FIIT, STU Ilkovičova 2, 842 16 Bratislava

MBVIT - projekt 1

Ondrej Ambruš, Michal Minár

Študijný program: Informatika Ročník: 2.

Predmet: Manažment bezpečnosti v IT Cvičiaci: Ing. Miroslav Galbavý

1 Použité skratky

VPN - virtuálne vzdialené pripojenie do internej siete firmy

GDPR - zákon prijatý Európskou Úniou na ochranu dát spotrebiteľov

RAID - spôsob zapojenia pevných diskov, tak aby sa minimalizovalo riziko straty dát

USB - rozhranie určené na komunikáciu dvoch zariadení

ISP - prevádzkovateľ prístupu na internet

UPS - záložný zdroj elektrickej energie formou batérii a rozsiahlych zariadení

MAN - typ počítačovej siete na prepojenie veľkého množstva zariadení

WiFi - bezdrôtová sieť

o365 - skrátene Microsoft office 365

HA - Hodnota aktíva

ÚZ - úroveň zraniteľnosti

GB - jednotka uložených dát (gigabyte)

Gb/s - je jednotka rýchlosti prenosu dát (gigabit za sekundu)

MR - skratka pre mieru rizika

PHA - aritmetický priemer hodnôt dotknutých aktív

DDoS - typ kybernetického útoku

2 Slovník pojmov

Windows 10 pro - operačný systém od spoločnosti Microsoft

Microsoft office 365 - balík kancelárskych nástrojov od spoločnosti microsoft

Jira - softvér na správu chýb, úloh, zmien, ktorý pomáha tímu zlepšiť efektivitu práce

Microsoft SharePoint - softvérové úložiskové miesto pre firmy založené na podobnom princípe ako samba, Onedrive alebo Google Drive

Microsoft teams - software na komunikáciu zamestnancov

3 Opis prostredia

Spoločnosť B.R.A. (Banka regionálnej asociácie) je slovenská súkromná banka s dlhoročnými skúsenosťami v oblasti bankovníctva.
Spoločnosť sídli v 2 budovách River Parku na Žižkovej ulici na -1. až 4. poschodí, spolu s prístupnou strechou, podzemnými garážami a kantínou. Zamestnanci pracujú prevažne z kancelárii a v prípade nutnosti z domu, odkiaľ sa dokážu pripojiť pomocou VPN. Všetci zamestnanci pracujú s vysoko citlivými údajmi, sú náležite poučení školeniami zaoberajúcimi sa dozornou radou a GDPR. Spolu so zamestnancami banky pracujú v budove číslo 2 aj externí pracovníci kantíny. Kuchári a upratovači sú najímaní externou spoločnosťou Index Nosluš a spoločnosť nemá právo zasahovať do ich výberu, pokiaľ bezprostredne neohrozujú chod a prevádzky banky.

V centrále banky pracujú uvedení kľúčoví zamestnanci:

- Generálny riaditeľ
- Manažment
- Riaditelia jednotlivých úsekov
- Systémový administrátori
- Databázový administrátori
- Sieťový administrátori
- Privátne bankovníctvo
- Technická podpora
- Personalisti
- Účtovníci

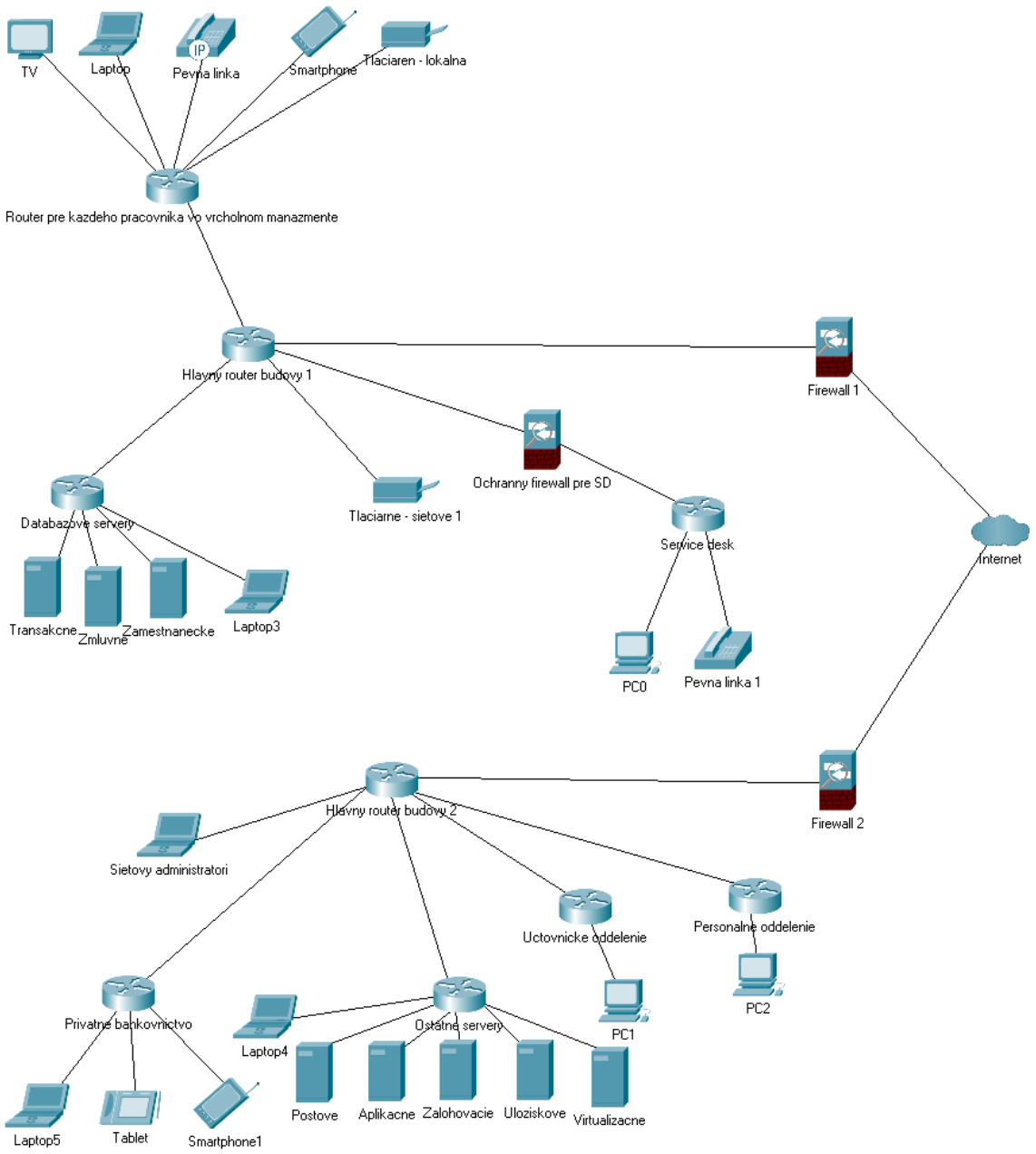
Obe budovy majú približne rovnaký tvar a rozloženie ako je znázornené v sekcii Umiestnenie aktív. V suteréne prvej budovy sa nachádzajú databázové servery, spolu s technickým skladom, za ktoré je zodpovedný tím databázových administrátorov, a parkovisko. Zvyšné servery (Virtualizačné, zálohovacie, úložiskové, aplikačné a záložné) sa nachádzajú v suteréne druhej budovy, za ktorých chod zodpovedá tím systémových administrátorov. Na prvom až štvrtom poschodí oboch budov sa nachádzajú kancelárie pre technickú podporu, vedenie, privátnych bankárov, administrátorov, hlavné miesto archívu, personálne a účtovnícke oddelenie. Všetky serveri sú nakonfigurované na RAID 10 pre ochranu údajov a fungujú na operačnom systéme "*Windows Server 2019 Datacenter*". Navyše má každý pracovník k dispozícii šifrovaný USB kľúč pre zálohu ich najcennejších údajov s kapacitou 128GB.

Serverovňa je chránená pred prípadným prerušením dodávky prúdu UPS systémom. Zmluva s ISP obsahuje špeciálne podmienky pre prípad odstávky siete, nakoľko transakcie musia byť nepretržite zaznamenávané.

Budovy sú navzájom prepojené optickým vláknom s rýchlosťou 200 Gbit za sekundu a tvoria sieť typu MAN. Celá firemná sieť je chránená firewallom pred prístupom na internet a jedným dodatočným firewallom pre technickú podporu na zvýšenie ochrany celej siete. Na každom poschodí sa nachádza otvorená WiFi oddelená od firemnej siete bez kontrolovaného prístupu.

Každý pracovník banky disponuje vlastným počítačom alebo laptopom, podľa pozície a potreby s ohľadom na aktuálne možnosti spoločnosti. Preferovaným operačným systémom je Windows 10 pro, spolu s kancelárskym balíkom Microsoft office 365 a prehľadným úložiskom dát "*SharePoint*". Komunikáciu zamestnancov zastrešuje aplikácia v rámci o365, a to Microsoft Teams, ktorá je šifrovaná.

4 Topológia firemnej siete



5 Metodika určovania rizík

V našej metodike zohľadňujeme 3 faktory pri výpočte miery rizika pre spoločnosť. Prvým z nich je hodnota aktíva, ktoré môže byť ohrozené. Jednotlivé aktíva rozdeľujeme do 4 kategórii vysvetlených v tabuľke Matica ohodnotenia aktív. Následne sa vyhľadajú zraniteľnosti spojené s danými aktívami a určí sa ich úroveň hrozby pomocou tabuliek Matica ohodnotenia úrovne zraniteľností a Matica ohodnotenia úrovne hrozieb. Výsledná miera rizika je určená Matica ohodnotenia rizík.

5.1 Matica ohodnotenia aktív

Ohodnotenie hodnoty aktív	
Hodnotenie	**Hodnota aktíva**
1	Aktívum je doplnkové a nie je potrebné na fungovanie podniku (zvyšuje pohodlie zamestnancov)
2	Aktívum podporuje fungovanie banky avšak jeho výpadok toto fungovanie nenaruší
3	Aktívum je nevyhnutné na správne fungovanie banky ale jeho narušenie znamená iba dočasné narušenie fungovanie
4	Aktívum je základom fungovania banky a jeho poškodenie môže znamenať trvalé narušenie fungovania

5.2 Matica ohodnotenia úrovne zraniteľností

Ohodnotenie zraniteľností					
Hodnota	**Prístupnosť zraniteľnosti**	**Hodnota**	**Jednoduchosť nápravy**	**Hodnota**	**Odhaliteľnosť zraniteľnosti**
0	Zraniteľnosť je nedostupná	3	Odstrániť zraniteľnosť je nemožné	5	Zraniteľnosť nie je odhaliteľná
1	Zraniteľnosť je dostupná na špecifickom mieste v budove	2	Odstrániť zraniteľnosť je veľmi náročné	3	Zraniteľnosť je ťažko odhaliteľná
2	Zraniteľnosť je prístupná kdekoľvek v budove	1	Odstrániť zraniteľnosť je stredne náročné	1	Zraniteľnosť je stredne odhaliteľná
3	Zraniteľnosť je prístupná kdekoľvek	0	Odstrániť zraniteľnosť je jednoduché	0	Zraniteľnosť je jasná na prvý pohľad

Stupnica	Riešenie
0 - 4 (Nízka - 1)	Zraniteľnosť nie je potrebné odstrániť
5 - 9 (Stredná - 2)	Zraniteľnosť by bolo vhodné odstrániť
>10 (Vysoká - 3)	Zraniteľnosť je nutné odstrániť

5.3 Matica ohodnotenia úrovne hrozieb

Ohodnotenie úrovne hrozby	
Hodnotenie	**Popis**
1 (Nízka)	Hrozba , ktorá neohrozuje aktíva spoločnosti ani jej reputáciu
2 (Stredná)	Hrozba ohrozujúca aktíva alebo reputáciu
3 (Vysoká)	Hrozba ohrozujúca aktíva a reputáciu

5.4 Matica ohodnotenia rizík

	Úroveň hrozby	1			2			3		
	Úroveň zraniteľnosti	1	2	3	1	2	3	1	2	3
Hodnota aktíva	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7

6 Identifikácia a ohodnotenie aktív

Nasledujúce dve tabuľky reprezentujú ceny jednotlivých softvérových, hardvérových a dokumentových aktív firmy. Celková cena dosahuje hodnoty približne 1.2 milióna eur.

6.1 Identifikácia

6.1.1 Softvér

Softvér				
#	**Licencia**	**Cena licencie**	**Počet**	**Celková hodnota**
1	Windows 10 pro	209	160	33440
2	Microsoft Office 365	109	206	22454
3	SAP	1357	30	40710
4	Windows Server 2019	7057	8	56456
5	Microsoft SQL Server	1899	3	5697
6	Jira	14	126	1764
7	Microsoft SharePoint	1399	1	1399

6.1.2 Hardvér

Hardvér				
#	**Zariadenie**	**Jednotková cena**	**Počet**	**Celková hodnota**
1	Wyse 5470 *(Počítač)*	779	84	65436
2	Dell Latitude 5410 *(Prenosný počítač)*	1319	76	100244
3	iPhone 12 Pro *(Mobilný telefón)*	1269	76	96444
4	Xerox VersaLink C605XL *(Tlačiareň)*	2119	6	12714
5	Xerox B215DNI *(Tlačiareň)*	207	16	3312
6	SuperMicro A+ 4124GO-NART *(Server)*	102000	5	510000
7	A+ Server 412GS-TNR *(Server)*	10000	3	30000
8	C8500-12X4QC *(Smerovač)*	134188	2	268376
9	CISCO ISR 4331 2ge 2NIM 1SM *(Smerovač)*	1378	7	9646
10	Cisco Firepower 2110 *(Firewall)*	5667	2	11334
11	Cisco IP Phone 8800 *(Pevná linka)*	259	50	12950
12	Cisco IP Phone 7800 *(Pevná linka)*	179	16	2864
13	iPad Pro 12.9" *(Tablet)*	1209	46	55614
14	LG 55NANO90 *(Televízor)*	599	16	9584

6.1.3 Dokumenty

Ohodnotenie aktív				
#	**Aktívum**	**Vlastník aktíva**	**Umiestnenie aktíva**	**Hodnota aktíva**
1	Klientské zmluvy	Účtovnícke oddelenie	Dokumentový archív	3
2	Pracovné zmluvy	Personálne oddelenie	Dokumentový archív	3
3	História transakcií	Databázový administrátor	Databázový server	4
4	Investičné profily	Generálny riaditeľ / manažment	Databázový server	4
5	Zákaznícke účty	Databázový administrátor	Databázový server	4

6.2 Ohodnotenie

6.2.1 Softvér

Ohodnotenie aktív				
#	**Aktívum**	**Vlastník aktíva**	**Umiestnenie aktíva**	**Hodnota aktíva**
21	Windows 10 pro	Používateľ	-	3
22	Microsoft Office 365	Používateľ	-	2
23	SAP	Systémový administrátor	Aplikačný server	4
24	Windows Server 2019	Systémový administrátor	Virtualizačný server	3
25	Microsoft SQL Server	Systémový administrátor	Databázový server	3
26	Jira	Systémový administrátor	Aplikačný server	2
27	Microsoft SharePoint	Systémový administrátor	Úložiskový server	2

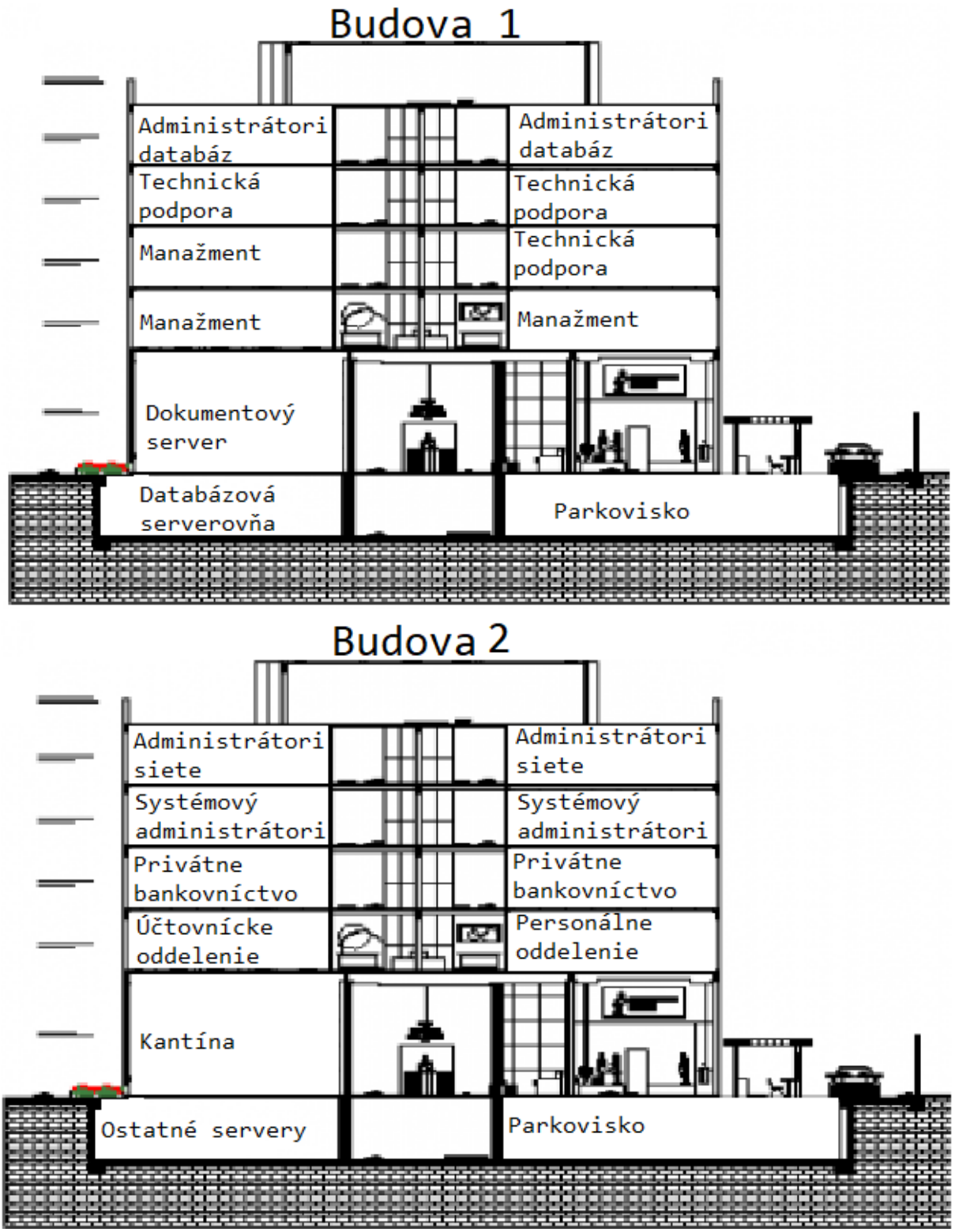
6.2.2 Dokumenty

Ohodnotenie aktív				
#	**Aktívum**	**Vlastník aktíva**	**Umiestnenie aktíva**	**Hodnota aktíva**
1	Klientské zmluvy	Účtovnícke oddelenie	Dokumentový archív	3
2	Pracovné zmluvy	Personálne oddelenie	Dokumentový archív	3
3	História transakcií	Databázový administrátor	Databázový server	4
4	Investičné profily	Generálny riaditeľ / manažment	Databázový server	4
5	Zákaznícke účty	Databázový administrátor	Databázový server	4

6.2.3 Hardvér

Ohodnotenie aktív				
#	**Aktívum**	**Vlastník aktíva**	**Umiestnenie aktíva**	**Hodnota aktíva**
7	Wyse 5470 *(Počítač)*	Používateľ	Technická podpora	3
8	Dell Latitude 5410 *(Prenosný počítač)*	Používateľ	Manažment	1
9	iPhone 12 Pro *(Mobilný telefón)*	Používateľ	Manažment	1
10	Xerox VersaLink C605XL *(Tlačiareň)*	Technický riaditeľ	Tech. pod./Privátne bank	2
11	Xerox B215DNI *(Tlačiareň)*	Technický riaditeľ	Manažment	2
12	SuperMicro A+ 4124GO-NART *(Server)*	Systémový administrátor	2. serverovňa	3
13	A+ Server 412GS-TNR *(Server)*	Databázový administrátor	Databázová serverovňa	4
14	C8500-12X4QC *(Smerovač)*	Sieťový administrátor	2. serverovňa	3
15	CISCO ISR 4331 2ge 2NIM 1SM *(Smerovač)*	Sieťový administrátor	Kancelárie	3
16	Cisco Firepower 2110 *(Firewall)*	Sieťový administrátor	2. serverovňa	3
17	Cisco IP Phone 8800 *(Pevná linka - Technická podpora)*	Používateľ	Technická podpora	2
18	Cisco IP Phone 7800 *(Pevná linka)*	Používateľ	Manažment	1
19	iPad Pro 12.9" *(Tablet)*	Používateľ	Manažment	1
20	LG 55NANO90 *(Televízor)*	Používateľ	Manažment	1

6.3 Umiestnenie aktív



7 Identifikácia hrozieb a návrh opatrení

Nasledujúca podkapitola obsahuje základnú identifikáciu hrozieb, klasifikáciu a návrh opatrení. Každá hrozba má naviac uvedenú tabuľku s vplyvom danej hrozby na aktíva firmy. Výsledná miera rizika je zaznačená v poslednom stĺpci tabuľky. Najvyššie hodnoty vyžadujú urgentnú implementáciu navrhovaných opatrení. V tabuľke identifikácie hrozieb a opatrení a matice ohodnotenia rizík sa zohľadňuje detailný prístup k ich ohodnoteniu. Samotné vysvetlenie dotknutých aktív a spôsob výpočtu jednotlivých stĺpcov PHA, ÚH, ÚZ, MR je vysvetlený v nasledujúcej kapitole Dotknuté aktíva.

7.1 Identifikácia hrozieb

Identifikácia hrozieb						
ID	**Identifikovaná hrozba**	**Príklad súvisiacej zraniteľnosti**	**PHA**	**ÚH**	**ÚZ**	**MR**
1	Zraniteľnosť v kancelárskom balíku *office 365*	Pomocou prílohy v e-maili s následným kliknutím sa dokáže spustiť vírus.	3	2	1	**3**
2	Odcudzenie firemného notebooku	Na notebooku sa nachádzajú nešifrované dáta	3	1	1	**2**
3	Odcudzenie prenosného média	Strata šifrovaného kľúču	3	1	1	**2**
4	Elektrický skrat	Nestabilná dodávka energie	3	1	1	**2**
5	Únik informácii z dokumentových archívov	Pri vstupe do archívov nie je potrebné sa preukazovať kartou na pohyb po budove	3	2	2	**4**
6	Zlá konfigurácia databázového servera Microsoft SQL	Prístupové role do databázových serverov má každý používateľ rovnaké.	4	3	3	**7**
7	Zlá konfigurácia Microsoft SharePoint	Voľný prístup pre neregistrovaných používateľov v rámci firemnej siete.	3	3	3	**6**
8	Živelná katastrofa (povodeň)	Serverové miestnosti sú umiestnené v suteréne. V prípade povodní sú nechránené.	3	2	2	**4**
9	Neautorizovaný zásah do systému iného používateľa	Zamestnanci si často nechávajú odblokované počítače na stole, čo môže mať za následok zneužitie ich prístupov	3	2	2	**4**
10	Odpozorovanie hesla zamestnancov technikou pozerania cez plece	Zamestnanci dochádzajúci do práce využívajú čas vo verejnej doprave na prácu, kde ich heslá, firemné dokumenty a iné môžu pozorovať tretie osoby	4	2	1	**4**
11	Otváranie podozrivých odkazov z e-mailov	Pri doručení e-mailu z tretej strany zamestnanci otvárajú odkazy bez bližšieho preskúmania	3	1	1	**2**

12	Poruchy a výpadky zariadení	Zariadenia staršie ako 10 rokov sú náchylnejšie na prehrievanie a výpadky	3	1	2	**3**
13	Požiar	Zastarané požiarne hlásiče bez certifikácie	3	1	2	**3**
14	Pohyb neautorizovaných osôb po priestoroch firmy	Zamestnanci kantíny sa môžu voľne pohybovať po priestoroch firmy	3	2	3	**5**
15	Nedostatočná politika hesiel	Heslá majú povinnosť byť dlhšie ako 8 znakov.	4	3	2	**6**
16	Technické zlyhanie úložiskových médií	Úložiskové média (HDD, SSD, USB kľúče) sú staršie ako 3 roky.	4	1	2	**4**
17	Minimálna ochrana pred DDoS útokmi	Chýbajúca platforma na ochranu pred útokmi typu DDoS	4	3	3	**7**
18	Voľné sťahovanie súborov z internetu	Počítače pripojené do internetovej siete si umožňujú sťahovať akékoľvek súbory	3	3	3	**6**
19	Zranenie zamestnanca na pracovisku	Zraniť sa dokáže v dôsledku nízkeho zábradlia na streche budovy, kde je spravená terasa	1	1	1	**0**
20	Zneužitie voľne dostupnej WIFI	WiFi nie je zabezpečená heslom a odpočúvanie treťou osobou nie je chránené	3	3	2	**5**
21	Voľne dostupné LAN konektory	V oboch budovách sú dostupné LAN konektory, ku ktorým má prístup akákoľvek osoba	3	2	2	**4**
22	Nedostatočne zabezpečená práca na diaľku	Zamestnancom nie je poskytnutý priestor na prácu z domu v dostatočne zabezpečenej miere	2	2	2	**3**

7.2 Dotknuté aktíva

Vysvetlenie dotknutých aktív a ich spojenie s hrozbami je uvedené v nasledujúcej časti. Hrozby sú identifikované poradovým číslom v predchádzajúcej a nasledujúcej tabuľke.

(1) Vďaka zraniteľnosti v kancelárskom balíku je možné kompromitovať celý operačný systém a sieť, na ktorom je pripojený, spolu s ďalšími zariadeniami, obsahujúce rovnakú zraniteľnosť. Dotknuté OS sú Windows 10 a Windows Server 2019, spolu s hardvérom. Kvôli bezpečnosti a predídeniu ďalších infikovaných laptopov, počítačov a serverov preto navrhujeme, aby sa implementoval antivírusový program na každé zariadenie a poučili sa zamestnanci (neotvárali neznáme prílohy, v prípade neistoty kontaktovali oddelenie technickej podpory a bezpečnosti).

(2) Pre prípad krádeže je náchylný len prenosný hardvér, a to najmä laptop. Mobil a tablet sú voči tomuto typu zraniteľnosti chránené vyhľadávacím programom od operátora, s ktorým má spoločnosť uzavretú dohodu. Opatrenie, ktoré odporúčame je, aby sa zamestnanci preškolili na platné pravidlá postupov pri práci s aktívami.

(3) Samotné odcudzenie šifrovaného USB kľúča a laptopu, ktorý majú zamestnanci pridelený na úschovu cenných dokumentov je zanedbateľná hrozba, avšak odporúčame podobne ako vyššie preškolenie zamestnancov.
(4) Na ochranu pred elektrickým skratom má firma nedostatočné zabezpečenú UPS miestnosť. Samotné zariadenia, ktoré by boli vystavené hrozbe sú zariadenia pripojené do elektrickej siete neustále (počítače, tlačiarne, serveri, smerovače, firewally a televízory). Navrhujeme, preto aby sa do budovy nainštaloval záložný zdroj, ktorý vydrží výpadok elektrickej energie na minimálne 24 hodín.
(5) V prípade neoprávneného vstupu do budovy nie sú budovy chránené. Samotný zoznam dotknutých aktív sú všetky fyzické dokumenty (klientské a pracovné zmluvy, databázové centrum je šifrované, v prípade odcudzenia sú teda histórie transakcií, investičné profily a zákaznícke účty chránené), všetko hardvérové vybavenie spoločnosti a všetky licencie na nešifrovaných serveroch, počítačoch a laptopoch. Navrhujeme obe budovy zabezpečiť kamerovým systémom, strážnou službou na časy od 18:00 do 07:00 nasledujúceho dňa.
(6) Prístupové oprávnenia sú nakonfigurované nesprávne z pohľadu bezpečnosti, nakoľko nie sú implementované žiadne opatrenia na riadenie prístupu a zamestnanci si jednotlivých používateľov navzájom vymieňajú bez vedomia administrátorov databáz. Samotné aktíva ohrozené uvedenou hrozbou sú všetky dokumentové aktíva uložené na databázových serveroch (história transakcii, investičné profily a zákaznícke účty), čo môže mať za následok kompromitáciu celého softvéru (serveru) a penalizáciu zo strany tvorcu daného softvéru. Navrhujeme preto, aby sa zaviedla politika riadeného prístupu a každý zamestnanec mal jedinečný účet spolu s prístupom nevyhnutným na vykonanie jeho povinností a náplne práce.
(7) Podobne ako tomu bolo vo vyššie uvedenej hrozbe, je nevyhnutné rovnaké kroky implementovať aj na Microsoft SharePoint, kde sú uvedené aj niektoré investičné profily spoločnosti, spolu s ich dlhodobými cieľmi.
(8) V prípade povodne sú najviac zraniteľné serverové miestnosti, ktoré sú umiestnené v podzemných priestoroch oboch budov (nachádzajúcich sa pri rieke). Dotknuté aktíva sú najmä tie na nižších podlažiach avšak mali by sa zaviesť opatrenia na zálohu nevyhnutných dokumentov pre chod spoločnosti a postaviť protipovodňovú hrádzu.
(9) Neautorizovaný zásah do cudzieho zariadenia sa týka najmä zariadení bezprostredne vlastniacich konkrétnym zamestnancom a poškodiť tak jeho pracovné dokumenty, prípadne sa dostať k dokumentom iných oddelení. Aktíva dotknuté uvedenou hrozbou kvôli tomu sú počítač, laptop, mobil a tablet. Navrhujeme poučiť zamestnancov o hrozbách, ktoré z uvedenej zraniteľnosti vyplývajú a nastaviť automatické uzamknutie obrazovky systémovými administrátormi v celej spoločnosti.
(10) V prípade pozorovania zamestnanca pri práci cestou do práce, je možné odpozorovať jeho heslo a dokumenty. Samotný hardvér nie je ohrozený, avšak týmto spôsobom môžu uniknúť dokumenty (pracovné a klientské zmluvy nahrané na zdieľanom úložisku, prípadne databázové dokumenty), v horšom prípade je možné pozorovať softvérové licencie s ich jedinečnými kľúčmi, ktoré identifikujú vlastníka softvérov (operačné systémy, databázové systémy, SAP, JIRA, o365).
(11) Otváranie cudzích mailov ako z overených zdrojov organizácie môže bezprostredne ohroziť všetky dokumenty v databázových systémoch, ku ktorým má používateľ prístup, kompromitovať zariadenia, na ktorých môže byť email otvorený a zničiť aj samotný hardvér, napadnúť zraniteľné serveri, ktoré sú voči týmto typom

útokov chránené firewallom a v neposlednej rade aj získať všetky licencie danej spoločnosti. Navrhujeme aby sa implementoval systém na odhalenie podvodných emailov a nainštaloval antivírusový program do všetkých zariadení pripojených na internet.

(12) V spoločnosti sa používa hardvér starší ako 10 rokov (počítače, laptopy, mobilné telefóny, smerovače, firewally, serveri tablety, pevné linky a tlačiarne), ktoré sú náchylnejšie na výpadok ako nové zariadenia. Navrhujeme preto aby sa do organizácie nakúpili nové zariadenia spolu s ich pravidelnou výmenou.

(13) V prípade požiaru, je organizácia chránená zastaranými požiarnymi hlásičmi, čo bezprostredne ohrozuje všetky aktíva spoločnosti. Navrhujeme preto výmenu hlásičov požiaru a informovanie hasičského zboru o dôležitosti dokumentov uložených v archívoch spoločnosti.

(14) Externí zamestnanci kantíny majú možnosť pohybovať sa v priestoroch banky bez potrebnej identifikácie, čo bezprostredne ohrozuje opäť všetky aktíva organizácie. Navrhujeme preto implementovať bezpečnostný systém na správu vstupov do budovy, kde každý zamestnanec jeden prístupový kľúč spojený s jeho pracovnou pozíciou a užívateľom.

(15) Nedostatočná politika hesiel môže viesť ku kompromitácii elektronických dokumentov (uložených na databázových serveroch spoločnosti), strate licencii a penalizácii zo strany vývojárov samotných softvérov. Opatrením je zvýšiť celkové požiadavky pri politike hesiel.

(16) Úložiskové médiá v organizácii sa používajú dlhšie ako je ich odporúčaná doba ich prevádzky, čo môže mať za následok stratu dokumentov uložených len na databázových systémoch (história transakcii, investičné profily a zákaznícke účty). Navrhujeme preto udržiavať médiá v ich odporúčanej dobe prevádzky a po jej uplynutí ich pravidelne meniť.

(17) Zraniteľnosti týkajúce sa prepojenia s internetom sú bežnou hrozbou pre organizácie. Najviac ohrozené aktíva sú samotný hardvér, ktorý sa môže pod náporom útoku poškodiť alebo úplne zhorieť. Navrhujeme preto, aby dôležitý hardvér (serveri, smerovače a firewally) boli pravidelne voči tomuto typu útokov testované a pravidelne menené.

(18) Sťahovanie súborov z internetu môže v sebe niesť stiahnutie škodlivých programov, čo môže mať za následok kompromitáciu operačného systému a jeho následné znefunkčnenie. Navrhujeme preto obmedziť možnosť sťahovať len súbory z úložísk organizácie a programy potrebné na prácu centrálne spravovať a pravidelne testovať.

(19) Na najvyššom poschodí oboch budov je možnosť prejsť sa po terase avšak výška zábradlia je v nedostatočnej výške, vďaka čomu môže dôjsť k úrazu zamestnanca, pri čom sa môžu poškodiť zariadenia, ktoré bude mať pri sebe (mobil, tablet, laptop). Navrhujeme zvýšiť celkovú bezpečnosť terasy a poučiť zamestnancov.

(20) V priestoroch oboch budov je voľne dostupná bezdrôtová sieť s prístupom na internet, ktorá je oddelená od siete organizácie. Aj napriek oddeleniu je však potrebné danú sieť monitorovať, nakoľko sa na ňu pripájajú zamestnanci svojimi mobilnými zariadeniami, kde môže dôjsť ku kompromitácii sieťových zariadení (smerovač, firewall) pomocou infikovaného mobilného zariadenia. Navrhujeme danú sieť zabezpečiť heslom a monitorovať.

(21) V priestoroch budov sú voľne dostupné LAN konektory, ktoré je možné zneužiť a odpočúvať tak premávku vo firemnej sieti, čo môže mať za následok kompromitáciu sieťových zariadení (smerovač, firewall). Navrhujeme preto nadbytočné konektory odstrániť a zabezpečiť ich voči voľnému zneužitiu.

(22) Zamestnanci majú možnosť pracovať z domu, avšak pri komunikácii po internete sa používajú zastarané šifrovacie algoritmy (DES). Najväčšia zraniteľnosť, ktorá z uvedeného vyplýva je, že útočníci dokážu odpočúvať komunikáciu na sieti a zachytia niektoré z dôležitých dokumentových aktív umiestnených na databázových serveroch (história transakcii, investičné profily, zákaznícke účty). Navrhujeme preto použiť novší šifrovací algoritmus (AES).

7.3 Navrhované opatrenia

Dotknuté aktíva sú označené pomocou ich ID z tabuliek v sekcií Ohodnotenie. Druhý stĺpec obsahuje navrhnuté bezpečnostné opatrenie tak, ako je definované v norme ISO 27002 a tretí stĺpec obsahuje čísla kapitol, v ktorých sa dané opatrenie nachádza.

Navrhované opatrenia			
ID	**Dotknuté aktíva**	**Bezpečnostné opatrenia z ISO 27002**	**ISO 27002**
1	Dokumenty: - Hardvér: 7, 8, 12, 13 Softvér: 21, 24	Mali by byť implementované opatrenia detekcie, predchádzania a obnovy na ochranu pred škodlivým softvérom, kombinované s budovaním povedomia používateľov.	12.2.1 Opatrenia proti škodlivému softvéru
2	Dokumenty: - Hardvér: 7 Softvér: -	Postupy na prácu s aktívami by mali byť vytvorené v súlade so schémou klasifikácie informácií, ktorá sa prijala v organizácii.	8.2.3 Zaobchádzanie s aktívami
3	Dokumenty: - Hardvér: 7 Softvér: -	Médiá obsahujúce informácie by mali byť chránené pred neautorizovanými prístupmi, pred zneužitím alebo poškodením pri prenose.	8.3.3 Fyzický prenos médií
4	Dokumenty: - Hardvér: 7, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 Softvér: -	Zariadenia by mali byť chránené pred výpadkami elektrickej energie a inými anomáliami spôsobenými zlyhaním dodávky podporných služieb.	11.2.2 Podporné služby
5	Dokumenty: 1, 2 Hardvér: Všetky Softvér: Všetky	Zabezpečené oblasti by mali byť chránené primeranými opatreniami na vstupe, aby sa zabezpečilo, že vstúpiť môžu len autorizované osoby.	11.1.2 Riadenie fyzických prístupov
6	Dokumenty:4, 5 Hardvér: - Softvér: 25	Mala by byť zavedená politika riadenia prístupu, dokumentovaná a preskúmavaná na základe pracovných a bezpečnostných požiadaviek.	9.1.1 Politika riadenia prístupov

7	Dokumenty: 4 Hardvér: - Softvér: 27	Mala by byť zavedená politika riadenia prístupu, dokumentovaná a preskúmavaná na základe pracovných a bezpečnostných požiadaviek.	9.1.1 Politika riadenia prístupov
8	Dokumenty: Všetky Hardvér: Všetky Softvér: Všetky	Malo by sa počítať s vytvorením a aplikovaním fyzickej ochrany pred prírodnými katastrofami, útokmi alebo nehodami	11.1.4 Ochrana pred externými hrozbami a hrozbami prostredia
9	Dokumenty: - Hardvér: 6, 7, 8, 18 Softvér: -	Zariadenia by mali byť umiestnené a chránené s cieľom obmedziť riziká vyplývajúce z hrozieb prostredia a riziká a príležitosti neautorizovaného prístupu.	11.2.1 Umiestnenie zariadení a ich ochrana
10	Dokumenty: Všetky Hardvér: - Softvér: Všetky	Všetci zamestnanci organizácie a v prípade, že je to potrebné, aj zmluvní partneri by mali absolvovať vhodné školenie v oblasti bezpečnostného povedomia a mali by sa im poskytovať pravidelne aktualizované verzie politík a postupov organizácie, tak ako si to vyžaduje ich pracovné zaradenie.	7.2.2 Povedomie o informačnej bezpečnosti, vzdelávanie a školiaca činnosť
11	Dokumenty: 3, 4, 5 Hardvér: 7, 8, 12, 13 Softvér: Všetky	Mali by byť implementované opatrenia detekcie, predchádzania a obnovy na ochranu pred škodlivým softvérom, kombinované s budovaním povedomia používateľov.	12.2.1 Opatrenia proti škodlivému softvéru
12	Dokumenty: - Hardvér: Všetky Softvér: -	Zariadenia by mali byť správne udržiavané, aby sa zaistila ich nepretržitá dostupnosť a integrita.	11.2.4 Údržba zariadení
13	Dokumenty: Všetky Hardvér: Všetky Softvér: Všetky	Malo by sa počítať s vytvorením a aplikovaním fyzickej ochrany pred prírodnými katastrofami, útokmi alebo nehodami.	11.1.4 Ochrana pred externými hrozbami a hrozbami prostredia
14	Dokumenty: Všetky Hardvér: Všetky Softvér: Všetky	Mala by sa navrhnúť a aplikovať fyzická bezpečnosť pre miestnosti, kancelárie a zariadenia.	7.1.1 Preverovanie
15	Dokumenty: 3, 4, 5 Hardvér: - Softvér: 21, 23, 24, 25, 26, 27	Systémy na riadenie hesiel by mali byť interaktívne a mali by poskytovať kvalitné heslá	11.1.3 Zabezpečenie kancelárií, miestností a prostriedkov
16	Dokumenty: 3, 4, 5 Hardvér: - Softvér: -	Pravidelne by sa mali robiť a testovať záložné kópie dôležitých informácií a softvéru v súlade so schválenou politikou zálohovania.	12.3.1 Zálohovanie informácií

17	Dokumenty: - Hardvér: 12, 13, 14, 15, 16 Softvér: -	Pravidelne by sa mali robiť a testovať záložné kópie dôležitých informácií a softvéru v súlade so schválenou politikou zálohovania.	12.3.1 Zálohovanie informácií
18	Dokumenty: - Hardvér: - Softvér: 21, 24	Na strategické riadenie inštalácie softvéru používateľmi by mali byť vytvorené a zavedené pravidlá.	12.6.2 Obmedzenia pri inštalácii softvéru
19	Dokumenty: - Hardvér: 8, 9, 19 Softvér: -	Mali by sa navrhnúť a aplikovať príslušné postupy pre prácu v zabezpečených oblastiach.	11.1.5 Práca v bezpečnostných priestoroch
20	Dokumenty: - Hardvér: 14, 15, 16 Softvér: -	Skupiny informačných služieb, používate ov a informačných systémov by mali byť na sieťach segregované (oddeľované).	13.1.3 Oddeľovanie sietí
21	Dokumenty: - Hardvér: 14, 15, 16 Softvér: -	Elektrická alebo telekomunikačná kabeláž prenášajúca dáta alebo podporujúce informačné služby by mala byť chránená pred odpočúvaním, manipuláciou alebo poškodením.	11.2.3 Bezpečnosť kabeláže
22	Dokumenty: - Hardvér: 7, 8, 9, 19 Softvér: 21, 24	Mali by sa vyvinúť a implementovať postupy, prevádzkové plány a politiky chrániace informácie prístupné a spracovávané pri práci na diaľku, alebo uložené na mieste odkiaľ sa vykonáva práca na diaľku.	6.2.2 Práca na diaľku

8 Záver

Po vykonaní bezpečnostnej analýzy rizík sme odhalili väčšie množstvo závažných zraniteľností a hrozieb, ktoré by mohli mať na spoločnosť katastrofálne následky. V tabuľke navrhovaných opatrení sú v stĺpci MR (miera rizika) zaznamenané opatrenia, ktoré by mali byť v čo najkratšom čase implementované. Po úspešnom nasadení všetkých navrhovaných opatrení bude zvýšenie bezpečnosti celej firmy na akceptovateľnú úroveň a lepšia pripravenosť v prípade katastrofy.

9 Zdroje

(1) International Organization for Standardization. (2013). Information technology — Security techniques — Information security management systems — Requirements (ISO/DIS Standard No. 27001)

(2) International Organization for Standardization. (2013). Information technology — Security techniques — Code of practice for information security controls (ISO/DIS Standard No. 27002)

(3) doc. Ing. Ladislav Hudec, CSc. (2014). *Analýza rizík*.