: Výpočet analýzy rizik kybernetické bezpečnsti.....53

Obrázek 34: Relační model databáze.....55
Obrázek 35: Ukázka hashování a šifrování dat do databáze.....56
Obrázek 36: Implementování šifry *AES-256*.....56
Obrázek 37: Ukázka dešifrování a kontrola hashe.....57
Obrázek 38: Ochrana proti SQL injection.....58
Obrázek 39: SQLmap testování aplikace.....59
Obrázek 40: XSS zranitelnost.....59
Obrázek 41: Kontrola Cross Site Scripting zranitelnosti.....60
Obrázek 42: Unit test pro algoritmus calculate_results.....61
Obrázek 43: Výsledek unit testu pro algoritmus calculate_results.....62
Obrázek 44: Uzavření session po 30 minutovém intervalu.....63
Obrázek 45: Script pro generování *CSRF* tokenu.....65
Obrázek 46: Implementace limitéru.....66
Obrázek 47: Zavolání limitéru do trasování.....66
Obrázek 48: Ukázka limitéru pro zpoždění odpovědi od serveru.....66