Zabezpečení informačního systému společnosti HFL

Bc. Lukáš Solárik, DiS. art.

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Lukáš Solárik, DiS.**
Osobní číslo:	**A16427**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Zabezpečení informačního systému společnosti HFL**
Téma anglicky:	**The Security of the HFL Company's Information System**

Zásady pro vypracování:

1. **Definujte základní pojmy týkající se bezpečnosti informačních systémů.**
2. **Analyzujte aktuální zákonné požadavky a povinnosti v předmětné problematice.**
3. **Stanovte obecný katalog hrozeb informačního systému.**
4. **Zpracujte audit informační bezpečnosti vybraného informačního systému.**
5. **Navrhněte zabezpečení vybraného informačního systému.**
6. **Implementujte navržené a další vrstvy zabezpečení IS.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978-80-7454-312-8.**
2. **STAUDEK, Jan a Petr HANÁČEK. Bezpečnost informačních systémů. 1. vyd. Praha: Úřad pro státní informační systém, 2000. 127 s. ISBN 80-238-5400-3.**
3. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN 8025101061.**
4. **BARTONĚK, Dalibor a Robert JURČA. Informační systémy. Kunovice: Evropský polytechnický institut, 2014. ISBN 978-80-7314-322-4.**
5. **DOBDA, Luboš. Ochrana dat v informačních systémech. 1. vyd. Praha: Grada Publishing, 1998, 286 s. ISBN 80-716-9479-7.**
6. **GDPR: Obecné nařízení o ochraně osobních údajů prakticky [online]. 2017. Dostupné z: https://www.gdpr.cz/.**

Vedoucí diplomové práce: **Ing. Martin Hromada, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. prosince 2017**

Termín odevzdání diplomové práce: **28. května 2018**

Ve Zlíně dne 8. prosince 2017

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že na moji diplomovou 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 – diplomovou 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 diplomové 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 diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové 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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 21. 5. 2018

.....
podpis diplomanta

ABSTRAKT

Cieľom diplomovej práce je implementácia zabezpečenia informačného systému spoločnosti Housing for Life. Teoretická časť práce pojednáva o zákonných požiadavkách vo vzťahu k informačnej bezpečnosti a taktiež je stanovený obecný katalóg hrozieb pre webový informačný systém. V praktickej časti je realizovaná analýza rizík vybraných hrozieb a návrh zabezpečenia s využitím dvojfaktorového overenia pri prihlasovaní. V závere praktickej časti je implementácia navrhnutých opatrení, ktoré umožnia vytvoriť ďalšie vrstvy zabezpečenia, čo zníži riziko získania prístupu a kontroly nad účtom.

Kľúčové slová: bezpečnosť, webový informačný systém, prihlásenie, dvojfaktorové overenie

ABSTRACT

The aim of the diploma thesis is to implement the Housing for Life information system security. The theoretical part of the thesis deals with the legal requirements in relation to information security and also provides a general catalogue of threats for the web information system. The practical part analyses the risks of selected threats and the proposal of security using two-factor authentication upon login. At the end of the practical part is the implementation of proposed measures that will allow the creation of additional layers of security, which will reduce the risk of gain access and control over the account.

Keywords: Security, Web information system, Login, Two-factor authentication

Poďakovanie a motto

Ďakujem doc. Ing. Martinovi Hromadovi, Ph.D. za cenné rady a odborné vedenie pri vypracovávaní tejto práce. Ďalej ďakujem Martinovi Marečkovi zo spoločnosti Housing for Life, SE za umožnenie realizácie tejto diplomovej práce a poskytnutie potrebných informácií. V neposlednom rade chcem poďakovať svojej rodine, ktorá ma podporovala počas celého štúdia.

„Nestrácaj čas vysvetľovaním, ľudia aj tak počujú len to, čo chcú počuť."

(Paulo Coelho)

Prehlasujem, že odovzdaná verzia diplomovej práce a verzia elektronická nahraná do IS/STAG, sú totožné.

OBSAH

ÚVOD

Či už chceme alebo nie, s informáciami v digitálnej podobe sa dnes stretávame doslova na každom kroku. Máme doma počítače, notebooky, tablety a skoro každý má v dnešnej dobe u seba minimálne jeden mobilný telefón. Jednou z vecí, čo majú tieto navonok rozdielne zariadenia spoločné, je ich obsah. Sú nositeľmi informácií. A nie hocijakých, ale tých najdôležitejších. V tomto okamžiku prichádza na rad otázka ich bezpečnosti, ktorú stále viac ľudí berie vážne a snažia sa o ich dokonalé zabezpečenie. V dnešnom svete počítačov a informačných technológií je však často veľmi náročné dosiahnuť aspoň uspokojivého stavu zabezpečenia, no nie celkom nemožné.

Svoju dôveru taktiež vkladáme do rôznych firiem a spoločností, ktoré po nás za účelom poskytovania kvalitných služieb niektoré z vyššie uvedených údajov vyžadujú, alebo ktoré im poskytujeme dobrovoľne. Preto by pre všetky spoločnosti malo byť prioritou chránenie údajov svojich zákazníkov a klientov vo svojich informačných systémoch a iných aplikáciách, na ktoré sa však v mnohých prípadoch valia útoky zo všetkých strán.

Cieľom diplomovej práce bude implementácia zabezpečenia informačného systému spoločnosti Housing for Life. Teoretická časť práce bude pojednávať o zákonných požiadavkách a povinnostiach vo vzťahu k informačnej bezpečnosti a to aj vo vzťahu k ukladaniu osobných a iných citlivých dát. V praktickej časti bude realizovaný audit informačnej bezpečnosti a návrh zabezpečenia a to aj s využitím Google autentizácie pre jednoznačnú identifikáciu. Implementácia ďalších opatrení umožní vytvoriť ďalšie vrstvy zabezpečenia, čo zníži riziko získania prístupu a kontroly nad účtom.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÉ POJMY TÝKAJÚCE SA BEZPEČNOSTI INFORMAČNÝCH SYSTÉMOV

I keď je to málo pravdepodobné, ale môže sa stať, že sa ešte niekto nestretol so žiadnym informačným systémom, dokonca ani s týmto termínom, je dôležité si ozrejmiť základné pojmy tejto problematiky hneď na začiatku a najhlavnejšie sú uvedené priamo v názve kapitoly a to informačný systém a jeho bezpečnosť.

1.1 Informácia

Je všeobecne známe, že každá veta, každé slovo, vyjadrené ústne alebo na papieri, je informácia. A či už je pravdivá, nepravdivá, pozitívna alebo negatívna, má nejakú hodnotu. Denne prijmeme nespočetné množstvo informácií, s ktorými môžeme nakladať rôzne. Môžeme ich ignorovať, uchovať v pamäti alebo ďalej predávať. Takisto sú aj rôzne spôsoby, akými tieto informácie preberáme alebo ukladáme. Príchodom počítačov sa stalo bežným komunikovať, uchovávať a predávať si informácie väčšinou už len „moderným“ spôsobom – digitálne.

Informácia teda už nie je len výsledok verbálnej alebo písomnej komunikácie medzi ľuďmi, uložením informácie v elektronickej podobe sa stáva skutočným, no stále nehmotným majetkom, preto sa dá povedať, že informácia je základnou stavebnou jednotkou informačného systému. [1]

1.2 Informačný systém

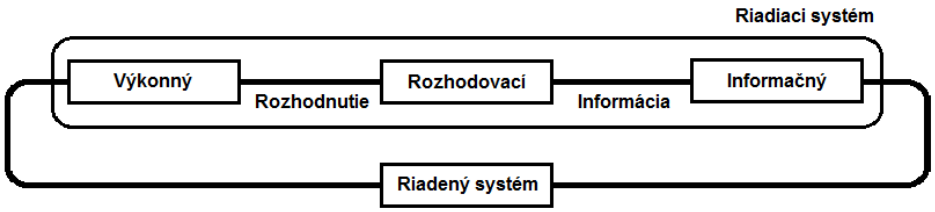
V rôznych literatúrach existuje veľa definícií informačného systému napríklad:

„Informačný systém je súbor ľudí, technických prostriedkov a metód zabezpečujúci zber, prenos, spracovanie, uchovanie dát za účelom prezentácie informácií pre potreby užívateľov.“ [2]

V predmetnej problematike však z technického hľadiska informačný systém môže znamenať systém, zložený z počítačového hardvéru a softvéru, ktorý spracováva a poskytuje užívateľom uložené informácie v podobe dát. [3]

Informačný systém býva považovaný za súčasť alebo podsystém riadiaceho systému, ktorého hlavnou úlohou je spracovanie a poskytovanie informácií riadiacemu systému, potrebných k výberu cieľov a nástrojov riadenia sociálno-ekonomických procesov. Na obráz-

ku (Obr. 1) je znázornený vzťah informačného systému k riadiacemu systému a ostatným podsystémom. [4]



Obr. 1. Vzťah IS k riadiacemu systému. [4]

Takže ako bolo uvedené v prvej definícii, nie je to len o technike, počítačoch, serveroch, skrátka o jednotkách a nulách. Nemenej dôležitú úlohu popri technickej stránke hrá tiež spracovateľ týchto informácií. Avšak je nutné hneď podotknúť, že zároveň sám človek, užívateľ informačného systému, je jednou z najväčších bezpečnostných hrozieb najmä pre dôvernosť dát informačného systému – informačnú bezpečnosť.

1.3 Informačná bezpečnosť

Informačná bezpečnosť predstavuje ochranu všetkých informácií vo všetkých formách (elektronická, papierová, atď.) počas ich celého životného cyklu, tzn. behom ich vzniku, spracovania, uloženia, prenosu a likvidácie. Cieľom informačnej bezpečnosti je zaistenie ochrany informácií pred narušením dôvernosti, integrity a dostupnosti, ktoré by mohlo mať za následok napríklad:

- získanie a únik dôverných informácií,
- neautorizovaná manipulácia s dátami,
- nedostupnosť služieb a dát. [1]

V prípade elektronickej formy informácií v podobe dát by teda mali byť chránené:

- v pokoji – malo by byť zabezpečené, že s k týmto dátam, uloženým na nejakom úložisku dostane len užívateľ, ktorý má povolený prístup,
- behom prenosu – prenášané dáta (najmä cez internet) by mali byť šifrované,
- pri používaní – aktivity užívateľa pri manipulácii s dátami by mali byť zaznamenávané. [5]

1.4 Desktopový vs. webový informačný systém

Podľa druhej definície informačného systému z kapitoly 1.2, sa systém skladá z počítačového hardvéru a softvéru, kde hardvérom môže byť označený stolný (osobný) počítač alebo server, a softvér predstavuje samotnú aplikáciu. Tie sa potom tiež rozdeľujú podľa typu zariadenia, na ktorom sú prevádzkované.

Momentálne sa rozoznávajú najmä 3 typy aplikácií – desktopové, webové a mobilné. V prípade informačných systémov sú to zatiaľ len prvé dve z menovaných, pokiaľ sa neráta mobilná verzia desktopovej alebo webovej aplikácie.

Desktopové aplikácie

Desktopová aplikácia je softvér alebo program, ktorý je nainštalovaný v operačnom systéme na stolnom alebo osobnom počítači. Najväčšou výhodou desktopových aplikácií je, že fungujú nezávisle na internetovom pripojení, čiže sú užívateľovi k dispozícii prakticky neustále. Taktiež sú väčšinou rýchle, no závisí to aj od výkonu hardvéru počítača. Ich hlavnou nevýhodou však je, že sa dajú ľahko zavírovať a potrebujú pravidelné bezpečnostné aktualizácie. [6]

Webové aplikácie

Webová aplikácia je program, ktorý sa nachádza na webovom serveri a užívateľským rozhraním je webový prehliadač. Prakticky je to teda webová stránka, ktorá však neslúži len na zobrazenie statického obsahu, ale jej súčasťou je tiež programový kód, ktorý zabezpečuje nejakú funkcionalitu – vykonáva užívateľom požadované operácie so zobrazovanými dátami. Výhodou webových aplikácií je, že všetky potrebné dáta sú dostupné všetkým užívateľom na jednom mieste. Taktiež užívateľ nemusí nič inštalovať. Sú však závislé na internetovom pripojení, čím sú zraniteľnejšie voči kybernetickým útokom. [6]

Keďže daný informačný systém beží na webovom serveri a užívateľ k nemu pristupuje z okna webového prehliadača, spadá do kategórie webových aplikácií. Na základe uvedených informácií sa teda bude v tejto práci naďalej používať termín webový informačný systém, prípadne webová aplikácia.

Prvá kapitola bola venovaná základným pojmom v oblasti informačných systémov a informačnej bezpečnosti. Nakoniec bol vysvetlený rozdiel medzi desktopovým a webovým informačným systémom a ich výhody, či nevýhody.

2 AKTUÁLNE ZÁKONNÉ POŽIADAVKY A POVINNOSTI V PREDMETNEJ PROBLEMATIKE

V tejto kapitole budú analyzované zákonné požiadavky a povinnosti vo vzťahu k informačnej bezpečnosti a ukladaniu osobných a iných citlivých dát, ktoré v súčasnej dobe najviac ovplyvňujú vývoj informačných systémov a iných aplikácií.

2.1 Nariadenie GDPR

GDPR (General Data Protection Regulation), alebo Všeobecné nariadenie na ochranu osobných údajov je nové nariadenie Európskej únie o ochrane fyzických osôb v súvislosti so spracovaním osobných údajov, ktoré v Českej republike nahradí súčasný súvisiaci zákon č. 101/2000 Zb., o ochrane osobných údajov.

Toto nariadenie prináša celú radu nových povinností a zásadným spôsobom sprísňuje pravidlá ich správy. Ako však uvádza Čermák [7] hneď na úvod svojho článku o požiadavkách GDPR: *„Nevím, proč se z toho dělá taková věda. Přijde mi to, jako kdyby doteď nikdo osobní data svých klientů nechránil, ignoroval požadavky Zákona 101 a čekal jen na nějaké nařízení z EU.“* a v podstate má autor celkom pravdu, pretože daný zákon vždy jasne, niekedy aj špecifickejšie stanovoval pravidlá a povinnosti ako zaobchádzať s osobnými údajmi, o čom svedčí aj prevodná tabuľka Zákona 101 a nariadenia GDPR, vydaná Úradom pre ochranu osobných údajov (dostupná na stránkach ÚOOÚ), v ktorej je vidieť, že každý článok nariadenia má svoje zastúpenie v nejakom paragrafe alebo odseku Zákona 101. Opačne tomu však viac-menej nie je.

Jedným z hlavných dôvodov tak veľkého rozruchu okolo nariadenia GDPR je, že spracovateľom osobných údajov za nedodržanie stanovených povinností a nariadení hrozia astronomické pokuty až do výšky 20 miliónov eur alebo 4% z ročného obratu. [8]

Dôležitou novinkou, najmä v oblasti vývoja a správy informačného systému, ktoré nariadenie prináša je, že osoba, ktorej sa zhromažďovanie osobných údajov týka, môže požadovať svoje údaje zmeniť, zmazať, preniesť, alebo má jednoducho právo sa dozvedieť aké a za akým účelom daná organizácia údaje spracováva a vo väčšine prípadov, až na stanovené výnimky jej musí správca údajov spoločnosti v plnom rozsahu vyhovieť. To znamená, že vyvíjaný informačný systém by už mal byť na všetky uvedené úkony pripravený. [7]

Nariadenie GDPR sa týka všetkých subjektov, ktoré na území EÚ spracovávajú osobné údaje jej občanov, čiže zamestnancov, zákazníkov, klientov alebo dodávateľov, no vymedzenie pojmu osobných údajov je pomerne široké a dá sa rozdeliť do niekoľkých kategórií:

- obecné osobné údaje (dátum narodenia, pohlavie, vek, ...),
- citlivé osobné údaje (rasový pôvod, náboženské vyznanie, zdravotný stav, ...),
- biometrické údaje (obraz tváre, odtlačok prsta, podpis, ...),
- genetické údaje (DNA, ...). [9]

Nariadenie taktiež pre vývojárov a prevádzkovateľov informačných systémov zavádza nový, celkom zaujímavý proces a to Privacy by design (v preklade z angl. Ochrana súkromia už pri návrhu), alebo ako sa priamo v nariadení uvádza Data protection by design and by default, čo by sa dalo preložiť ako ochrana osobných údajov už pri návrhu a v predvolenom nastavení. U nás je to celkom nový pojem, no v okolitom svete to však nie je ničím novým. [10]

Je to vlastne súhrn metód, ktorých cieľom je aplikovať ochranu súkromia už do návrhu informačných systémov a obchodných postupov, ktoré by sa dali rozdeliť na sedem základných princípov:

- pro-aktívny než reaktívny prístup,
- ochrana súkromia v predvolenom nastavení,
- ochrana súkromia je integrovaná už v návrhu procesov,
- bezchybná funkčnosť,
- bezpečnosť dát počas ich celý životný cyklus,
- transparentnosť dát pre subjekt aj spracovateľa,
- rešpektovanie súkromia užívateľa. [10]

S príchodom nariadenia GDPR sú tiež vo svete IT často spomínané a diskutované pojmy ako anonymizácia, pseudonymizácia, či šifrovanie osobných údajov. Pre väčšinu ľudí majú tieto pojmy celkom rovnaký význam, no v skutočnosti ich podstata je veľmi rozdielna. [11]

Anonymizácia údajov je proces, v ktorom sa napríklad z databázy odstránia všetky identifikačné údaje, ktoré by mohli pomôcť znovu prepojiť spracovávané údaje s konkrétnou osobou. [12]

Pseudonymizácia je v podstate podobný, avšak nie nevratný proces, pri ktorom sa identifikačné údaje osoby alebo kľúče natrvalo neodstránia, no sú uložené tak, aby nemohli byť priradené danej osobe bez znalosti ďalších informácií. [12]

Nakoniec šifrovanie je od predošlých dvoch postupov celkom odlišný proces, ktorého podstatou je spracovávané údaje o danej osobe ukladať zašifrované, čiže nečitateľné pre osoby, ktoré k tomu nie sú oprávnené. [12]

Ďalšie doporučené postupy a procesy:

- zavedená politika silných hesiel,
- nezdieľať administrátorské práva s partnermi, či dodávateľmi,
- spoločná správa identity a oprávnení s využitím viacfaktorového overenia,
- používanie SSL/TLS certifikátov,
- logovanie administratívnych úkonov,
- logovať prístupy k osobným údajom. [13]

2.2 Zákon o kybernetickej bezpečnosti

Cieľom zákona č. 181/2014 Zb., o kybernetickej bezpečnosti je zvýšiť bezpečnosť kybernetického priestoru ako takého, najmä však kritickej infraštruktúry a informačných systémov, ktorých ohrozenie alebo narušenie by mohlo mať vážne dopady na fungovanie štátu.

Stanovuje spôsoby, akými má byť zaistená kybernetická bezpečnosť a reakcie na kybernetické hrozby alebo riešenie vzniknutých bezpečnostných incidentov. [14]

Zákon vymenováva dané odvetvia kritickej infraštruktúry, na ktoré sa kybernetická bezpečnosť najmä vzťahuje:

- energetika,
- doprava,
- bankovníctvo,
- infraštruktúra finančných trhov,
- zdravotníctvo,
- vodné hospodárstvo,
- digitálna infraštruktúra,
- chemický priemysel. [15]

Zákon taktiež definuje základné pojmy z oblasti kybernetickej bezpečnosti:

- kybernetický priestor – digitálne prostredie umožňujúce vznik, spracovanie a výmenu informácií,
- kybernetická bezpečnosť – súhrn prostriedkov k zaisteniu ochrany kybernetického priestoru,
- kybernetický bezpečnostný incident – udalosť, ktorá predstavuje narušenie bezpečnosti informácií, služieb alebo sietí elektronických komunikácií,
- stav kybernetického nebezpečenstva – stav, pri ktorom príde alebo by mohlo prísť k porušeniu alebo ohrozeniu záujmov ČR. [16]

Zákon v ďalšom paragrafe jasne vymenováva nasledujúce konkrétne subjekty a osoby, ktorým sa ukladajú povinnosti v oblasti kybernetickej bezpečnosti:

- poskytovateľ služby elektronických komunikácií a subjekt zaisťujúci sieť elektronických komunikácií,
- subjekt zaisťujúci významnú sieť,
- správca informačného systému kritickej informačnej infraštruktúry,
- správca komunikačného systému kritickej informačnej infraštruktúry,
- správca významného informačného systému,
- správca a prevádzkovateľ informačného systému základnej služby,
- prevádzkovateľ základnej služby a
- prevádzkovateľ digitálnej služby. [15]

Podľa uvedených bodov sa teda jedná len o subjekty, ktoré v rámci ČR zabezpečujú významnú elektronickú komunikáciu alebo prevádzkujú kritickú infraštruktúru.

Vymenované subjekty musia dodržiavať stanovené zákonné povinnosti, ktorých neplnenie môže viesť k uloženiu pokuty až 100 000Kč. [14]

Aj keď sa Zákon priamo nevzťahuje na subjekty súkromného sektora, pre vývojárov a správcov komerčných informačných systémov a iných aplikácií by však mohol byť daný Zákon a najmä Vyhláška o kybernetickej bezpečnosti, ktorá z neho vychádza, vhodnou metodikou pri ich vývoji. [14]

Vyhláška č. 316/2014 Zb., o kybernetickej bezpečnosti hovorí o bezpečnostných opatreniach, kybernetických bezpečnostných incidentoch, reaktívnych opatreniach a o stanovení náležitostí podania v oblasti kybernetickej bezpečnosti. [17]

Veľmi užitočnou pomôckou môže byť druhá časť Vyhlášky, o bezpečnostných opatreniach, najmä Hlava II o technických opatreniach, ktorá hovorí o fyzickej bezpečnosti a definuje rôzne ochranné a preventívne nástroje alebo prostriedky, ktoré by mali byť použité pri vývoji a správe informačných systémov (kritickej informačnej infraštruktúry).

Napríklad paragraf 18 definuje nástroje overovania identity užívateľa, kde špecifikuje parametre bezpečného hesla, ktoré musí:

- mať dĺžku aspoň osem znakov,
- obsahovať najmenej jedno veľké, malé písmeno, číslicu alebo iný znak,
- byť menené maximálne každých sto dní. [17]

Podľa § 19 Vyhlášky, musí byť v systéme použitý nástroj pre riadenie prístupových oprávnení, ktorý má zaistiť riadenie prístupu k jednotlivým aplikáciám, dátam, ich čítaniu, zápisu a pre zmenu oprávnení. [17]

Nakoniec dôležitým bodom tiež môže byť § 21, v ktorom sa hovorí o zaznamenávaní a monitorovaní činností informačného systému (kritickej informačnej infraštruktúry) a jeho užívateľov, či administrátorov, kde zodpovedné orgány a osoby musia zaistiť použitie nástrojov pre zaznamenávanie a zber informácií o prevádzkových a bezpečnostných činnostiach a následnú ochranu získaných dát pred neoprávneným čítaním alebo zmenou. [17]

Podľa odseku 2 tohto paragrafu nástroj musí zaznamenávať napríklad:

- prihlásenie a odhlásenie užívateľov a administrátorov,
- činnosti vykonané administrátorom,
- činnosti vedúce k zmene prístupových oprávnení,
- varovné alebo chybové hlásenia,
- prístupy k týmto záznamom o činnostiach a pokusy o manipuláciu s nimi. [17]

Druhá kapitola tejto práce bola zameraná na analýzu zákonných požiadaviek a povinností v predmetnej problematike. Bolo popísané nové Nariadenie Európskej únie o ochrane osobných údajov GDPR a Zákon o kybernetickej bezpečnosti.

3 OBECNÝ KATALÓG HROZIEB INFORMAČNÉHO SYSTÉMU

V nasledujúcej kapitole budú priblížené obecné princípy bezpečnosti informačného systému. Ďalej bude popísaný projekt OWASP, z ktorého bude vychádzať obecný katalóg hrozieb informačného systému, v ktorom sú uvedené ich špecifické vlastnosti a postupy, možní pôvodcovia a následné dopady v prípade ich úspešného prevedenia.

3.1 Bezpečnosť a bezpečnostné hrozby informačného systému

Podľa IT komunity bezpečnosť desktopového IS závisí hlavne od úrovne zabezpečenia a zraniteľnosti koncových zariadení, lokálnej (podnikovej) siete a schopnosti zamestnanca rozoznať potenciálne nebezpečenstvo v podobe snahy útočníka napadnúť daný systém alebo získať kontrolu nad jeho účtom apod. Zabezpečenie samotnej aplikácie (počítačového softwaru) v tomto prípade hrá menej významnú rolu, samozrejme okrem štandardného zabezpečenia pomocou prihlasovacieho mena a hesla, ktorého zároveň hlavnou úlohou je identifikácia konkrétneho užívateľa v rámci informačného systému. Pokiaľ sa však útočníkovi podarí získať kontrolu nad počítačom, je o krok bližšie k získaniu prístupu k dátam informačného systému. Preto sa všetka pozornosť zameriava na zabezpečenie podnikovej siete, samotných počítačov a iných koncových zariadení. [18]

U webového informačného systému je to však naopak. Z technického hľadiska je najzraniteľnejším článkom celého systému práve samotná aplikácia, pretože je súčasťou internetu, takže ktokoľvek, kto pozná presnú adresu môže zobraziť jej úvodnú stránku, alebo vo väčšine prípadov priamo prihlasovací formulár. Kľúčovým faktorom je teda úroveň zabezpečenia danej webovej aplikácie. [19]

Niektoré znaky majú však spoločné, ako napríklad spomínaný ľudský faktor, čo je asi najväčší kameň úrazu, pretože veľa útočníkov sa už nezameriava na prelomenie zabezpečenia aplikácie, ale práve na užívateľov. Využívajú ich nevedomosti, slabej informovanosti o možných hrozbách a tiež zvedavosti – v určitých prípadoch je to časovo i technicky menej náročné než skúšať napríklad útok hrubou silou alebo iných techník na prelomenie hesla. Typickým príkladom takého útoku môže byť napríklad veľmi rozšírený phishing.

3.1.1 Phishing a Spear Phishing

Phishing je druh nevyžiadanej pošty, ktorej cieľom útočníka je donútiť adresáta k zadaniu citlivých údajov alebo nakaziť jeho počítač nejakým malwarom. Jeho názov je odvodený

od anglického slova fishing, čo v preklade znamená rybolov. Princípom tohto útoku je, že útočník v emaile svoju obeť vyzve k otvoreniu prílohy, ktorá sa tvári napríklad ako PDF alebo RTF dokument, no v skutočnosti však obsahuje škodlivý kód, alebo ho vyzve ku kliknutiu na odkaz, ktorý potom obeť presmeruje na pripravenú webovú stránku, v ktorom sa nachádza jednoduchý kód (exploit), ten zneužíva konkrétnu zraniteľnosť v systéme alebo aplikácii a zaistí tak stiahnutie škodlivého kódu do jeho počítača. [20]

Spáchané následky tohto škodlivého kódu a celého útoku môžu byť pre užívateľa a napokon i pre rôzne systémy, ktoré používa, katastrofálne. Existuje však ešte nebezpečnejšia obdoba phishingu a tou je **Spear phishing**.

Zatiaľ čo pri klasickom phishingu sú emaily odosielané na veľké množstvo emailových adries a vďaka jeho štruktúre, zlej gramatike alebo podozrivého odosielateľa emailu, ho poučený zamestnanec alebo skúsený a obozretný užívateľ internetu dokáže rozpoznať, email spear phishingu je adresovaný jednej konkrétnej osobe a tvári sa, že prichádza alebo dokonca skutočne prichádza od (taktiež zneužitej) osoby, ktorú obeť dobre pozná. Preto sa spear (z angl. harpúna) phishing nazýva aj **cielený phishing**.

Najhoršie na celej skutočnosti je, že aj dobre informovaná a poučená obeť tohto typu phishingu nemá šancu rozpoznať, že sa jedná o phishing a teda účinnosť takéhoto útoku je väčšinou stopercentná.

Samozrejme, že prevedenie a hlavne príprava celého útoku (i oproti tradičnému phishingu) je veľmi zdĺhavá a náročná, ale napríklad v podnikovej sfére, keď sa jedna firma proste rozhodne, že zdiskredituje konkurenčnú firmu, tak to urobí stoj čo stoj a tieto faktory potom nehrajú žiadnu rolu. [21]

V prípade bežného človeka, býva predmetom záujmu útočníka väčšinou bankový alebo iný účet. Cieľom útočníka je prinútiť svoju obeť, aby sa prihlásila do jej internetového bankovníctva. Útočník pošle falošný email v mene jeho banky, ktorého obsah (výhodná ponuka, dôležité informácie apod.) nabáda kliknúť na priložený odkaz s cieľom prihlásiť sa do internetového bankovníctva. Obeť je po kliknutí presmerovaná na podvrhnutú stránku útočníka, ktorá vyzerá identicky ako skutočná prihlasovacia stránka jej banky, s tým rozdielom, že URL adresa je iná, ale spravidla podobná alebo minimálne pozmenená, čiže keď si neoverí na akej stránke sa to vlastne nachádza, vôbec nezistí, že sa jedná o podvrh. Následne zadaním svojich prihlasovacích údajov do formulára útočník okamžite získa prístupové údaje obete a môže vyprázdniť celé jej konto.

Vďaka týmto a podobným útokom začali banky a ďalšie finančné alebo iné inštitúcie používať dvojfaktorové overenie, čo je okrem iných zabezpečení tiež predmetom tejto diplomovej práce.

Problémom však je, že ľudia neberú rôzne výstrahy a upozornenia vážne. Sú príliš pohodlní aby si dvojfaktorové overenie aktivovali, alebo nastavenie a používanie tohto typu zabezpečenia je pre nich náročné, takže túto bezpečnostnú funkciu skrátka nevyužívajú. Potom sa však v kombinácii s ich nevedomosťou, zvedavosťou, krátkozrakosťou, ba dokonca niekedy aj ľahostajnosťou, stávajú obeťami tohto a podobných útokov a neuvedomujú si, že ako zamestnanci nejakej firmy sa takýmto správaním stávajú zároveň hrozbou pre jej informačný systém a firmu ako takú.

3.1.2 Užívateľ ako hrozba

Z pohľadu dôvernosti dát je najväčšou hrozbou pre ktorýkoľvek podnikový informačný systém sám užívateľ, pretože všetky vyššie uvedené prípady môžu nastať aj vo firme. Ako zamestnanec nejakého podniku, musí mať samozrejme prístup k všetkým dátam, ktoré potrebuje k vykonávaniu svojej práce a obecne platí, že čím vyššie je v hierarchii firmy postavený, tým má väčšie práva v systéme a prístup k viacerým, podrobnejším a citlivejším údajom ako jeho podriadení. Celý systém je tak dobrovoľne, no nevyhnutne vystavený riziku úniku dôležitých dát. Nejedna firma už má túto trpkú skúsenosť, že jej vlastní zamestnanci úmyselne vyniesli citlivé dáta von z firmy. Väčšinou sú to pracovníci, ktorí sa nepohodnú s vedením firmy a ako odplatu sa rozhodli dôležité informácie, ku ktorým majú prístup ukradnúť a následne použiť, zverejniť, predať konkurencii alebo inak výhodne speňažiť. Nie výnimočne sa tiež stáva, že tak robia potajomky dlhší čas a podnik si to ani nemusí všimnúť.

Uvádza sa, že za viac ako 80% bezpečnostných incidentov sú zodpovední práve samotní zamestnanci, no vo väčšine prípadov však nekonajú úmyselne, ale skôr z neznalosti alebo nedbanlivosti. [22]

Stávajú sa obeťami napríklad vyššie uvedených útokov a zvlášť obľúbeným cieľom sú vrcholoví manažéri, čiže zamestnanci s vyššími privilégiami a prístupmi v systéme, kde má útočník väčšie šance sa dostať k najväčšiemu množstvu citlivejších a utajovanejších informácií.

V obidvoch prípadoch úmyselného, či neúmyselného konania zamestnancov je ochrana predmetných dát veľmi náročná, najmä z dôvodu ich dostupnosti, kde podmienkou je, aby požadované informácie boli pre oprávneného používateľa prístupné v okamžiku jej potreby. Asi najúčinnejšou zbraňou je zavedenie princípu najnižších privilégií, ktorý môže pomôcť k minimalizovaniu rozsahu prípadného úniku dát.

Táto metóda informačnej bezpečnosti funguje na princípe prideľovania užívateľom len takých povolení, ktoré sú nevyhnutné k vykonávaniu ich práce. Napríklad obyčajný užívateľ nepotrebuje administrátorské práva do aplikácie a naopak, nejaký programátor nemusí mať prístup k finančným záznamom spoločnosti. Princíp najnižších privilégií je široko uznávaný spôsob ochrany dát a môže byť aplikovaný na ktorejkoľvek vrstve systému. Môže sa vzťahovať na koncových užívateľov, systémy, procesy, siete, databázy, aplikácie a všetky ostatné aspekty IT prostredia. [23]

3.2 Projekt OWASP

Pre stanovenie katalógu hrozieb bol vybraný medzinárodný projekt OWASP – Open Web Application Security Project (v preklade z angl. Otvorený projekt pre bezpečnosť webových aplikácií). Je to projekt založený v roku 2001, ktorého hlavným cieľom, ako už z názvu vyplýva, je zlepšovanie bezpečnosti webových aplikácií. [24]

Projekt OWASP je najmä otvorená komunita, ktorá podporuje organizácie vo vývoji a údržbe bezpečných aplikácií. Bezplatne na ich stránkach môže užívateľ nájsť rôzne bezpečnostné nástroje, štandardy, knihy o testovaní bezpečnosti aplikácií, apod. [25]

Tento projekt taktiež pravidelne (cca každé 3-4 roky) vydáva zoznam TOP 10 najkritickejších bezpečnostných rizík pre webové aplikácie. Cieľom tohto projektu je zvýšiť povedomie o zabezpečení webových aplikácií tým, že identifikuje niektoré z najkritickejších rizík, ktorým organizácia čelí. Na projekt TOP 10 sa odkazuje veľa noriem, kníh, nástrojov, spoločností a organizácií, vrátane Oracle, Symantec, MITRE, PCI DSS, DISA, FTC a mnoho ďalších. Pri hľadaní zdrojov a informácií som natrafil dokonca na projekt MVA (Microsoft Virtual Academy) spoločnosti Microsoft, ktorá ako podklady pre analýzu zraniteľností aplikácií vo svojich výukových programoch využíva práve spomínaný projekt OWASP TOP 10. [26]

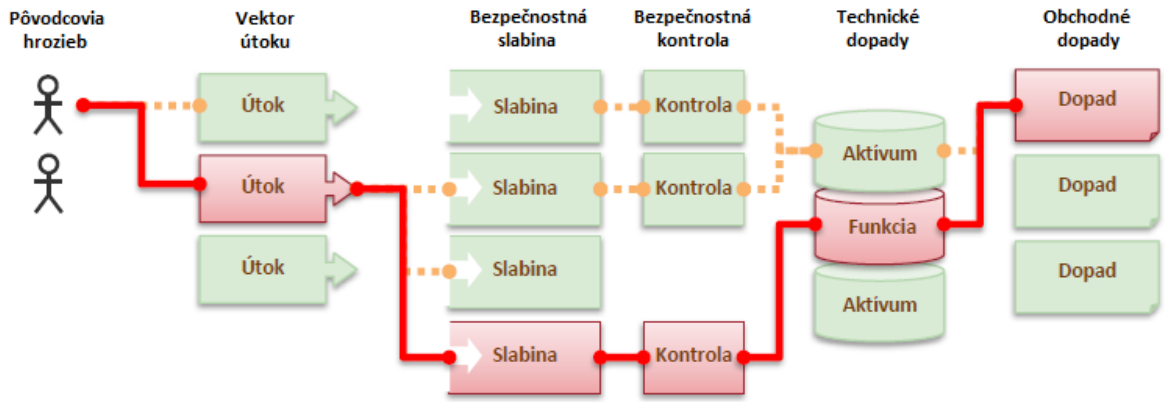
Podľa OWASP TOP 10 tiež projekt Skener webu pod záštitou NIC.CZ zdarma poskytuje prevádzkovateľom webov testovanie webových aplikácií. [27] Taktiež EÚ využíva tento projekt vo svojich nariadeniach ako metodiku pre splnenie ich požiadaviek. [28]

Dá sa teda povedať, že projekt OWASP je široko prijímaný a uznávaný odbornou IT komunitou a jeho dokument TOP 10 môže byť použitý pre účely stanovenia katalógu hrozieb pre webový informačný systém.

3.2.1 Bezpečnostné riziká aplikácií

K napadnutiu nejakého podniku alebo organizácie môžu útočníci použiť veľa rôznych ciest prostredníctvom danej aplikácie. Každá z týchto ciest má svoju úroveň náročnosti prevedenia útoku a predstavuje určité riziko, ktoré môže alebo nemôže byť akceptovateľné a následne spôsobené škody tiež môžu byť zanedbateľné alebo môžu doviesť danú organizáciu až k úplnému zastaveniu činnosti.

Na obrázku (Obr. 2) sú znázornené jednotlivé cesty, zraniteľnosti a rôzne možnosti, ktoré môže útočník využiť. Z obrázku je pekne vidieť, že jednotlivé útoky, slabiny a zraniteľnosti sú navzájom prepojené a vybraným typom útoku môže útočník využiť viacero slabín systému. Čiže keď to nejde jednou cestou, môže skúsiť využiť inú.



Obr. 2. Zraniteľnosti a rôzne možnosti ako ich využiť. [25]

Takisto to funguje aj opačne. Keď sa útočníkovi podarí objaviť nejakú zraniteľnosť systému, môže skúsiť viacero vektorov útoku na zneužitie tejto slabiny k prelomeniu zabezpečenia.

3.2.2 Identifikácia rizík

Projekt OWASP TOP 10 identifikuje riziká pre podniky a organizácie všeobecne, na základe prieskumov, štatistík a získaných informácií od niekoľko rôznych organizácií.

Tab. 1. Tabuľka klasifikácie rizík. [25]

Pôvodcovia hrozieb	Zneužiteľnosť slabiny	Rozšírenie slabiny	Zistiteľnosť slabiny	Technický dopad	Obchodné dopady
Špecifické pre aplikáciu	**Ľahká 3**	**Rozsiahle 3**	**Ľahká 3**	**Vážny 3**	Špecifické pre podnik
	Priemerná 2	**Bežné 2**	**Priemerná 2**	**Stredný 2**	
	Náročná 1	**Vzácne 1**	**Náročná 1**	**Malý 1**	

Ku každej z hrozieb uvedených v nasledujúcej kapitole, sú poskytnuté všeobecné informácie o pravdepodobnosti a dopade na aplikáciu a všeobecné klasifikovanie jednotlivých rizík podľa jednoduchej schémy v tabuľke (Tab. 1), ktorá je založená na Metodológii hodnotenia rizík OWASP, a z ktorej bude vychádzať analýza rizík v praktickej časti.

Celkové riziko pre organizáciu sa môže určiť spojením všetkých týchto faktorov. V tomto obecnom katalógu však nie sú uvedené (vyčíslené) riziká pre pôvodcov hrozieb a obchodné dopady na organizáciu, pretože každá aplikácia, systém alebo organizácia je jedinečná. To znamená, že pre vybranú aplikáciu nemusí existovať pôvodca hrozby, ktorý by využil danú zraniteľnosť, alebo vykonaný útok nemusí mať zásadný vplyv na fungovanie organizácie.

Preto je na každej organizácii, aby si určila svoje priority a podľa tohto katalógu stanovila, aké veľké riziko môže každá hrozba predstavovať pre jej činnosť, pretože ako sa v dokumente uvádza, účelom projektu TOP 10 nie je urobiť analýzu rizík za nás.

3.3 Katalóg hrozieb pre webový IS

V tejto podkapitole sú uvedené jednotlivé hrozby, zraniteľnosti alebo priamo útoky na webové aplikácie, ktoré vychádzajú z projektu OWASP a jeho najnovšieho dokumentu TOP 10 najkritickejších rizík z roku 2017. Zoznam je doplnený aj o ďalšie dve hrozby katalógu z roku 2013, ktoré by vzhľadom na povahu informačného systému mohli znamenať potenciálne riziko.

Každá hrozba obsahuje stručné informácie o pôvodcoch hrozieb, prevedení útoku, zneužitej bezpečnostnej slabine, technických a obchodných dopadoch na aplikáciu a organizáciu,

ktoré sú zároveň jednotlivými faktormi k nasledujúcemu stanoveniu a zhodnoteniu celkových rizík.

3.3.1 Injektovanie

K zraniteľnosti injektovaním, napr. SQL, dochádza vtedy, keď sa ako súčasť SQL dotazu odosielajú do interpreta nedôveryhodné dáta (príkazy). Tieto dáta resp. príkazy môžu prinútiť interpret na vykonanie nechcených, neplánovaných príkazov alebo umožnenie prístupu k dátam bez riadneho povolenia. [25]

Pôvodcovia hrozieb

Útočníkom môže byť každý, kto môže posielať nedôveryhodné dáta do systému, tzn. externí užívatelia, interní užívatelia alebo administrátori. [25]

Vektor útoku

Útočník posiela jednoduché textové príkazy, ktoré zneužívajú syntax cieľového interpreta. Injekčným vektorom môže byť takmer každý zdroj dát vrátane interných. [25]

Bezpečnostná slabina

Zraniteľnosti injektovaním vznikajú, keď aplikácia posiela do interpreta nedôveryhodné dáta. Tieto chyby sú veľmi rozšírené, obzvlášť v starších kódoch. Väčšinou sa nachádzajú v SQL dotazoch. Zraniteľnosti injektovaním sa ľahko zisťujú skúmaním kódu. S nájdením týchto chýb môžu útočníkom pomôcť rôzne skenery. [25]

Technické dopady

Injektovanie môže mať za následok stratu alebo narušenie integrity, zodpovednosti či dostupnosti. Injektovanie môže niekedy viesť ku kompletnému ovládnutiu hostiteľského servera. [25]

Obchodné dopady

Je treba zvážiť obchodnú hodnotu predmetných dát a platformy, na ktorej beží interpret. Môžu byť ukradnuté, zmenené alebo odstránené všetky dáta. Môže dôjsť k poškodeniu povesti spoločnosti. [25]

Zhodnotenie rizík

Tab. 2. Hodnotenie rizík - Injektovanie. [25]

Zneužiteľnosť	Rozšírenie	Zistiteľnosť	Dopad
ĽAHKÁ	**BEŽNÉ**	**ĽAHKÁ**	**VÁŽNY**

3.3.2 Chybná autentizácia

Funkcie aplikácií, ktoré zabezpečujú overovanie a správu relácie, nie sú vykonané správne, čo útočníkovi umožňuje kompromitovať heslá, kľúče alebo tokeny relácií alebo môžu zneužiť ďalšie iné slabiny v implementácii k tomu, aby prevzali identitu iných používateľov. [25]

Pôvodcovia hrozieb

Útočníkmi môžu byť anonymní externí útočníci, ale aj užívatelia s vlastnými účtami, ktorí chcú ukradnúť účty iných užívateľov. Tiež je treba vziať do úvahy interných užívateľov systému (napr. pracovníkov organizácie), ktorí chcú zakryť svoje činy. [25]

Vektor útoku

Útočník využíva trhliny v autentizácii alebo vo funkciách správy relácie (príkladom môžu byť nechránené účty, heslá a identifikátory relácií) na to, aby sa vydával za legitímne prihláseného užívateľa. [25]

Bezpečnostná slabina

Najväčšiu chybu robia práve samotní vývojári systému keď sa snažia vytvárať vlastné riešenia autentizácie a postupy riadenia relácie, napriek tomu, že ich správne vytvorenie je veľmi ťažké. V dôsledku toho majú tieto vlastné riešenia často nedostatky v odhlasovaní, správe hesiel a ich dobe platnosti, zapamätaní si prihlásenia, tajných otázkach a podobných oblastiach. Preto sa odporúča využívať dostupné hotové a overené riešenia autentizácie užívateľov apod. Nájdenie nedostatkov v autentizácii niekedy môže byť ťažké, pretože každá implementácia je jedinečná, no pre skúseného útočníka to vo veľa prípadoch nemusí byť žiadny problém. [25]

Technické dopady

Chyby tohto typu môžu umožniť napadnutia niektorých, či dokonca všetkých účtov. Keď je útok úspešný, útočník môže vykonávať všetko, čo môže robiť daná obeť. Najčastejším cieľom sú preto privilegované účty. [25]

Obchodné dopady

V stávke je obchodná hodnota predmetných dát alebo funkcií aplikácie. Pre organizáciu môžu byť následky odcudzenia alebo zverejnenia dát katastrofálne. Taktiež je treba zvážiť obchodný vplyv zverejnenia danej zraniteľnosti. [25]

Zhodnotenie rizík

Tab. 3. Hodnotenie rizík – Chybná autentizácia. [25]

Zneužiteľnosť	Rozšírenie	Zistiteľnosť	Dopad
ĽAHKÁ	**BEŽNÉ**	**PRIEMERNÁ**	**VÁŽNY**

3.3.3 Expozícia citlivých dát

Veľa webových aplikácií nechráni dostatočne citlivé dáta užívateľov alebo klientov, ako napríklad kreditné karty alebo autorizačné údaje. Tieto slabo chránené dáta útočníci môžu ukradnúť či modifikovať, aby mohli vykonávať rôzne podvody s kreditnými kartami, krádeže identity alebo iné zločiny. Citlivé dáta si zaslúžia osobitnú ochranu a mali by byť šifrované. [25]

Pôvodcovia hrozieb

Je treba brať do úvahy každého, kto môže získať prístup k citlivým dátam a ich zálohám. Predmetom sú dáta v pokoji, presúvané dáta aj dáta v prehliadačoch užívateľov. Ohrozenie môže prísť zvonku aj zvnútra. [25]

Vektor útoku

Útočníkovi sa zvyčajne nepodarí priamo prelomiť šifrované dáta. Snažia sa napríklad ukradnúť kľúče, používajú útoky typu Man in the middle, alebo kradnú nešifrované dáta priamo zo servera, či už pri prenose, alebo z prehliadača užívateľa za pomoci ďalších nástrojov alebo útokov. [25]

Bezpečnostná slabina

Najčastejšou chybou jednoducho je, že citlivé dáta nie sú šifrované. Takisto časté je generovanie a správa slabých šifrovacích kľúčov a používanie slabých algoritmov, zvlášť potom slabých techník hashovania hesla. Veľmi časté a ľahko odhaliteľné sú slabiny prehliadača, avšak takéto nedostatky sú ťažko využiteľné vo veľkom meradle. Zistenie nedostatkov na strane servera je pre externých útočníkov ťažké kvôli obmedzenému prístupu a tieto chyby sú tiež zvyčajne ťažko zneužiteľné. [25]

Technické dopady

Uvedené chyby často ohrozujú všetky údaje, ktoré by mali byť prioritne chránené. Zvyčajne sa jedná o informácie, ktoré obsahujú citlivé údaje, ako sú zdravotné záznamy, osobné údaje, kreditné karty, atď. [25]

Obchodné dopady

Organizácia musí zvážiť obchodnú i osobnú hodnotu stratených dát a vplyv na jej povesť. Tiež si treba uvedomiť, akú právnu zodpovednosť nesie, ak sú tieto dáta nechránené, najmä v tomto období s príchodom nariadenia GDPR. [25]

Zhodnotenie rizík

Tab. 4. Hodnotenie rizík - Expozícia citlivých dát. [25]

Zneužiteľnosť	Rozšírenie	Zistiteľnosť	Dopad
PRIEMERNÁ	**ROZSIAHLE**	**PRIEMERNÁ**	**VÁŽNY**

3.3.4 XML Externé Entity (XXE)

Mnoho starších alebo zle nakonfigurovaných XML procesorov vyhodnocuje externé odkazy v rámci XML dokumentov. Zraniteľnosť XXE umožňuje útočníkovi vložiť jeho nebezpečné XML externé entity. Cieľom takéhoto útoku je získanie citlivých informácií, ako napríklad odhalenie súborov a ich štruktúru v internom systéme. [25]

Pôvodcovia hrozieb

V úvahu musíme brať každého, kto môže posielať nedôveryhodné dáta do systému, čiže externí užívatelia, interní užívatelia alebo administrátori. [25]

Vektor útoku

Útočníci môžu využiť zraniteľné procesory XML. Využívajú tento zraniteľný kód, rôzne závislosti alebo iné integrácie k nahraniu alebo vloženiu škodlivého obsahu do XML dokumentu. [25]

Bezpečnostná slabina

V základnom nastavení mnoho starších procesorov XML umožňuje špecifikovať externé entity, URI, ktorá je dereferencovaná a vyhodnocovaná počas spracovania XML. Špecific-

ké nástroje môžu automaticky objaviť tento problém kontrolou závislostí a konfigurácie. Ďalšie vyžadujú aj manuálne kroky na zistenie a vyriešenie tohto problému. [25]

Technické dopady

Tieto chyby je možné použiť na extrahovanie dát, vykonanie vzdialených príkazov na serveri, skenovanie interných súborov, vykonanie DoS (Denial of Service) útoku a ďalších. V konečnom dôsledku je možné túto zraniteľnosť využiť aj na spáchanie kybernetického útoku s ešte rozsiahlejšími dôsledkami. [25]

Obchodné dopady

Obchodný dopad na podnikanie môže byť vážny a závisí od potrieb ochrany všetkých dotknutých aplikácií a údajov. [25]

Zhodnotenie rizík

Tab. 5. Hodnotenie rizík - XML Externé Entity (XXE). [25]

Zneužiteľnosť	Rozšírenie	Zistiteľnosť	Dopad
PRIEMERNÁ	**BEŽNÉ**	**ĽAHKÁ**	**VÁŽNY**

3.3.5 Prelomenie kontroly prístupu

Ako už názov napovedá, podstatou zraniteľnosti v tomto prípade je nedostatočná kontrola alebo riadenie prístupových práv. Táto zraniteľnosť vzniká nesprávnym alebo nedostatočným nastavením toho, čo môžu alebo nemôžu riadne prihlásení a overení užívatelia robiť. Prelomenie kontroly prístupu môže viesť až k získaniu úplnej kontroly nad systémom a jeho zneužitiu. [25]

Pôvodcovia hrozieb

Útočníkmi môžu byť anonymní externí útočníci, ale aj užívatelia s vlastnými účtami, ktorí chcú ukradnúť účty iných užívateľov. Útočníci sa správajú ako obyčajní užívatelia, správcovia alebo používajú privilegované funkcie, alebo vytvárajú, pristupujú, aktualizujú alebo odstraňujú každý záznam. [25]

Vektor útoku

Využívanie kontroly prístupu je základnou zručnosťou útočníkov. K tomu im môžu pomôcť rôzne nástroje, ktoré dokážu zistiť absenciu kontroly prístupu, ale nemôžu overiť, či

je funkčná. Kontrola prístupu je zistiteľná najlepšie pomocou ručných prostriedkov, prípadne automaticky v určitých frameworkoch. [25]

Bezpečnostná slabina

Slabé stránky kontroly prístupu sú bežné kvôli nedostatku automatizovanej detekcie a nedostatku efektívneho funkčného testovania vývojármi aplikácií. Najlepší spôsob, ako zistiť chýbajúce alebo neefektívne riadenie prístupu je manuálne testovanie. [25]

Technické dopady

Útočníci môžu túto zraniteľnosť využiť na prístup k neoprávneným funkciám alebo údajom, ako sú prístup k účtom ostatných používateľov, prezeranie citlivých súborov, zmena údajov iných používateľov, zmenu prístupových práv atď. [25]

Obchodné dopady

Dopad na podnikanie organizácie môže byť veľmi vážny, v závislosti na povahe a objeme zneužitých dát. [25]

Zhodnotenie rizík

Tab. 6. Hodnotenie rizík - Prelomenie kontroly prístupu. [25]

Zneužiteľnosť	Rozšírenie	Zistiteľnosť	Dopad
PRIEMERNÁ	**BEŽNÉ**	**PRIEMERNÁ**	**VÁŽNY**

3.3.6 Nezabezpečená konfigurácia

Dobré zabezpečenie vyžaduje mať definované a nasadené bezpečné nastavenie aplikácie, frameworkov, aplikačného servera, webového servera, databázového servera a platformy. Bezpečnostné nastavenia by mali byť definované, implementované a dodržiavané, pretože predvolené hodnoty sú často riskantné. Navyše by mal byť softvér priebežne aktualizovaný. [25]

Pôvodcovia hrozieb

Potenciálnou hrozbou pre systém môžu byť anonymní externí útočníci i užívatelia s vlastnými účtami, ktorí sa môžu pokúsiť kompromitovať systém. Taktiež treba vziať do úvahy interných pracovníkov, ktorí chcú zakryť svoje činy. [25]

Vektor útoku

Útočník sa snaží dostať k predvoleným účtom, nepoužívaným stránkam, neopraveným chybám, nechráneným súborom a adresárom atď., aby získal neoprávnený prístup do systému alebo informácie o ňom. [25]

Bezpečnostná slabina

Nezabezpečená konfigurácia sa môže objaviť na akejkoľvek úrovni aplikácie vrátane platformy, webového servera, aplikačného servera, databázy, frameworku alebo vlastného kódu. Na správnej konfigurácii celého komplexu musia spolupracovať vývojári a správcovia systému, či serveru. Na detekciu chýbajúcich záplat, chybnej konfigurácie, predvolených účtov, nepotrebných služieb, sú vhodné automatizované skenery. [25]

Technické dopady

Tieto zraniteľnosti poskytujú útočníkovi neautorizovaný prístup k niektorým dátam alebo funkciám systému. Môžu ale viesť aj k celkovej kompromitácii systému. [25]

Obchodné dopady

Systém môže byť úplne kompromitovaný, bez toho aby o tom vedeli samotní vývojári či správcovia systému. Postupne môžu byť ukradnuté alebo menené všetky dáta organizácie. Náklady spojené s obnovou dát môžu byť značné. [25]

Zhodnotenie rizík

Tab. 7. Hodnotenie rizík - Nezabezpečená konfigurácia. [25]

Zneužiteľnosť	Rozšírenie	Zistiteľnosť	Dopad
ĽAHKÁ	**ROZSIAHLE**	**ĽAHKÁ**	**STREDNÝ**

3.3.7 Cross-Site Scripting (XSS)

Chyby typu XSS nastávajú vtedy, keď aplikácia prijme nedôveryhodné dáta a odošle ich webovému prehliadaču bez riadneho overenia alebo escapovania. Táto zraniteľnosť útočníkom umožňuje spúšťať svoje skripty v prehliadači obete, ktoré môžu ukradnúť užívateľské relácie, pretvoriť webové stránky alebo presmerovať užívateľa na nebezpečné stránky útočníka. [25]

Pôvodcovia hrozieb

Každý, kto môže posielať nedôveryhodné dáta do systému, vrátane externých užívateľov, interných užívateľov a administrátorov. [25]

Vektor útoku

Útočník posiela útočné skripty v podobe textového reťazca, ktoré zneužívajú interpret v prehliadači obete. Vektorom útoku môže byť skoro každý zdroj údajov vrátane interných zdrojov, napríklad dát z databázy. [25]

Bezpečnostná slabina

XSS je druhou najrozšírenejšou bezpečnostnou chybou webových aplikácií. Zraniteľnosť XSS nastáva, keď aplikácia vkladá užívateľom poskytnuté dáta do webovej stránky, ktorú posiela do prehliadača, bez riadnej validácie alebo escapovania tohto obsahu. Existujú tri typy zraniteľností XSS:

- stored (persistent) – trvalý,
- reflected (non-persistent) – dočasný,
- DOM based (založené na objektovom modely dokumentu) – lokálny.

Nájsť väčšinu XSS zraniteľností na strane servera je celkom jednoduché: testovaním alebo analýzou kódu. [25]

Technické dopady

Útočníci môžu spúšťať skripty v prehliadači obete, čo im umožňuje ukradnúť užívateľskú reláciu, zmeniť obsah stránok, vložiť nebezpečný obsah, presmerovať užívateľa, zmocniť sa užívateľovho prehliadača za použitia malwaru apod. [25]

Obchodné dopady

Je nutné zvážiť obchodnú hodnotu napadnutého systému a všetkých dát, ktoré spracováva, takisto zverejnenie zraniteľnosti môže mať vážny obchodný dopad. [25]

Zhodnotenie rizík

Tab. 8. Hodnotenie rizík - Cross-Site Scripting (XSS). [25]

Zneužiteľnosť	Rozšírenie	Zistiteľnosť	Dopad
ĽAHKÁ	**ROZSIAHLE**	**ĽAHKÁ**	**STREDNÝ**

3.3.8 Nezabezpečená deserializácia

Nezabezpečená deserializácia – proces získania dát štruktúrovaných pomocou nejakého formátu (napr. JSON) a ich prevedenie na objekt [29] – môže vážne ohroziť bezpečné fungovanie logiky aplikácie, viesť k DoS útokom a najhoršie až k vzdialenému spusteniu kódu. [25]

Pôvodcovia hrozieb

Pôvodcom hrozby môže byť každý, kto môže posielať nedôveryhodné dáta do systému, vrátane externých užívateľov, interných užívateľov a administrátorov. [25]

Vektor útoku

Zneužitie chýb v deserializácii je pomerne náročné a existuje viacero postupov na rôzne platformy. Napríklad na nejakom PHP fóre sa útočník môže snažiť zmeniť serializovaný objekt uloženej cookie, ktorá obsahuje údaje o prihlásenom užívateľovi tak, aby mu dal administrátorské práva. [25]

Bezpečnostná slabina

Niektoré nástroje môžu objaviť chyby v deserializácii, ale na jej potvrdenie je často potrebná pomoc človeka. Očakáva sa, že sa zvýši povedomie o nedostatkoch deserializácie, keďže sa vyvinul nástroj na identifikáciu a riešenie tohto problému. [25]

Technické dopady

Dopad nedostatkov v deserializácii nemožno podceňovať. Táto zraniteľnosť môže viesť k útokom na vzdialené spustenie kódu, čo je jeden z najzávažnejších útokov na informačný systém. [25]

Obchodné dopady

Obchodný dopad na podnikanie môže byť vážny a závisí od potrieb ochrany všetkých dotknutých aplikácií a údajov. [25]

Zhodnotenie rizík

Tab. 9. Hodnotenie rizík - Nezabezpečená deserializácia. [25]

Zneužiteľnosť	Rozšírenie	Zistiteľnosť	Dopad
NÁROČNÁ	**BEŽNÉ**	**PRIEMERNÁ**	**VÁŽNY**

3.3.9 Použitie komponentov so známymi zraniteľnosťami

Komponenty, napr. knižnice, frameworky a ďalšie softvérové moduly, väčšinou bežia s najvyššími oprávneniami. Ak je zraniteľný komponent zneužitý, útok môže uľahčiť závažnú stratu dát alebo ovládnutie servera. Aplikácie používajúce komponenty so známymi zraniteľnosťami môžu zmariť ďalšiu ochranu aplikácií a umožniť rad útokov a závažných dopadov. [25]

Pôvodcovia hrozieb

Niektoré súčasti systému, ako napr. prídavné knižnice (väčšinou tretích strán), môžu byť pomocou automatických nástrojov identifikované a následne zneužité. Ide o útočníkov, ktorí konajú zámerne, ale aj náhodne. [25]

Vektor útoku

Útočník zistí automatickým skenovaním alebo pri ručnom prehľadávaní stránok zraniteľný komponent. Útok prispôsobí danej zraniteľnosti a potom ho prevedie. Čím je však zraniteľná súčasť hlbšie v aplikácii, tým je útok náročnejší. [25]

Bezpečnostná slabina

Väčšina vývojárov nevenuje dostatočnú pozornosť tomu, či sú ich komponenty a knižnice aktuálne. Vývojári často ani nevedia, aké knižnice presne využívajú (najmä pri „zdedení" správy aplikácie), nehovoriac o číslach ich verzií. Celú situáciu ešte komplikujú závislosti medzi jednotlivými komponentmi, ktoré sú často prepojené alebo na seba nejakým spôsobom nadväzujú. [25]

Technické dopady

Po identifikovaní určitej zraniteľnosti, útočník môže použiť niektorý z vyššie popísaných útokov alebo postupov napr. injektovanie, XSS, prelomenie prístupu do aplikácie apod. Dopad na aplikáciu potom môže byť minimálny, alebo tiež môže viesť až k úplnému prevzatiu kontroly nad serverom a následnej kompromitácii dát. [25]

Obchodné dopady

Dopad na činnosť organizácie závisí od rozsahu útoku na funkcionalitu, ktorú daná napadnutá aplikácia zabezpečuje. Závažnosť dopadu môže byť nevýznamný, alebo môže znamenať úplnú kompromitáciu a kontrolu nad systémom. [25]

Zhodnotenie rizík

Tab. 10. Hodnotenie rizík - Použitie komponentov so známymi zraniteľnosťami. [25]

Zneužiteľnosť	Rozšírenie	Zistiteľnosť	Dopad
PRIEMERNÁ	**ROZSIAHLE**	**PRIEMERNÁ**	**STREDNÝ**

3.3.10 Nedostatočné zaznamenávanie a monitorovanie činnosti

Nedostatočné zaznamenávanie (logovanie) a monitorovanie ani tak nie je priamo zraniteľnosťou alebo bezpečnostnou „dierou“, spolu však s chýbajúcou alebo neefektívnou integráciou reakcie na incidenty, umožňuje útočníkom ďalej napádať systém, nabúrať sa do ďalších systémov a manipulovať, extrahovať alebo zničiť dáta. [25]

Pôvodcovia hrozieb

Útočníkmi môžu byť anonymní externí útočníci, ale aj užívatelia s vlastnými účtami, čiže prakticky každý užívateľ systému. [25]

Vektor útoku

Využitie nedostatočného logovania a monitorovania činnosti je základom takmer každého významného incidentu. Útočníci sa spoliehajú na tento fakt a oneskorenú reakciu správcov na dosiahnutie svojich cieľov bez toho, aby boli odhalení. [25]

Bezpečnostná slabina

Jednou stratégiou na zistenie, či je systém dostatočné monitorovaný, je preskúmanie zaznamenaných protokolov po penetračnom testovaní. Každá akcia testerov by mala byť dostatočne zaznamenaná, pre pochopenie, aké škody môže útočník spôsobiť. [25]

Technické dopady

Najúspešnejšie útoky začínajú skúmaním a skúšaním zraniteľnosti. Povolením pokračovania takýchto testovacích útokov dôsledkom nedostatočného monitorovania, prípadne nedôslednej kontroly logov, sa môže zvýšiť pravdepodobnosť úspešného vykonania plánovaného útoku takmer na 100%. [25]

Obchodné dopady

Systém môže byť kompromitovaný, bez toho aby o tom vedeli samotní vývojári či správcovia systému. Postupne môžu byť ukradnuté alebo menené všetky dáta organizácie. [25]

Zhodnotenie rizík

Tab. 11. Hodnotenie rizík - Nedostatočné zaznamenávanie a monitorovanie činnosti. [25]

Zneužiteľnosť	Rozšírenie	Zistiteľnosť	Dopad
PRIEMERNÁ	**ROZSIAHLE**	**NÁROČNÁ**	**STREDNÝ**

3.3.11 Cross-Site Request Forgery (CSRF)

Útok tohto typu donúti prehliadač prihláseného užívateľa do nejakej aplikácie podvrhnúť serveru HTTP požiadavku, vrátane jej autorizačných informácií, ktorú server vykoná v domnienke, že ide o legitímnu požiadavku obete. [30]

Pôvodcovia hrozieb

Útočníkom môže byť ktokoľvek, kto môže podstrčiť škodlivý obsah do prehliadača užívateľa aplikácie, čiže anonymní externí útočníci, ale aj užívatelia s vlastnými účtami. [30]

Vektor útoku

Útočník vytvorí škodlivý dotaz na zraniteľnú stránku a pomocou rôznych techník donúti obeť požiadavku odoslať. Pokiaľ je užívateľ v aplikácii prihlásený, útok bude úspešný. [30]

Bezpečnostná slabina

Útok typu CSRF využíva toho, že väčšina webových aplikácií neoveruje legitímnosť spracovávaného požiadavku. Táto zraniteľnosť sa dá odhaliť pomocou penetračného testovania alebo analýzou kódu. [30]

Technické dopady

Útočník môže donútiť svoju obeť odoslať nejaký formulár, ktorého cieľom je nejaká akcia, napríklad banková transakcia, alebo vykonanie zmien v účte apod. [30]

Obchodné dopady

Je treba zvážiť hodnotu dotknutých dát a dopad na povesť organizácie. [30]

Zhodnotenie rizík

Tab. 12. Hodnotenie rizík - Cross-Site Request Forgery (CSRF). [30]

Zneužiteľnosť	Rozšírenie	Zistiteľnosť	Dopad
PRIEMERNÁ	**BEŽNÉ**	**ĽAHKÁ**	**STREDNÝ**

3.3.12 Neošetrené presmerovanie a predávanie

Webové aplikácie často presmerovávajú svojich užívateľov na iné webové stránky a k určeniu URL adresy používajú neoverené údaje, pomocou ktorých môžu útočníci presmerovať obeť na svoje škodlivé stránky alebo získať prístup k neoprávneným stránkam. [31]

Pôvodcovia hrozieb

Každý, kto môže podviesť a donútiť užívateľov odoslať požiadavky na stránky danej aplikácie. [31]

Vektor útoku

Útočník spravidla vytvorí odkaz na presmerovanie a donúti obeť, aby naň klikla. Keďže odkaz smeruje známu a overenú stránku, obeť naň zrejme klikne. [31]

Bezpečnostná slabina

Aplikácie často svojich užívateľov presmerovávajú na iné stránky a používajú k tomu neoverené parametre, čo umožňuje útočníkovi podstrčiť ľubovoľnú cieľovú stránku. [31]

Technické dopady

Takéto neoverené presmerovania môžu umožniť obídenie kontroly prístupu alebo sa pokúsiť nainštalovať škodlivý software. [31]

Obchodné dopady

Je nutné zvážiť dopad na dôveru zákazníkov. [31]

Zhodnotenie rizík

Tab. 13. Hodnotenie rizík - Neošetrené presmerovanie a predávanie. [31]

Zneužiteľnosť	Rozšírenie	Zistiteľnosť	Dopad
PRIEMERNÁ	**VZÁCNE**	**ĽAHKÁ**	**STREDNÝ**

V katalógu boli stanovené všeobecne najbežnejšie a najzávažnejšie hrozby pre webový informačný systém. U jednotlivých hrozieb boli stručne popísané spôsoby prevedenia útokov, ich pôvodcovia, slabiny, ktoré využívajú a možné dopady na aplikáciu. Taktiež pre každú hrozbu boli všeobecne definované riziká, ktoré v následnej analýze rizík pomôžu stanoviť skutočné riziko pre vybraný informačný systém.

3.4 Zhrnutie teoretickej časti

Cieľom teoretickej časti bolo uvedenie čitateľa do problematiky informačných systémov, zákonných požiadaviek s nimi spojenými a poukázanie na možné hrozby, ktoré ich ohrozujú. Teoretická časť práce bola rozdelená na tri celky. V prvej kapitole boli definované základné pojmy v oblasti informačných systémov. Druhá kapitola bola venovaná zákonným požiadavkám a povinnostiam vo vzťahu k informačnej bezpečnosti a nakoniec v záverečnej kapitole teoretickej časti bol stanovený obecný katalóg aktuálne najzávažnejších hrozieb pre webové informačné systémy a iné webové aplikácie.

II. PRAKTICKÁ ČÁST

4 AUDIT INFORMAČNEJ BEZPEČNOSTI VYBRANÉHO INFORMAČNÉHO SYSTÉMU

V nasledujúcej kapitole bude stručne predstavená spoločnosť, pre ktorú je informačný systém vyvíjaný, následne samotný webový informačný systém a jeho aktuálny stav zabezpečenia a taktiež bude realizovaná analýza rizík vybraných bezpečnostných hrozieb.

4.1 Spoločnosť Housing for Life, SE

Holding Housing for Life, SE je mladá česká spoločnosť, ktorá však vďaka mnohoročným skúsenostiam jej tímu stále silnie a rastie. Spoločnosť bola založená z prvotnej myšlienky urobiť bývanie dostupnejšie, mať kompletný servis ohľadom hlavných životných otázok pod jednou strechou – od nájdenia vhodnej nehnuteľnosti, cez financovanie až po prepis a optimalizáciu energií. Zjednodušiť ľuďom možnosti využitia podpory štátu v oblasti energetických úspor aj v oblasti pôžičiek na bývanie od štátu pre mladé rodiny. Cieľom tejto myšlienky bolo, aby mali klienti celý proces pod kontrolou.

Mottom spoločnosti HFL je: „Vo všetkom hľadaj to pozitívne.“ Samozrejme, že nie je všetko jednoduché, ale občas sa z neriešiteľného problému stáva len drobná banalita, stačí len iný uhol pohľadu.

4.2 Popis informačného systému HFL

Predmetný informačný systém je webová aplikácia, písaná v jazyku PHP, ktorá ukladá dáta do databázového systému MySQL. Primárne je určená najmä na ukladanie a spracovanie údajov o klientoch spoločnosti HFL a rôzne operácie s týmito dátami (generovanie zmlúv apod.), preto celá aplikácia a v nej uložené dáta sú momentálne síce jediným, ale i v budúcnosti asi najdôležitejším aktívom tohto systému.

Momentálne je prístup do aplikácie určený výhradne zamestnancom firmy HFL a jej spolupracovníkom – zamestnancom niektorej z ich partnerských firiem, čiže overeným a riadne zaregistrovaným užívateľom, no i tak bude v stanovení pôvodcov hrozieb zohľadnená aj táto skupina užívateľov, pretože v blízkej budúcnosti, vlastne hneď po uvedení systému do ostrej prevádzky, bude systém prístupný i klientom, najmä z dôvodov nariadenia GDPR o dostupnosti všetkých spracovávaných údajoch dotknutých osôb.

Čo sa týka bezpečnostnej politiky a riadenia prístupu, informačný systém pracuje na princípe whitelistov. Existujú štyri spôsoby aplikovania bezpečnostnej politiky, z ktorých bola táto možnosť vybraná:

- promiskuitná – všetko je užívateľovi dovolené, nulové zabezpečenie,
- povoľná – čo nie je užívateľovi zakázané, je dovolené (blacklist), predstavuje nižšiu úroveň bezpečnosti,
- prísna – čo nie je užívateľovi dovolené, je zakázané (whitelist), predstavuje vyššiu úroveň bezpečnosti,
- paranoidná – skoro všetko je užívateľom zakázané, absolútne zabezpečenie.

Najbezpečnejším riešením kontroly prístupu by bolo použitie poslednej možnosti, tá je však v praxi ťažko udržateľná a v prípade vybraného informačného systému nereálna, pretože aplikovanie tejto možnosti predpokladá úplnú izoláciu od okolitého sveta (internetu). [32]

Preto bola vybraná tretia možnosť, kde má každý užívateľ stanovený svoj whitelist práv, kde je jasne určené, kam môže pristupovať a aké operácie smie vykonávať.

4.3 Prehľad a stanovenie miery rizík definovaných hrozieb

V teoretickej časti bol stanovený obecný katalóg možných hrozieb, zraniteľností a útokov na webový informačný systém. Obecné stanovenie miery rizík pomôže odhaliť najzávažnejšie hrozby, na ktoré je dôležité sa zamerať pri návrhu zabezpečenia systému.

4.3.1 Výpočet miery rizík

Miera rizika sa vypočíta podľa štandardného modelu:

$$Riziko = Pravdepodobnosť * Dopad \quad (1)[33]$$

Pravdepodobnosť v tomto prípade je stanovená prvými tromi faktormi a to zneužiteľnosť, rozšírenie a zistiteľnosť. Tie sú podľa závažnosti jednotlivých faktorov ohodnotené na stupnici od 1 do 3, kde 3 predstavuje najvyššiu pravdepodobnosť. Tieto hodnoty sa spriemerujú a vynásobia hodnotou technického dopadu, čím sa získa celková miera rizika.

Po vypočítaní miery rizika sa podľa nasledujúcej tabuľky (Tab. 14) určí jeho celková závažnosť rozdelením na tri časti: nízka, stredná alebo vysoká.

Tab. 14. Stupnica miery a závažnosti rizika. [33]

Miera rizika	Celková závažnosť
1 až 3	nízka
4 až 6	stredná
7 až 9	vysoká

4.3.2 Tabuľka hrozieb

V tabuľke (Tab. 15) sa nachádza zoznam všetkých hrozieb z katalógu s farebným a bodovým ohodnotením rizík a mierou rizika vypočítanou podľa vyššie uvedeného vzorca č. 1.

Tab. 15. Zoznam hrozieb z katalógu s hodnotením a mierou rizík. [25]

Hrozba	Zneužiteľ-nosť	Rozšírenie	Zistiteľnosť	Technický dopad	Miera
Injektovanie	**Ľahká 3**	**Bežné 2**	**Ľahká 3**	**Vážny 3**	**8**
Autentizácia	**Ľahká 3**	**Bežné 2**	**Priemerná 2**	**Vážny 3**	**7**
Expozícia citlivých dát	**Priemerná 2**	**Rozsiahle 3**	**Priemerná 2**	**Vážny 3**	**7**
XXE	**Priemerná 2**	**Bežné 2**	**Ľahká 3**	**Vážny 3**	**7**
Prelomenie kontroly prístupu	**Priemerná 2**	**Bežné 2**	**Priemerná 2**	**Vážny 3**	**6**
Nezabezpečená konfigurácia	**Ľahká 3**	**Rozsiahle 3**	**Ľahká 3**	**Stredný 2**	**6**
XSS	**Ľahká 3**	**Rozsiahle 3**	**Ľahká 3**	**Stredný 2**	**6**
Deserializácia	**Náročná 1**	**Bežné 2**	**Priemerná 2**	**Vážny 3**	**5**
Zraniteľné komponenty	**Priemerná 2**	**Rozsiahle 3**	**Priemerná 2**	**Stredný 2**	**4,7**
Logovanie a monitorovanie	**Priemerná 2**	**Rozsiahle 3**	**Náročná 1**	**Stredný 2**	**4**
CSRF	**Priemerná 2**	**Bežné 2**	**Ľahká 3**	**Stredný 2**	**4,7**
Presmerovanie a predávanie	**Priemerná 2**	**Vzácne 1**	**Ľahká 3**	**Stredný 2**	**4**

4.3.3 Celková závažnosť rizík

V grafe (Graf 1) je porovnaná závažnosť rizík všetkých hrozieb. Z grafu je vidieť, že viac ako polovica všetkých hrozieb predstavuje vysoké riziko, čo je veľmi závažná skutočnosť. Naproti tomu, žiadna hrozba nie je klasifikovaná ako nízke riziko, i keď niektoré posledné hrozby majú k tomuto zaradeniu celkom blízko.

Graf 1. Celková závažnosť rizika [Zdroj: vlastný]

4.4 Hodnotenie stavu zabezpečenia

Vybraný informačný systém je prakticky na začiatku svojej cesty, tak ako aj jeho zabezpečenie. Na jeho vývoj je použitý jednoduchý, ale efektívny framework, ktorý v základnom nastavení, tak ako väčšina frameworkov, obsahuje rad rôznych nástrojov, knižníc a tiež bezpečnostných prvkov.

Niektoré prvky museli byť upravené a prispôsobené k potrebám aplikácie. K týmto defaultným zabezpečeniam pribudli tiež aj niektoré ďalšie prvky i vlastné riešenia, vyvíjané podľa rôznych štandardov a noriem. Jedná sa o zabezpečenie proti najznámejším a v praxi najčastejšie sa vyskytujúcim zraniteľnostiam a hrozbám, ako napríklad SQL Injection, XSS, CSRF apod.

Súčasný stav zabezpečenia je znázornený v tabuľke (Tab. 16) pomocou checklistu hodnotenia stavu bezpečnosti, ktorý vychádza z definovaného katalógu hrozieb a je v súlade s normou ISO 27002. Hodnotenie je rozdelené na štyri stupne stavu zabezpečenia:

- Implementované – aplikácia má daný prvok ochrany nasadený a aktívny, je proti danej hrozbe dostatočne chránená.
- Neimplementované – aplikácia nemá daný prvok ochrany nasadený a neplánuje sa s jeho nasadením do systému.

- Plánované – aplikácia nemá daný prvok ochrany nasadený, plánuje sa jeho nasadenie do systému.
- Zlepšiť – aplikácia má daný prvok ochrany (čiastočne) nasadený a aktívny, ale je nutné jeho funkciu preveriť, upraviť alebo zlepšiť.

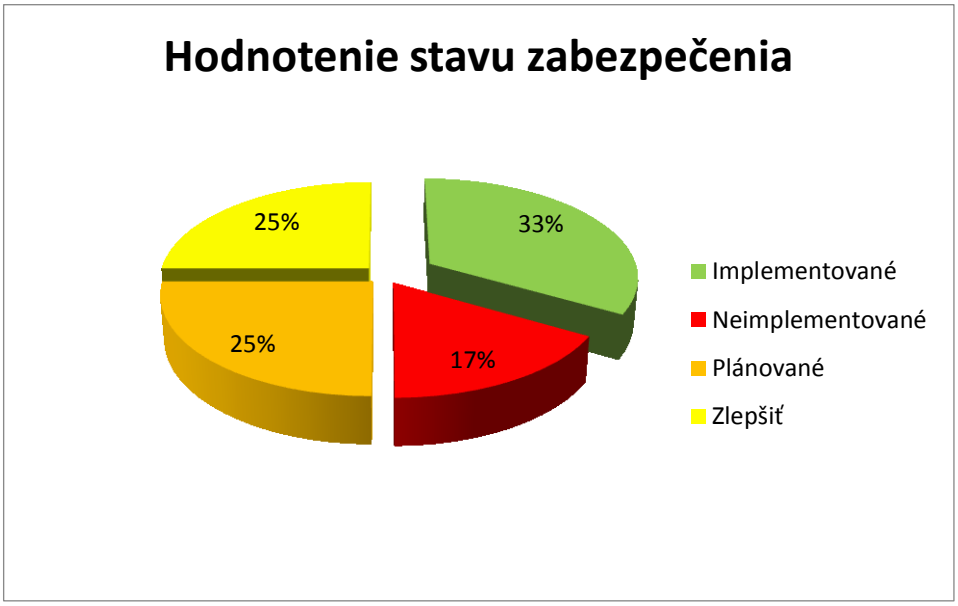
Tab. 16. Checklist hodnotenia stavu bezpečnosti. [Zdroj: vlastný]

Hrozba	Implementované	Neimplementované	Plánované	Zlepšiť
Injektovanie	**X**			
Autentizácia a správa relácie				**X**
Expozícia citlivých dát			**X**	
XXE		**X**		
Kontrola prístupu	**X**			
Zabezpečenie konfigurácie				**X**
XSS	**X**			
Deserializácia		**X**		
Zraniteľné komponenty			**X**	
Logovanie a monitorovanie				**X**
CSRF	**X**			
Presmerovanie a predávanie			**X**	

Z tabuľky je vidieť, že aplikácia má implementovanú ochranu proti injektovaniu, XSS a CSRF útokom a taktiež má dostatočne vyriešenú kontrolu prístupu. Prvé tri z menovaných boli súčasťou základnej ochrany vybraného frameworku. Takisto aj riešenie autentizácie a správy relácie, ktoré je veľmi dobre navrhnuté a perfektne funkčné. Nachádza sa však v kategórii Zlepšiť, pretože k štandardnému prihlasovaniu pomocou prihlasovacieho mena a hesla pribudne ďalší faktor overenia užívateľa pomocou mobilného zariadenia, čo je tiež predmetom tejto diplomovej práce. V tejto kategórii sa ešte nachádza zabezpečenie konfigurácie a logovanie a monitorovanie, ktoré by sa dali definovať skôr ako nedostatky než hrozby. Netreba ich však podceniť a budú navrhnuté riešenia na ich odstránenie, spoločne s hrozbami v kategórii Plánované.

Nakoniec zostali hrozby v kategórii Neimplementované. Zatiaľ sa však nevyužívajú žiadne komponenty zraniteľné týmito hrozbami, takže sa momentálne neuvažuje o žiadnom zabezpečení.

Celkové súčasné zabezpečenie je dobre znázornené percentuálne pomocou grafu (Graf 2).



Graf 2. Hodnotenie stavu zabezpečenia [Zdroj: vlastný]

Z grafu vyplýva, že aplikácia v súčasnej fáze má určitú základnú úroveň zabezpečenia pred najbežnejšími hrozbami, táto miera je však pomerne dosť nízka. Obsahuje prvky, ktoré sú pre ďalší vývoj nevyhovujúce a je nutné ich nejakým spôsobom upraviť alebo vylepšiť.

4.5 Vybrané bezpečnostné hrozby

S ohľadom na relevantnosť hrozieb na predmetný informačný systém sa môže upraviť zoznam hrozieb pre analýzu rizík, ktorým sa bude venovať najväčšia pozornosť pri zabezpečovaní informačného systému. Čiže na základe faktu, že daná aplikácia v aktuálnej fáze vývoja systému nepoužíva XML a podobné prvky, v blízkej budúcnosti sa neuvažuje o využití týchto funkcionalít a vzhľadom na malú pravdepodobnosť napadnutia systému pomocou týchto zraniteľností, boli z definovaného katalógu vybrané nasledujúce hrozby:

1. Injektovanie,
2. Chybná autentizácia,
3. Expozícia citlivých dát,
4. Prelomenie kontroly prístupu,
5. Nezabezpečená konfigurácia,

6. Cross-Site Scripting (XSS),
7. Použitie komponentov so známymi zraniteľnosťami,
8. Nedostatočné zaznamenávanie a monitorovanie činnosti,
9. Cross-Site Request Forgery (CSRF),
10. Neošetrené presmerovanie a predávanie.

V ďalšej fáze sa vypočíta pravdepodobnosť, stanoví celkové riziko uvedených hrozieb a odhadne ich závažnosť pre vybraný informačný systém. Následne sa musí urobiť informované rozhodnutie, ako so získanými informáciami naložiť a vykonať patričné opatrenia na zníženie alebo najlepšie úplné eliminovanie týchto rizík.

4.6 Analýza rizík vybraných hrozieb

V tejto podkapitole budú z dôvodu získania skutočného obrazu o miere rizík analyzované riziká vybraných hrozieb pri súčasnom stave zabezpečenia, tzn. plánovaných, ale aj implementovaných riešení zabezpečenia.

Na analýzu rizík existuje veľa spôsobov a prístupov. V práci je stanovené jediné aktívum a to informačný systém, resp. dáta, ktoré obsahuje, preto k vypracovaniu analýzy rizík je použitý prístup podľa Metodológie riadenia rizík OWASP [33], ktorá vychádza zo štandardných metodík a je prispôsobená na zabezpečenie webových aplikácií.

4.6.1 Identifikácia rizík

Prvým krokom je identifikácia rizika. K výpočtu celkového rizika je potrebné poznať mieru pravdepodobnosti a dopad, ktorý je rozdelený na technický dopad a dopad na podnikanie. Musia sa teda získať informácie o pôvodcoch hrozieb, danom útoku, zraniteľnosti a dopade úspešného útoku na aplikáciu a podnikanie.

K tomuto účelu práve poslúži stanovený katalóg hrozieb, v ktorom sú všeobecne definované niektoré z týchto faktorov. Úlohou je pre každú hrozbu z katalógu určiť jednotlivé faktory a aplikovať všetky získané dáta pre vybranú spoločnosť.

Pri identifikovaní rizík je všeobecne najlepšie rátať s najhorším možným scenárom, ktorý predstavuje najvyššie celkové riziko, čo umožní získať presnejší obraz o miere skutočného rizika pre aplikáciu.

4.6.2 Odhad pravdepodobnosti

Odhadom pravdepodobnosti sa určí približná miera toho, že útočník odhalí a zneužije danú zraniteľnosť. Odhad nemusí byť celkom presný, cieľom je orientačne zistiť, či je pravdepodobnosť nízka, stredná alebo vysoká.

Pre určenie pravdepodobnosti je potrebné poznať jednotlivé faktory o pôvodcoch hrozieb a zraniteľnostiach, ktoré môžu zneužiť. Tieto faktory sú určené v rámci danej kategórie súborom otázok a rôznych odpovedí, pričom každá možnosť je bodovo ohodnotená na stupnici od 0 po 9, kde 0 predstavuje minimálnu a 9 najvyššiu pravdepodobnosť. Pri hodnotení sa vyberie jedna možnosť, ktorá najlepšie vystihuje skupinu útočníkov, stav alebo scenár (dopad). V prípade, že dané bodové hodnotenie vybranej možnosti presne nevystihuje úroveň pravdepodobnosti, môže byť podľa potreby zmenené.

Nakoniec hodnota celkovej pravdepodobnosti je získaná priemerom hodnôt všetkých faktorov pôvodcov hrozieb a zraniteľností.

Pôvodcovia hrozieb

Prvá časť odhadu pravdepodobnosti sa týka pôvodcov hrozieb. Jej cieľom je odhadnúť pravdepodobnosť vykonania úspešného útoku na aplikáciu pomocou série otázok, ktoré zisťujú potrebnú zdatnosť útočníka, ako môže byť k útoku finančne motivovaný, aké prostriedky potrebuje k vykonaniu útoku a ako veľká je skupina útočníkov v rámci organizácie alebo mimo nej, ktorá by mohla útok vykonať. Pri hodnotení je vybraný najhorší možný prípad.

Úroveň zručnosti

Aká úroveň technickej zručnosti útočníka sa predpokladá na zneužitie zraniteľnosti?

a) penetračné zručnosti, (1)
b) sieťové a programovacie zručnosti, (3)
c) pokročilí užívatelia počítačov, (5)
d) nejaké technické zručnosti, (6)
e) žiadne technické zručnosti. (9) [33]

Motivácia

Ako motivovaní sú útočníci k nájdeniu a zneužitiu danej zraniteľnosti?

a) nízka alebo žiadna odmena, (1)

b) možná odmena, (4)
c) vysoká odmena. (9) [33]

Možnosti

Aké prostriedky a možnosti potrebujú útočníci k nájdeniu a zneužitiu danej zraniteľnosti?

a) úplný prístup alebo nákladné prostriedky, (0)
b) špeciálny prístup alebo prostriedky, (4)
c) nejaký prístup alebo prostriedky, (7)
d) žiadny prístup ani prostriedky. (9) [33]

Veľkosť

Ako veľká je skupina útočníkov?

a) vývojári, (1)
b) systémoví administrátori, (2)
c) intranetoví užívatelia, (4)
d) partneri, (5)
e) prihlásení užívatelia, (6)
f) anonymní užívatelia internetu. (9) [33]

Miera pravdepodobnosti pre dané hrozby

V nižšie uvedenej tabuľke (Tab. 17) je súhrn vybraných možností a ich bodového hodnotenia pre danú hrozbu.

Tab. 17. Súhrn vybraných možností pre určenie miery pravdepodobnosti pôvodcov hrozieb. [Zdroj: vlastný]

Hrozba	Pôvodcovia hrozieb			
	Zručnosti	Motivácia	Možnosti	Veľkosť
Injektovanie	d) 6	c) 9	c) 7	e) 6
Autentizácia	c) 5	b) 4	d) 9	f) 9
Expozícia citlivých dát	b) 3	b) 6	b) 4	e) 6
Prelomenie kontroly prístupu	b) 3	b) 5	c) 7	f) 9

Nezabezpečená konfigurácia	c) 5	a) 1	c) 7	f) 9
XSS	c) 5	b) 7	c) 7	e) 6
Zraniteľné komponenty	b) 3	b) 4	b) 4	c) 4
Logovanie a monitorovanie	c) 4	a) 2	c) 7	f) 9
CSRF	b) 3	a) 3	c) 7	e) 6
Presmerovanie a predávanie	b) 3	a) 2	c) 7	f) 9

Zraniteľnosti

Druhá séria otázok pre odhad pravdepodobnosti je zameraná na teoretické vlastnosti daných hrozieb – ako náročné ich je zistiť a zneužiť, ako sú rozšírené v celkovom meradle hrozieb a ako sú monitorované a kontrolované v rámci danej aplikácie.

Zistiteľnosť

Ako náročné je pre útočníka objaviť túto zraniteľnosť?

a) prakticky nemožné, (1)
b) náročné, (3)
c) ľahké, (7)
d) bežne dostupnými automatizovanými nástrojmi. (9) [33]

Zneužiteľnosť

Ako náročné je pre útočníka zneužiť túto zraniteľnosť?

a) teoretické, (1)
b) náročné, (3)
c) ľahké, (7)
d) bežne dostupnými automatizovanými nástrojmi. (9) [33]

Rozšírenie

Aké je rozšírenie tejto zraniteľnosti?

a) vzácne, (1)
b) bežné, (4)

c) rozsiahle, (7)

d) veľmi rozsiahle. (9) [33]

Detekcia zneužitia

Aká je pravdepodobnosť, že sa zneužitie (včas) zistí?

a) automatizovaná detekcia v aplikácii, (1)

b) zaznamenávaná a kontrolovaná, (3)

c) zaznamenávaná bez kontroly, (8)

d) nezaznamenávaná. (9) [33]

Miera pravdepodobnosti pre dané hrozby

Získané údaje z tejto série otázok sú uvedené v nasledujúcej tabuľke (Tab. 18).

Tab. 18. Súhrn vybraných možností pre určenie miery pravdepodobnosti zraniteľností. [Zdroj: vlastný]

Hrozba	Pôvodcovia hrozieb			
	Zistiteľnosť	Zneužiteľnosť	Rozšírenie	Detekcia zneužitia
Injektovanie	c) 7	c) 7	b) 4	a) 1
Autentizácia	b) 3	c) 7	b) 4	b) 3
Expozícia citlivých dát	b) 3	b) 3	c) 7	d) 9
Prelomenie kontroly prístupu	b) 3	b) 3	b) 4	a) 1
Nezabezpečená konfigurácia	c) 7	c) 7	c) 7	d) 9
XSS	c) 7	c) 7	c) 7	a) 1
Zraniteľné komponenty	b) 3	b) 3	c) 7	d) 9
Logovanie a monitorovanie	a) 1	b) 3	c) 7	d) 9
CSRF	c) 7	b) 3	b) 4	a) 1
Presmerovanie a predávanie	c) 7	b) 3	a) 1	d) 9

Stanovenie celkovej pravdepodobnosti

Boli ohodnotené jednotlivé faktory, z ktorých sa následne vypočíta miera celkovej pravdepodobnosti spriemerovaním všetkých získaných hodnôt. Výsledné hodnoty sú uvedené v tabuľke (Tab. 19).

Tab. 19. Hodnotenie celkovej pravdepodobnosti. [Zdroj: vlastný]

Hrozba	Priemer	Hodnotenie pravdepodobnosti
Injektovanie	**5,875**	Stredná
Autentizácia	**5,5**	Stredná
Expozícia citlivých dát	**5,125**	Stredná
Prelomenie kontroly prístupu	**4,375**	Stredná
Nezabezpečená konfigurácia	**6,5**	Veľká
XSS	**5,875**	Stredná
Zraniteľné komponenty	**4,625**	Stredná
Logovanie a monitorovanie	**5,25**	Stredná
CSRF	**4,25**	Stredná
Presmerovanie a predávanie	**5,125**	Stredná

Z tabuľky je vidieť, že celková pravdepodobnosť napadnutia systému nie je až tak vysoká, i keď niektoré faktory sú ohodnotené najvyšším stupňom pravdepodobnosti. U niektorých hrozieb je celkový výsledok ovplyvnený aktívnym monitorovaním a zaznamenávaním činnosti danej hrozby.

4.6.3 Odhad dopadu

Pri odhadovaní dopadu je dôležité si uvedomiť, že existujú dva druhy dopadu. Prvým je technický dopad na aplikáciu, dáta a funkcie. Druhým a v praxi cennejším druhom, je obchodný dopad na podnikanie spoločnosti, ktorá aplikáciu prevádzkuje.

Technický dopad

Otázky na technické dopady sú rozdelené na faktory, ktoré sa týkajú základných bezpečnostných atribútov a to: dôvernosť, integrita, dostupnosť a tiež aj zodpovednosť. Cieľom je odhadnúť úroveň dopadu pri využití zraniteľnosti. Väčšinou rozsah a citlivosť uniknutých

dát závisí od typu účtu, nad ktorým útočník získal kontrolu, záleží však aj od konkrétneho typu prevedeného útoku. Pri hodnotení prvých troch faktorov sa ráta najmä s najhorším scenárom dopadu, i keď u niektorých hrozieb už zabezpečenie existuje, pretože ak sa útočníkovi podarí prelomiť primárnu ochranu proti danému útoku, ostatné formy zabezpečenia sú už väčšinou málo efektívne. Posledný faktor ohľadom vysledovateľnosti súvisí s logovaním a monitorovaním činnosti aplikácie a užívateľov, ktoré je hodnotené podľa súčasného stavu nastavených procesov monitorovania podozrivej aktivity ohľadom daných hrozieb.

Strata dôvernosti

Aké množstvo údajov môže pri útoku uniknúť a aká je ich citlivosť?

a) minimálne, necitlivé údaje, (2)
b) minimálne, citlivé údaje, (6)
c) rozsiahle, necitlivé údaje, (6)
d) rozsiahle, citlivé údaje, (7)
e) všetky dáta. (9) [33]

Strata integrity

Aké množstvo dát môže byť poškodených a aké je poškodenie rozsiahle?

a) minimálne, mierne poškodenie, (1)
b) minimálne, vážne poškodenie, (3)
c) rozsiahle, mierne poškodenie, (5)
d) rozsiahle, vážne poškodenie, (7)
e) poškodenie všetkých dát. (9) [33]

Strata dostupnosti

Koľko služieb môže „spadnúť“ a aké sú dôležité?

a) minimum, vedľajšie služby, (1)
b) minimum, hlavné služby, (5)
c) rozsiahle, vedľajšie služby, (5)
d) rozsiahle, hlavné služby, (7)
e) všetky služby. (9) [33]

Strata zodpovednosti

Je útočník vysledovateľný?

a) plne vysledovateľný, (1)
b) prípadne vysledovateľný, (7)
c) úplne anonymný. (9) [33]

Miera technického dopadu pre dané hrozby

V tabuľke (Tab. 20) sa nachádzajú získané údaje pre určenie technického dopadu vybraných hrozieb.

Tab. 20. Súhrn vybraných možností pre určenie miery technického dopadu. [Zdroj: vlastný]

Hrozba	Technický dopad			
	Strata dôvernosti	Strata integrity	Strata dostupnosti	Strata zodpovednosti
Injektovanie	e) 9	e) 9	e) 9	a) 1
Autentizácia	e) 9	e) 9	e) 9	a) 1
Expozícia citlivých dát	d) 7	c) 5	a) 1	b) 7
Prelomenie kontroly prístupu	d) 7	d) 7	d) 7	a) 1
Nezabezpečená konfigurácia	c) 6	c) 5	a) 1	a) 1
XSS	a) 2	d) 7	c) 5	a) 1
Zraniteľné komponenty	c) 6	c) 5	c) 5	b) 7
Logovanie a monitorovanie	a) 2	c) 5	d) 7	b) 7
CSRF	b) 6	b) 3	c) 5	b) 4
Presmerovanie a predávanie	a) 2	c) 5	c) 5	a) 3

Obchodný dopad

Nakoniec je uvedená séria faktorov, ktorá sa týka obchodného dopadu na organizáciu. Otázky zisťujú aké finančné škody môže útok napáchať, aký dopad môže mať na povesť organizácie, ako veľmi boli porušené zásady a koľkých osôb sa môže prípadný únik údajov

dotknúť (predpokladaný počet zamestnancov a klientov v budúcnosti). Cieľom je stanoviť mieru negatívneho vplyvu zneužitia vybraných zraniteľností na spoločnosť, ktorá danú aplikáciu používa.

Finančné škody

Aké finančné škody budú napáchané zneužitím zraniteľnosti?

a) menej ako náklady na odstránenie zraniteľnosti, (1)
b) malý vplyv na ročný zisk, (3)
c) významný vplyv na ročný zisk, (7)
d) bankrot. (9) [33]

Poškodenie dobrého mena

Môže zneužitie zraniteľnosti spôsobiť poškodenie dobrého mena spoločnosti?

a) minimálne poškodenie, (1)
b) strata hlavných (kľúčových) zákazníkov, (3)
c) strata povesti, (5)
d) poškodenie značky. (9) [33]

Nedodržanie zásad

Aké veľké porušenie predstavuje nedodržanie zásad?

a) malé porušenie, (2)
b) jednoznačné porušenie, (5)
c) porušenie veľkého rozsahu. (7) [33]

Porušenie ochrany osobných údajov

Koľko osobných údajov môže byť zverejnených?

a) jednej osoby, (3)
b) stovky ľudí, (5)
c) tisíce ľudí, (7)
d) milióny ľudí. (9) [33]

Miera obchodného dopadu pre dané hrozby

V tabuľke (Tab. 21) sa nachádzajú získané údaje pre určenie miery obchodného dopadu vybraných hrozieb pre danú aplikáciu.

Tab. 21. Súhrn vybraných možností pre určenie miery obchodného dopadu. [Zdroj: vlastný]

Hrozba	Obchodný dopad			
	Finančné škody	Poškodenie dobrého mena	Nedodržanie zásad	Osobné údaje
Injektovanie	c) 7	d) 9	c) 7	c) 7
Autentizácia	c) 7	d) 9	c) 7	c) 7
Expozícia citlivých dát	c) 7	d) 9	c) 7	c) 7
Prelomenie kontroly prístupu	c) 7	c) 5	b) 5	b) 5
Nezabezpečená konfigurácia	b) 3	b) 3	b) 5	b) 5
XSS	c) 7	c) 5	b) 5	b) 5
Zraniteľné komponenty	b) 3	b) 3	b) 5	b) 5
Logovanie a monitorovanie	b) 3	b) 3	b) 5	b) 4
CSRF	b) 3	c) 5	a) 2	b) 5
Presmerovanie a predávanie	a) 1	a) 2	a) 2	b) 4

Stanovenie dopadu

Spriemerovaním získaných hodnôt jednotlivých faktorov sa vypočíta miera pre technický a obchodný dopad zvlášť, podľa ktorej sa určí ich závažnosť. Výsledky hodnotenia sú uvedené v nasledujúcej tabuľke (Tab. 22).

Tab. 22. Celková závažnosť technického a obchodného dopadu. [Zdroj: vlastný]

Hrozba	Technický dopad		Obchodný dopad	
	Priemer	Hodnotenie dopadu	Priemer	Hodnotenie dopadu
Injektovanie	**7**	Vysoký	**7,5**	Vysoký

Autentizácia	**7**	Vysoký	**7,5**	Vysoký
Expozícia citlivých dát	**5**	Stredný	**7,5**	Vysoký
Prelomenie kontroly prístupu	**5,5**	Stredný	**5,5**	Stredný
Nezabezpečená konfigurácia	**3,25**	Stredný	**4**	Stredný
XSS	**3,75**	Stredný	**5,5**	Stredný
Zraniteľné komponenty	**5,75**	Stredný	**4**	Stredný
Logovanie a monitorovanie	**5,25**	Stredný	**3,75**	Stredný
CSRF	**4,5**	Stredný	**3,75**	Stredný
Presmerovanie a predávanie	**3,75**	Stredný	**2,25**	Nízky

Z tabuľky (Tab. 22) vyplýva, že výsledky hodnotenia obidvoch dopadov sú celkom na tej istej úrovni, i keď čo sa týka vypočítaných priemerov, niektoré sa blížia k hornej, iné zasa k spodnej hranici hodnotenia, avšak celková závažnosť je rovnaká.. Rozdiel je vidieť u dvoch zraniteľností – expozícia citlivých dát a presmerovanie. V prípade expozície je celkom logické, že dopad na podnikanie bude vysoký, naopak je prekvapením, že niektorá zraniteľnosť má iba nízky obchodný dopad.

4.6.4 Určenie celkovej miery rizika

Kombináciou získaných hodnôt pravdepodobnosti s hodnotami najprv technického a potom obchodného dopadu podľa tabuľky (Tab. 23), sa získa konečné hodnotenie závažnosti rizika pre jednotlivé hrozby.

V tabuľke je uvedených päť úrovní miery rizík:

- **Poznámka** – hrozba predstavuje úplne zanedbateľné riziko, ktoré možno označiť len ako poznámku vo výslednom protokole.
- **Nízka** – hrozba predstavuje malé riziko a netreba jej venovať extra pozornosť.
- **Stredná** – hrozba predstavuje nezanedbateľné riziko, ktorému by sa mala venovať väčšia pozornosť.
- **Vysoká** – hrozba predstavuje skutočne veľké riziko, ktoré by malo byť prioritne minimalizované.

- **Kritická** – hrozba predstavuje extrémne riziko pre všetky zúčastnené strany a musia sa vynaložiť všetky možné prostriedky na jej okamžité zabezpečenie.

Tab. 23. Tabuľka pre určenie celkovej miery rizika. [33]

Celková miera rizika				
Dopad	VYSOKÝ	Stredná	Vysoká	Kritická
	STREDNÝ	Nízka	Stredná	Vysoká
	NÍZKY	Poznámka	Nízka	Stredná
		MALÁ	STREDNÁ	VEĽKÁ
	Pravdepodobnosť			

Napríklad v prípade tretej hrozby, expozície citlivých dát, je miera pravdepodobnosti stredná a miera technického dopadu tiež stredná, takže z technického hľadiska je podľa tabuľky (Tab. 24) celková miera rizika taktiež stredná. Na druhej strane pri určovaní obchodného rizika, kde obchodný dopad hrozby je vysoký, z tabuľky (Tab. 24) vyplýva, že miera rizika pre podnik je tiež už vysoká.

Uvedeným spôsobom boli vyhodnotené i ostatné miery rizika daných hrozieb a kompletná tabuľka so všetkými údajmi je obsahom prílohy č. 1.

Tab. 24. Celkové miery rizika pre aplikáciu a podnik. [Zdroj: vlastný]

Hrozba	Miera rizika pre aplikáciu	Miera rizika pre podnik
Injektovanie	Vysoká	Vysoká
Autentizácia	Vysoká	Vysoká
Expozícia citlivých dát	Stredná	Vysoká
Prelomenie kontroly prístupu	Stredná	Stredná
Nezabezpečená konfigurácia	Vysoká	Vysoká
XSS	Stredná	Stredná
Zraniteľné komponenty	Stredná	Stredná
Logovanie a monitorovanie	Stredná	Stredná

CSRF	Stredná	Stredná
Presmerovanie a predávanie	Stredná	Nízka

Ako je vidieť z tabuľky, nečakane, ale našťastie žiadna hrozba nedosiahla kritickej úrovne miery rizika i keď hodnotenie niektorých jednotlivých faktorov tomu nasvedčovalo. Stále sa tu nachádza relatívne veľký počet hodnotení ako vysoké. Celková miera rizika všetkých hrozieb či z technického, či z obchodného hľadiska by sa však dala zhodnotiť ako stredná. V praxi by sa však nemalo podceniť ani najmenšie riziko.

4.7 Popis aktuálneho stavu zabezpečenia

Ako bolo v úvode kapitoly spomenuté, systém už obsahuje bezpečnostné opatrenia na niektoré z uvedených hrozieb. V tejto kapitole budú popísané implementované prvky zabezpečenia a ďalšie procesy, ktoré sú súčasťou aktuálneho zabezpečenia vybraného informačného systému.

Nespornou výhodou informačného systému HFL je, že i keď je to webová aplikácia, nie je verejne prístupná širokej verejnosti užívateľov internetu. To znamená, že na rozdiel od iných webových aplikácií nemá verejnú sekciu ako napríklad úvodnú alebo prezentačnú internetovú stránku firmy s možnosťou prihlásenia do IS. Lepšie povedané, firma samozrejme má takéto stránky, kde prezentuje svoje aktivity alebo ponúka svoje produkty, tieto stránky sú však fyzicky oddelené a nie sú súčasťou adresárovej štruktúry informačného systému.

Takisto sa nikde na týchto stránkach nenachádza žiadny hypertextový odkaz na konkrétne stránky, registráciu alebo prihlásenie do informačného systému. Už aj tento fakt, že potenciálny, nezainteresovaný útočník alebo nejaký internetový robot ani nevie o existencii IS, respektíve o ňom vie, ale nedokáže bez (ne)vedomej pomoci niektorého z užívateľov zistiť jeho „polohu“ (URL adresu), je jednou z výhod a ďalším dôležitým zabezpečením webového informačného systému. Týmto sa jednoducho, ale účinne eliminuje riziko snahy napadnutia informačného systému hrubou silou. V opačnom prípade útočník môže prakticky neustále skúšať rôzne techniky a nástroje na zistenie prístupových údajov, prelomenie hesiel, sieťové odpočúvanie, či skúšať prekonať iné z foriem zabezpečenia informačného systému.

Väčšina takýchto útokov sa síce dá detegovať, je však čím ďalej zložitejšie a namáhavejšie sa pred nimi brániť, pretože neustále vznikajú nové spôsoby a nástroje ako rôzne typy zabezpečení prelomiť. Takisto útočníci objavujú nové „trhliny“ (zraniteľné miesta) priamo v princípoch, či zdrojových kódoch samotných programovacích jazykov, alebo ostatných externých moduloch a pluginoch, ktoré aplikácia využíva. Príkladom môže byť obľúbený útok SQL Injection.

Na tieto hrozby vývojári reagujú tzv. patchmi (z angl. „záplatami“) – opravnými aktualizáciami alebo vydaním novej zabezpečenej verzie programu, či programovacieho jazyka.

4.7.1 SQL Injection

Injektovanie, v tomto prípade konkrétne SQL injektovanie je asi najznámejší a v praxi najrozšírenejší útok na webové aplikácie, pri ktorom útočník využíva skutočnosti, že užívateľom zadávané dáta do systému nie sú pred vykonaním príkazu ich uloženia do databázy riadne ošetrené. V PHP verzii 5.1 bolo implementované rozšírenie PDO (PHP Document Object), ktoré tento útok stopercentne eliminuje.

I keď snáď na všetkých diskusných fórach a internetových stránkach pri témach ohľadom zastaraného príkazu „mysql_query“ a pod., každý skúsený vývojár upozorňuje:

- „POZOR na SQL Injection“,
- „escapujte užívateľom zadávané dáta“,
- „používajte parametrizované dotazy“,
- „používajte PDO“,

stále sa na internete dá nájsť veľa webových stránok nezabezpečených proti tomuto útoku. A stačí celkom málo, pri (správnom) použití štandardných nástrojov, napríklad PDO, je tento problém v podstate vyriešený.

4.7.2 XSS

Zabezpečenie proti XSS útokom je riešené pomocou tzv. XSS filtra. Jeho úlohou je jednoducho „odstrániť“ každý potenciálny kód v hocijakých dátach a zobraziť ho ako obyčajný text bez toho, aby bol vykonaný. Týmto filtrom prechádza každý reťazec na výstupe.

4.7.3 CSRF

V prípade zabezpečenia proti CSRF útokom sú použité tzv. tokeny, ktoré sú skryté vo všetkých formulároch a sú vyžadované pri ich spracovávaní serverom. Tým sa zabráni nechcenému alebo neoprávnenému spracovaniu formulára, ktorý mohol byť podvrhnutý obeti nejakého útočníka.

4.7.4 Kontrola prístupu

V každej aplikácii je dôležité nastavenie prístupových práv jednotlivým užívateľom, tzn., že každý užívateľ musí mať jasne definované povolenia a obmedzenia k akým funkciám alebo stránkam aplikácie pristupovať smie a ktoré má zakázané. Existuje viacero modelov kontroly prístupu. Najbežnejší je asi RBAC (Role-Based Access Control, v preklade z angl. Kontrola prístupu na základe rolí) model, založený na overovaní role prihláseného užívateľa a jej preddefinovaných oprávnení. Tento model však nevyhovoval politike kontroly prístupu v aplikácii, pretože dokáže overiť iba skupinu užívateľov a nie práva užívateľa samotného. Preto bol vybraný model ABAC (Attribute-Based Access Control), niekedy nazývaný aj Activity-Based Access Control model, ktorý pre rozhodovanie používa booleovskú logiku. Tento model v podstate tiež využíva prvky RBAC modelu, že užívatelia sú zaradení do skupín, čo umožňuje rýchle nastavenie práv. Pri overovaní je však rozdiel, že systém nekontroluje iba rolu užívateľa, ale či má právo k danej akcii. Pri definovaní práv jednotlivým užívateľom sa tak môžu i v rámci jednej skupiny užívateľov, napríklad Manažérom, nastaviť rôzne práva k prístupu k určitým akciám. Jednoducho sa teda nastaví, čo všetko užívateľ smie vykonať alebo kam môže pristupovať a ostatné má zakázané, čiže aplikuje bezpečnostnú politiku na princípe whitelistov.

4.7.5 Proces vytvorenia, registrácie a prihlásenia užívateľa

Vytvorenie užívateľa

V princípe vytvorenie užívateľa funguje tak, že administrátor informačného systému na podnet vedúceho alebo iného zodpovedného pracovníka firmy, pomocou formulára vytvorí účet pre budúceho užívateľa:

- V prvom kroku zadá jeho pracovnú emailovú adresu.
- Z mena emailovej adresy sa automaticky vygeneruje prihlasovacie meno do aplikácie, toto meno je vždy unikátne, tak ako daná emailová adresa.
- Zo zoznamu vyberie spoločnosť, ktorej je pracovníkom.

- Vyberie rolu (prakticky takú všeobecnú, neoficiálnu pozíciu) užívateľa, čo je v podstate skupina práv, podľa ktorej sú prednastavené povolenia k jednotlivým akciám v informačnom systéme.
- V ďalšom kroku môže administrátor podľa povahy a potrieb danej pozície užívateľa konkrétne jednotlivé práva k akciám pridať, či odobrať. Môže teda vybrať rolu nižšej úrovne a pridať práva k niektorým akciám z vyššej úrovne alebo opačne, vybrať rolu vyššej úrovne a nepotrebné práva odobrať. Mimo zabezpečenia a kategorizácie užívateľov ide najmä o zjednodušenie a urýchlenie procesu vytvorenia užívateľa pre administrátora, pretože počet možných práv je už v tejto fáze vysoký a postupným vývojom aplikácie ďalšie akcie a s nimi spojené práva pribúdajú.
- Nakoniec administrátor takto vyplnený formulár odošle na spracovanie serverom.
- Po skontrolovaní všetkých vyplnených údajov a úspešnom spracovaní formulára, sa vytvorený užívateľ uloží do databázy a súčasne server automaticky odošle registračný email na uvedenú emailovú adresu.

Registrácia a aktivácia užívateľa

Po prijatí registračného emailu sa teraz môže užívateľ zaregistrovať do systému a následne musí svoj účet aktivovať. Celý proces prebieha vo viacerých krokoch:

- V registračnom emaile je užívateľ vyzvaný ku kliknutiu na odkaz s vygenerovaným unikátnym kódom, ktorý ho presmeruje na registračnú stránku informačného systému.
- Na tejto stránke sa nachádza formulár, kde na začiatku sú predvyplnené polia s prihlasovacím menom a emailovou adresou. Tieto údaje sa nedajú upraviť a pre užívateľa majú len informatívny charakter. V nasledujúcich dvoch poliach si užívateľ vytvorí silné heslo a pre kontrolu ho zopakuje. Ďalej vyplní svoje meno, priezvisko a nakoniec vyberie pohlavie.
- Po úspešnej registrácii znovu systém automaticky odošle užívateľovi email, tento krát s aktivačným odkazom. Po kliknutí na tento odkaz sa účet aktivuje a užívateľ sa následne môže prihlásiť do systému. Aktivácia nového účtu je štandardným postupom pri registrácii a okrem toho sa v aktivačnom emaile nachádzajú ďalšie informácie a pokyny.

Niekto by mohol povedať, že vo formulári chýba CAPTCHA, čo je jeden celkom dôležitý bezpečnostný prvok, ktorý sa u formulárov tohto typu zvyčajne používa. Pravdepodobne sa s ním už každý stretol, pretože sa často vyskytuje napríklad pri vytváraní emailových účtov alebo pri registrácii do rôznych diskusných fór, webových stránok a aplikácií.

Pre vysvetlenie, skratka CAPTCHA v preklade z angličtiny znamená Plno automatický verejný Turingov test na odlíšenie počítačov a ľudí, čiže jeho hlavnou úlohou je overovanie, či užívateľ, ktorý sa snaží zaregistrovať na stránku, je skutočne človek alebo internetový robot. Overenie väčšinou spočíva v zobrazení obrázku s deformovaným alebo inak upraveným textom a úlohou užívateľa je tento text správne dešifrovať a opísať do príslušného políčka, pričom sa predpokladá, že internetový robot i pri použití pokročilej technológie OCR (Optické rozpoznávanie znakov) nedokáže text rozoznať a teda neprejde testom. Dôvodom, prečo sa CAPTCHA používa je, že inak by na takto nezabezpečených stránkach pomocou internetových robotov denne vznikali tisíce falošných účtov, alebo spamových komentárov napríklad na diskusných fórach. [34]

Ako už bolo však na začiatku kapitoly spomenuté, informačný systém HFL je pred verejnosťou uzavretý a registračná stránka je bez „pozvánky“ (registračného odkazu) nedostupná, takže žiadny externý užívateľ ani robot sa na ňu nedostane a preto nie je nutné ju pomocou CAPTCHA zabezpečovať.

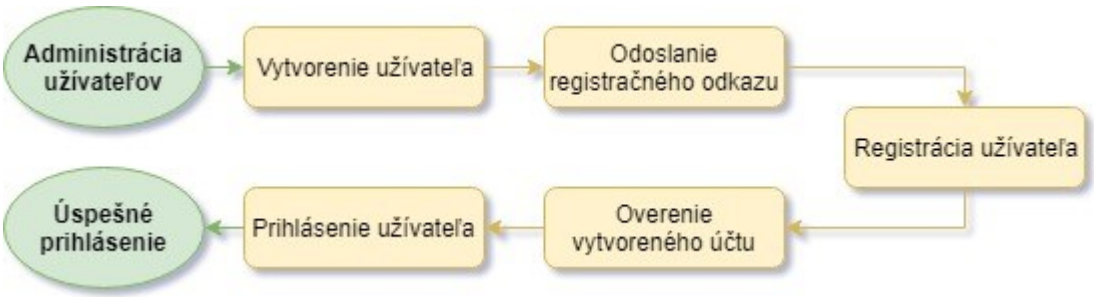
Registračný odkaz je jednorazový, takže aj keby sa niekomu podarilo dostať k tomuto odkazu alebo i základnej časti adresy a snažil by sa ju jednoducho vložiť do URL riadka prehliadača, nič by mu to nepomohlo, pretože bez všetkých potrebných a hlavne správnych parametrov, ktorý musí adresa obsahovať, sa registračná stránka (druhýkrát) nezobrazí, ale presmeruje užívateľa na chybovú stránku.

Celý tento proces vytvorenia a registrácie užívateľov sa na prvý pohľad môže zdať zdĺhavý a možno komplikovaný, je to však pre daného užívateľa len jednorazová akcia, ktorú nebude musieť viackrát opakovať.

V ďalšej fáze vývoja informačného systému sa počíta s pristupovaním do informačného systému aj klientom spoločnosti a proces vytvorenia a registrácie užívateľa bude musieť byť upravený, aby sa mohol každý klient zaregistrovať samostatne, bez nutnosti vytvárania účtu správcom systému.

Prihlásenie užívateľa

Prihlásenie do systému už je len jeden klasický úkon, ktorý väčšina ľudí robí denne niekoľkokrát. Užívateľ do príslušných polí zadá získané prihlasovacie meno a vytvorené heslo a po overení správnosti zadaných údajov je presmerovaný na domovskú stránku informačného systému. Na obrázku (Obr. 3) je znázornený proces od vytvorenia po prihlásenie užívateľa.



Obr. 3. Proces od vytvorenia po prihlásenie užívateľa. [Zdroj: vlastný]

Toto jednoduché zabezpečenie len pomocou hesla však už v dnešnej dobe nestačí, preto bude v ďalšej kapitole navrhnuté lepšie zabezpečenie pomocou dvojfaktorového overenia.

V tejto kapitole bola predstavená spoločnosť a predmetný informačný systém. Ďalej boli stanovené miery rizík, na základe ktorých boli vybrané bezpečnostné hrozby a nakoniec bol popísaný súčasný stav zabezpečenia informačného systému.

Hlavným cieľom tejto kapitoly však bolo realizovanie analýzy rizík, z ktorej vyplýva, že každá hrozba predstavuje relatívne vysoké riziko získania kontroly nad systémom a možnému prístupu a zneužitiu dát.

5 NÁVRH ZABEZPEČENIA INFORMAČNÉHO SYSTÉMU HFL

Predmetom tejto kapitoly je návrh zabezpečenia vybraného informačné systému, v ktorom bude na začiatku využitý checklist hodnotenia stavu bezpečnosti zo štvrtej kapitoly.

Najprv by mal celý systém prejsť kontrolou implementovaných prvkov zabezpečenia, či naozaj je toto zabezpečenie dostačujúce a plne funkčné a môže sa toto riziko hrozieb označiť ako odstránené alebo minimalizované na najmenšiu možnú mieru. V opačnom prípade sa navrhnú opatrenia na zlepšenie tohto zabezpečenia.

Následne sa musí pozornosť zamerať na hrozby z kategórie Plánované a Zlepšiť. V tomto prípade, na určenie poradia a prioritných cieľov zabezpečenia, budú využité výsledky z analýzy rizík, podľa ktorých sa pôjde postupne od najrizikovejších hrozieb po hrozby predstavujúce menšie riziko.

V prvom rade by teda mali byť navrhnuté riešenia pre zraniteľnosti z kategórie Plánované, pretože pre ne neexistujú dosiaľ žiadne bezpečnostné opatrenia, čo predstavuje vyššie riziko, než slabiny, ktoré už nejaké zabezpečenie majú, i keď nie je veľmi dostačujúce.

Z uvedených dôvodov bude postup návrhu opatrení nasledovný:

1. Nastavenie šifrovania citlivých dát,
2. Zabezpečenie zraniteľných komponentov,
3. Odstránenie akéhokoľvek presmerovania a predávania,
4. Zabezpečenie konfigurácie,
5. Nastavenie logovania a monitorovania dôležitých procesov,
6. Dvojfaktorové overenie.

Pri zabezpečovaní sa bude väčšia pozornosť venovať najmä vybraným hrozbám, čo však neznamená, že ostatné nebudú zabezpečené. Do úvahy sa musia vždy brať všetky hrozby a nesmie sa nespoliehať na to, že riziko zneužitia zraniteľnosti je malé, alebo ju nemá kto zneužiť a napadnúť tak systém. Na takýto štýl uvažovania už doplatilo veľa vývojárov a firiem.

5.1 Nastavenie šifrovania citlivých dát

Zabezpečeniu citlivých dát by sa mala venovať väčšia pozornosť ako čomukoľvek inému. Všetky citlivé dáta, napr. heslá, osobné údaje alebo čísla kreditných kariet by mali byť za-

bezpečené či už „v pokoji“ (uložené na nejakom dátovom nosiči), pri ich používaní alebo prenose.

Najlepším riešením preto je ich zašifrovanie, aby ich akákoľvek neoprávnená osoba nemohla prečítať. Mali by sa používať silné šifrovacie algoritmy a kľúče.

Pri šifrovaní ukladaných hesiel by sa mali taktiež používať tzv. soli – niekoľkobitové textové reťazce, ktoré sa vkladajú do šifrovacieho procesu a zabezpečia, aby i v prípade získania súboru s uloženými heslami, útočník nebol schopný odkryť heslá napr. pomocou dúhovej tabuľky.

Štandardným zabezpečením by už malo byť aj použitie SSL/TLS certifikátu, aby sa zabránilo útočníkovi jednoducho sledovať sieťovú komunikáciu a ukradnúť napr. užívateľskú reláciu obete, pomocou ktorej by získal prístup k jeho dátam alebo jeho oprávnenia v aplikácii.

5.2 Zabezpečenie zraniteľných komponentov

Najlepším riešením zabezpečenia by bolo nepoužívať komponenty, ako napríklad rôzne knižnice alebo nástroje, ktorých autorom nie je samotný vývojár danej aplikácie, čo je však prakticky nemožné. Drvivá väčšina projektov alebo aplikácií používa prídavné knižnice tretích strán, pretože veľmi uľahčujú prácu. Väčšinou je používanie alternatívnych riešení, či prostriedkov alebo vytváranie vlastných knižníc (časovo) náročné, nad sily i skúseného programátora, niekedy aj nebezpečné, jednoducho neefektívne a zbytočné, preto sa nedá používaniu rôznych komponentov vyhnúť. Ako pekný príklad sa môže uviesť najrozšírenejšia javascriptová knižnica jQuery, ktorá výrazne zjednodušuje manipuláciu s obsahom stránky, reakciu na udalosti, animácie a používanie AJAXu, takže sa bez nej, alebo jej (náročnejších) alternatív nezaobíde žiadny väčší projekt.

Veľa vydavateľov komponentov však nevydáva bezpečnostné záplaty pre ich staršie verzie, ale väčšinou zraniteľnosti opravujú až v ďalších verziách, preto je veľmi dôležité mať aktualizované všetky komponenty na najnovšie verzie.

Na zabezpečenie takýchto zraniteľností sa teda najprv musia identifikovať všetky používané prídavné komponenty a ich verzie. Môže sa pomocou špeciálnych verejných databáz zistiť, či sú nejako bezpečnostne deravé, ale následne ich je aj tak nutné aktualizovať na najnovšie verzie. Taktiež by mal byť stanovený bezpečnostný proces riadenia používaných komponentov.

5.3 Odstránenie akéhokoľvek presmerovania

Zraniteľnosti tohto typu sú často zneužívané útočníkmi k napadnutiu systému pomocou phishingu, preto je veľmi dôležité jej predísť. Znovu najlepším riešením je nepoužívať žiadne odkazy na externé stránky, ani presmerovania v rámci internej siete a nepoužívať cieľovú adresu ako užívateľské parametre. Pokiaľ sa však nedá tejto technike vyhnúť, mali by byť aspoň všetky parametre riadne overené a autorizované pre daného užívateľa.

Zabezpečenie tejto zraniteľnosti vo vybranom informačnom systéme zakázaním akéhokoľvek presmerovania by nemal byť až taký problém ako v predchádzajúcom prípade, pretože aj keď aplikácia takéto presmerovania používa, väčšinou vždy sa dá tento problém jednoducho vyriešiť alternatívnou metódou, bez použitia presmerovania.

Úlohou je teda preskúmaním kódu aplikácie nájsť všetky možné presmerovania a skontrolovať, či je cieľová URL adresa súčasťou niektorého z parametrov. V prípade objavenia takéhoto presmerovania, malo by byť buď zabezpečené, v lepšom prípade upravené bez použitia presmerovania alebo pokiaľ je to možné, jednoducho odstránené.

5.4 Zabezpečenie konfigurácie

V praxi často dochádza k zneužitiu zraniteľností následkom nezabezpečenej konfigurácie najmä pomocou nezmenených defaultných nastavení frameworku, administrátorského prostredia, jeho účtov a hesiel. Takisto obľúbenou technikou útočníkov je prezeranie a získavanie informácií z chybových hlásení servera alebo vypisovaním adresárovej štruktúry na serveri.

Aby nedošlo k zneužitiu týchto zraniteľností musia sa:

- odstrániť defaultné nastavenia použitého frameworku,
- odstrániť alebo upraviť defaultné nastavenia účtov a hesiel,
- odstrániť nepoužívané stránky a časti kódov,
- zakázať výpisy adresárovej štruktúry servera,
- zakázať výpisy chybových a iných informačných hlásení zo zásobníka servera v produkčnej verzii,
- opraviť chyby.

5.5 Nastavenie logovania a monitorovania dôležitých procesov

V aplikácii, či na serveri by mali byť monitorované a zaznamenané všetky aktivity, ktoré by mohli pomôcť predísť alebo včas odhaliť a zabrániť prípadnému útoku, odcudzeniu alebo strate dát.

K tomu pre zabezpečenie hlavne integrity dát, by mali byť tiež nastavené procesy zaznamenávania manipulácie s dátami, aby sa napr. zo spätnej analýzy dalo určiť kto, kedy, aké (prípadne aj ako) dáta upravil alebo zmazal.

Monitorovanie a zaznamenávanie procesov by sa dalo rozdeliť do piatich skupín:

- aktivita užívateľov – prihlasovanie, registrácia atď.,
- manipulácia s dátami – editácia, presun, mazanie atď.,
- bezpečnostné varovania a hlásenia – zaznamenávanie podozrivej, nebezpečnej aktivity v systéme,
- aplikačné upozornenia a chybové hlásenia – väčšinou informačné hlásenia dôležité pre údržbu a vývoj systému na zistenie kde, ako a prečo aplikácia zlyhala pri plnení požiadavku užívateľa,
- systémové upozornenia a chybové hlásenia – podobné ako u aplikačných.

Všetky ukladané logy by mali obsahovať identifikačné, časové a lokalizačné údaje, aby bolo presne jasné kto, kedy a v ktorej časti alebo vrstve aplikácie danú akciu vykonal. Veľmi dôležité je, aby žiadne takéto záznamy a súbory s logmi neboli dostupné alebo viditeľné pre užívateľa alebo potenciálneho útočníka.

Užitočným doplnkom by mohlo byť, keby logovanie a monitorovanie bolo automatizovaným procesom, ktorý by bol sám schopný odhaliť a okamžite upozorniť administrátora na nezvyčajnú alebo podozrivú aktivitu v aplikácii.

5.6 Dvojfaktorové overenie

Momentálne aplikácia používa štandardné prihlasovanie pomocou prihlasovacieho mena a hesla. V dnešnej dobe však toto jednoduché prihlasovanie z viacero bezpečnostných dôvodov nestačí.

Veľkým bezpečnostným trendom je prechod na dvojfaktorové overovanie užívateľa pri prihlasovaní, ktoré zabezpečí, že aj keď sa útočníkovi podarí zistiť alebo prelomiť heslo, nepodarí sa mu do účtu dostať, pretože by musel mať alebo poznať ďalší faktor overenia.

V informačnej bezpečnosti existujú tri faktory overenia:

1. faktor **znalosti** – niečo, čo užívateľ pozná, ako napríklad klasické heslo,
2. faktor **vlastníctva** – niečo, čo užívateľ má, napríklad čipová karta, USB kľúč, alebo mobilný telefón (smartfón),
3. faktor **charakteristiky** – niečo, čo užívateľ je, čiže nejaká jeho unikátna vlastnosť, ako napríklad najčastejšie odtlačok prsta, rozpoznanie tváre, hlasu alebo podpis.

Najmä prvé dva faktory sú jednotlivo celkom ľahko napadnuteľné. Ich kombináciou sú však rádovo oveľa bezpečnejšie, pretože je veľmi ťažké jednému užívateľovi naraz ukradnúť heslo aj telefón. Samozrejme, že faktor charakteristiky je asi najbezpečnejší, pretože ukradnúť užívateľovi odtlačok prsta, tvár alebo hlas, prakticky jeho identitu, je omnoho ťažšie, no overovanie pomocou týchto znakov je v praxi takisto náročné a väčšinou zatiaľ i zdĺhavé. Výnimkou môže byť spomenutý odtlačok prsta, ktorý sa už dlho používa na autentizáciu v rôznych odvetviach, najnovšie sa vyskytuje na overenie identity i v smartfónoch. Zatiaľ však nebolo vyvinuté dostatočne funkčné a otestované riešenie pre účely dvojfaktorového overovania pomocou tohto biometrického znaku pri prihlasovaní užívateľa. [35]

Preto pre kombináciu s prvým faktorom najefektívnejším druhým faktorom pre overenie stále zostáva faktor vlastníctva, čiže nejaká vec alebo zariadenie, ktorú musí mať užívateľ pri prihlasovaní u seba. A najčastejším zariadením, ktoré má väčšina ľudí vždy poruke je mobilný telefón.

Overenie pomocou mobilného telefónu spočíva v tom, že generuje jednorazové, väčšinou 6-miestne kódy, ktoré sú vyžadované danou aplikáciou po zadaní prihlasovacieho mena a hesla. Najčastejšie sa tieto kódy generujú buď SMS správou poslanou do telefónu užívateľa, alebo pomocou mobilnej aplikácie Google Authenticator, nainštalovanej v smartfóne užívateľa.

Veľa ľudí tento typ overenia berie ako veľkú novinku a je pre nich veľakrát ťažké pochopiť princíp alebo zmysel jeho použitia. Neuvedomujú si to, ale stretávajú sa s ním však už veľmi dlho a celkom často pri bežnej veci ako je výber peňazí z bankomatu. K tomu potrebujú vložiť niečo, čo majú – platobnú kartu a zadať niečo, čo poznajú – PIN kód. Jedno bez druhého je im, alebo útočníkovi k ničomu. Inak sa s týmto typom overenia môžu internetoví užívatelia stretnúť väčšinou pri vstupe do emailových účtov alebo internetového bankovníctva.

Cieľom je teda implementovať dvojfaktorové overenie a pridať tak ďalšiu vrstvu zabezpečenia pri prihlasovaní užívateľa do vybraného informačného systému.

V tejto kapitole boli navrhnuté nové bezpečnostné opatrenia, ktoré by mali pomôcť maximálne zabezpečiť vybraný informačný systém a najmä všetky dáta, ktoré spracováva a uchováva.

6 IMPLEMENTÁCIA NAVRHNUTÝCH A DALŠÍCH VRSTIEV ZABEZPEČENIA IS

V tejto kapitole sú implementované navrhnuté opatrenia k zlepšeniu zabezpečenia vybraného informačného systému. U každého typu zabezpečenia sú popísané jednotlivé spôsoby a postupy, prípadne komplikácie pri implementácii.

6.1 Nastavenie šifrovania citlivých dát

Šifrovanie citlivých dát je veľmi zdĺhavý a zložitý proces, ktorý vyžaduje veľa nastavovania a testovania, či šifrovanie a spätné dešifrovanie nemá nejakým spôsobom negatívny vplyv na integritu a taktiež dostupnosť predmetných dát.

Na šifrovanie dát sa môže použiť viacero spôsobov. Jednou z tých menej náročných, no tiež aj menej efektívnych možností, je využiť šifrovacie funkcie danej databázy, v ktorej sú dáta uložené. Tu však nastáva problém, že pri načítaní dát, ich databáza samozrejme automaticky i dešifruje, čiže v prípade použitia útoku SQL Injection, sa útočník dostane k nezašifrovaným dátam. Je to však stále lepšie riešenie, ako žiadne šifrovanie.

Pre elimináciu tohto rizika, bolo teda vybrané asymetrické šifrovanie pomocou verejného a súkromného kľúča na strane aplikácie, kde údaje v databáze budú zašifrované pomocou verejného kľúča a iba backendové aplikácie budú mať povolené tieto dáta dešifrovať pomocou súkromného kľúča.

Vzhľadom na náročnosť celého procesu, je toto zabezpečenie stále vo fáze vývoja a keďže ani z pohľadu nariadenia GDPR ako sa uvádza v článku 32 nariedenia o Zabezpečení spracovania: „*S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování...*“ [36], nemusia byť dáta nevyhnutne šifrované, s uvedením do ostrej prevádzky sa zbytočne neponáhľa a celý proces je zameraný na kvalitu a spoľahlivosť tohto zabezpečenia.

Týmto spôsobom sú dáta zabezpečené „v pokoji“, čo znamená, že i po prípadnom získaní týchto dát z nejakého disku apod., ich útočník nedokáže dešifrovať.

Ďalším implementovaným opatrením, bola inštalácia SSL/TLS certifikátu, čo zabezpečí, že dáta budú pri prenose šifrované a zabezpečené proti odpočúvaniu sieťovej komunikácie.

6.2 Zabezpečenie zraniteľných komponentov

Veľa prídavných knižníc ponúka pre integráciu do systému viacero možností:

- Stiahnuť a ručne nainštalovať vybranú verziu na server.
- Pomocou odkazu na domovskú stránku knižnice s vždy najaktuálnejšou verziou.
- Pomocou odkazu na domovskú stránku knižnice s číslom vybranej verzie.
- Pomocou odkazu na Google API.

Vybraný framework, na ktorom beží predmetný informačný systém používal viacero online riešení integrácie rôznych prídavných modulov, väčšinou pomocou druhej, prípadne tretej možnosti. Veľa programovacích tutoriálov, návodov alebo kníh tieto možnosti vrelo odporúča. Z prieskumov a diskusných fór však vychádza, že najlepšie je mať nainštalovanú offline verziu na serveri v adresári a radšej manuálne sledovať a kontrolovať aktuálnosť danej používanej verzie, pretože:

- najnovšia verzia komponentu nemusí byť kompatibilná so starou, čiže niektoré aplikáciou používané funkcie môžu byť premenované alebo inak upravené, ba dokonca z rôznych dôvodov úplne odstránené, čo môže v aplikácii znamenať totálne zrútenie niektorých, možno aj hlavných funkcií. Z jedného pohľadu taktiež veľkým negatívom je, že používaním tohto typu načítania knižnice v produkčnej verzii aplikácie, sa zmeny verzie prejavia okamžite a môže trvať veľmi dlho než sa na túto zmenu príde a v najhoršom prípade môže trvať ešte dlhšie, než sa zistí, že používaním tejto novej verzie prestali fungovať niektoré funkcie, ktoré môžu zabezpečovať nejaké dôležité procesy alebo iné operácie napríklad pri ukladaní rôznych záznamov. Takáto chyba by mohla znamenať úplné narušenie integrity ukladaných dát.
- ani najnovšia verzia nie je zárukou bezchybného fungovania a hlavne zabezpečenia. Môžu sa v nej vyskytnúť tzv. zero-day zraniteľnosti, na ktoré sa užívateľmi alebo vývojármi príde až časom a najmä väčšinou neskôr než nejakými hackermi.

Mali by sa teda používať len ošetrené, komunitou otestované a časom overené verzie všetkých komponentov.

Keďže vo vybranej aplikácii neboli zistené žiadne problémy v kompatibilite súčasných a najnovších verzií používaných prídavných nástrojov, rozšírení a knižníc, boli všetky aktualizované na najnovšie verzie. Takisto bol vypracovaný plán na monitorovanie bezpečnosti komponentov a zisťovanie ich aktuálnych verzií, v ktorom budú pravidelne kontrolované

nové aktualizácie všetkých používaných komponentov, ktoré budú pred nasadením do produkčnej verzie najprv riadne preskúmané a otestované z pohľadu bezpečnosti i kompatibility s predmetným informačným systémom.

6.3 Odstránenie akéhokoľvek presmerovania

Aplikácia má implementované vlastné riešenie smerovania medzi stránkami v rámci systému, ktoré priame presmerovania pomocou skutočných cieľových adries v parametroch v URL nepodporuje. Systém bol i napriek tomu preskúmaný podľa doporučeného návrhu zabezpečenia a bolo zistených niekoľko prípadov použitia presmerovania. Väčšina odkazovala na externé stránky, ktoré boli nekompromisne odstránené a iba v niektorých prípadoch bolo použité alternatívne riešenie pre zachovanie funkcionality.

6.4 Zabezpečenie konfigurácie

Aktuálny stav zabezpečenia proti týmto zraniteľnostiam bol celkom dobrý, boli však nájdené nejaké nedostatky vymenované v návrhu zabezpečenia. I keď sa na začiatku vývoja premazali potenciálne nepotrebné časti kódu alebo stránky, neustálym vývojom aplikácie vždy postupne pribudnú ďalšie, ktorých odstránenie sa v priebehu vývoja z dôvodu časovej tiesne väčšinou odkladá, až sa na ne nakoniec zabudne, takže v rámci zabezpečenia sa teraz všetky zase odstránili.

Okrem týchto relatívne neškodných nedostatkov však boli počas analýzy objavené aj vážnejšie skutočnosti, kde jeden z nedávno pridaných komponentov dovoľoval vypísať štruktúru adresárov, čo je inak od začiatku zakázané. Keďže z danej knižnice sa používa viacero funkcií, bola iba táto funkcionalita natvrdo odstránená.

Takisto sa v malej miere vyskytli i nepoužívané prednastavené účty a rozhrania niektorých doplnkov. Tie boli podľa potreby buď upravené, alebo odstránené.

6.5 Nastavenie logovania a monitorovania dôležitých procesov

Podľa návrhu bolo implementované logovanie a monitorovanie všetkých navrhnutých procesov ako napríklad:

- vytvorenie a registrácia užívateľa,
- úspešné / neúspešné prihlásenie užívateľa do systému,
- pridanie, úprava alebo odstránenie rôznych záznamov klienta alebo užívateľa,

- zlyhania alebo pokusy o prelomenie kontroly prístupu,
- nezvyčajná / podozrivá / nebezpečná aktivita v aplikácii,
- aplikačné a systémové upozornenia a chybové hlásenia.

V aplikácii taktiež už boli nastavené automatizované procesy a postupy na zaznamenávanie, monitorovanie, upozorňovanie a reagovanie na niektoré podozrivé aktivity spojené s útokmi typu SQL Injection, XSS atď. Podobné procesy boli vytvorené aj pre ostatné a ďalšie hrozby a zraniteľnosti z uvedeného katalógu hrozieb.

Nakoniec boli vypracované postupy a reakcie na rôzne „katastrofické“ scenáre, ktoré by mohli informačný systém postihnúť.

6.6 Dvojfaktorové overenie

Z uvedených možností v návrhu zabezpečenia bola vybraná kombinácia prvých dvoch faktorov overenia, tzn. faktory znalosti a vlastníctva – v prvom kroku použitím štandardného prihlasovania pomocou prihlasovacieho mena a hesla, doplneným o zadanie jednorazového číselného kódu z mobilného telefónu s využitím aplikácie Google Authenticator, a to z dvoch hlavných dôvodov:

- overovanie pomocou SMS správy nie je veľmi bezpečné, pretože textové správy posielané na mobilný telefón nie sú šifrované a môžu byť zachytené útočníkom. Ten potom môže odoslaný kód ukradnúť a použiť ho na prihlásenie namiesto užívateľa.
- SMS správy musia byť zasielané pomocou externej služby, väčšinou nejakej telefónnej spoločnosti, čo môže byť dosť nákladné.

Všetci pracovníci spoločnosti i jej zmluvných partnerov budú musieť k vstupu do informačného systému používať dvojfaktorové overenie pomocou aplikácie Google Authenticator a sú na to patrične technicky vybavení. Používajú smartfóny a tablety s operačným systémom Android alebo iOS, pre ktoré je aplikácia dostupná na stiahnutie v ich obchode s aplikáciami.

Bohužiaľ sa však variantu overenia pomocou SMS celkom vyhnúť nedá a bude sa v budúcnosti musieť používať i táto možnosť, pretože nie každý klient vybranej spoločnosti má smartfón alebo tablet a nemohol by tak využívať zabezpečené prihlasovanie pomocou dvojfaktorového overenia. A aj keď tento spôsob nie je najbezpečnejší, obecne však

platí, že je to stále lepšie a bezpečnejšie, než obyčajné prihlasovanie pomocou mena a hesla.

6.6.1 Implementácia dvojfaktorového overenia

Z technického hľadiska bola podľa rôznych návodov a tutoriálov do systému implementovaná knižnica, obsahujúca rôzne funkcie, ktoré zabezpečujú procesy generovania a overovania potrebných kľúčov a kódov. K nej bolo potrebné vytvoriť ďalšie ovládače a funkcie, ktoré tejto knižnici určujú kedy, kde a ako sa majú kódy vytvoriť alebo použiť.

V samotnej implementácii sa nevyskytli väčšie komplikácie. Knižnica umožňuje viacero nastavení a niektoré funkcie sa museli optimalizovať pre potreby informačného systému. Menšie problémy však nastali so zakomponovaním do súčasného procesu registrácie užívateľov, ktorý musel byť upravený tak, aby si mohol nastaviť dvojfaktorové overenie a spárovať svoj účet v systéme s mobilnou aplikáciou. Celkom to narušilo nastavené postupy overení, ukladaní dát, predávania zadaných parametrov alebo presmerovaní na patričné stránky po úspešnej, či neúspešnej akcii.

Medzitým systém ešte musí rozlišovať užívateľov podľa toho, či sa jedná o zamestnanca alebo klienta spoločnosti. V rámci bezpečnostnej politiky spoločnosti, musí každý pracovník používať dvojfaktorové overenie prihlásenia do systému pomocou mobilnej aplikácie Google Authenticator. Od klientov toto však nemožno vyžadovať, pretože zatiaľ nebola uvedená do prevádzky alternatíva s posielaním SMS správ pre tých, ktorí nepoužívajú smartfón. To znamená, že nový zamestnanec, ktorý sa registruje do systému a po novom aj súčasní zamestnanci, ktorí už účet vytvorený majú, sa do systému neprihlásia, pokiaľ si dvojfaktorové overenie nenastavia. Klienti pri registrácii dostanú na výber, či si chcú dvojfaktorové overenie nastaviť. Keď nie, budú sa naďalej prihlasovať len klasickým spôsobom s tým, že ak si to rozmyslia, môžu si ho dodatočne aktivovať v nastaveniach svojho účtu.

Základom pre správne fungovanie dvojfaktorového overenia je spárovať danú aplikáciu s užívateľským účtom informačného systému. To je riešené pomocou tajného kľúča, ktorý sa skladá z šestnástich náhodne vybraných znakov vopred definovanej tabuľky. Tento kľúč sa po úspešnej registrácii automaticky priradí danému užívateľovi a uloží do databázy. Užívateľ tento kľúč nemusí nikam zadávať a prakticky ho bežný užívateľ ani nikdy neuvidí. Celý proces prebieha na pozadí a je dôležité, aby kľúč zostal v tajnosti, pretože inak by potenciálny útočník mohol pomocou tohto kľúča spárovať aplikáciu na svojom telefóne

s účtom užívateľa, no pre úspešné prihlásenie a odcudzenie účtu by však potreboval vedieť ešte heslo užívateľa. Preto bude tajný kľúč pred uložením do databázy ešte zašifrovaný podobne ako ostatné citlivé údaje.

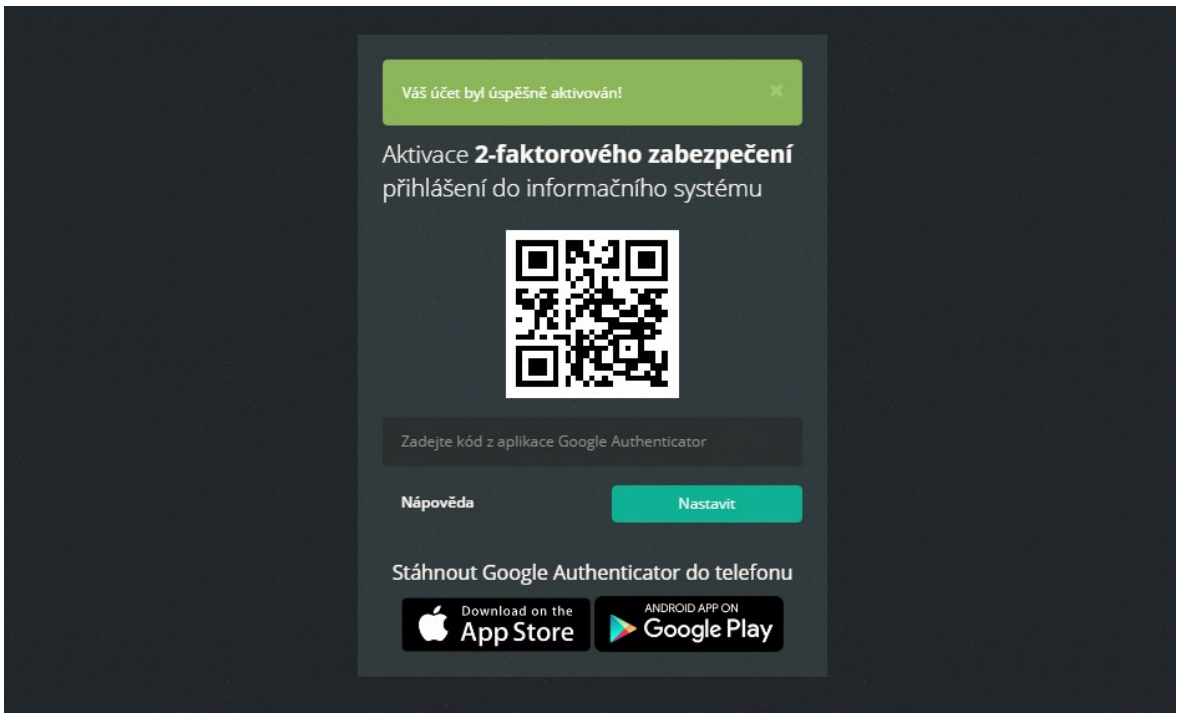
Kľúč je neoddeliteľnou súčasťou procesu, pretože na jeho základe sa generujú šesťmiestne overovacie kódy, čím sa jednoznačne identifikuje užívateľ, pre ktorého je kód určený.

Proces generovania jednorazových kódov je celkom zložitý algoritmus, ktorý obsahuje viacero krokov kódovania, šifrovania apod. Tento spôsob generovania je štandardizovaný a popisujú ho internetové štandardy RFC 4226 a RFC 6238. Tie taktiež popisujú, že overovacie kódy okrem tajného kľúča sú generované aj na základe aktuálneho časového údaju, ktorý je jedným z šifrovacích parametrov pri získavaní kódu. V mobilnej aplikácii sú kódy generované každých 30 sekúnd, no v informačnom systéme je hlavne z dôvodu časovej synchronizácie servera a aplikácie nastavená platnosť jedného kódu až na jednu minútu.

Celý proces spočíva v tom, že informačný systém a mobilná aplikácia fungujú nezávisle na sebe a používajú pre vytváranie a overenie kódov rovnaký algoritmus. Výhodou tohto riešenia je, že aplikácia nevyžaduje pripojenie na internet, čiže obe strany okrem vopred dohodnutého a uloženého tajného kľúča nie sú žiadnym iným spôsobom permanentne prepojené, čo eliminuje riziko sieťového odpočúvania pri komunikácii alebo sieťovom prenose nejakých dát.

6.6.2 Použitie overenia v praxi

Z pohľadu užívateľa celý proces prebieha tak, že po úspešnej registrácii a aktivácii účtu je aplikáciou vyzvaný, aby si nastavil dvojfaktorové overenie, ako je ukázané na obrázku (Obr. 4).

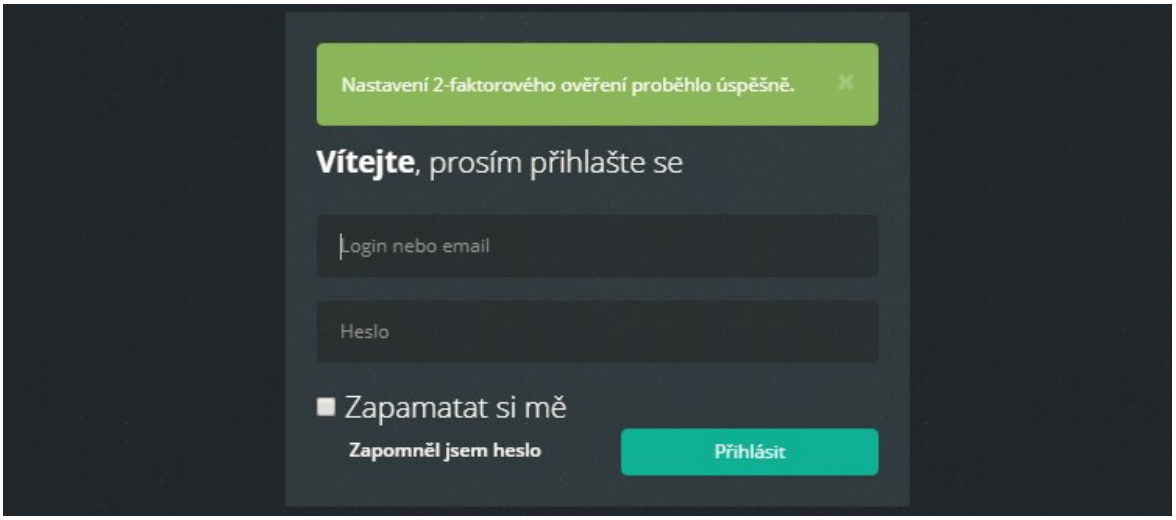


Obr. 4. Nastavenie dvojfaktorového overenia. [Zdroj: vlastný]

V tomto kroku je tiež súčasne vytvorený tajný kľúč a spolu s ďalšími parametrami sú súčasťou QR kódu. Nachádza sa tam aj názov aplikácie a emailová adresa. Sú to len informačné údaje vyžadované aplikáciou Google Authenticator, ktoré sa zobrazujú v zozname pri generovaní kódov, aby užívateľ vedel, ku ktorému systému kód patrí a pomocou akého emailového účtu má aplikáciu spárovanú, pretože táto aplikácia umožňuje generovanie kódov pre účty rôznych systémov a aplikácii, nielen pre služby Google.

Aplikácia Google Authenticator pre spárovanie umožňuje potrebné parametre zadať ručne (v prípade, že užívateľ pozná tajný kľúč) alebo ich načítať z QR kódu pomocou čítačky, ktorú v prípade jej absencie v smartfóne užívateľovi ponúkne na stiahnutie. Aby bol však pre užívateľa celý proces čo najviac zjednodušený a bezpečnejší, bola vybraná metóda pomocou načítania QR kódu, pretože užívateľ nemusí prepisovať žiadne kódy alebo parametre, čím sa odstráni riziko zadania chybných údajov a takisto sa zabráni odcudzeniu tajného kľúča treťou osobou.

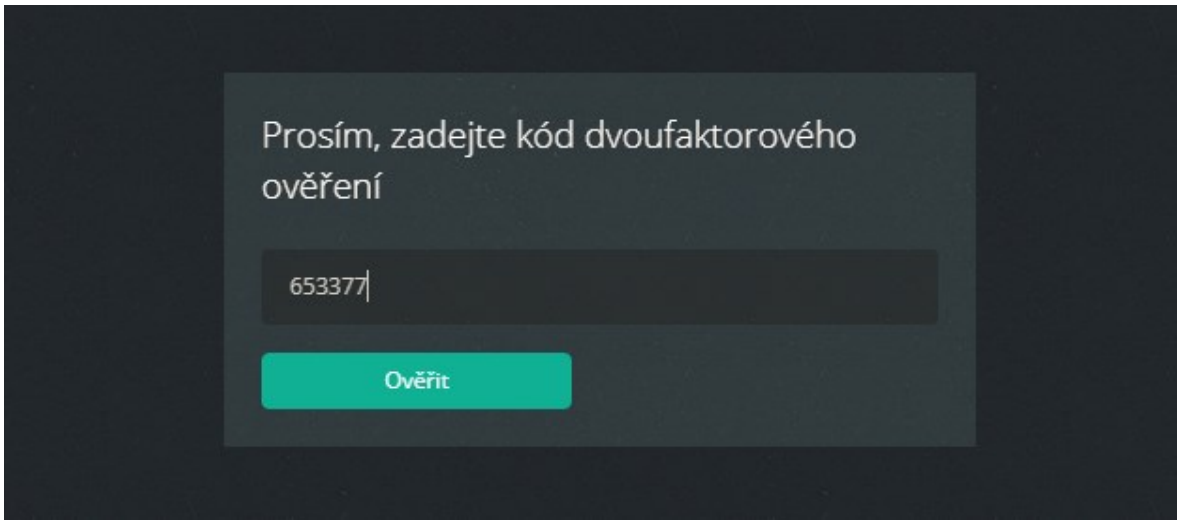
Daný QR kód s parametrami sa teda naskenuje pomocou aplikácie Google Authenticator. Tá ich automaticky načíta, uloží a na ich základe začne okamžite generovať overovacie kódy. Pre potvrdenie spárovania užívateľ zadá do príslušného políčka vygenerovaný overovací kód a pokiaľ sa kódy zhodujú, užívateľ je presmerovaný na prihlasovaciu stránku a môže sa prihlásiť do systému (Obr. 5).



Obr. 5. Zadanie kódu dvojfaktorového overenia. [Zdroj: vlastný]

Po úspešnom prihlásení sa opäť objaví okno na zadanie overovacieho kódu ako je vidieť na obrázku (Obr. 6). Pomocou aplikácie zistí nový kód a vloží ho do tohto formulára. Po overení správnosti kódu je užívateľ úspešne prihlásený a presmerovaný na domovskú stránku informačného systému.

Vývojový diagram celého procesu od registrácie až po prihlásenie užívateľa s využitím dvojfaktorového overenia je súčasťou prílohy č. 2.



Obr. 6. Zadanie kódu dvojfaktorového overenia. [Zdroj: vlastný]

6.6.3 Ďalšie možnosti využitia aplikácie Google Authenticator

Využitie tejto aplikácie nie je nijak obmedzené a nemusí sa použiť len na jej hlavný účel overenia užívateľa pri prihlásení. Po spárovaní účtu užívateľa s aplikáciou sa môže kedykoľvek vyžadovať zadanie šesťmiestneho kódu, ktorý môže byť použitý napríklad na účel overenia identity užívateľa k prístupu do chránenej sekcie systému, alebo na potvrdenie nejakej dôležitej alebo chúlostivej akcie. Podobne to často býva i v internetovom bankovníctve, kde napríklad pri prevode peňazí sa na potvrdenie transakcie vyžaduje u väčšiny bánk zadanie overovacieho kódu prijatom pomocou SMS správy.

Cieľom poslednej kapitoly diplomovej práce bolo popísanie postupu a samotná implementácia navrhnutých bezpečnostných prvkov do vybraného webového informačného systému s dôrazom na vylepšené zabezpečenie procesu prihlásenia užívateľa pomocou dvojfaktorového overenia s využitím mobilnej aplikácie Google Authenticator.

6.7 Zhrnutie praktickej časti

V praktickej časti bol na začiatku čitateľ stručne zoznámený s predmetným webovým informačným systémom a spoločnosťou, pre ktorú je systém vyvíjaný. Po zhodnotení stavu zabezpečenia bola následne vykonaná analýza rizík vybraných hrozieb, na základe ktorej bolo v ďalšej kapitole navrhnuté zabezpečenie informačného systému. V poslednej kapitole praktickej časti boli implementované všetky navrhnuté bezpečnostné opatrenia.

ZÁVER

Cieľom diplomovej práce bol návrh a implementácia zabezpečenia a dvojfaktorového overenia pri prihlasovaní užívateľa do webového informačného systému spoločnosti Housing for Life, SE. Práca obsahuje šesť kapitol a bola rozdelená na teoretickú a praktickú časť, kde obidve časti obsahujú tri kapitoly.

V prvej kapitole boli definované základné pojmy v oblasti informačných systémov. Bolo definované čo je informácia, informačný systém, informačná bezpečnosť a v závere kapitoly bol vysvetlený rozdiel medzi desktopovým a webovým informačným systémom

Druhá kapitola pojednáva o zákonných požiadavkách a povinnostiach vo vzťahu k informačnej bezpečnosti, kde boli priblížené požiadavky prichádzajúceho Nariadenia Európskej únie na ochranu osobných údajov (GDPR) a Zákon o kybernetickej bezpečnosti.

V poslednej kapitole teoretickej časti bola všeobecne popísaná bezpečnosť a bezpečnostné hrozby pre informačný systém a medzinárodný projekt OWASP, na základe ktorého bol stanovený obecný katalóg hrozieb pre webový informačný systém. Ten obsahuje popis jednotlivých hrozieb, možnosti a spôsoby prevedenia útokov, ich pôvodcov, slabiny, ktoré využívajú a technické, či obchodné dopady na aplikáciu.

Na začiatku praktickej časti bol stručne predstavený informačný systém a spoločnosť, pre ktorú je systém vyvíjaný. Nasledoval prehľad a stanovenie miery rizík hrozieb z definovaného katalógu. Určila sa ich celková závažnosť, na základe ktorej boli vybrané bezpečnostné hrozby pre analýzu rizík. Tá pozostávala z viacerých častí. Pomocou identifikácie rizík a odhadu pravdepodobnosti a dopadu na aplikáciu, či organizáciu, sa určili celkové miery rizík jednotlivých hrozieb, podľa ktorých boli navrhnuté nové bezpečnostné opatrenia pre vybraný informačný systém, čo bolo predmetom piatej kapitoly.

V poslednej kapitole diplomovej práce bola realizovaná samotná implementácia všetkých navrhnutých bezpečnostných opatrení. Zvlášť venovaná pozornosť bola implementácii dvojfaktorového overenia s využitím mobilnej aplikácie Google Authenticator, čo pridalo ďalšiu vrstvu zabezpečenia v procese prihlásenia užívateľa do vybraného informačného systému, ktorá ochráni užívateľa pred odcudzením a následným zneužitím jeho účtu, a v konečnom dôsledku taktiež pomôže ochrániť všetky údaje zamestnancov, partnerov a najmä klientov spoločnosti, čo v spojení s ostatnými vrstvami zabezpečenia bolo cieľom a je hlavným prínosom tejto diplomovej práce.

ZOZNAM POUŽITEJ LITERATÚRY

[1] JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978-80-7454-312-8.

[2] KUČERÁK, Dušan. Informačný systém. *IPA Slovakia: More Than Expected* [online]. Žilina, 2017 [cit. 2018-05-15]. Dostupné z: https://www.ipaslovakia.sk/sk/ipa-slovnik/informacny-system

[3] Informační systém. *IT Slovník.cz: Počítačový slovník* [online]. 2018 [cit. 2018-05-16]. Dostupné z: https://it-slovnik.cz/pojem/informacni-system

[4] BARTONĚK, Dalibor a Robert JURČA. *Informační systémy*. Kunovice: Evropský polytechnický institut, 2014. ISBN 978-80-7314-322-4.

[5] ČERMÁK, Miroslav. Informační bezpečnost: Životní cyklus informace. *CleverAndSmart* [online]. 2012, 23.5.2010, 14.10.2012 [cit. 2018-05-16]. Dostupné z: https://www.cleverandsmart.cz/informacni-bezpecnost-zivotni-cyklus-informace/

[6] Desktopové a webové aplikace: Rozdíl. *Webnode* [online]. 2012. Dostupné z: https://sluzby-internet.webnode.cz/web/desktopove-a-webove-aplikace-rozdil/

[7] ČERMÁK, Miroslav. Jak se snadno vypořádat s požadavky GDPR. *CleverAndSmart* [online]. 2017, 28.9.2017, 10.3.2018 [cit. 2018-05-16]. Dostupné z: https://www.cleverandsmart.cz/jak-se-snadno-vyporadat-s-pozadavky-gdpr/

[8] GDPR. *IDS Advisory* [online]. 2018. Dostupné z: http://www.idsa.cz/cs/gdpr

[9] PECHANEC, Igor. Nařízení GDPR z pohledu IT. *Igorovo* [online]. 2017, 14.8.2017. Dostupné z: https://www.pechanec.cz/Blog/ViewPost.aspx?pageid=4&ItemID=124&mid=12

[10] Privacy by design by default: Kde končí filozofia a začína prax?. *Trend.sk* [online]. 2017, 23.3.2017. Dostupné z: https://blog.etrend.sk/martin-sasinek/privacy-by-design-by-default-kde-konci-filozofia-a-zacina-prax.html

[11] Anonymizace a pseudonymizace jsou dvě rozdílná slova. *GDPR: Obecné nařízení o ochraně osobních údajů prakticky* [online]. 2017, 20.9.2017. Dostupné z: https://www.gdpr.cz/blog/anonymizace-a-pseudonymizace-jsou-dve-rozdilna-slova/

[12] KOHÚTOVÁ, Zuzana. Anonymizace, pseudonymizace a šifrování osobních údajů jako bezpečnostní opatření dle GDPR: Anonymisation. Pseudonymization. Encryption. *FlyEye* [online]. 2017, 13.9.2017. Dostupné z: https://www.fly-eye.cz/blog-detail-1.html

[13] PECHANEC, Igor. Nařízení GDPR z pohledu IT: Závěrečný díl trilogie o nařízení GDPR pro IT. *Igorovo* [online]. 2017, 31.8.2017. Dostupné z: https://www.pechanec.cz/Blog/ViewPost.aspx?pageid=4&ItemID=127&mid=12

[14] Co přináší zákon o kybernetické bezpečnosti. *T-SOFT: This is IT!* [online]. 2015, 13.1.2015. Dostupné z: http://www.tsoft.cz/zakon-o-kyberneticke-bezpecnosti/

[15] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti. *Zákony pro lidi* [online]. 2018. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181/zneni-20180307

[16] Kybernetická bezpečnost: O čem je nový zákon?. *Root.cz* [online]. 2015, 16.1.2015. Dostupné z: https://www.root.cz/clanky/kyberneticka-bezpecnost-o-cem-je-novy-zakon/

[17] Vyhláška č. 316/2014 Sb. o kybernetické bezpečnosti. *Zákony pro lidi* [online]. 2018. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-316

[18] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[19] DOBDA, Luboš. *Ochrana dat v informačních systémech*. Praha: Grada, 1998. ISBN 80-716-9479-7.

[20] ČERMÁK, Miroslav. Spam, scam, hoax nebo phishing?. *CleverAndSmart* [online]. 2015, 25.5.2016 [cit. 2018-05-16]. Dostupné z: https://www.cleverandsmart.cz/spam-scam-hoax-nebo-phishing/

[21] ČERMÁK, Miroslav. Spear phishing je cílený phishing, kterému se lze jen těžko bránit. *CleverAndSmart*[online]. 2012, 26.9.2012 [cit. 2018-05-16]. Dostupné z: https://www.cleverandsmart.cz/spear-phishing-je-cileny-phishing-kteremu-se-lze-jen-tezko-branit/

[22] ČERMÁK, Miroslav. Základní bezpečnostní pravidla pro zaměstnance. *CleverAndSmart* [online]. 2012, 17.12.2012 [cit. 2018-05-16]. Dostupné z: https://www.cleverandsmart.cz/zakladni-bezpecnostni-pravidla-pro-zamestnance/

[23] Principle of least privilege (POLP). *TechTarget: SearchSecurity* [online]. 2017 [cit. 2018-05-17]. Dostupné z: https://searchsecurity.techtarget.com/definition/principle-of-least-privilege-POLP

[24] About The Open Web Application Security Project. *OWASP* [online]. 2018, 30.1.2018 [cit. 2018-05-17]. Dostupné z: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

[25] OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks. *OWASP* [online]. 2017 [cit. 2018-05-17]. Dostupné z: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

[26] OWASP Top 10 - 2013: The Ten Most Critical Web Application Security Risks. *OWASP* [online]. 2013 [cit. 2018-05-17]. Dostupné z: https://www.owasp.org/index.php/Top_10_2013

[27] Skener webu. *CZ.NIC* [online]. 2018 [cit. 2018-05-17]. Dostupné z: https://www.skenerwebu.cz/

[28] PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) č. 1179/2011. *EUR-Lex: Access to European Union law EUR-Lex Access to European Union law* [online]. 2011, 18.11.2011 [cit. 2018-05-17]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32011R1179

[29] OWASP: Deserialization Cheat Sheet. *OWASP* [online]. 2018, 13.5.2018 [cit. 2018-05-17]. Dostupné z: https://www.owasp.org/index.php/Deserialization_Cheat_Sheet

[30] OWASP Top 10 - 2013: A8-Cross-Site Request Forgery (CSRF). *OWASP* [online]. 2013 [cit. 2018-05-17]. Dostupné z: https://www.owasp.org/index.php/Top_10_2013-A8-Cross-Site_Request_Forgery_(CSRF)

[31] OWASP Top 10 - 2013: A10-Unvalidated Redirects and Forwards. *OWASP* [online]. 2013 [cit. 2018-05-17]. Dostupné z: https://www.owasp.org/index.php/Top_10_2013-A10-Unvalidated_Redirects_and_Forwards

[32] STAUDEK, Jan a Petr HANÁČEK. *Bezpečnost informačních systémů*. 1. vyd. Praha: Úřad pro státní informační systém, 2000. 127 s. ISBN 80-238-5400-3.

[33] OWASP: Risk Rating Methodology. *OWASP* [online]. 2016 [cit. 2018-05-17]. Dostupné z: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[34] PODOLINSKÝ, Ján. CAPTCHA: Čo to je a ako sa s ňou vysporiadať. *BlindRevue: IT technológie pre osoby so zrakovým postihnutím* [online]. 2016, 15.11.2016 [cit. 2018-05-17]. Dostupné z: https://blindrevue.sk/captcha-pokrivene-obrazky-pristupne-ci-nepristupne/

[35] VALÁŠEK, Michal. Seznam.cz je konečně bezpečnější: Dvoufaktorové ověření zavedl pozdě, ale zato špatně. *Hospodářské noviny* [online]. 2018, 2.5.2018 [cit. 2018-05-17]. Dostupné z: https://tech.ihned.cz/internet/c1-66126470-seznam-cz-je-konecne-bezpecnejsi-dvoufaktorove-overeni-zavedl-pozde-ale-zato-spatne

[36] Článek 32 EU obecné nařízení o ochraně osobních údajů: "Zabezpečení zpracování". *PrivazyPlan: Gets your data protection on course* [online]. 2017, 16.12.2017 [cit. 2018-05-17]. Dostupné z: http://www.privacy-regulation.eu/cs/32.htm

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

AJAX	Asynchronous JavaScript And XML
API	Application Programming Interface
apod.	a podobne
atď.	a tak ďalej
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CSRF	Cross-Site Request Forgery
ČR	Česká republika
DOM	Document Object Model
EÚ	Európska únia
GDPR	General Data Protection Regulation
HFL	Housing For Life
IS	Informačný systém
ISO	International Organization for Standardization
IT	Informačné technológie
JSON	JavaScript Object Notation
napr.	napríklad
OCR	Optical Character Recognition
OWASP	Open Web Application Security Project
PDO	PHP Document Object
PDF	Portable Document Format
PHP	Hypertext Preprocessor
QR	Quick Response
RFC	Request For Comments
RTF	Rich Text Format

SQL	Structured Query Language
SE	Societas Europaea
SMS	Short Message Service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
ÚOOÚ	Úrad pre ochranu osobných údajov
vs.	versus
WWW	World Wide Web
XML	eXtensible Markup Language
XSS	Cross-Site Scripting
Zb.	Zbierka

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM GRAFOV

ZOZNAM PRÍLOH

PRÍLOHA P I: ANALÝZA RIZÍK

Hrozba	Pôvodcovia hrozieb				Zraniteľnosti					
	Zručnosti	Motivácia	Možnosti	Veľkosť	Zistiteľnosť	Zneužiteľnosť	Rozšírenie	Detekcia zneužitia	Priemer	Pravdepodobnosť
Injektovanie	6	9	7	6	7	7	4	1	**5,875**	Stredná
Autentizácia	5	4	9	9	3	7	4	3	**5,5**	Stredná
Expozícia citlivých dát	3	6	4	6	3	3	7	9	**5,125**	Stredná
Prelomenie kontroly prístupu	3	5	7	9	3	3	4	1	**4,375**	Stredná
Nezabezpečená konfigurácia	5	1	7	9	7	7	7	9	**6,5**	Veľká
XSS	5	7	7	6	7	7	7	1	**5,875**	Stredná
Zraniteľné komponenty	3	4	4	4	3	3	7	9	**4,625**	Stredná
Logovanie a monitorovanie	4	2	7	9	1	3	7	9	**5,25**	Stredná
CSRF	3	3	7	6	7	3	4	1	**4,25**	Stredná
Presmerovanie a predávanie	3	2	7	9	7	3	1	9	**5,125**	Stredná

Hrozba	Technické dopady						Obchodné dopady					
	Strata dôvernosti	Strata integrity	Strata dostupnosti	Strata zodpovednosti	Priemer	Dopad	Finančné škody	Poškode-nie dobré-ho mena	Nedodržanie zásad	Osobné údaje	Priemer	Dopad
Injektovanie	9	9	9	1	**7**	Vysoký	7	9	7	7	**7,5**	Vysoký
Autentizácia	9	9	9	1	**7**	Vysoký	7	9	7	7	**7,5**	Vysoký
Expozícia citlivých dát	7	5	1	7	**5**	Stredný	7	9	7	7	**7,5**	Vysoký
Prelomenie kontroly prístupu	7	7	7	1	**5,5**	Stredný	7	5	5	5	**5,5**	Stredný
Nezabezpečená konfigurácia	6	5	1	1	**3,25**	Stredný	3	3	5	5	**4**	Stredný
XSS	2	7	5	1	**3,75**	Stredný	7	5	5	5	**5,5**	Stredný
Zraniteľné komponenty	6	5	5	7	**5,75**	Stredný	3	3	5	5	**4**	Stredný
Logovanie a monitorovanie	2	5	7	7	**5,25**	Stredný	3	3	5	4	**3,75**	Stredný
CSRF	6	3	5	4	**4,5**	Stredný	3	5	2	5	**3,75**	Stredný
Presmerovanie a predávanie	2	5	5	3	**3,75**	Stredný	1	2	2	4	**2,25**	Nízky

Hrozba	Miera rizika pre aplikáciu	Miera rizika pre podnik
Injektovanie	Vysoká	Vysoká
Autentizácia	Vysoká	Vysoká
Expozícia citlivých dát	Stredná	Vysoká
Prelomenie kontroly prístupu	Stredná	Stredná
Nezabezpečená konfigurácia	Vysoká	Vysoká
XSS	Stredná	Stredná
Zraniteľné komponenty	Stredná	Stredná
Logovanie a monitorovanie	Stredná	Stredná
CSRF	Stredná	Stredná
Presmerovanie a predávanie	Stredná	Nízka

PRÍLOHA P II: VÝVOJOVÝ DIAGRAM PROCESU PRIHLÁSENIA