Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Bezpečnostní analýza webové aplikace

Matěj Řezníček

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Matěj Řezníček

Provoz a ekonomika

Název práce

Bezpečnostní analýza webové aplikace

Název anglicky

Web application security analysis

Cíle práce

Cílem práce bude bezpečnostní analýza webové aplikace. Bude provedena identifikace a kvantifikace aktiv, hrozeb a zranitelností a stanovena rizika působící na aplikaci, včetně jejich hodnoty. Dále budou navržena protiopatření vedoucí k redukci významných rizik.

Metodika

Bezpečnostní analýza rizik webové aplikace bude provedena kvalitativní metodou vycházející z metodiky FRAP. Pomocí řízených rozhovorů se zástupci společnosti, která aplikaci provozuje, bude zjištěno, jaká aktiva do procesu zajištění provozu aplikace vstupují, jaká je jejich hodnota, jaké na ně působí hrozby a jaká je pravděpodobnost jejich výskytu. Dále budou stanoveny zranitelnosti aktiv vůči konkrétním hrozbám. Ze zjištěných skutečností bude sestavena matice rizik obsahující veškerá rizika působící na společnost, včetně vyčíslení jejich závažnosti. Budou navržena protiopatření vedoucí k redukci konkrétních rizik.

Doporučený rozsah práce

30-40 stran

Klíčová slova

analýza rizik, webová aplikace, informační systém, informace, data, informační bezpečnost, aktiva, hrozby, zranitelnosti, protiopatření

Doporučené zdroje informací

ANDRESS, Jason. The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Editor Russ Rogers. Amsterdam: Elsevier, 2011, xviii, 171 s. ISBN 978-159-7496-537.

DOUCEK, P. *Řízení bezpečnosti informací : 2. rozšířené vydání o BCM.* Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

HARKINS, Malcolm. Managing risk and information security protect to enable. Kindle ed. New York: Apress, 2013. ISBN 978-143-0251-149.

MLYNEK, J. Zabezpečení obchodních informací. Brno: Computer Press, 2007. ISBN 978-80-251-1511-4

SMEJKAL, V. – RAIS, K. *Řízení rizik ve firmách a jiných organizacích.* Praha: Grada, 2010. ISBN 978-80-247-3051-6.

Předběžný termín obhajoby

2015/16 ZS – PEF

Vedoucí práce

Ing. Marek Pícka, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 26. 11. 2015

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 26. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 28. 11. 2015

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Bezpečnostní analýza webové aplikace" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30. 11. 2015 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Marku Píckovi, Ph.D. za rady a vstřícnost při konzultacích a vedení mé práce a vedení společnosti, které mi umožnilo ve svém prostředí vypracovat tuto práci za poskytnutou příležitost.

Bezpečnostní analýza webové aplikace

Web application security analysis

Souhrn

Tato práce se zabývá kvalitativní analýzou rizik webové aplikace určené pro bytová družstva a společenství vlastníků jednotek. Teoretická část práce obsahuje východiska pro analýzu, základní rozdělení metodik, které lze pro analýzu využít, a popis vybraných z nich. Dále jsou zde rozebrány postupy, jak identifikovat a kvantifikovat aktiva, hrozby a zranitelnosti a z daných hodnot vypočítat hodnoty rizik. V analytické části jsou výše uvedené postupy aplikovány. Výsledkem práce je seznam rizik působících na tuto aplikaci včetně jejich stanovené hodnoty a návrh opatření, která by mohla, v případě zavedení, zjištěná rizika zmírňovat.

Summary

The thesis deals with qualitative risk analysis of web application designed for housing cooperatives and estate owners associations. The theoretical part of this thesis contains background of the analysis, basic classification of risk analysis methods and description of the chosen ones. There are also described processes of assets, threats and vulnerabilities identification and quantification and process of risk calculation. In the analytical part of the thesis the above mentioned knowledge is applied. The result is a list of the risks affecting the application containing their grades and list of proposed countermeasures which could reduce these risks.

Klíčová slova: analýza rizik, webová aplikace, informační systém, informace, data, informační bezpečnost, aktiva, hrozby, zranitelnosti, protiopatření

Keywords: risk analysis, web application, information system, information, data, security, assets, threats, vulnerabilities, countermeasures

Obsah

1 Úvod

V současné době chtějí lidé mít veškeré služby, které potřebují, na dosah ruky a přístupné z pohodlí domova. To je díky internetu a informačním technologiím možné a můžeme říct i běžné. Lidé do internetových aplikací a úložišť poskytují velká množství informací, a to včetně informací, které vykazují značnou míru citlivosti. Toto můžeme snadno demonstrovat třeba na příkladu internetového bankovnictví. Klient může snadno a rychle zkontrolovat zda a jak vysoká mu přišla mzda, nicméně tato informace je pak udržována několik měsíců i let v informačních systémech banky. Pro klienta má internetové bankovnictví ekonomický význam v podobě uspořeného času odpovídajícího návštěvě pobočky, pro banku má význam zejména ve snížení provozních nákladů vynaložených na obsloužení klienta pobočkovým pracovníkem.

Kromě výhod je však provoz takových systémů svázán s určitými riziky, před nimiž je potřeba informace, klienty a společnost chránit. Z pohledu uživatele obvykle tato ochrana spočívá ve volbě dostatečně silného přístupového hesla do konkrétní aplikace a ochraně před zavedením škodlivého kódu na jeho stanici pomocí antivirového programu. Z pohledu provozovatele služby však zabezpečení klientových dat může znamenat zavedení několikastupňové komplexní ochrany systému.

Na otázku, proti jakým rizikům a jakým způsobem je vhodné a efektivní aplikaci a potažmo společnost chránit, může odpovědět analýza rizik. Ta má za cíl zmapovat současný stav v oblasti zabezpečení a popsat, jaké hrozby a jak moc ohrožují aktiva společnosti.

O provedení takové analýzy jsem byl požádán vedením společnosti, která vyvíjí a provozuje webovou aplikaci pro bytová družstva. Tato analýza se pak stala předmětem mé bakalářské práce.

Jelikož by analýza rizik a zejména její závěry mohly být zneužity pro vedení útoku proti dané společnosti a aplikaci, nejsou v této práci uváděny jejich skutečné názvy, ani jména osob podílejících se na analýze.

2 Cíle práce a metodika

Cílem této práce je zpracovat analýzu rizik webové aplikace a poskytnout tak jejímu provozovateli informace o tom, jakým hrozbám jsou aktiva podílející se na provozu této aplikace vystavena a jaká opatření připadají v úvahu, pokud se společnost rozhodne rizika snižovat.

Cíle práce

Z hlediska struktury byly vytyčeny následující cíle:

- identifikace a kvantifikace aktiv
- identifikace a kvantifikace hrozeb
- identifikace a kvantifikace zranitelností
- vyhodnocení rizik
- návrh opatření pro redukci rizik

Metodika práce

Pro zpracování této práce byla využita odborná literatura zabývající se bezpečností a zabezpečením informací a analýzou rizik informačních systémů. Dalšími podklady pro zpracování tohoto dokumentu byly odborné články z tištěných i elektronických médií zabývajících se problematikou analýzy rizik a normy pokrývající oblast bezpečnosti informací.

Úvodní, teoretická, část práce (třetí kapitola) obsahuje východiska pro analýzu, vysvětlení základních pojmů, které v analýze vystupují, vztahů mezi nimi a způsoby zvládání rizik. Jsou zde také popsány metody identifikace a kvantifikace aktiv, hrozeb a zranitelností, výpočtu rizik a volby vhodných protiopatření reagujících na zjištěná rizika.

Ve čtvrté kapitole je uveden stručný uživatelský popis analyzované aplikace.

Analytická část práce, pátá kapitola, obsahuje samotnou analýzu rizik. Jsou zde ilustrovány postupné kroky procesu stanovení hodnoty aktiv, hrozeb, zranitelností a rizik a prezentovány zjištěné skutečnosti.

3 Teoretická východiska

3.1. Informace společnosti a bezpečnost

3.1.1. Informace v podniku

Jedním ze zásadních předpokladů úspěšnosti obchodní společnosti je efektivní využití informací. Zejména pak těch, které konkurenční organizace nemají k dispozici.

V podnicích jsou informace využívány při rozhodovacích procesech, při řízení společnosti a při obchodní činnosti a existují a jsou zpracovávány v různých formách. Mohou se vyskytovat například v podobě písemného dokumentu, mluveného slova, telefonního sdělení, atp. V současnosti je však největší množství informací udržováno v elektronické podobě za využití informačních systémů a vzhledem k neustálému rozvoji informačních technologií se očekává postupný nárůst jak celkového objemu, tak i podílu informací v elektronické formě vůči ostatním formám informací.[1]

Vzhledem k tomu, že informace se počítají mezi největší konkurenční výhody na současném trhu, mají pro každou společnost svou určitou hodnotu.[2]

3.1.2. Hodnota informací

K tomu, jaká je hodnota informace, lze dospět různými cestami. Hodnota informace může odpovídat částce, kterou by musela organizace vynaložit na znovuzískání ztracené informace a její zpracování. Může odpovídat velikosti ztráty, kterou utrpí podnik při částečném zastavení výroby v důsledku nedostupnosti informace, anebo se může jednat například o ztrátu, kterou firma utrpěla v důsledku toho, že konkurenční společnost získala její strategické dokumenty.[3]

Ocenit informaci může pouze její vlastník, který „má nejlepší představu o tom, co by se stalo v případě zničení, ztráty, zneužití nebo nedostupnosti informace a tuto představu dokáže vyjádřit v číslech.“[4]

1 MLÝNEK, J., *Zabezpečení obchodních informací*, s. 1-3
2 Tamtéž
3 RODRYČOVÁ, D., STAŠA, P., *Bezpečnost informací jako podmínka prosperity firmy*, s. 17
4 Tamtéž

3.1.3. Ochrana informací

Porušení bezpečnosti informací (bezpečnostní incident) může vést kromě finančních ztrát také „ke ztrátě dobrého jména společnosti, důvěry klientů, zániku společnosti, ale v některých případech až ke snížení výkonu hospodářství, oslabení měny či ztrátám na životech.“[5]

Z těchto i dalších důvodů je třeba informace chránit, tedy učinit taková opatření, aby byla zajištěna jejich důvěrnost (s informací se mohou seznamovat pouze oprávněné osoby), dostupnost (informace je pro osobu, která je oprávněna se s ní seznamovat k dispozici v okamžiku, kdy s ní potřebuje pracovat) a integrita (informaci lze důvěřovat a spolehnout se na to, že nebyla pozměněna).[6]

3.1.4. Realizace zabezpečení elektronických informací

Zavedení systémového zabezpečení informačního systému vyžaduje realizaci následujících na sebe navzájem navazujících kroků:

- deklaraci bezpečnostního záměru managementem společnosti
- provedení analýzy rizik
- vypracování bezpečnostní politiky informačních systémů, která na základě závěrů analýzy rizik definuje východiska pro další aktivity společnosti v oblasti informační bezpečnosti
- podrobné rozpracování principů a zásad obsažených v bezpečnostní politice do systémových politik a ostatních bezpečnostních předpisů
- postupná realizace doporučených bezpečnostních opatření
- provádění kontrol a auditů stavu zabezpečení a případné odstraňování nalezených nedostatků
- zajištění periodického provádění analýzy rizik a aktualizace předpisové základy společnosti.[7]

5 ČERMÁK, M., *Řízení informačních rizik v praxi*, s. 11
6 Tamtéž
7 MLÝNEK, J., *Zabezpečení obchodních informací*, s. 13-16

3.2. Základní pojmy analýzy rizik

3.2.1. Aktivum

Aktivem se rozumí všechno, co má pro společnost určitou hodnotu.[8]

Nejjednodušším dělením aktiv je dělení na hmotná a nehmotná, kdy mezi hmotná aktiva počítáme například nemovitosti, hardware, kabelové rozvody, atp., a mezi nehmotná aktiva lze zařadit například informace, know-how, software, či předměty autorského práva.[9]

Základní charakteristikou aktiva je jeho hodnota, která vyjadřuje jeho cenu nebo důležitost (kritičnost) pro daný subjekt. Může však samozřejmě reprezentovat i kombinaci obojího.

Aktivum se hodnotí zejména na základě pořizovací ceny či jiné jeho finanční hodnoty, důležitosti aktiva pro existenci a chod společnosti, nákladů, které by bylo třeba vynaložit na překlenutí vzniklé škody na aktivu, dále lze uvažovat rychlost odstranění škody a případně další, pro dané aktivum, specifická hlediska.[10]

3.2.2. Hrozba

Hrozbou se rozumí náhodně nebo úmyslně vyvolaná událost, která může mít nežádoucí vliv na bezpečnost nebo může způsobit škodu. Hrozbou může být například požár, krádež, ale i chyba obsluhy.[11]

Hrozba může pocházet z vnějšího nebo z vnitřního prostředí organizace. Na aktiva může působit dočasně i trvale, ale její působení se také může měnit v čase.[12]

Základní charakteristikou hrozby je její úroveň, která se určuje na základě nebezpečnosti (schopnosti způsobit škodu), přístupu (pravděpodobnosti, že hrozba svým působením získá přístup k aktivu) a motivace (zájmu iniciovat hrozbu vůči aktivu) dané hrozby.[13]

---

8 ISO/IEC 27000:2009(E). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*, s. 2

9 DOUCEK, P. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM, s. 57*

10 SMEJKAL, V., RAIS, K., *Řízení rizik ve firmách a jiných organizacích*, s. 95

11 Tamtéž

12 ČERMÁK, M., *Řízení informačních rizik v praxi*, s. 62

13 SMEJKAL, V., RAIS, K., cit. 10, s. 95

3.2.3. Zranitelnost

Zranitelnost je slabé místo aktiva, které může být zneužito hrozbou k uplatnění nežádoucího vlivu.[14]

Základní charakteristikou zranitelnosti je její úroveň, která se hodnotí na základě citlivosti aktiva (náchylnosti být poškozeno danou hrozbou) a jeho kritičnosti (důležitosti pro danou organizaci).[15]

3.2.4. Protiopatření

„Protiopatření je postup, proces, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby.“[16]

Pro zmírnění působení hrozby se běžně kombinuje více opatření, z nichž každé plní svou konkrétní roli. Jedná se obvykle sadu protiopatření vedoucích k odstrašení, zdržení, detekci, reakci a obnově po útoku. Důležitou roli zde hraje fakt, že účinnost jednotlivých opatření klesá v uvedeném pořadí a že žádná sada protiopatření není 100% účinná.[17]

Charakteristikami protiopatření jsou jeho efektivita (nakolik sníží účinek hrozby) a náklady, do kterých se promítají náklady na pořízení, zavedení a následný provoz řešení.[18]

3.2.5. Riziko

Riziko vzniká vzájemným působením hrozby a aktiva. Jediné, co úroveň rizika snižuje jsou použitá protiopatření. Úroveň rizika vyjadřuje míru ohrožení aktiva, míru nebezpečí, že dojde k uplatnění hrozby a ke vzniku škody. [19]

14 ISO/IEC 27000:2009(E). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*, s. 2

15 SMEJKAL, V., RAIS, K., *Řízení rizik ve firmách a jiných organizacích,* s. 95

16 SMEJKAL, V., RAIS, K., cit. 15, s. 96

17 ČERMÁK, M., *Řízení informačních rizik v praxi*, s. 111-112

18 SMEJKAL, V., RAIS, K., cit. 15, s. 96

19 Tamtéž

3.3. Vztahy v analýze rizik

- Aktivum motivuje útočníka k realizaci hrozby, vůči které má určitou zranitelnost. Aktivum je před hrozbami chráněno protiopatřeními.
- Hrozba překonává protiopatření, a využívá zranitelností. Působí na aktivum a způsobuje tím škodu. Pro svou aktivaci vyžaduje zdroje.
- Protiopatření chrání aktiva před působením hrozeb. Může hrozby odrazovat, detekovat, zmírňovat, nebo jim zabraňovat.[20]

3.4. Způsoby zvládání rizik

3.4.1. Monitoring

Rizika neexistují izolovaně. Větší množství rizik muže působit v jeden moment zároveň na jedno nebo i více aktiv. V některých případech se dokonce může stát, že velké množství malých rizik bude mít dopad ekvivalentní dopadu jednoho kritického rizika. Výše rizika navíc může být proměnlivá v čase. Takřka kdykoli se totiž změnit velikosti dopadu, hodnoty hrozby nebo míry zranitelnosti.

Rizika by se z výše uvedených důvodů měla monitorovat, aby je společnost měla pod kontrolou a věděla, jaké hrozby na ní zrovna působí, či jaký způsobem se vyvíjí.[21]

3.4.2. Retence

Retence, známá také jako akceptace, je metoda zvládání rizik spočívající v tom, že proti riziku se nepodnikají žádné aktivní kroky. Mnohdy je tato metoda zvládání rizik nejvýhodnější. Mělo by se k ní však přistupovat spíše u rizik vedoucích k malým ztrátám a s nízkou pravděpodobností výskytu. Použití této metody by mělo vždy být zdůvodněno. V ideálním případě písemně s uvedením data, jména a podpisu manažera, který o retenci rizika rozhodl. Retenci nelze použít, v případě, že hrozí porušení zákonů nebo předpisů.[22]

3.4.3. Redukce

Redukce rizika spočívá v návrhu a zavádění opatření vedoucích ke snížení rizika prostřednictvím snižování hrozeb nebo zranitelností. Tedy odstraněním příčin rizika. Tuto

20 SMEJKAL, V., RAIS, K., *Řízení rizik ve firmách a jiných organizacích,* s. 96
21 ČERMÁK, M., *Řízení informačních rizik v praxi,* s. 123
22 Tamtéž

metodu zvládání rizik se doporučuje použít pro snižování rizik s vysokou frekvencí výskytu. Nehledě na to, zda způsobují malou nebo velkou ztrátu.[23]

3.4.4. Pojištění

Pojištění je metoda snižující následky rizik. Lze ji použít pro zvládání rizik působících například na zaměstnance nebo nemovitosti, které jsou součástí informačního systému. Doporučuje se použít v případech, kdy pravděpodobnost výskytu hrozeb je spíš nižší, ale dopad pro společnost by mohl mýt kritické následky.[24]

3.4.5. Transfer a sdílení

Pokud hovoříme o transferu rizika, hovoříme v podstatě o outsourcingu informačního systému, kdy jeho provoz a přirozeně s ním spojená rizika společnost přenáší na specializovanou firmu. Příkladem může být pronájem výpočetního střediska.

O sdílení rizika pak lze hovořit například v případě společného provozování výpočetního střediska s dceřinou společností.

Tyto dva způsoby zvládání rizika však mohou také společnosti generovat nová, tzv. druhotná rizika, jež musí řídit. Je tedy třeba vhodnost této metody zvládání rizik nejprve řádně uvážit.[25]

3.4.6. Vyhnutí se riziku

Tato metoda zvládání rizik není příliš mnoho využívána. Mnohdy by totiž vyhnutí se riziku znamenalo přestat provozovat danou činnost. Může však najít uplatnění při upgradu na novou verzi operačního systému krátce po jejím uvolnění.[26]

3.5. Postup analýzy rizik

„Analýza rizik informačního systému slouží k odhadu ztrát, které mohou vzniknout působením hrozeb na informační systém, a dává přehled o stupni nebezpečnosti jednotlivých hrozeb, o zranitelnostech hodnoceného informačního systému a o rizicích, jimž je hodnocený systém vystaven.“[27]

23 ČERMÁK, M., *Řízení informačních rizik v praxi*, s. 124
24 Tamtéž
25 Tamtéž
26 Tamtéž, s. 125
27 MLÝNEK, J., *Zabezpečení obchodních informací*, s. 18

Samotná analýza se skládá z identifikace a kvantifikace aktiv, hrozeb a zranitelností.[28]

3.5.1. Hranice analýzy rizik

Hranice analýzy rizik vymezuje, která aktiva společnosti do analýzy budou vstupovat a která ne. Určuje se „na základě cíle, ke kterému má analýza sloužit. Může se jednat o provedení analýzy rizik pouze v dílčí části informačního systému […] nebo provedení plošné analýzy rizik v rámci celého informačního systému společnosti.“[29]

3.5.2. Hloubka analýzy rizik

Hloubka analýzy rizik je stanovena zejména tím, jak moc budou aktiva agregována, dále tím, zda budou uvažovány pouze typické hrozby nebo bude prováděna identifikace všech možných hrozeb a množstvím respondentů zapojených do analýzy.[30]

3.5.3. Metody analýzy rizik

Existují dva základní typy metod analýzy rizik. Kvantitativní metody využívající matematické a statistické nástroje k vyjádření rizika a kvalitativní metody, při kterých je míra rizika vyjadřována za pomoci adjektiv nebo diskrétních škál namísto přesného matematického vyčíslení.[31]

„Výhodou kvantitativních metod je silná podpora matematického aparátu, a tedy snadná pochopitelnost, srozumitelnost a jednoznačnost“ výsledků.[32] Nevýhodou je časová náročnost a vyšší náročnost na zdroje a programové vybavení.[33]

Výhodami kvalitativních metod, které jsou založeny zejména „na expertním odhadu jednotlivých aktiv, hrozeb a zranitelností a pro jejich vyjádření se užívá slovního nebo číselného hodnocení,“[34] je menší náročnost na zdroje a snazší proveditelnost analýzy. Nevýhodou pak zejména fakt, že výsledkem kvalitativní analýzy není peněžní hodnota odpovídající ztrátě při realizaci hrozby, což má za následek horší kontrolu efektivnosti nákladů vynaložených na opatření vedoucí ke zvládání rizik.[35]

28 ČERMÁK, M., *Řízení informačních rizik v praxi*, s. 22
29 MLÝNEK, J., *Zabezpečení obchodních informací*, s. 19
30 ČERMÁK, M., cit. 28, s. 34
31 KARABACAK, B.,SOGUKPINAR, I., ISRAM: information security risk analysis method. *Computers*, s. 148
32 ČERMÁK, M., cit. 28, s. 28
33 ČERMÁK, M., Analýza rizik: kvantitativní vs. kvalitativní. *Clever and Smart*
34 ČERMÁK, M., Analýza rizik: kvalitativní analýza rizik. *Clever and Smart*
35 ČERMÁK, M., Analýza rizik: kvantitativní vs. kvalitativní. *Clever and Smart*

Karabacak a Sogukpinar tvrdí, že vzhledem ke složité struktuře a rozsáhlosti dnešních informačních systémů jsou analytické metody využívající kvantitativní výpočty nevhodné. Jako důvody uvádějí komplikovanost a velikou náročnost analýzy a matematických výpočtů, pomocí kterých se rizika nad daným systémem modelují, ale také fakt, že kvantitativní výpočty nemusí být schopny modelovat dnešní komplikované rizikové scénáře. Jako vhodnější uvádějí metody kvalitativní, u kterých však poukazují na nedostatky v podobě přirozené diskutabilnosti výsledků a rizika, že výsledky analýzy budou zatíženy subjektivními názory toho, kdo analýzu rizik provádí. [36]

Některá literatura navíc vedle kvantitativních a kvalitativních metod uvádí ještě metody kombinované, které vycházejí z matematických zákonitostí, nicméně se díky kvalitativnímu hodnocení blíží více skutečnosti než předpoklady, z nichž vychází kvantitativní metody.[37]

Jako nejběžnější kvalitativní metoda analýzy rizik je uváděna metoda účelových interview (metoda Delphi), spočívající „v řízeném kontaktu mezi experty hodnotící skupiny a příslušnými představiteli hodnoceného subjektu.“[38] Metoda Delphi pro analýzu využívá soubor předem diskutovaných otázek. Výhodou této metody je menší náročnost na zdroje a čas a možnost zaznamenat specifika posuzovaného systému. Kritizována je absence jednoznačného finančního vyjádření rizik.[39]

Mezi kvalitativními metodami analýzy rizik však získává na oblibě také metoda FRAP (Facillitated Risk Analysis Process). Při ní je kladen důraz na workshopy a na komunikaci mezi pracovníky podílejícími se na analýze. Metodika spočívá v rozdělení analyzovaného systému na dílčí oblasti a následné provedení analýzy pro každou konkrétní oblast. Metodika nevyužívá žádné předem definované sady otázek, ale předpokládá, že výsledky analýzy získané na pracovních jednáních jsou na úrovni, která odpovídá odbornosti a znalosti prostředí analyzovaného systému jednotlivých zúčastněných.[40]

Zřejmě nejznámější kvalitativní metodou analýzy rizik je metoda CRAMM, kterou v literatuře uvádí prakticky všichni autoři.[41] [42] [43] [44] Tato metoda, původně vyvinutá pro potřeby vlády Velké Británie, je v současnosti široce využívána tam, kde je vyžadován

36 KARABACAK, B.,SOGUKPINAR, I., ISRAM: information security risk analysis method. *Computers*, s. 148
37 SMEJKAL, V., RAIS, K., *Řízení rizik ve firmách a jiných organizacích,* s. 17
38 Tamtéž, s. 18
39 Tamtéž, s. 18
40 MLÝNEK, J., *Zabezpečení obchodních informací,* s. 31
41 MLÝNEK, J., cit. 40, s. 29
42 ČERMÁK, M., *Řízení informačních rizik v praxi,* s. 28

soulad s normami a standardy definujícími požadavky na bezpečnost informací. Dalším reprezentantem kategorie kvantitativních metod analýzy rizik je například metodika COBRA .[45]

3.5.4. Identifikace aktiv

Identifikací aktiv se rozumí vytvoření úplného výčtu aktiv, které leží uvnitř hranice analýzy rizik. Tato aktiva lze rozdělit do čtyř základních kategorií:

a) „informace

b) hardware

c) software

d) budovy a místnosti, v nichž se aktiva typu a) až c) fyzicky nacházejí.“[46]

K identifikaci aktiv lze využít například BPA (Business Processes Analysis). Vzhledem k předpokladu, že pro provedení procesně orientované analýzy je důležitá znalost společnosti, doporučuje Čermák identifikaci aktiv řídit, nicméně ji nechat provést interně, zaměstnanci společnosti.[47]

Vzhledem k tomu, že v případě analýzy rozsáhlých informačních systémů může být identifikovaných aktiv velké množství, lze přistoupit k seskupení aktiv podobných vlastností. Tato skupina aktiv pak pro účely další analýzy vystupuje jako jedno aktivum.[48] Lze tak třeba seskupit původně identifikovaných sto počítačů, jimiž společnost disponuje, do jednoho celku a optimalizovat tak následné kroky hodnocení hrozeb a zranitelností, které jsou prováděny pro každé identifikované aktivum, respektive skupinu aktiv.

3.5.5. Kvantifikace aktiv

Při provádění analýzy rizik potřebujeme také znát hodnotu aktiv ležících uvnitř její hranice.[49] K tomu lze využít například metodu BIA (Business Impact Analysis), tedy metodu hodnocení dopadů vycházející ze standardu BS 25999. V rámci BIA jde o to, určit možný dopad narušení bezpečnosti organizace na obchodní výsledky, reputaci, zaměstnance a data společnosti.[50]

43 KARABACAK, B.,SOGUKPINAR, I., ISRAM: information security risk analysis method. *Computers*, s. 148
44 SMEJKAL, V., RAIS, K., cit. 37, s. 18
45 Tamtéž
46 MLÝNEK, J., *Zabezpečení obchodních informací*, s. 19
47 ČERMÁK, M., *Řízení informačních rizik v praxi*, s. 45
48 SMEJKAL, V., RAIS, K., *Řízení rizik ve firmách a jiných organizacích*, s. 99
49 MLÝNEK, J., cit. 46, s. 20
50 Business impact analysis (BIA) at heart of disaster recovery planning. *ComputerWeekly.com* [online].

Hodnota fyzického aktiva je obvykle stanovena s ohledem na aktuální pořizovací cenu aktiva s obdobnými parametry. Cenu informací lze určit na základě nejhoršího možného negativního dopadu v případě, že by došlo k narušení jeho důvěrnosti, dostupnosti nebo integrity. Tyto tři situace nejsou vzájemně podmíněny a je tedy třeba uvažovat pro každé aktivum každou situaci jednotlivě.[51]

Mezi dopady však zřejmý vztah existuje. V naprosté většině případů totiž jakékoli narušení bezpečnosti organizace bude mít za následek finanční ztrátu firmy. Buďto přímo, nebo prostřednictvím jiného dopadu. [52].

„Při odhadu možných negativních dopadů pro společnost v případě vyzrazení, modifikace a nedostupnosti informační jednotky se doporučuje vzít v úvahu následující oblasti dopadu:

- přímé finanční ztráty,
- ztráta dobrého jména společnosti, negativní vliv na pověst společnosti,
- porušení právních předpisů a smluvních závazků,
- narušení důvěrnosti ve vztahu k osobním údajům osob,
- zhoršení výkonu činnosti společnosti,
- ohrožení obchodních zájmů společnosti
- ohrožení dodržení zákonnosti (při vyšetřování trestných činů je zapotřebí, aby informace nebyly poskytnuty neoprávněné osobě, nebyly neoprávněně modifikovány a byly dostupné),
- narušení veřejného pořádku (únik informací, předčasné zveřejnění informací nebo nedostupnost informací společnosti může mít za následek protestní akce, demonstrace, atd.)
- ohrožení bezpečnosti zaměstnanců společnosti a osob.“[53]

3.5.6. Identifikace hrozeb

V kroku identifikace hrozeb je potřeba identifikovat, jaké hrozby působí na jaká aktiva. Hrozby lze dle původu rozdělit na hrozby prostředí a hrozby způsobené člověkem. Ty pak navíc rozlišujeme na úmyslné a neúmyslné.[54]

51 MLÝNEK, J., *Zabezpečení obchodních informací*, s. 21
52 ČERMÁK, M., *Řízení informačních rizik v praxi*, s. 57
53 MLÝNEK, J., cit. 51, s. 22
54 ČERMÁK, M., cit. 52, s. 62

Obvykle se při identifikaci hrozeb vychází z použité metodiky analýzy rizik (CRAMM, COBRA, atp.), kde je uveden seznam hrozeb působících na jednotlivé typy aktiv. Lze však vyjít i ze zkušenosti expertů, kteří analýzu provádějí.[55]

Mlýnek v literatuře uvádí přehled nejčastěji uvažovaných hrozeb následovně:

- „infiltrace neoprávněné osoby do IS, nepovolené užití aplikace,
- porucha počítače (serveru, pracovní stanice), hardwarového zařízení,
- porucha síťových služeb,
- porucha softwaru,
- chyba uživatele IS,
- nedostatek pracovníků (například z důvodu epidemie),
- výpadek dodávky elektřiny,
- porucha klimatizace,
- poškození vodou,
- poškození požárem,
- krádež,
- přírodní katastrofa (požár, zemětřesení, záplavy),
- teroristická akce.“[56]

S Čermákem jsou v tomto ohledu takřka zajedno, byť ten uvádí podrobnější výčet. Celkem zmiňuje 40 různých hrozeb.[57]

3.5.7. Kvantifikace hrozeb

Hodnocení hrozeb spočívá ve stanovení úrovně hrozby pro každý pár hrozba-aktivum. Při hodnocení se vychází z faktorů jako jsou nebezpečnost (schopnost hrozby způsobit škodu), přístup (pravděpodobnost, že se hrozba svým působením dostane k aktivu) a motivace (zájem iniciovat hrozbu vůči aktivu).[58]

Pro hodnocení úrovně hrozeb nicméně neexistuje exaktní algoritmus, a tak je výsledná hodnota založena zejména na úsudku hodnotících osob. Oporu však lze najít ve

55 MLÝNEK, J., *Zabezpečení obchodních informací*, s. 26
56 Tamtéž, s. 26
57 ČERMÁK, M., *Řízení informačních rizik v praxi*, s. 65 - 66
58 SMEJKAL, V., RAIS, K., *Řízení rizik ve firmách a jiných organizacích*, s. 95

statistice a evidenci dosavadních bezpečnostních incidentů, pokud je má organizace k dispozici.[59]

3.5.8. Identifikace a kvantifikace zranitelností

V tomto kroku analýzy rizik jde o to najít a popsat slabá místa bezpečnosti, která by mohla být zneužita hrozbami. Ta se mohou vyskytovat na úrovni fyzické, logické, organizační, personální a technické bezpečnosti.

Východiskem pro stanovení míry zranitelnosti je úroveň stávajících protiopatření. Podle Čermáka lze implementovaná protiopatření identifikovat v zásadě dvěma možnými přístupy. První tkví ve studiu dokumentace (politik, technických specifikací) a porovnání opravdu implementovaných opatření s touto dokumentací a vytvoření jejich seznamu. Může se však stát, že v organizaci budou nalezena protiopatření, která jsou zanesena v politikách, ale nejsou ve společnosti implementována a naopak. Tento přístup, kdy je v podstatě prováděn audit společnosti však z důvodu možného přehlédnutí nebo opomenutí některých skutečností nedoporučuje. Druhý, doporučený, postup využívá již vytvořený seznam protiopatření. Na základě tohoto seznamu je pak třeba identifikovat, která opatření už jsou zavedena a tyto zkontrolovat, zda pracují správně a efektivně. Pokud se vyskytne opatření, které v seznamu není, doporučuje Čermák jeho doplnění. Pro určení hodnoty zranitelnosti se posuzuje, zda jsou opatření eliminující příslušnou hrozbu zavedena, zdokumentována, kontrolována a zlepšována. V případě kombinace analýzy rizik a hodnocení zranitelností s penetračními testy je možné pro určení hodnoty zranitelností použít i výsledky těchto testů. Navíc je vhodné vyhodnotit i to, zda existují důkazy o selháních bezpečnostních opatření a zda existují a v jakém stavu připravenosti jsou havarijní plány, a to pro případ, kdy by došlo k uplatnění hrozby i přes zavedená protiopatření.[60]

59 ČERMÁK, M., *Řízení informačních rizik v praxi*, s. 67
60 Tamtéž, s. 84-87

3.6. Vyhodnocení rizik

„Matematicky je riziko dáno funkcí R (A, H, Z) tří proměnných (A, H, Z), které po řadě reprezentují jednotlivá aktiva, hrozby a zranitelnosti […] Výpočet výše rizika […] je dán vztahem: R(A, H, Z) = a*h*z, kde a je hodnota aktiva A, h je výše hrozby H pro aktivum A, a z je výše zranitelnosti Z vzhledem k hrozbě H.“[61]

Výsledek této funkce pak určuje do jaké kategorie, na základě stanovené škály, riziko spadá.

3.6.1. Výběr vhodných opatření

V této fázi analýzy jsou vytvořeny tzv. tabulky křížových referencí. Jedna z tabulek obsahuje seznam existujících hrozeb a vůči každé z nich navržená opatření a druhá obsahuje seznam navržených opatření, kde je pro každé opatření uvedeno na jaké hrozby působí.[62]

U jednotlivých opatření je dále uveden přínos opatření. Při jeho stanovení je brána v úvahu efektivita opatření, problematičnost, časová náročnost zavedení opatření a celkové náklady na opatření (na zavedení a jeho následný provoz).[63]

61 *ČERMÁK, M., Řízení informačních rizik v praxi*, s. 104 - 105
62 MLÝNEK, J., *Zabezpečení obchodních informací*, s. 33
63 ČERMÁK, M., cit. 61, s. 114

4 Popis analyzované aplikace

Analyzovaná aplikace DružWeb je webová aplikace určená pro bytová družstva (BD) a společenství vlastníků jednotek (SVJ), která těmto spolkům umožňuje:

- snadno založit a provozovat vlastní internetové stránky, bytová družstva tak mohou jednoduše splnit zákonnou povinnost,
- spravovat elektronickou domovní nástěnku včetně možnosti zasílání SMS či emailových notifikací na nové příspěvky,
- ukládat a spravovat důležité domovní dokumenty,
- hlásit závady prostřednictvím internetového formuláře s možností připojení dokumentů či fotografií,
- správu informací o domě,
- správu databáze členů BD/SVJ, obyvatel domu a jejich kontaktních údajů.
- využívat vzorové dokumenty,
- získat právní poradenství a konzultace,
- spravovat revize v domě, vč. možnosti odebírání notifikací v případě, že je revize potřeba obnovit.

5 Analytická část

5.1. Rozhodnutí o provedení analýzy rizik

Management společnosti rozhodl o provedení analýzy rizik webové aplikace DružWeb. Za tímto účelem byla zorganizována schůzka, na které byly vedení společnosti představeny možné varianty provedení této analýzy. Na základě poskytnutých informací vedení rozhodlo, že bude požadovat orientační analýzu provedenou pomocí kvalitativních metod. Metodika použitá pro analýzu bude vycházet z metodiky FRAP, která ale bude mírně přizpůsobena potřebám a požadavkům společnosti.

Od analýzy management společnosti očekává zejména určení klíčových aktiv dané webové aplikace a popsání největších rizik, která na tato aktiva působí.

5.2. Stanovení hranice analýzy rizik

Na základě požadavku společnosti Družstevní web, s.r.o. byla hranice analýzy rizik stanovena následovně:

Předmětem analýzy rizik budou veškerá hmotná i nehmotná aktiva vlastněná společností Družstevní web, s.r.o., jejichž ztráta či poškození by mohla mít přímý dopad na dostupnost a korektní funkčnost analyzované webové aplikace DružWeb a obchody realizované prostřednictvím této aplikace.

Mimo hranice analýzy rizik se budou nacházet aktiva třetích stran podílející se na chodu aplikace, která společnost nakoupila jako službu od externích poskytovatelů, a to včetně veškerých prvků síťové infrastruktury.

5.3. Stanovení hloubky analýzy rizik

Identifikovaná aktiva, kde to bude možné, budou agregována do celků, a to tak, že aktiva stejného typu, umístěná ve stejné lokalitě, budou tvořit pro účely této analýzy jeden celek.

V rámci analýzy bude bráno v úvahu 40 typických hrozeb, které uvádí Čermák ve své literatuře.[64] Výčet uvažovaných hrozeb je také uveden v Příloze č. 3.

Do procesu identifikace a kvantifikace aktiv, hrozeb a zranitelností bude zapojen zejména vlastník analyzované webové aplikace. V případě potřeby však lze zapojit i

64 ČERMÁK, M., *Řízení informačních rizik v praxi*, s. 65 - 66

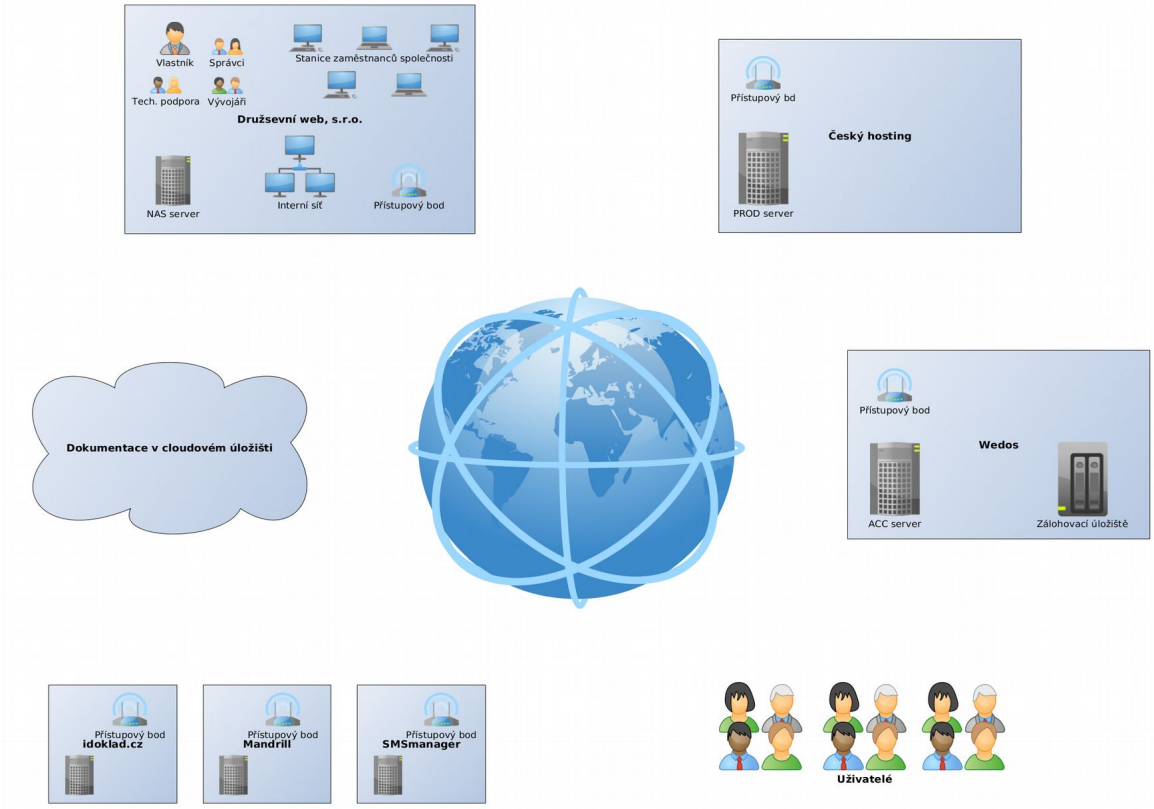
experty, kteří jsou zároveň zaměstnanci společnosti, jako například správce aplikace, vývojáře, pracovníka technické podpory, apod.

5.4. Zahájení analýzy rizik

Na úvod byla svolána schůzka s vedením společnosti, na které byl představen cíl analýzy, popsány procesy a postupy vedoucí k jeho dosažení a vysvětleny pojmy využívané v analýze rizik. Dále na této schůzce bylo potvrzeno, že hlavním respondentem bude vlastník aplikace.

5.5. Identifikace aktiv

Za účelem identifikace aktiv, která do analýzy rizik vstupují, byl vlastník aplikace pozván na workshop, na kterém mu bylo vysvětleno proč a jak je identifikaci aktiv třeba provést. Na tomto workshopu bylo popsáno fungování systému a aktiva potřebná k jeho bezchybnému provozu. Vznikl vizuální model analyzované aplikace a první verze dokumentu Seznam aktiv.



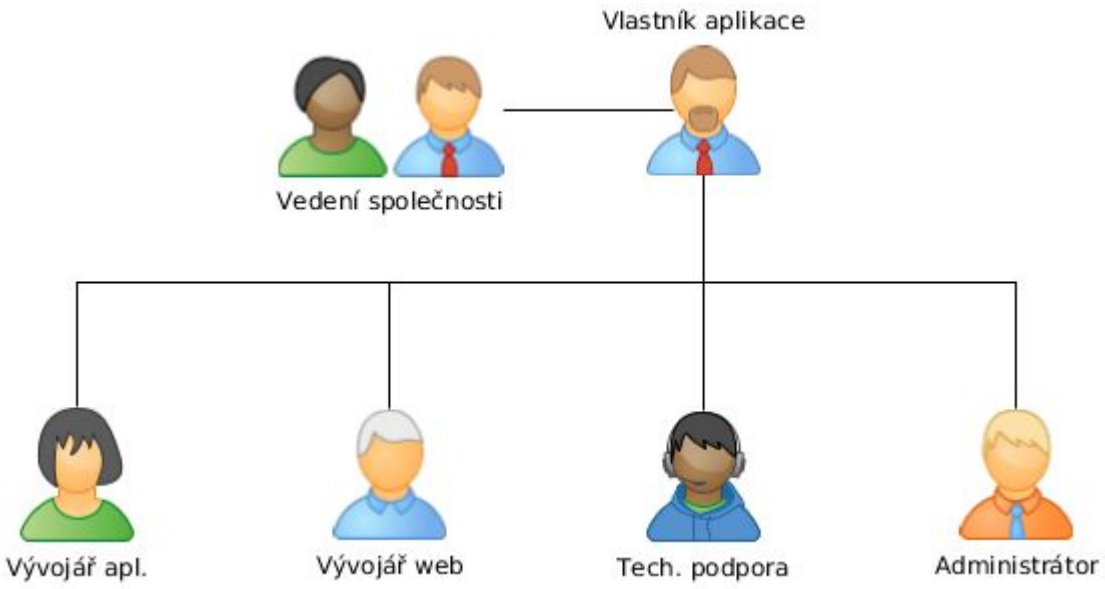
Obrázek 1: Vizuální model aplikace

ID	Kategorie aktiva	Specifikace aktiva
1	Prostory – Budovy	Budova - serverovna
2	Lidé – Dodavatelé	obsluha serverovny
3	Hardware – Servery	HW server
4	Jiná	virtuální server
5	Lidé – Dodavatelé	administrátor virtuálního serveru
6	Software – Operační systémy	operační systém serveru
7	Software – Aplikace	aplikace Sympo
8	Software – Aplikace	frontend apliakce

Tabulka 1: Ukázka podoby první verze dokumentu Seznam aktiv

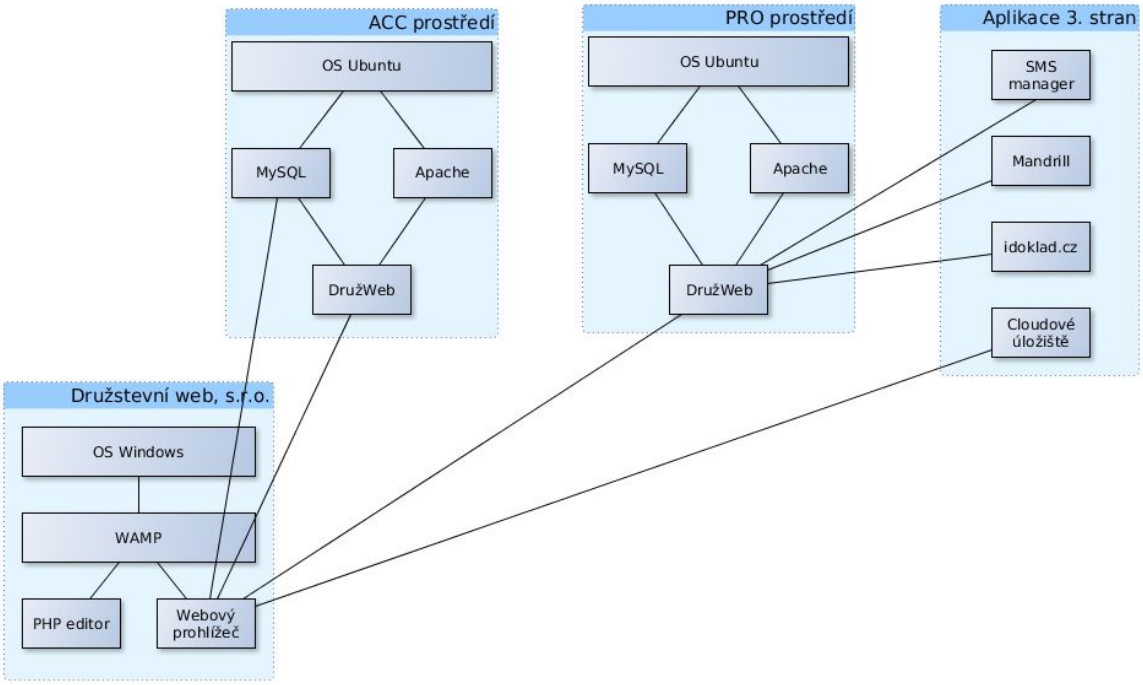
Analyzovaný systém byl následně dekomponován do 3 vrstev – organizační, logické a fyzické. Účelem této dekompozice bylo popsání a pochopení vztahů mezi jednotlivými aktivy.

Organizační model znázorňuje vztahy mezi jednotlivými lidmi, kteří jsou součástí systému. Z obrázku č. 3 je patrné, že vlastník aplikace je členem vedení společnosti a zaměstnanci, podílející se na vývoji a provozu aplikace jsou mu přímo podřízeni.



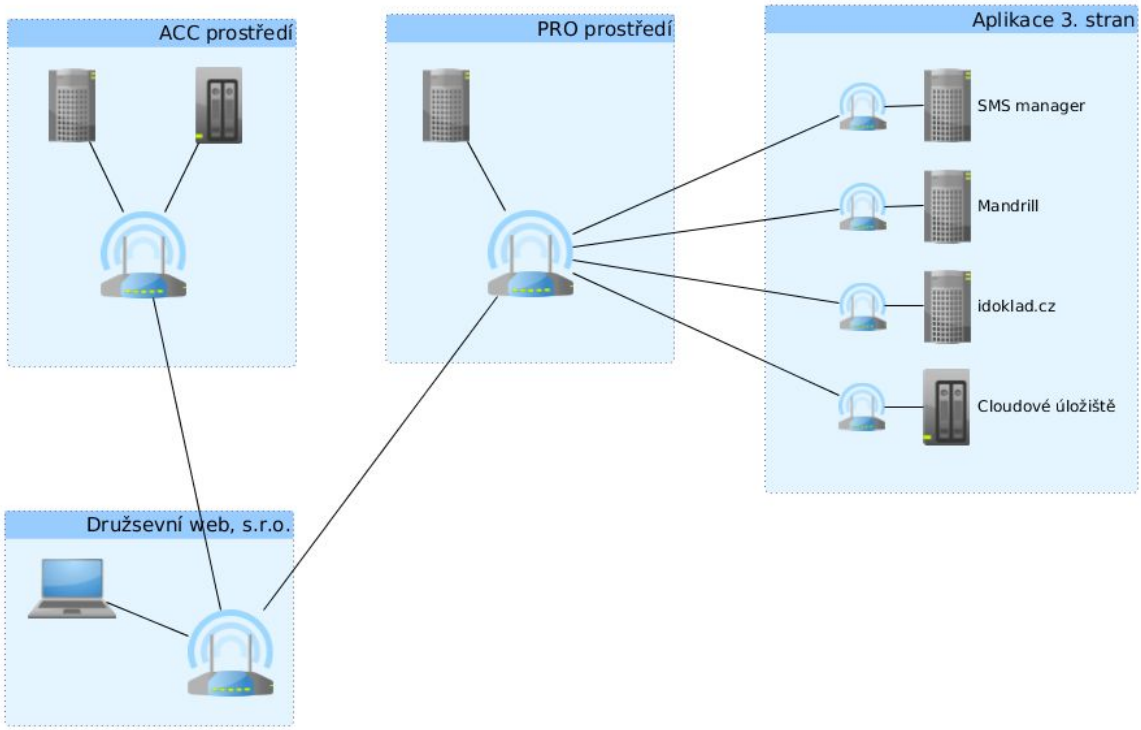
Obrázek 2: Organizační model aplikace DružWeb

Logický model na obrázku č. 4 znázorňuje operační systémy, softwarové komponenty a vazby mezi nimi, nezbytné pro správné fungování aplikace.



Obrázek 3: Logický model aplikace DružWeb

Na obrázku č. 5 je zakreslen fyzický model aplikace, popisující konkrétní hardwarové elementy potřebné pro funkci a obsluhu aplikace.



Obrázek 4: Fyzický model aplikace DružWeb

Na základě výše znázorněné dekompozice byl dokument Seznam aktiv aktualizován a doplněn o nově identifikovaná aktiva. Vznikla tak jeho druhá verze.

ID	Kategorie aktiva	Specifikace aktiva
1	Prostory – Místnosti – Kanceláře	Kanceláře společnosti Družstevní web, s.r.o. - Praha
2	Lidé – Management	Představenstvo společnosti
3	Lidé – Management	Vlastník aplikace
4	Lidé – Správci – Aplikace	Administrátor aplikace + DB
5	Lidé – Uživatelé	Technická podpora aplikace
6	Lidé – Správci	Vývojář aplikace
7	Lidé – Správci	Vývojář webových stránek
8	Hardware – Klienti – PC	PC pro technickou podporu
9	Hardware – Klienti – PC	PC pro administrátora aplikace

Tabulka 2: Ukázka podoby druhé verze dokumentu Seznam aktiv

Posledním krokem identifikace aktiv je jejich agregace dle dohodnuté hloubky analýzy. Agregováni do jedné skupiny aktiv byli zaměstnanci společnosti, a to s přihlédnutím zejména k tomu, že jelikož všichni pracují ve stejné lokalitě, budou na ně působit stejné hrozby. Bylo by tedy neefektivní hodnotit každého zvlášť. Dále byly agregovány počítače zaměstnanců společnosti a data dle kategorie a geografické polohy úložiště. Jeden celek tak tvoří důvěrná produkční data, druhý celek interní produkční data, třetí celek tvoří testovací data, atp. V souladu se stanovenou hranicí analýzy byla dále vyřazena aktiva, která jsou společností nakoupena jako služba od dodavatelských společností. Jedná se zejména o pronajaté HW komponenty. Výše uvedené změny byly zaneseny do třetí verze dokumentu Seznam aktiv.

ID	Kategorie aktiva	Specifikace aktiva
1	Lidé	Personál společnosti
2	Hardware – Klienti – PC	PC personálu společnosti
3	Hardware – Servery – Zálohovací	Lokální zálohovací NAS server pro vývojáře
4	Software – Operační systémy	OS Ubuntu – PRO prostředí
5	Software – DB	MySQL – PRO DB
6	Software – Aplikace	Virtuální webový server Apache – PRO prostředí
7	Software – Aplikace	Aplikace „Družweb“ - PRO prostředí
8	Software – Operační systémy	OS Ubuntu – ACC prostředí

Tabulka 3: Ukázka podoby třetí verze dokumentu Seznam aktiv

5.6. Kvantifikace aktiv

Po identifikaci aktiv je potřeba provést jejich kvantifikaci, nebo-li hodnocení. Pro kvantifikaci byla použita 4 pásma.

Stupeň	Zratka	Výše dopadu	Popis dopadu
1	N	Nízká	Malé škody
2	S	Střední	Vážné škody
3	V	Vysoká	Velmi vážné škody
4	K	Kritická	Přežití je ohroženo

Tabulka 4: Hodnota aktiv

Aktivum bylo hodnoceno na základě atributů uvedených v Příloze č. 1, přičemž výše finanční ztráty pro jednotlivá pásma byla stanovena na základě rozhodnutí managementu společnosti jako procentní podíl finanční ztráty k ročnímu obratu finančních prostředků generovaného aplikací DružWeb. Ten je pro letošní rok odhadován ve výši 500 000 Kč.

Vlastníkem byla stanovena hodnota fyzických i informačních aktiv a zanesena do čtvrté verze dokumentu Seznam aktiv, a to včetně informace, na základě čeho byla tato hodnota stanovena. Fyzická aktiva vlastník ohodnotil konkrétní sumou reprezentující náklady na znovupořízení aktiva v případě jeho úplného zničení, informační aktiva hodnotil zvlášť pro situace, kdy by došlo k narušení důvěrnosti, integrity a dostupnosti dat. Hodnotu informačního aktiva následně reprezentuje nejvyšší z daných tří hodnot. Tyto informace pak byly konsolidovány do konečné podoby dokumentu Seznam aktiv, který je Přílohou č. 2 této analýzy.

ID	Kategorie aktiva	Specifikace aktiva	Hodnota aktiva	Stupeň
1	Lidé	Personál společnosti	Vysoká	3
2	Hardware – Klienti – PC	PC personálu společnosti	Nízká	1
3	Hardware – Servery – Zálohovací	Lokální zálohovací NAS server pro vývojáře	Nízká	1
4	Software – Operační systémy	OS Ubuntu – PRO prostředí	Střední	2
5	Software – DB	MySQL – PRO DB	Vysoká	3
6	Software – Aplikace	Virtuální webový server Apache – PRO prostředí	Nízká	1
7	Software – Aplikace	Aplikace „Družweb“ - PRO prostředí	Kritická	4
8	Software – Operační systémy	OS Ubuntu – ACC prostředí	Střední	2
9	Software – DB	MySQL – ACC DB	Nízká	1

Tabulka 5: Ukázka dokumentu Seznam aktiv

5.7. Identifikace hrozeb

V souladu se stanovenou hloubkou analýzy jsou v rámci analýzy uvažovány hrozby uvedené v Příloze č. 3. Zde je také uvedeno, jaké atributy bezpečnosti konkrétní hrozba ovlivňuje (důvěrnost - CNF, integrita - INT, dostupnost - AVL), jaký je možný původ hrozby (vyšší moc - ENV, úmysl - DLB, nehoda - ACC) a na jaký typ aktiv daná hrozba může působit (hardware - HW, software - SW, síť - NET, média - MED, data - DTA, personál - STF, prostory - SPC).

ID	Hrozba	CNF	INT	AVL	DLB	ACC	ENV
1	Blesk		x	x			x
2	Požár			x	x	x	x
3	Voda		x	x	x	x	x
4	Tornádo			x			x
5	Prach		x	x	x	x	x
6	Zemětřesení		x	x			x
7	Nepřípustná teplota		x	x	x	x	x
8	Nepřípustná vlhkost		x	x	x	x	x

Tabulka 6: Ukázka dokumentu Identifikace hrozeb - identifikace původce hrozby a atributu aktiva, na který hrozba může působit

ID	Hrozba	HW	SW	NET	MED	DTA	STF	SPC
1	Blesk	x		x				x
2	Požár	x		x	x			x
3	Voda	x		x	x			x
4	Tornádo							x
5	Prach	x			x			
6	Zemětřesení	x		x				x
7	Nepřípustná teplota	x			x			
8	Nepřípustná vlhkost	x		x	x			

Tabulka 7: Ukázka dokumentu Identifikace – identifikace toho, na jaké typy aktiv hrozba může působit

Konkrétní hrozby pak byly přiřazeny k jednotlivým aktivům v závislosti na tom, zda je pro ně daná hrozba relevantní. Tedy zda může působit na aktivum dle jeho typu a zda dané aktivum v případě výskytu ohrozí. Vznikla tak první verze dokumentu Seznam hrozeb.

Aktivum ID	Aktivum	Hrozba ID	Hrozba
1	Personál společnosti	14	Nedostatek personálu
		17	Průmyslová havárie v okolí
		18	Demonstrace v okolí
		20	Terorismus
2	PC personálu společnosti	1	Blesk
		2	Požár
		3	Voda
		6	Zemětřesení
		7	Nepřípustná teplota
		8	Nepřípustná vlhkost
		9	Elektrostatický náboj
		10	Intenzivní magnetické pole
		11	Přerušení dodávky elektřiny
		13	Kolísání napětí
		15	Chyba administrátora
		16	Chyba uživatele
		20	Terorismus
		22	Krádež a vandalismus
		34	Selhání HW
		40	Vyzařování

Tabulka 8: Ukázka první verze dokumentu Seznam hrozeb

5.8. Kvantifikace hrozeb

Následně byly hrozby hodnoceny. Byla stanovena pravděpodobnost výskytu konkrétní hrozby vůči konkrétnímu aktivu (pro každou dvojici aktivum - hrozba). Hodnocení probíhalo s přihlédnutím k faktorům, jako jsou dosavadní četnost výskytu, stáří a parametry vybavení, motivace osob a atraktivita aktiva. Hrozby byly hodnoceny dle následující škály:

Stupeň	Zratka	Úroveň hrozby	Pravděpodobnost výskytu hrozby
1	N	Nízká	Nepravděpodobná
2	S	Střední	Pravděpodobná
3	V	Vysoká	Vysoce pravděpodobná
4	K	Kritická	Jistá

Tabulka 9: Hodnocení hrozeb

Vznikla tak druhá verze dokumentu Seznam hrozeb, který výše uvedené hodnocení hrozeb obsahuje, a to včetně komentáře, na základě čeho byla ta která hodnota stanovena.

Pro názornost je na obrázku níže příklad hodnocení hrozeb identifikovaných pro aktivum „Personál společnosti.“ Celý dokument je Přílohou č. 4.

Aktivum ID	Aktivum	Hrozba ID	Hrozba	Pravděpodobnost výskytu	Hodnota hrozby	Komentář
1	Personál společnosti	14	Nedostatek personálu	nepravděpodobná	1	Mohlo by nastat v případě prudkého růstu společnosti. Ten se však neočekává.
		17	Průmyslová havárie v okolí	pravděpodobná	2	Ve staré zástavbě se může stát, ale společnost sídlí v prvním nadzemním patře
		18	Demonstrace v okolí	nepravděpodobná	1	Žádné významné objekty v okolí nejsou
		20	Terorismus	nepravděpodobná	1	Společnost není atraktivní cíl, ani se v její blízkosti žádné nevyskytují.

Tabulka 10: Ukázka dokumentu Seznam aktiv

Úroveň hrozby při hodnocení nepřekročila úroveň 3 – vysoce pravděpodobná. To je zapříčiněno zejména faktem, že aktiva společnosti nejsou dostatečně atraktivní, aby indikovala vyšší hodnotu hrozby. Bohužel se v případě společnosti Družstevní web, s.r.o. nelze opřít o evidenci výskytu bezpečnostních incidentů, protože proces jejich hlášení a evidence není zaveden. Společnost však dle vyjádření vlastníka dosud útokům cíleným na její aktiva nečelila.

5.9. Identifikace a kvantifikace zranitelností

Identifikace zranitelností probíhala na základě porovnání stávajících zavedených opatření vůči seznamu opatření, která uvádí Čermák ve své literatuře[65]. Bylo určeno, zda je dané opatření ve společnosti zavedeno a jaká je jeho vyspělost. Tedy, zda je zavedeno, dokumentováno, kontrolováno a zlepšováno. To je zaneseno v první verzi dokumentu Seznam zranitelností.

ID	Opatření	Zavedeno	Dokumentováno	Kontrolováno	Zlepšováno
1	**Personální – je potřeba zajistit dostatečný počet kvalitních pracovníků**				
1.1	Při přijímání zaměstnanců				
1.1.1	Reference – reference uváděné v životopise by měly být ověřeny				
1.1.2	Vzdělání – doklady o dosažení vzdělání by měly být ověřeny				
1.1.3	Totožnost – ověření totožnosti by mělo být provedeno pomocí dalšího dokladu	x			
1.1.4	Bezúhonnost - bezúhonnost uchazeče o zaměstnání by měla být ověřena				
1.1.5	Smlouva – součástí smlouvy by měla být klauzule o zachování mlčenlivosti				x

Tabulka 11: Ukázka první verze dokumentu Seznam zranitelností

65 ČERMÁK, M., *Řízení informačních rizik v praxi*, s. 89-100

V tomto dokumentu je také uvedeno, jaká z uvedených protiopatření snižují jaké hrozby. I tyto informace byly čerpány z Čermákovy knihy.[66]

ID	Hrozby	Opatření
1	Blesk	2.5.1
2	Požár	2.3.6, 2.3.8, 2.3.9, 2.5.2, 2.7
3	Voda	2.5.3, 2.7.2
4	Tornádo	2.1.4, 2.1.6
5	Prach	n/a
6	Zemětřesení	n/a
7	Nepřípustná teplota	2.7
8	Nepřípustná vlhkost	2.7

Tabulka 12: Ukázka mapování opatření na hrozby které snižují

Na základě informací získaných z fáze identifikace zranitelností byla v navazujím kroku každé dvojici aktivum-hrozba odhadnuta výše zranitelnosti. Pro stanovení stupně zranitelnosti byla využita následující stupnice:

Stupeň	Zkratka	Zranitelnost	Opatření
1	N	Nízká	Opatření jsou zavedena, dokumentována, kontrolována a zlepšována.
2	S	Střední	Opatření jsou zavedena, dokumentována a kontrolována.
3	V	Vysoká	Opatření jsou zavedena a dokumentována.
4	K	Kritická	Žádná opatření nejsou zavedena, dokumentována, kontrolována a zlepšována.

Tabulka 13: Stupnice pro hodnocení opatření

Vznikla tak druhá verze dokumentu Seznam zranitelností, která je Přílohou č. 5 této práce.

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
1	14	1	Společnost má dostatek zaměstnanců, jejich kvalifikaci doplňuje o tematická školení	Nízká	1
	17	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	18	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	20	1	Dle vzhledu a označení budovy není možné určit její účel	Střední	2

Tabulka 14: Ukázka dokumentu Seznam zranitelností

66 ČERMÁK, M., *Řízení informačních rizik v praxi*, s. 101

5.10. Vyhodnocení rizik

Na základě dříve získaných informací byla v této fázi analýzy vypočítána velikost rizik působících na webovou aplikaci DružWeb, respektive na společnost tuto aplikaci provozující. Riziko bylo vypočítáno pro každou trojici aktivum, hrozba, zranitelnost, a to pomocí funkce R(A,H,Z)=*a*h*z*, kde *a* je hodnota aktiva A, *h* je výše hrozby H pro aktivum A, a *z* je výše zranitelnosti Z vzhledem k hrozbě H. Funce R může v našem případě nabývat hodnot z intervalu <1;64>, což je dáno tím, že hodnota aktiva *a*, hodnota hrozby *h* i úroveň zranitelnosti *z* mohou nabývat celočíselných hodnot z intervalu <1;4>.

Výsledek výše uvedené funkce určí, do které z kategorií nízká, střední, vysoká či kritická bude konkrétní riziko patřit. Tato pásma a jejich hranice byla představena managementu společnosti, kterým byla následně odsouhlasena. Kategorie jsou uvedeny v tabulce níže:

Stupeň	Zkratka	Výše rizika	Popis	Od	Do
1	N	Nízké	Riziko nevyžaduje žádnou akci	1	8
2	S	Střední	Riziko je možné akceptovat a dále monitorovat	9	18
3	V	Vysoká	Riziko by mělo být zvládáno podle plánu	24	36
4	K	Kritická	Riziko musí být ihned zvládáno	48	64

Tabulka 15: Rozdělení rizik

Níže jsou graficky znázorněna jednotlivá pásma v závislosti na hodnotě aktiva, hodnotě hrozby a míry zranitelnosti. Zelená reprezentuje nízké riziko, žlutá střední riziko, oranžová barva vysoké riziko a červená barva riziko kritické.

hodnota aktiva: 1

hodnota hrozby / úroveň zranitelnosti	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

hodnota aktiva: 2

hodnota hrozby / úroveň zranitelnosti	1	2	3	4
1	2	4	6	8
2	4	8	12	16
3	6	12	18	24
4	8	16	24	32

hodnota aktiva: 3

hodnota hrozby / úroveň zranitelnosti	1	2	3	4
1	3	6	9	12
2	6	12	18	24
3	9	18	27	36
4	12	24	36	48

hodnota aktiva: 4

hodnota hrozby / úroveň zranitelnosti	1	2	3	4
1	4	8	12	16
2	8	16	24	32
3	12	24	36	48
4	16	32	48	64

Tabulka 16: Vizualizace úrovně rizika

Pro účely výpočtu rizika byla vytvořena matice rizik, která je přiložena jako Příloha č. 6.

5.11. Vyhodnocení opatření

Vzhledem k tomu, že zavedená opatření ve společnosti byla porovnávána se sadou základních opatření a žádné protiopatření nad jejich rámec nebylo identifikováno, je zřejmé, že zavedená opatření jsou jejich podmnožinou. Je tedy třeba zvážit, která opatření ze základní sady zavést, aby byla efektivně zvládána identifikovaná rizika od nejkritičtějších po nejnižší. Pro účely identifikace toho, jaká z navrhovaných protiopatření snižují jaká rizika a naopak na jaká rizika působí jaká opatření, vznikl dokument Seznam opatření. V tomto dokumentu jsou zanesena veškerá protiopatření ze základní sady, která nejsou ve společnosti dosud implementována a mají vliv na alespoň jedno identifikované riziko z kategorie vysoké nebo střední. U každého opatření bylo hodnoceno, jaká je předpokládaná účinnost, náročnost zavedení, časová náročnost zavedení a nákladnost v souladu s níže uvedenými stupnicemi, které byly odsouhlaseny s vedením společnosti.

Stupeň	Zkratka	Účinnost opatření
1	N	Nepatrně minimalizuje riziko.
2	S	Částečně minimalizuje riziko.
3	V	Významně minimalizuje riziko.
4	K	Zcela minimalizuje riziko.

Tabulka 17: Hodnocení účinnosti opatření

Stupeň	Zkratka	Snadnost zavedení opatření
1	N	Zavedení opatření je téměř nemožné.
2	S	Zavedení opatření vyžaduje nadprůměrné znalosti.
3	V	Zavedení opatření vyžaduje průměrné znalosti.
4	K	Zavedení opatření je velice snadné.

Tabulka 18: Hodnocení snadnosti zavedení opatření

Stupeň	Zkratka	Časová náročnost zavedení opatření
1	N	Čas potřebný pro zavedení opatření se pohybuje řádově v měsících.
2	S	Čas potřebný pro zavedení opatření se pohybuje řádově v týdnech.
3	V	Čas potřebný pro zavedení opatření se pohybuje řádově v dnech.
4	K	Čas potřebný pro zavedení opatření se pohybuje řádově v hodinách.

Tabulka 19: Hodnocení časové náročnosti opatření

Stupeň	Zkratka	Náklady na zavedení a provoz opatření	Hodnota
1	N	Extrémně vysoké náklady.	50 000 Kč +
2	S	Vysoké náklady.	15 000 – 50 000 Kč
3	V	Středně vysoké náklady.	5 000 – 15 000 Kč
4	K	Nízké náklady.	< 5 000 Kč

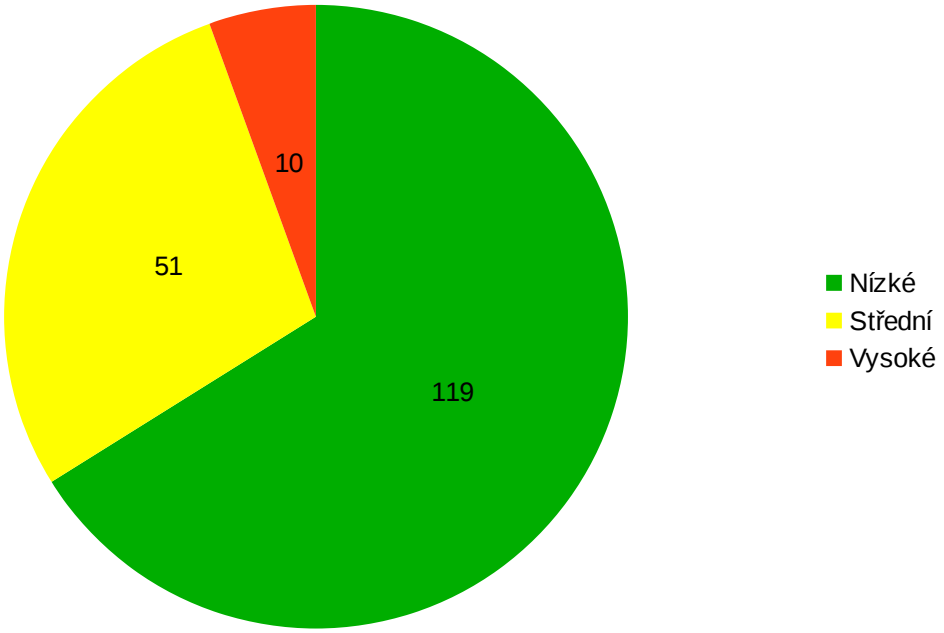
Tabulka 20: Hodnocení nákladů na zavedení a provoz opatření

Opatření mající všechny hodnoty stanoveny na úroveň 4 byla označena za efektivní, nenáročná na zavedení, časově nenáročná a levná. Naproti tomu opatření, u kterých se hodnoty pohybují v nízkých číslech, mohou být neefektivní, náročná na zavedení, časově náročná nebo drahá.

Dokument Seznam opatření, přiložený jako Příloha č. 7, tak může může být managementu společnosti výraznou oporou při rozhodování jakým způsobem identifikovaná rizika zvládat.

6 Výsledky analýzy rizik

V rámci analýzy rizik bylo identifikováno celkem 181 rizik působících na společnost. Z toho je 0 kritických, 10 vysokých, 51 středních a 119 nízkých.



Obrázek 5: Koláčový graf kategorií nalezených rizik

Nejvíce ohrožená je samotná aplikace DružWeb (produkční i testovací instance) tím, že selže. Je to zapříčiněno vysokou hodnotou těchto aktiv a faktem, že proti pravděpodobné hrozbě „selhání SW“ nebyla ve společnosti identifikována žádná protiopatření. Dále jsou tato aktiva významně ohrožena chybami uživatele a neautorizovaným přístupem do IS.

Dalším z vysoce ohrožených aktiv jsou produkční data v systému, která mají vysokou hodnotu a jsou ohrožována hrozbami „chyba uživatele“ a neautorizovaným přístupem do IS.

Posledním aktivem, na které působí vysoké riziko, je personál společnosti, který je ohrožen průmyslovou havárií.

Tato rizika, spadající do kategorie vysokých rizik, je potřeba řešit prioritně, jelikož v případě jejich realizace mohou mít zásadní dopad na společnost.

Pro rizika z kategorie střední by bylo vhodné zvážit, zavedení protiopatření pro snížení rizika, nicméně tato rizika je možné akceptovat a dále monitorovat.

Proti rizikům z kategorie nízká, není potřeba podnikat žádné kroky.

Společnost by v každém případě měla zavést proces hlášení a evidence bezpečnostních incidentů, která může poskytnout přesné informace o tom, jaké hrozby na společnost reálně působí, jak často a s jakými dopady.

Dále by měla být zavedena pravidelná (alespoň jednou ročně) kontrola nastavení přístupových oprávnění. Kontrola by se měla zaměřovat na to, zda nejsou aktivní některé nepoužívané účty (například účty zaměstnanců, kteří už pro společnost nepracují) nebo zda oprávnění daných účtů nejsou s ohledem na potřeby zaměstnance příliš silná.

V souvislosti s nastavením přístupových oprávnění by měla být stanovena také pravidla pro přidělování a správu privilegovaných účtů sloužících k obcházení systémových kontrol v případě potřeby. Tyto účty by měly být přidělovány pouze pokud je to nutné a měl by být udržován jejich seznam. Privilegia by také měla být přidělována pouze k účtům, které nejsou běžně využívány při práci a měla by být pravidelně kontrolována.

Dalším doporučením je zavedení provozního deníku, do kterého budou zapisovány informace o tom, kdy, proč a jaké změny v systému proběhly, kdo změny provedl a pod jakým účtem.

Tato opatření jsou snadno zaveditelná, relativně nenákladná a poskytnou vedení firmy konkrétnější informace o tom, co a kdy se v systému děje. Vzhledem k tomu, že analýzou nebylo nalezeno žádné kritické riziko, je vhodné zavedení dalších, náročnějších, případně nákladnějších opatření naplánovat v delším časovém horizontu, kdy už bude management společnosti disponovat informacemi získanými prostřednictvím výše uvedených opatření.

Zároveň, pokud pokud by management společnosti uvažoval o zavedení některého z náročnějších řešení (např. omezení práva zápisu na vyměnitelná média, vytvoření plánů obnovy po havárii a plánů kontinuity podnikání), je nutné zvážit provedení podrobné analýzy rizik, která by dokázala přesně porovnat možnou ztrátu způsobenou působením hrozby a nákladů na zavedení těchto opatření. Vždy totiž platí, že zavádět opatření dražší než jsou možné dopady hrozby, kterou má opatření potlačovat, je neefektivní.

7 Závěr

Tato bakalářská práce se věnuje analýze rizik webové aplikace z pohledu jejího provozovatele. Celá analýza probíhala v několika postupných krocích.

Nejprve bylo třeba identifikovat a kvantifikovat aktiva, která v rámci provozu aplikace vystupují. Celkem se jednalo o 22 aktiv, respektive skupin aktiv, majících vliv na provoz aplikace. Fyzická aktiva byla hodnocena na základě nákladů, které by musela společnost vynaložit v případě, že by aktivum bylo zničeno. U aktiv typu data byly stanoveny nejprve tři hodnoty, které reprezentovaly dopad na společnost v případě, že by došlo k narušení jejich důvěrnosti (data by získala neoprávněná osoba), dostupnosti (data by nebyla dostupná pro oprávněné osoby v momentě, kdy k nim potřebují přistupovat) nebo integrity (data by byla pozměněna – nedalo by se jim důvěřovat). Poté z těchto 3 hodnot byla vybrána ta nejvyšší, která nadále představovala hodnotu informační jednotky.

Dalším krokem byla identifikace a kvantifikace hrozeb. Pro účely identifikace byl použit seznam 40 typických hrozeb, které mohou působit na informační systémy. Pro každé z dříve popsaných aktiv pak bylo uváženo, které z těchto hrozeb na něj mohou působit. Každé vzniklé dvojici aktivum-hrozba byla posléze ve spolupráci s vedením společnosti odhadnuta pravděpodobnost, s jakou se může za daných podmínek hrozba vyskytnout.

Ve třetí fázi analýzy rizik byla hodnocena zavedená protiopatření, která ve společnosti snižují působení hrozeb. Na základě zjištěných informací byla každému páru aktivum-hrozba přisouzena další hodnota, tentokrát reprezentující zranitelnost.

Všechna aktiva, hrozby a zranitelnosti byly zařazeny do jedné ze čtyř kategorií, přičemž každá kategorie je reprezentována číslem 1-4.

Konečná hodnota rizika byla stanovena prostým součinem tří výsledných hodnot. Jednotlivá rizika mohla nabývat hodnot z intervalu <1;64>, na jejichž základě byla rizika zařazena do kategorií „kritické,“ „vysoké,“ „střední“ nebo „nízké.“

Celkem bylo v rámci analýzy zjištěno 181 rizik, z toho 0 kritických, 10 vysokých, 51 středních a 119 nízkých.

Pro řešení nízkých a středních rizik byl připraven seznam protiopatření, která by mohla být ve společnosti zavedena, aby tato rizika minimalizovala. U každého protiopatření je uveden jeho popis, informace o tom, na jaká rizika nalezená v rámci

analýzy působí, a také jaká je jeho odhadovaná efektivita, náročnost zavedení, časová náročnost a náklady na zavedení a provoz.

Management společnosti by měl po prezentaci této zprávy co nejdříve rozhodnout o tom, jak bude proti rizikům postupováno, jak budou zvládána a kdo za to bude zodpovědný.

Na tomto místě je však třeba připomenout i fakt, že rizika mohou být kromě akceptace, monitoringu nebo redukce pomocí zavádění protiopatření, zvládána i dalšími způsoby, jako jsou pojištění, transfer a sdílení rizika nebo vyhnutí se riziku.

8 Seznam použité literatury

Knižní publikace:

ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. V Tribunu EU vyd. 1. Brno: Tribun EU, 2009, 134 s. Knihovnicka.cz. ISBN 978-80-7399-731-1.

DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Vyd. 1. Brno: Computer Press, c2007, vi, 154 s. ISBN 978-80-251-1511-4.

RODRYČOVÁ, Danuše a Pavel STAŠA. *Bezpečnost informací jako podmínka prosperity firmy*. 1. vyd. Praha: Grada, 2000, 143 s. Manažer. ISBN 80-716-9144-5.

SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, 2010, 354 s. Expert (Grada). ISBN 9788024730516.

Články v seriálové publikaci:

KARABACAK, Bilge a Ibrahim SOGUKPINAR. ISRAM: information security risk analysis method. *Computers*. 2005, **24**(2): 147-159. DOI: 10.1016/j.cose.2004.07.004. ISSN 01674048. Dostupné také z: http://linkinghub.elsevier.com/retrieve/pii/S0167404804001890

Normy:

ISO/IEC 27000:2009(E). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Ed.1. Switzerland: International Organization for Standardization., 2009.

Webové stránky:

Business impact analysis (BIA) at heart of disaster recovery planning. *ComputerWeekly.com* [online]. 2011 [cit. 2015-09-28]. Dostupné z: http://www.computerweekly.com/podcast/Business-impact-analysis-BIA-at-heart-of-disaster-recovery-planning

ČERMÁK, Miroslav. Analýza rizik: kvalitativní analýza rizik. *Clever and Smart* [online]. 2010, 2013 [cit. 2015-09-21]. Dostupné z: http://www.cleverandsmart.cz/analyza-rizik-kvalitativni-analyza-rizik/

ČERMÁK, Miroslav. Analýza rizik: kvantitativní analýza rizik. *Clever and Smart* [online]. 2010, 2012 [cit. 2015-09-21]. Dostupné z: http://www.cleverandsmart.cz/analyza-rizik-kvantitativni-analyza-rizik/

ČERMÁK, Miroslav. Analýza rizik: kvantitativní vs. kvalitativní. *Clever and Smart* [online]. 2010, 2011 [cit. 2015-09-21]. Dostupné z: http://www.cleverandsmart.cz/analyza-rizik-kvantitativni-vs-kvalitativni/

9 Seznam obrázků

10 Seznam tabulek

11 Seznam použitých zkratek

ACC	Testovací prostředí
BD	Bytové družstvo
BIA	Business Impact Analysis
BPA	Business Processes Analysis
COBRA	Consultative, Objective and Bi-functional Risk Analysis
CRAMM	CCTA Risk Analysis and Management Methodology
FRAP	Facillitated Risk Analysis Process
IS	Informační systém
PRO	Produkční prostředí
SVJ	Společenství vlastníků jednotek

12 Přílohy

Příloha č. 1 – Atributy hodnocení aktiv

Příloha č. 2 – Seznam aktiv

Příloha č. 3 – Identifikace hrozeb

Příloha č. 4 – Seznam hrozeb

Příloha č. 5 – Seznam zranitelností

Příloha č. 6 – Matice rizik

Příloha č. 7 – Seznam opatření

Příloha č. 1 – Atributy hodnocení aktiv

Stupeň	1	2	3	4
Zkratka	N	S	V	K
Výše dopadu	Nízká	Střední	Vysoká	Kritická
Popis dopadu	Malé škody	Vážné škody	Velmi vážné škody	Přežití je ohroženo
Finanční ztráta	0-5%	5-10%	10-30%	30% a více
Ztráta produktivity	Na několik minut zpomaleny nebo přerušeny obchodní činnosti společnosti	Na několik hodin zpomaleny nebo přerušeny obchodní činnosti společnosti	Na několik dnů zpomaleny nebo přerušeny obchodní činnosti společnosti	Na několik týdnů zpomaleny nebo přerušeny obchodní činnosti společnosti
Ztráta image	Během dne jedna nepříznivá reportáž v médiích	Během dne několik nepříznivých reportáží v médiích	Několik dnů trvající nepříznivé reportáže v médiích	Několik týdnů trvající nepříznivé reportáže v médiích
Porušení legislativy a předpisů	Drobné porušení – řešeno napomenutím	Porušení – vyšetřování a udělena pokuta	Závažné porušení – vyšetřování, soudní proces a udělena pokuta	Velmi závažné porušení – soudní proces, společnosti hrozí zánik
Ztráta důvěry klientů	Nemá zásadní dopad na důvěru	Část klientů odchází ke konkurenci	Značná část klientů odchází ke konkurenci	Naprostá většina klientů odchází ke konkurenci
Ztráta důvěry vlastníků	Nemá zásadní dopad na důvěru vlastníků	Ztráta důvěry vlastníků, dochází ke změnám v managementu	Značná ztráta důvěry vlastníků, dochází ke kompletní změně managementu	Naprostá ztráta důvěry. Vlastníci posílají společnost do konkurzu
Dopad na činnost a zájmy státu	Má velmi malé dopady na činnost a zájmy státu	Ohrožuje stabilitu měny a výkon hospodářství. Hrozí stávky určitých zájmových skupin	Ohrožuje stabilitu měny a výkon hospodářství. Hrozí občanské nepokoje	Vážně ohrožuje stabilitu měny a výkon hospodářství. Hrozí státní převrat
Dopad na životní prostředí	Nepatrné následky na životní prostředí	Krátkodobé poškození životního prostředí bez vlivu na ekosystém	Závažné střednědobé poškození životního prostředí	Velmi vážné dlouhodobé poškození životního prostředí s dopadem na ekosystém
Dopad na jednotlivce	Ohrožení bezpečnosti jedné osoby, poškození zdraví, zranění, žádné léčení	Ohrožení bezpečnosti více osob, poškození zdraví, zranění, hospitalizace	Ztráta života jedné osoby, nevratné poškození zdraví, zranění více osob	Ztráta života více osob, významné nevratné poškození zdraví

Příloha č. 2 – Seznam aktiv

ID	Kategorie aktiva	Specifikace aktiva	Hodnota aktiva	Stupeň
1	Lidé	Personál společnosti	Vysoká	3
2	Hardware – Klienti – PC	PC personálu společnosti	Nízká	1
3	Hardware – Servery – Zálohovací	Lokální zálohovací NAS server pro vývojáře	Nízká	1
4	Software – Operační systémy	OS Ubuntu – PRO prostředí	Střední	2
5	Software – DB	MySQL – PRO DB	Vysoká	3
6	Software – Aplikace	Virtuální webový server Apache – PRO prostředí	Nízká	1
7	Software – Aplikace	Aplikace „Družweb“ - PRO prostředí	Kritická	4
8	Software – Operační systémy	OS Ubuntu – ACC prostředí	Střední	2
9	Software – DB	MySQL – ACC DB	Nízká	1
10	Software – Aplikace	Virtuální webový server Apache – ACC prostředí	Nízká	1
11	Software – Aplikace	Aplikace „Družweb“ - ACC prostředí	Kritická	4
12	Data – Důvěrná	Důvěrná produkční data	Kritická	4
13	Data – Veřejná	Veřejná produkční data	Nízká	1
14	Data – Interní	Interní produkční data	Střední	2
15	Data – Důvěrná	Dokumentace v cloudovém úložišti	Střední	2
16	Data – Přísně důvěrná	Zálohy na lokálním NAS serveru	Vysoká	3
17	Data – Přísně důvěrná	Zálohy na zálohovacím WEDOS serveru	Kritická	4
18	Data – Přísně důvěrná	Data uložená v aplikaci pro fakturace (idoklad.cz)	Kritická	4
19	Data – Interní	Interní data pro účely testování	Nízká	1
20	Data – Důvěrná	Data uložená v aplikaci pro rozesílání emailů (Mandrill)	Vysoká	3
21	Data – Důvěrná	Data uložená v aplikaci pro rozesílání SMS (SMSmanager)	Vysoká	3
22	Software – Aplikace	Základní SW balík pro personál společnosti	Nízká	1

Příloha č. 3 – Identifikace hrozeb

ID	Hrozba	CNF	INT	AVL	DLB	ACC	ENV
1	Blesk		x	x			x
2	Požár			x	x	x	x
3	Voda		x	x	x	x	x
4	Tornádo			x			x
5	Prach		x	x	x	x	x
6	Zemětřesení		x	x			x
7	Nepřípustná teplota		x	x	x	x	x
8	Nepřípustná vlhkost		x	x	x	x	x
9	Elektrostatický náboj		x	x			x
10	Intenzivní magnetické pole		x	x	x	x	x
11	Přerušení dodávky elektřiny			x	x	x	x
12	Přerušení dodávky vody				x	x	x
13	Kolísání napětí		x	x	x	x	x
14	Nedostatek personálu			x	x	x	
15	Chyba administrátora	x	x	x	x	x	
16	Chyba uživatele	x	x	x	x	x	
17	Průmyslová havárie v okolí			x		x	
18	Demonstrace v okolí			x		x	
19	Kyberterorismus	x	x	x	x		
20	Terorismus			x	x		
21	Odposlech	x			x		
22	Krádež a vandalismus	x		x	x		
23	Falšování identity	x	x	x	x		
24	Neautorizovaný přístup k médiím	x	x	x	x		
25	Neautorizovaný přístup do IS	x	x	x	x		
26	Použití neautorizovaného SW		x	x	x		
27	Použití škodlivého SW	x	x	x	x		
28	Infiltrace komunikace		x		x		
29	Přesměrování zpráv	x	x	x	x	x	
30	Zneužití zdrojů			x	x		
31	Přetížení zdrojů		x	x	x	x	
32	Selhání záložních zdrojů napájení		x	x	x	x	
33	Selhání klimatizace		x	x	x	x	
34	Selhání HW	x	x	x	x	x	
35	Selhání SW	x	x	x	x	x	
36	Selhání NET		x	x	x	x	
37	Selhání média		x	x	x	x	
38	Selhání veřejné sítě		x	x	x	x	
39	Selhání tiskového zařízení			x	x	x	
40	Vyzařování	x				x	

ID	Hrozba	HW	SW	NET	MED	DTA	STF	SPC
1	Blesk	x		x				x
2	Požár	x		x	x			x
3	Voda	x		x	x			x
4	Tornádo							x
5	Prach	x			x			
6	Zemětřesení	x		x				x
7	Nepřípustná teplota	x			x			
8	Nepřípustná vlhkost	x		x	x			
9	Elektrostatický náboj	x		x	x	x		
10	Intenzivní magnetické pole	x		x	x	x		
11	Přerušení dodávky elektřiny	x		x		x		
12	Přerušení dodávky vody	x						
13	Kolísání napětí	x		x				
14	Nedostatek personálu						x	
15	Chyba administrátora	x	x	x	x	x		
16	Chyba uživatele	x	x	x	x	x		
17	Průmyslová havárie v okolí						x	
18	Demonstrace v okolí						x	
19	Kyberterorismus		x	x		x		
20	Terorismus	x		x	x		x	x
21	Odposlech			x				
22	Krádež a vandalismus	x	x		x	x		
23	Falšování identity						x	
24	Neautorizovaný přístup k médiím				x	x		
25	Neautorizovaný přístup do IS		x			x		
26	Použití neautorizovaného SW							
27	Použití škodlivého SW		x	x		x		
28	Infiltrace komunikace							
29	Přesměrování zpráv							
30	Zneužití zdrojů							
31	Přetížení zdrojů		x					
32	Selhání záložních zdrojů napájení	x						
33	Selhání klimatizace	x			x		x	
34	Selhání HW	x						
35	Selhání SW		x					
36	Selhání NET							
37	Selhání média				x			
38	Selhání veřejné sítě							
39	Selhání tiskového zařízení	x						
40	Vyzařování	x						

Příloha č. 4 – Seznam hrozeb

Aktivum ID	Aktivum	Hrozba ID	Hrozba	Pravděpodobnost výskytu	Hodnota hrozby	Komentář
1	Personál společnosti	14	Nedostatek personálu	nepravděpodobná	1	Mohlo by nastat v případě prudkého růstu společnosti. Ten se však neočekává.
		17	Průmyslová havárie v okolí	pravděpodobná	2	Ve staré zástavbě se může stát, ale jsme první nadzemní patro
		18	Demonstrace v okolí	nepravděpodobná	1	Žádné významné objekty v okolí nejsou.
		20	Terorismus	nepravděpodobná	1	Společnost není atraktivní cíl, ani se v její blízkosti žádné nevyskytují.
2	PC personálu společnosti	1	Blesk	nepravděpodobná	1	Nepravděpodobná hrozba, společnost sídlí v údolí pod významně výše položeným mostem.
		2	Požár	pravděpodobná	2	Pod společností sídlí autoservis.
		3	Voda	nepravděpodobná	1	Společnost nesídlí v záplavové oblasti, zatečení srážek je nepravděpodobné
		6	Zemětřesení	nepravděpodobná	1	V našich geografických podmínkách nepravděpodobné
		7	Nepřípustná teplota	nepravděpodobná	1	V našich geografických podmínkách nepravděpodobné
		8	Nepřípustná vlhkost	nepravděpodobná	1	V našich geografických podmínkách nepravděpodobné
		9	Elektrostatický náboj	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		10	Intenzivní magnetické pole	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		11	Přerušení dodávky elektřiny	nepravděpodobná	1	V místě sídla firmy nepravděpodobné
		13	Kolísání napětí	pravděpodobná	2	Možná hrozba
		15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		20	Terorismus	nepravděpodobná	1	Společnost není atraktivní cíl, ani se v její blízkosti žádné nevyskytují.
		22	Krádež a vandalismus	pravděpodobná	2	Vzhledem k lokalitě sídla firmy, je hrozba pravděpodobná
		34	Selhání HW	pravděpodobná	2	Pravděpodobná hrozba, HW má pouze omezenou životnost
		40	Vyzařování	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
3	Lokální zálohovací NAS server pro vývojáře	1	Blesk	nepravděpodobná	1	Nepravděpodobná hrozba, společnost sídlí v údolí pod významně výše položeným mostem.
		2	Požár	pravděpodobná	2	Pod společností sídlí autoservis.
		3	Voda	nepravděpodobná	1	Společnost nesídlí v záplavové oblasti, zatečení srážek je nepravděpodobné
		6	Zemětřesení	nepravděpodobná	1	V našich geografických podmínkách nepravděpodobné
		7	Nepřípustná teplota	nepravděpodobná	1	V našich geografických podmínkách nepravděpodobné
		8	Nepřípustná vlhkost	nepravděpodobná	1	V našich geografických podmínkách nepravděpodobné
		9	Elektrostatický náboj	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		10	Intenzivní magnetické pole	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		11	Přerušení dodávky elektřiny	nepravděpodobná	1	V místě sídla firmy nepravděpodobné
		13	Kolísání napětí	pravděpodobná	2	Možná hrozba
		15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		20	Terorismus	nepravděpodobná	1	Společnost není atraktivní cíl, ani se v její blízkosti žádné nevyskytují.
		22	Krádež a vandalismus	pravděpodobná	2	Vzhledem k lokalitě sídla firmy, je hrozba pravděpodobná
		34	Selhání HW	pravděpodobná	2	Pravděpodobná hrozba, HW má pouze omezenou životnost
		40	Vyzařování	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali

Aktivum ID	Aktivum	Hrozba ID	Hrozba	Pravděpodobnost výskytu	Hodnota hrozby	Komentář
4	OS Ubuntu – PRO prostředí	15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		25	Neautorizovaný přístup do IS	nepravděpodobná	1	Nepravděpodobná hrozba
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba
		31	Přetížení zdrojů	nepravděpodobná	1	Přetížení zdrojů je nepravděpodobné, uživatelů není mnoho (nízké tisíce) a pro cílený útok není společnost dostatečně atraktivní.
		35	Selhání SW	pravděpodobná	2	SW může být poškozen
5	MySQL – PRO DB	15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		25	Neautorizovaný přístup do IS	vysoce pravděpodobná	3	Mohou být zneužity přístupové údaje uživatelů aplikace
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba
		31	Přetížení zdrojů	nepravděpodobná	1	Přetížení zdrojů je nepravděpodobné, uživatelů není mnoho (nízké tisíce) a pro cílený útok není společnost dostatečně atraktivní.
		35	Selhání SW	pravděpodobná	2	Možná hrozba
6	Virtuální webový server Apache – PRO prostředí	15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		25	Neautorizovaný přístup do IS	nepravděpodobná	1	Nepravděpodobná hrozba
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba
		31	Přetížení zdrojů	nepravděpodobná	1	Přetížení zdrojů je nepravděpodobné, uživatelů není mnoho (nízké tisíce) a pro cílený útok není společnost dostatečně atraktivní.
		35	Selhání SW	pravděpodobná	2	Možná hrozba
7	Aplikace „Družweb“ - PRO prostředí	15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		22	Krádež a vandalismus	nepravděpodobná	1	Krádež aplikace je nepravděpodobná, není dostatečně atraktivní aktivum
		25	Neautorizovaný přístup do IS	vysoce pravděpodobná	3	Mohou být zneužity přístupové údaje uživatelů aplikace
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba
		31	Přetížení zdrojů	nepravděpodobná	1	Přetížení zdrojů je nepravděpodobné, uživatelů není mnoho (nízké tisíce) a pro cílený útok není společnost dostatečně atraktivní.
		35	Selhání SW	pravděpodobná	2	Možná hrozba
8	OS Ubuntu – ACC prostředí	15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		25	Neautorizovaný přístup do IS	nepravděpodobná	1	Nepravděpodobná hrozba
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba
		31	Přetížení zdrojů	nepravděpodobná	1	Přetížení zdrojů je nepravděpodobné, uživatelů není mnoho (nízké tisíce) a pro cílený útok není společnost dostatečně atraktivní.
		35	Selhání SW	pravděpodobná	2	SW může být poškozen

Aktivum ID	Aktivum	Hrozba ID	Hrozba	Pravděpodobnost výskytu	Hodnota hrozby	Komentář
9	MySQL – ACC DB	15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		25	Neautorizovaný přístup do IS	vysoce pravděpodobná	3	Mohou být zneužity přístupové údaje uživatelů aplikace
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba
		31	Přetížení zdrojů	nepravděpodobná	1	Přetížení zdrojů je nepravděpodobné, uživatelů není mnoho (nízké tisíce) a pro cílený útok není společnost dostatečně atraktivní.
		35	Selhání SW	pravděpodobná	2	Možná hrozba
10	Virtuální webový server Apache – ACC prostředí	15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		25	Neautorizovaný přístup do IS	nepravděpodobná	1	Nepravděpodobná hrozba
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba
		31	Přetížení zdrojů	nepravděpodobná	1	Přetížení zdrojů je nepravděpodobné, uživatelů není mnoho (nízké tisíce) a pro cílený útok není společnost dostatečně atraktivní.
		35	Selhání SW	pravděpodobná	2	Možná hrozba
11	Aplikace „Družweb“ - ACC prostředí	15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		22	Krádež a vandalismus	nepravděpodobná	1	Krádež aplikace je nepravděpodobná, není dostatečně atraktivní aktivum
		25	Neautorizovaný přístup do IS	vysoce pravděpodobná	3	Mohou být zneužity přístupové údaje uživatelů aplikace
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba
		31	Přetížení zdrojů	nepravděpodobná	1	Přetížení zdrojů je nepravděpodobné, uživatelů není mnoho (nízké tisíce) a pro cílený útok není společnost dostatečně atraktivní.
		35	Selhání SW	pravděpodobná	2	Možná hrozba
12	Důvěrná produkční data	9	Elektrostatický náboj	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		10	Intenzivní magnetické pole	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		11	Přerušení dodávky elektřiny	nepravděpodobná	1	V místě uložení dat nepravděpodobné
		15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		22	Krádež a vandalismus	pravděpodobná	2	
		25	Neautorizovaný přístup do IS	vysoce pravděpodobná	3	Mohou být zneužity přístupové údaje uživatelů aplikace
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba

Aktivum ID	Aktivum	Hrozba ID	Hrozba	Pravděpodobnost výskytu	Hodnota hrozby	Komentář
13	Veřejná produkční data	9	Elektrostatický náboj	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		10	Intenzivní magnetické pole	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		11	Přerušení dodávky elektřiny	nepravděpodobná	1	V místě uložení dat nepravděpodobné
		15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		22	Krádež a vandalismus	pravděpodobná	2	
		25	Neautorizovaný přístup do IS	vysoce pravděpodobná	3	Mohou být zneužity přístupové údaje uživatelů aplikace
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba
14	Interní produkční data	9	Elektrostatický náboj	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		10	Intenzivní magnetické pole	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		11	Přerušení dodávky elektřiny	nepravděpodobná	1	V místě uložení dat nepravděpodobné
		15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		22	Krádež a vandalismus	pravděpodobná	2	
		25	Neautorizovaný přístup do IS	vysoce pravděpodobná	3	Mohou být zneužity přístupové údaje uživatelů aplikace
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba
15	Dokumentace v cloudovém úložišti	9	Elektrostatický náboj	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		10	Intenzivní magnetické pole	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		11	Přerušení dodávky elektřiny	nepravděpodobná	1	V místě uložení dat nepravděpodobné
		15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		22	Krádež a vandalismus	nepravděpodobná	1	
		25	Neautorizovaný přístup do IS	nepravděpodobná	1	Do systému přistupuje pouze omezená skupina lidí (zaměstnanci společnosti), zneužití jejich přístupových oprávnění je nepravděpodobné
16	Zálohy na lokálním NAS serveru	9	Elektrostatický náboj	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		10	Intenzivní magnetické pole	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		11	Přerušení dodávky elektřiny	nepravděpodobná	1	V místě uložení dat nepravděpodobné
		15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		16	Chyba uživatele	vysoce pravděpodobná	3	Chyba uživatele je vysoce pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		22	Krádež a vandalismus	nepravděpodobná	1	Vzhledem k lokalitě uložení dat je hrozba pravděpodobná
		25	Neautorizovaný přístup do IS	nepravděpodobná	1	Do systému přistupuje pouze omezená skupina lidí (zaměstnanci společnosti), zneužití jejich přístupových oprávnění je nepravděpodobné

Aktivum ID	Aktivum	Hrozba ID	Hrozba	Pravděpodobnost výskytu	Hodnota hrozby	Komentář
21	Data uložená v aplikaci pro rozesílání SMS (SMSmanager)	9	Elektrostatický náboj	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		10	Intenzivní magnetické pole	nepravděpodobná	1	Dosud jsme se s touto hrozbou nesetkali
		11	Přerušení dodávky elektřiny	nepravděpodobná	1	V místě uložení dat nepravděpodobné
		15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		22	Krádež a vandalismus	nepravděpodobná	1	
		25	Neautorizovaný přístup do IS	nepravděpodobná	1	Do systému přistupuje pouze omezená skupina lidí (zaměstnanci společnosti), zneužití jejich přístupových oprávnění je nepravděpodobné
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba
22	Základní SW balík pro personál společnosti	15	Chyba administrátora	pravděpodobná	2	Chyba administrátora je pravděpodobná hrozba
		19	Kyberterorismus	nepravděpodobná	1	Společnost není atraktivní cíl
		25	Neautorizovaný přístup do IS	nepravděpodobná	1	Do systému přistupuje pouze omezená skupina lidí (zaměstnanci společnosti), zneužití jejich přístupových oprávnění je nepravděpodobné
		27	Použití škodlivého SW	pravděpodobná	2	Možná hrozba
		35	Selhání SW	pravděpodobná	2	SW může být poškozen

Příloha č. 5 – Seznam zranitelností

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
1	14	1	Společnost má dostatek zaměstnanců, jejich kvalifikaci doplňuje o tematická školení	Nízká	1
	17	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	18	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	20	1	Dle vzhledu a označení budovy není možné určit její účel	Střední	2
2	1	1	Na budově je instalován hromosvod.	Nízká	1
	2	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	3	1	Společnost sídlí mimo záplavové oblasti, aktiva jsou, kde je to možné, umisťována mimo místa možného úniku vody	Střední	2
	6	1	N/A	Kritická	4
	7	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	8	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	9	1	N/A	Kritická	4
	10	1	N/A	Kritická	4
	11	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	1
	13	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	1
	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	20	1	Dle vzhledu a označení budovy není možné určit její účel	Střední	2
	22	2	Vzhled a označení budovy neprozrazuje její účel, je instalován alarm a bezpečnostní dveře, pro úschovu důležitých aktiv jsou využívány uzamykatelné kontejnery, skříně a trezory, do společnosti nemá přístup veřejnost, záložní data a média jsou umístěny mimo sídlo společnosti,	Střední	2
	34	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	40	1	Obvodové zdi jsou silné a pevné	Vysoká	3

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
3	1	1	Na budově je instalován hromosvod.	Nízká	1
	2	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	3	1	Společnost sídlí mimo záplavové oblasti, aktiva jsou, kde je to možné, umisťována mimo místa možného úniku vody	Střední	2
	6	1	N/A	Kritická	4
	7	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	8	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	9	1	N/A	Kritická	4
	10	1	N/A	Kritická	4
	11	1	Instalován nepřerušitelný zdroj napájení UPS	Nízká	1
	13	2	Instalován nepřerušitelný zdroj napájení UPS	Nízká	1
	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	20	1	Dle vzhledu a označení budovy není možné určit její účel	Střední	2
	22	2	Vzhled a označení budovy neprozrazuje její účel, je instalován alarm a bezpečnostní dveře, pro úschovu důležitých aktiv jsou využívány uzamykatelné kontejnery, skříně a trezory, do společnosti nemá přístup veřejnost, záložní data a média jsou umístěny mimo sídlo společnosti,	Střední	2
	34	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	40	1	Obvodové zdi jsou silné a pevné	Vysoká	3
4	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	25	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2
	31	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	35	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
5	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	25	3	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2
	31	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	35	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
6	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	25	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2
	31	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	35	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
7	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	22	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	25	3	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2
	31	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	35	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
8	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	25	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2
	31	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	35	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
9	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	25	3	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2
	31	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	35	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
10	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	25	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2
	31	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	35	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
11	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	22	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	25	3	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2
	31	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	35	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
12	9	1	N/A	Kritická	4
	10	1	N/A	Kritická	4
	11	1	Instalován nepřerušitelný zdroj napájení UPS	Nízká	1
	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	22	2	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	25	3	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
13	9	1	N/A	Kritická	4
	10	1	N/A	Kritická	4
	11	1	Instalován nepřerušitelný zdroj napájení UPS	Nízká	1
	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	22	2	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	25	3	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
14	9	1	N/A	Kritická	4
	10	1	N/A	Kritická	4
	11	1	Instalován nepřerušitelný zdroj napájení UPS	Nízká	1
	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	22	2	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	25	3	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
15	9	1	N/A	Kritická	4
	10	1	N/A	Kritická	4
	11	1	Instalován nepřerušitelný zdroj napájení UPS	Nízká	1
	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	22	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	25	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
16	9	1	N/A	Kritická	4
	10	1	N/A	Kritická	4
	11	1	Instalován nepřerušitelný zdroj napájení UPS	Nízká	1
	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	22	2	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	25	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
17	9	1	N/A	Kritická	4
	10	1	N/A	Kritická	4
	11	1	Instalován nepřerušitelný zdroj napájení UPS	Nízká	1
	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	22	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	25	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
18	9	1	N/A	Kritická	4
	10	1	N/A	Kritická	4
	11	1	Instalován nepřerušitelný zdroj napájení UPS	Nízká	1
	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	22	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	25	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
19	9	1	N/A	Kritická	4
	10	1	N/A	Kritická	4
	11	1	Instalován nepřerušitelný zdroj napájení UPS	Nízká	1
	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	16	3	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	22	1	Aplikace je velmi dobře hodnocena z pohledu bezpeč	Nízká	1
	25	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2
20	9	1	N/A	Kritická	4
	10	1	N/A	Kritická	4
	11	1	Instalován nepřerušitelný zdroj napájení UPS	Nízká	1
	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	22	1	Aplikace je velmi dobře hodnocena z pohledu bezpeč	Nízká	1
	25	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2

Aktivum ID	Hrozba ID	Hodnota hrozby	Zavedená opatření	Zranitelnost	Hodnota zranitelnosti
21	9	1	N/A	Kritická	4
	10	1	N/A	Kritická	4
	11	1	Instalován nepřerušitelný zdroj napájení UPS	Nízká	1
	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	22	1	Aplikace je velmi dobře hodnocena z pohledu bezpeč	Nízká	1
	25	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2
22	15	2	Zaměstnanci společnosti jsou pravidelně školeni, je prováděna pravidelná kontrola dodržování bezpečnostní politiky	Střední	2
	19	1	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4
	25	1	Je přesně určeno, kdo může spravovat přístupová oprávnění, pro každého jednotlivce nebo skupinu jsou dokumentována zavedená přístupvá oprávnění, nepoužívané účty jsou rušeny a pravidelně kontrolovány, defaultní účty jsou přejmenovány, názvy účtů neindikují jejich účel, k ověření uživatele je využíváno heslo, heslo se při zadávání nezbrazuje na obrazovce, defaultní hesla jsou změněna, při ukončení práce by se měl uživatel odhlásit od počítače, po určité době nečinnosti se počítač uzamkne, systém nevrací informaci o tom, který přihlašovací údaj je chybný, přístup do systému a k datů je poskytován pouze oprávněným uživatelům.	Střední	2
	27	2	je nasazen prostředek na detekci škodlivého kódu a je zajištěna jeho pravidelná aktualizace	Střední	2
	35	2	Nebyla identifikována žádná zavedená bezpečnostní opatření	Kritická	4

Příloha č. 6 – Matice rizik

Riziko ID	Aktivum ID	Hrozba ID	Hodnota aktiva	Hodnota hrozby	Hodnota zranitelnosti	Riziko
1	1	14	3	1	1	3
2	1	17	3	2	4	24
3	1	18	3	1	4	12
4	1	20	3	1	2	6
5	2	1	1	1	1	1
6	2	2	1	2	4	8
7	2	3	1	1	2	2
8	2	6	1	1	4	4
9	2	7	1	1	4	4
10	2	8	1	1	4	4
11	2	9	1	1	4	4
12	2	10	1	1	4	4
13	2	11	1	1	1	1
14	2	13	1	2	1	2
15	2	15	1	2	2	4
16	2	16	1	3	2	6
17	2	20	1	1	2	2
18	2	22	1	2	2	4
19	2	34	1	2	4	8
20	2	40	1	1	3	3
21	3	1	1	1	1	1
22	3	2	1	2	4	8
23	3	3	1	1	2	2
24	3	6	1	1	4	4
25	3	7	1	1	4	4
26	3	8	1	1	4	4
27	3	9	1	1	4	4
28	3	10	1	1	4	4
29	3	11	1	1	1	1
30	3	13	1	2	1	2
31	3	15	1	2	2	4
32	3	16	1	3	2	6
33	3	20	1	1	2	2
34	3	22	1	2	2	4
35	3	34	1	2	4	8
36	3	40	1	1	3	3
37	4	15	2	2	2	8
38	4	19	2	1	4	8
39	4	25	2	1	2	4
40	4	27	2	2	2	8

Riziko ID	Aktivum ID	Hrozba ID	Hodnota aktiva	Hodnota hrozby	Hodnota zranitelnosti	Riziko
41	4	31	2	1	4	8
42	4	35	2	2	4	16
43	5	15	3	2	2	12
44	5	16	3	3	2	18
45	5	19	3	1	4	12
46	5	25	3	3	2	18
47	5	27	3	2	2	12
48	5	31	3	1	4	12
49	5	35	3	2	4	24
50	6	15	1	2	2	4
51	6	16	1	3	2	6
52	6	19	1	1	4	4
53	6	25	1	1	2	2
54	6	27	1	2	2	4
55	6	31	1	1	4	4
56	6	35	1	2	4	8
57	7	15	4	2	2	16
58	7	16	4	3	2	24
59	7	19	4	1	4	16
60	7	22	4	1	2	8
61	7	25	4	3	2	24
62	7	27	4	2	2	16
63	7	31	4	1	4	16
64	7	35	4	2	4	32
65	8	15	2	2	2	8
66	8	19	2	1	4	8
67	8	25	2	1	2	4
68	8	27	2	2	2	8
69	8	31	2	1	4	8
70	8	35	2	2	4	16
71	9	15	1	2	2	4
72	9	16	1	3	2	6
73	9	19	1	1	4	4
74	9	25	1	3	2	6
75	9	27	1	2	2	4
76	9	31	1	1	4	4
77	9	35	1	2	4	8
78	10	15	1	2	2	4
79	10	16	1	3	2	6
80	10	19	1	1	4	4

Riziko ID	Aktivum ID	Hrozba ID	Hodnota aktiva	Hodnota hrozby	Hodnota zranitelnosti	Riziko
81	10	25	1	1	2	2
82	10	27	1	2	2	4
83	10	31	1	1	4	4
84	10	35	1	2	4	8
85	11	15	4	2	2	16
86	11	16	4	3	2	24
87	11	19	4	1	4	16
88	11	22	4	1	2	8
89	11	25	4	3	2	24
90	11	27	4	2	2	16
91	11	31	4	1	4	16
92	11	35	4	2	4	32
93	12	9	4	1	4	16
94	12	10	4	1	4	16
95	12	11	4	1	1	4
96	12	15	4	2	2	16
97	12	16	4	3	2	24
98	12	19	4	1	4	16
99	12	22	4	2	2	16
100	12	25	4	3	2	24
101	12	27	4	2	2	16
102	13	9	1	1	4	4
103	13	10	1	1	4	4
104	13	11	1	1	1	1
105	13	15	1	2	2	4
106	13	16	1	3	2	6
107	13	19	1	1	4	4
108	13	22	1	2	2	4
109	13	25	1	3	2	6
110	13	27	1	2	2	4
111	14	9	2	1	4	8
112	14	10	2	1	4	8
113	14	11	2	1	1	2
114	14	15	2	2	2	8
115	14	16	2	3	2	12
116	14	19	2	1	4	8
117	14	22	2	2	2	8
118	14	25	2	3	2	12
119	14	27	2	2	2	8
120	15	9	2	1	4	8

Riziko ID	Aktivum ID	Hrozba ID	Hodnota aktiva	Hodnota hrozby	Hodnota zranitelnosti	Riziko
121	15	10	2	1	4	8
122	15	11	2	1	1	2
123	15	15	2	2	2	8
124	15	16	2	3	2	12
125	15	19	2	1	4	8
126	15	22	2	1	2	4
127	15	25	2	1	2	4
128	16	9	3	1	4	12
129	16	10	3	1	4	12
130	16	11	3	1	1	3
131	16	15	3	2	2	12
132	16	16	3	3	2	18
133	16	19	3	1	4	12
134	16	22	3	1	2	6
135	16	25	3	1	2	6
136	17	9	4	1	4	16
137	17	10	4	1	4	16
138	17	11	4	1	1	4
139	17	15	4	2	2	16
140	17	19	4	1	4	16
141	17	22	4	1	2	8
142	17	25	4	1	2	8
143	17	27	4	2	2	16
144	18	9	4	1	4	16
145	18	10	4	1	4	16
146	18	11	4	1	1	4
147	18	15	4	2	2	16
148	18	19	4	1	4	16
149	18	22	4	1	2	8
150	18	25	4	1	2	8
151	18	27	4	2	2	16
152	19	9	1	1	4	4
153	19	10	1	1	4	4
154	19	11	1	1	1	1
155	19	15	1	2	2	4
156	19	16	1	3	2	6
157	19	19	1	1	4	4
158	19	22	1	1	1	1
159	19	25	1	1	2	2
160	19	27	1	2	2	4

Riziko ID	Aktivum ID	Hrozba ID	Hodnota aktiva	Hodnota hrozby	Hodnota zranitelnosti	Riziko
161	20	9	3	1	4	12
162	20	10	3	1	4	12
163	20	11	3	1	1	3
164	20	15	3	2	2	12
165	20	19	3	1	4	12
166	20	22	3	1	1	3
167	20	25	3	1	2	6
168	20	27	3	2	2	12
169	21	9	3	1	4	12
170	21	10	3	1	4	12
171	21	11	3	1	1	3
172	21	15	3	2	2	12
173	21	19	3	1	4	12
174	21	22	3	1	1	3
175	21	25	3	1	2	6
176	21	27	3	2	2	12
177	22	15	1	2	2	4
178	22	19	1	1	4	4
179	22	25	1	1	2	2
180	22	27	1	2	2	4
181	22	35	1	2	4	8

Příloha č. 7 – Seznam opatření

Navrhovaná opatření	Popis opatření	Omezuje rizika (ID)	Efektivita opatření	Časová náročnost zavedení	Náklady na zavedení a provoz	Náklady na opatření
1.2.4	Hlášení – veškeré nestandardní stavy, incidenty a podezření na ně by měly být hlášeny	43	1	4	4	4
		44				
		57				
		58				
		85				
		86				
		96				
		97				
		115				
		124				
		131				
		132				
		139				
		147				
		164				
		172				
1.2.5	Šetření – v případě porušení či podezření na porušení bezpečnostní politiky by mělo být zahájeno šetření	43	2	3	4	4
		44				
		47				
		57				
		58				
		62				
		85				
		86				
		90				
		96				
		97				
		101				
		115				
		124				
		131				
		132				
		139				
		143				
		147				
		151				
		164				
		168				
		172				
		176				

Navrhovaná opatření	Popis opatření	Omezuje rizika (ID)	Efektivita opatření	Časová náročnost zavedení	Náklady na zavedení a provoz	Náklady na opatření
1.2.6	Vyvození důsledků – v případě porušení bezpečnostní politiky by měly být vyvozeny důsledky	43	2	3	4	4
		44				
		47				
		57				
		58				
		62				
		85				
		86				
		90				
		96				
		97				
		101				
		115				
		124				
		131				
		132				
		139				
		143				
		147				
		151				
		164				
		168				
		172				
		176				
2.11	Evakuační plány – evakuační plány by měly být vypracovány a pravidelně testovány	2	1	2	2	2
		3				
3.1.10	Přidělená přístupová oprávnění by měla být pravidelně kontrolována	46	4	3	4	4
		61				
		89				
		99				
		100				
		118				
3.1.2	Požadavek na zřízení, zrušení a změnu přístupu by měl existovat v písemné podobě	46	1	4	4	4
		61				
		89				
		99				
		100				
		118				
3.1.8	Uživatel by měl podepsat, že mu přístup byl zřízen a rozumí podmínkám přístupu	46	2	3	4	4
		61				
		89				
		99				
		100				
		118				

Navrhovaná opatření	Popis opatření	Omezuje rizika (ID)	Efektivita opatření	Časová náročnost zavedení	Náklady na zavedení a provoz	Náklady na opatření
3.1.9	Uživatel by měl mít možnost zjistit, kam má přiděleny přístupy	46	2	2	3	4
		61				
		89				
		99				
		100				
		118				
3.2.2	Všechna privilegia v systému by měla být zdokumentována	46	3	2	2	3
		61				
		89				
		99				
		100				
		118				
3.2.3	Požadavek na přidělení nebo odebrání privilegií by měl existovat v písemné podobě	46	1	4	4	4
		61				
		89				
		99				
		100				
		118				
3.2.4	Měl by být udržován seznam přidělených privilegií	46	3	3	3	4
		61				
		89				
		99				
		100				
		118				
3.2.5	Privilegia by měla být přidělována, jen pokud je to nutné	46	3	3	4	4
		61				
		89				
		99				
		100				
		118				
3.2.6	Privilegia by měla být přidělována k jiným účtům než které jsou používány pro práci	46	3	3	4	4
		61				
		89				
		99				
		100				
		118				
3.2.7	Přidělená privilegia by měla být pravidelně kontrolována	46	3	3	4	4
		61				
		89				
		99				
		100				
		118				

Navrhovaná opatření	Popis opatření	Omezuje rizika (ID)	Efektivita opatření	Časová náročnost zavedení	Náklady na zavedení a provoz	Náklady na opatření
3.5.1	Do sítě by nemělo být možné připojovat neautorizovaná zařízení	46	3	2	3	4
		61				
		89				
		99				
		100				
		118				
3.5.10	Sít' by měla umožnit šifrování.	46	3	2	3	3
		61				
		89				
		99				
		100				
		118				
3.5.11	Přístup do jiných sítí a internetu by měl být povolen pouze vybraným uživatelům.	46	1	2	3	4
		61				
		89				
		99				
		100				
		118				
3.5.2	V síti by měly být povoleny jen vybrané protokoly.	46	1	2	3	3
		61				
		89				
		99				
		118				
3.5.3	Komunikace by měla být povolena jen na vybraných portech.	46	2	2	3	3
		61				
		89				
		99				
		100				
		118				
3.5.4	Síť by měla být segmentována a rozdělena do zón.	46	1	2	3	3
		61				
		89				
		99				
		100				
		118				
3.5.5	Jednotlivé zóny by od sebe měly být odděleny firewallem.	46	1	2	3	3
		61				
		89				
		99				
		100				
		118				

Navrhovaná opatření	Popis opatření	Omezuje rizika (ID)	Efektivita opatření	Časová náročnost zavedení	Náklady na zavedení a provoz	Náklady na opatření
3.5.6	Správa aktivních prvků by měla být možná pouze po autentizaci.	46	3	3	4	4
		61				
		89				
		99				
		100				
		118				
3.5.7	Topologie sítě, konfigurace aktivních prvků by měla být dokumentována.	46	2	2	3	3
		61				
		89				
		99				
		100				
		118				
3.5.8	Konfigurace aktivních prvků by měla být zálohována.	46	3	3	4	4
		61				
		89				
		99				
		100				
		118				
3.5.9	Provoz na síti by měl být filtrován na základě dokumentovaných pravidel.	46	2	2	3	3
		61				
		89				
		99				
		100				
		118				
3.6.10	OS by měl po přihlášení uživateli zobrazit počet neúspěšných pokusů o přihlášení.	46	2	2	3	4
		61				
		89				
		99				
		100				
		118				
3.6.11	OS by měl poskytovat správný čas, měla by být zajištěna synchronizace času.	46	1	2	4	4
		61				
		89				
		99				
		118				
3.6.12	V OS by měly běžet jen nezbytně nutné služby, ostatní služby by měly být vypnuty.	46	2	2	4	4
		61				
		89				
		99				
		100				
		118				

Navrhovaná opatření	Popis opatření	Omezuje rizika (ID)	Efektivita opatření	Časová náročnost zavedení	Náklady na zavedení a provoz	Náklady na opatření
3.6.13	Nepotřebné programy by měly být z operačního systému odstraněny.	46	2	3	4	4
		61				
		89				
		99				
		100				
		118				
3.6.4	OS by měl být schopen omezit dobu připojení uživatele.	46	2	2	4	4
		61				
		89				
		99				
		100				
		118				
3.6.6	OS by měl zobrazit hlášení, že přístup je umožněn pouze oprávněným uživatelům	46	1	2	4	4
		61				
		89				
		99				
		100				
		118				
3.6.8	OS by měl omezit počet pokusů o přihlášeni a účet na určitou dobu zablokovat.	46	3	2	4	4
		61				
		89				
		99				
		100				
		118				
3.6.9	OS by měl po přihlášení uživateli zobrazit datum po sledního přihlášení.	46	2	2	4	4
		61				
		89				
		99				
		100				
		118				
3.7.3	Přistup k datům a funkcím aplikace by měl být řízen prostřednictvím nabídek.	46	2	2	3	3
		61				
		89				
		99				
		100				
		118				
3.8.1	Právo zapisovat na vyjímatelná média by mělo být povoleno jen vybraným osobám.	46	4	2	3	3
		61				
		89				
		99				
		100				
		118				

Navrhovaná opatření	Popis opatření	Omezuje rizika (ID)	Efektivita opatření	Časová náročnost zavedení	Náklady na zavedení a provoz	Náklady na opatření
3.8.2	Právo pořizovat tiskové kopie by mělo být povoleno jen vybraným osobám.	46	3	2	3	4
		61				
		89				
		99				
		100				
		118				
5.10.3	Měl by být nasazen prostředek umožňující kontrolu integrity souborů.	47	3	2	3	3
		62				
		90				
		101				
		143				
		151				
		168				
		176				
5.11.1	Plány obnovy po havárii (DRP) a plán zajištění kontinuity (BCP) by měl existovat.	2	4	2	2	3
		3				
		45				
		49				
		59				
		64				
		70				
		87				
		92				
		98				
		133				
		140				
		148				
		165				
		173				
5.11.2	Plány by měly být pravidelně testovány a aktualizovány.	2	3	3	3	3
		3				
		45				
		49				
		59				
		64				
		70				
		87				
		92				
		98				
		133				
		140				
		148				
		165				
		173				

Navrhovaná opatření	Popis opatření	Omezuje rizika (ID)	Efektivita opatření	Časová náročnost zavedení	Náklady na zavedení a provoz	Náklady na opatření
5.11.3	Měly by být stanoveny osoby odpovědné za tvorbu a aktualizaci těchto plánů.	2	2	3	4	4
		3				
		45				
		49				
		59				
		64				
		70				
		87				
		92				
		98				
		133				
		140				
		148				
		165				
		173				
5.7.1	Úroveň auditování a monitorování by měla být stanovena na základě provedené AR	48	2	2	3	3
		49				
		63				
		64				
		70				
		91				
		92				
5.7.2	Seznam událostí, které se mají auditovat, by měl být definován.	48	2	2	3	3
		49				
		63				
		64				
		70				
		91				
		92				
5.7.3	Minimálně by se měl auditovat úspěšný a odmítnutý přístup do systému nebo aplikace.	48	2	3	3	4
		49				
		63				
		64				
		70				
		91				
		92				
5.7.4	Auditovat úspěšný a odmítnutý přístup k datům, funkcím a použití privilegií je doporučeno.	48	2	3	3	3
		49				
		63				
		64				
		70				
		91				
		92				

Navrhovaná opatření	Popis opatření	Omezuje rizika (ID)	Efektivita opatření	Časová náročnost zavedení	Náklady na zavedení a provoz	Náklady na opatření
5.7.5	Auditní záznam by měl obsahovat ID události, ID uživatele, ID zařízení, datum a čas.	48	1	3	3	4
		49				
		63				
		64				
		70				
		91				
		92				
5.7.6	Auditní záznamy a nástroje by měly být chráněny, aby nedošlo k narušeni jejich integrity.	48	1	2	3	3
		49				
		63				
		64				
		70				
		91				
		92				
5.7.7	Mělo by být stanoveno, jak reagovat na výskyt jednotlivých událostí.	48	2	3	3	3
		49				
		63				
		64				
		70				
		91				
		92				
5.8	Provozní deník — veškeré zásahy do systému by měly být zaznamenány do provozního deníku, mělo by v něm být uvedeno: čas, kdy k zásahu došlo, důvod k zásahu, kdo zásah provedl a pod jakým účtem, v čem přesně zásah spočíval, co bylo učiněno pro okamžitou obnovu a zabránění opakováni události.	49	2	3	4	4
		64				
		70				
		92				